Федеральное государственное образовательное бюджетное
учреждение высшего профессионального образования
«ФИНАНСОВЫЙ УНИВЕРСИТЕТ ПРИ ПРАВИТЕЛЬСТВЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

Кафедра «Информационная безопасность»

УТВЕРЖДАЮ
Ректор
М.А. Эскиндаров
«__» _____ 2013 г.

Е.А. Дербин, С.М. Климов

# ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**Учебное пособие**

Для студентов, обучающихся по направлению
090900.68 «Информационная безопасность»

*Рекомендовано Ученым советом факультета «Анализ рисков и экономическая безопасность»*
*(протокол №___ от _____ 2013 г.)*
*Одобрено кафедрой «Информационная безопасность»*
*(протокол №___ от _____ 2013 г.)*

Москва 2013

**УДК** **004.451(073)**

**ББК** **32.973я73**

**Д 5**

**Рецензенты:** **д.т.н. Боданов Ю.В.** – начальник управления НИЦ 4 ЦНИИ Минобороны России
**к.т.н. А.А. Малюк** – профессор кафедры «Кибербезопасность» НИЯУ МИФИ

**Д 5** **Е.А. Дербин, С.М. Климов «Организационные основы обеспечения информационной безопасности предприятия».** Учебное пособие для студентов, обучающихся по направлению: 090900.68 «Информационная безопасность» – М.: Финансовый университет, кафедра «Информационная безопасность», 2013 – 266 с.

Учебное пособие «Организационные основы обеспечения информационной безопасности предприятия» содержит материалы лекций по разделу учебной дисциплины «Организационные и правовые основы обеспечения информационной безопасности», исполненные в виде базовых схем и тезисов, представляющих содержание рассматриваемых вопросов в удобной для усвоения форме.

**УДК** **004.451(073)**

**ББК** **32.973я73**

***Электронное учебное издание***

***Евгений Анатольевич Дербин, Сергей Михайлович Климов***

**Организационные основы обеспечения информационной безопасности предприятия**

**Учебное пособие**

Компьютерный набор, верстка Е.А. Дербин

Формат 60x90/16. Гарнитура *Times New Roman*

Усл. п.л. 17,0. Изд. № 13.24. – 2013. Тираж – 50 экз.

Заказ № _____

**Отпечатано в Финансовом университете**

# ОГЛАВЛЕНИЕ

# Глава 1.
# ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК КОМПЛЕКСНАЯ ЗАДАЧА РЕАЛИЗАЦИИ ПРАВОВЫХ, ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР

**1.1.** Информационная безопасность: сущность и содержание.

**1.2.** Угрозы информационной безопасности и задачи по их нейтрализации.

**1.3.** Содержание обеспечения информационной безопасности.

## Литература:


**1.** Доктрина информационной безопасности Российской Федерации, 2000 г. Поручение Президента РФ 2000 г. № Пр-1895

**2.** Федеральный закон РФ №310-ФЗ «О безопасности» от 26 декабря 2010 г.

**3.** Стрельцов А.А. Информационная безопасность Российской Федерации. - М.: Высшая школа, 2003.


Оглавление

# 1.1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СУЩНОСТЬ И СОДЕРЖАНИЕ

## 1.1.1. ПОНЯТИЕ ИНФОРМАЦИИ В АКТАХ ДЕЙСТВУЮЩЕГО ЗАКОНОДАТЕЛЬСТВА

**ФЗ «Об информации, информатизации и защите информации», ст. 2:**

информация - «сведения о липах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления»;

персональные данные - «сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность»;

конфиденциальная информация - «документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ»;

документированная информация (документ) - «зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать»;

информационные ресурсы- «отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах и др.)».

**Закон РФ «О средствах массовой информации»:**

массовая информация - «предназначенные для неограниченного круга лиц печатные, аудио-сообщения, аудиовизуальные и иные сообщения и материалы».

**ФЗ «Об участии в международном информационном обмене»:**

информационные продукты - «документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для их удовлетворения»;

информационные услуги - «действия субъектов (собственников и владельцев) по обеспечению пользователей информационными продуктами».

**Закон РФ «О государственной тайне», ст. 2:**

государственная тайна - «защищаемые государством сведения в области его военной, внешне-политической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ»;

**ФЗ «О рекламе», ст. 2:**

реклама - «распространяемая в любой форме, с помощью любых средств информация о физическом или юридическом лице, товарах, идеях и начинаниях, которая предназначена для неопределенного круга лиц и призвана формировать или поддерживать интерес к этим физическому, юридическому лицу, товарам, идеям и начинаниям и способствовать реализации товаров, идей и начинаний»

## 1.1.2. БАЗОВЫЕ ОПРЕДЕЛЕНИЯ

| | |
|---|---|
| **ИНФОРМАЦИЯ** | – сведения о лицах, предметах, фактах, событиях, явлениях и процессах |
| **ИНФОРМАЦИОННАЯ СФЕРА** | – область деятельности субъектов, связанная с созданием, преобразованием и потреблением информации;<br>– совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений и технических взаимодействий |
| **ИНФОРМАЦИОННОЕ ОБЩЕСТВО** | – общество, структуры, техническая база и человеческий потенциал приспособленные для оптимального превращения знаний в информационный ресурс и переработки последнего |
| **ИНФОРМАЦИОННЫЙ РЕСУРС** | – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах – библиотеках, архивах, фондах, банках данных и др. |

# 1.1.2а. БАЗОВЫЕ ОПРЕДЕЛЕНИЯ

| | |
|---|---|
| **ИНФОРМАЦИОННЫЙ ОБЪЕКТ** | **– информация или ее носитель** |
| **ИНФОРМАЦИОННАЯ ОБСТАНОВКА** | **– совокупность условий и факторов, оказывающих влияние на состояние и функционирование информационных объектов** |
| **УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** | **– повышение вероятности ущерба информацион-ному объекту в виде:**<br>***утраты элементов его структуры;***<br>***нарушения его внешних и внутренних связей, а также программ и функций;***<br>***потери способности к развитию*** |
| **ИНФОРМАЦИОННАЯ ОПАСНОСТЬ** | **– состояние информационной обстановки, характеризуемое обострением угроз в информационной сфере** |
| **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** | **– состояние информационной обстановки, характеризуемое надежной защищенностью информационного объекта от угроз и его способностью их нейтрализовывать** |

# 1.1.3. ОСОБЕННОСТИ И СВОЙСТВА ИНФОРМАЦИИ

**1. Свойство физической неотчуждаемости.** При передаче информации от одного лица к другому и юридического закрепления этого факта процедура отчуждения информации должна заменяться передачей прав на ее использование и передаваться вместе с этими правами.

**2. Свойство обособляемости.** Для включения в оборот информация всегда овеществляется в виде символов, знаков, волн и обособляется от ее производителя, существует отдельно и независимо как самостоятельный объект правоотношений и предается в такой форме от одного субъекта к другому.

**3. Свойство информационной вещи (информационного объекта).** Информация передается и распространяется только на материальном носителе или с помощью материального носителя, что позволяет распространить на информационную вещь (объект) совместное и взаимосвязанное действие института авторского права и института вещной собственности.

**4. Свойство тиражируемости (распространяемости).** Одна и та же информация (содержание) может принадлежать одновременно неограниченному кругу лиц. Отсюда следует, что юридически необходимо закреплять объем прав по использованию информации лицами, обладающими такой информацией.

**5. Свойство организационной формы.** Информация, находящаяся в обороте, представляется в документированном виде. Это дает возможность юридически закреплять факт «принадлежности» документа конкретному лицу и позволяет относить к информационным вещам (объектам) как отдельные документы, так и сложные организационные информационные структуры.

**6. Свойство экземплярности.** Информация распространяется, как правило, на материальном носителе, вследствие чего возможен учет экземпляров информации через учет носителей, содержащих информацию. Это дает возможность учитывать документированную информацию и связывать ее содержательную сторону информации с ее отображением на носителе, вводить понятие учитываемой копии документа и механизма регистрации информации

# 1.1.4. ИНФОРМАЦИЯ КАК ИНФОРМАЦИОННЫЙ ОБЪЕКТ

# 1.1.5. КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ РЕСУРСОВ, ПРОДУКТОВ И УСЛУГ

## по виду информации

- правовая;
- научно-техническая;
- политическая;
- финансово-экономическая;
- статистическая;
- о стандартах и регламентах;
- метрологическая;
- социальная;
- о здравоохранении;
- о чрезвычайных ситуациях;
- персональная;
- кадастры (земельный, градостроительный, имущественный, лесной, другие).

## по способу доступа

- открытая информация;
- информация ограниченного доступа:
  государственная тайна,
  конфиденциальная информация,
  коммерческая тайна,
  профессиональная тайна,
  служебная тайна,
  персональные данные,
  личная тайна

## по виду носителя

- на бумаге;
- на машиночитаемых носителях;
- в виде изображения на экране ЭВМ;
- в памяти ЭВМ;
- в канале связи;
- на других видах носителей.

## по способу формирования и распространения

- стационарные;
- передвижные (мобильные).

## по организации хранения и использования

- традиционные формы:
  массив документов,
  фонд документов,
  архив;
- автоматизированные формы:
  Интернет,
  банк данных,
  автоматизированная нформационная система (сеть),
  база знаний.

## по форме собственности

- общероссийское национальное достояние;
- государственная собственность;
- федеральная собственность;
- собственность субъектов РФ;
- совместная (федеральная и субъектов федерации);
- муниципальная собственность:
- частная собственность;
- коллективная собственность.

## ИНФОРМАЦИОННЫЕ ПРОДУКТЫ

- **документы, данные;**
- **подборки документов, данных;**
- **справки, аналитические справки;**
- **базы данных, банки данных;**
- **другие виды**

## УСЛУГИ ПО ИНФОРМАЦИОННОМУ ОБСЛУЖИВАНИЮ

- **поиск и обработка информации, выдача данных, хранение;**
- **услуги по пользованию Интернет, АИС, БД, их сетями:**
  консультационные,
  по передаче информации,
  по доступу к Интернет, по пользованию электронной почтой и формированию личных сайтов

# 1.1.6. ИНФОРМАЦИОННЫЕ ОТНОШЕНИЯ

**Информационные отношения** – обособленная, однородная группа общественных отношений, возникающих при обращении информации в информационной сфере в результате осуществления информационных процессов – в порядке реализации информационных прав и свобод, а также в порядке исполнения обязанностей органами государственной власти и местного самоуправления по обеспечению гарантий информационных прав и свобод

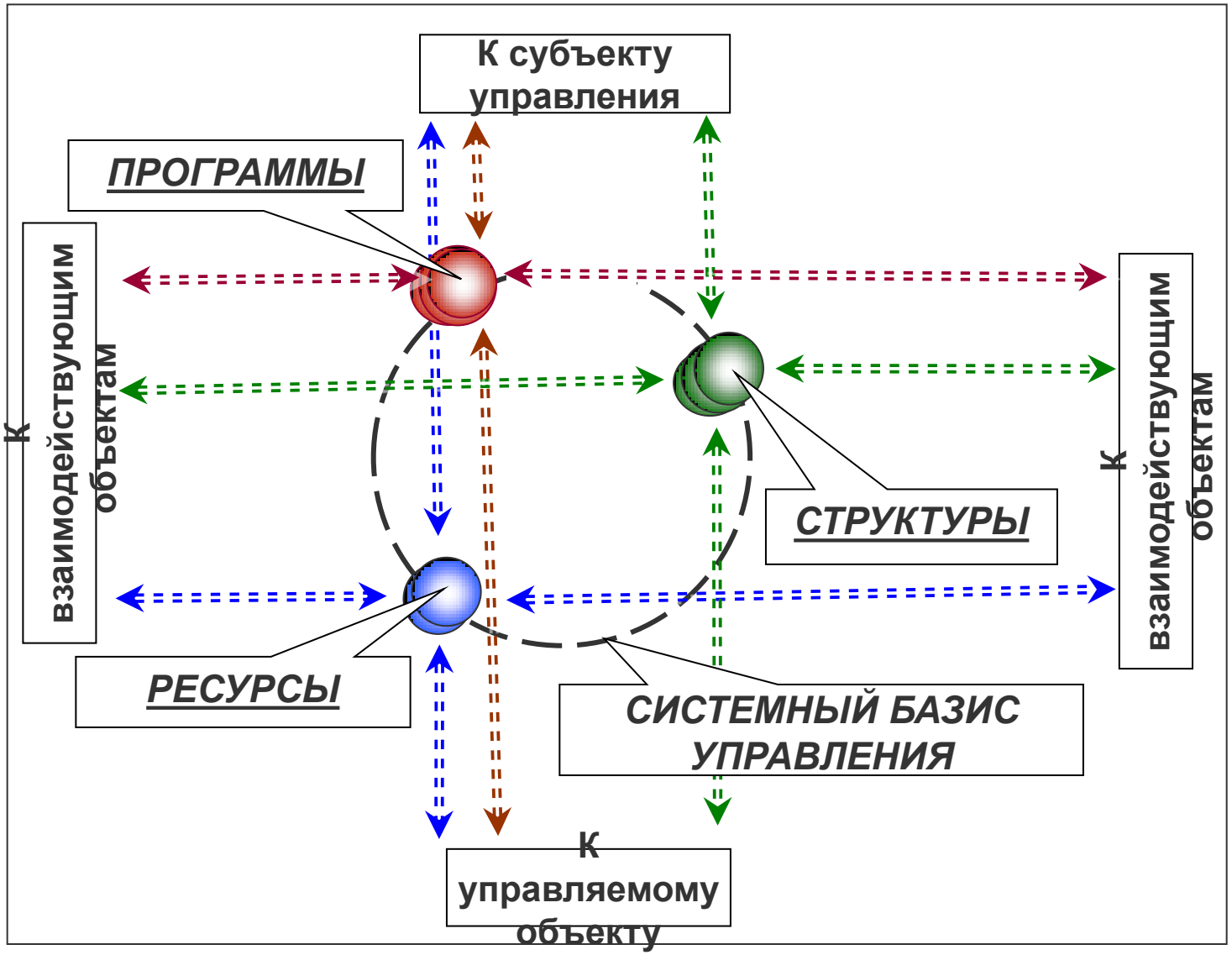
**Особенности информационных отношений**:

- возникают, развиваются и прекращаются в информационной сфере при обращении информации;
- опосредуют государственную политику признания, соблюдения и защиты информационных прав и свобод человека и гражданина в информационной сфере;
- отражают особенности применения публично-правовых и гражданско-правовых методов правового регулирования при осуществлении информационных прав и свобод с учетом специфических особенностей и юридических свойств информации и информационных объектов

ГРАЖДАНСКО-ПРАВОВОЙ АСПЕКТ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ → Объясняется особенностями реализации информационных прав и свобод, в первую очередь, имущественных прав и прав собственности на информационные ресурсы в информационной сфере

ПУБЛИЧНО-ПРАВОВОЙ АСПЕКТ ИНФОРМАЦИОННЫХ ОТНОШЕНИЙ → Объясняется необходимостью:
обеспечения гарантий осуществления информационных конституционных прав и свобод граждан,
государственного управления информационными процессами формирования и использования государственных информационных ресурсов,
создания и применения государственных информационных систем и средств их обеспечения, а также средств и механизмов информационной безопасности

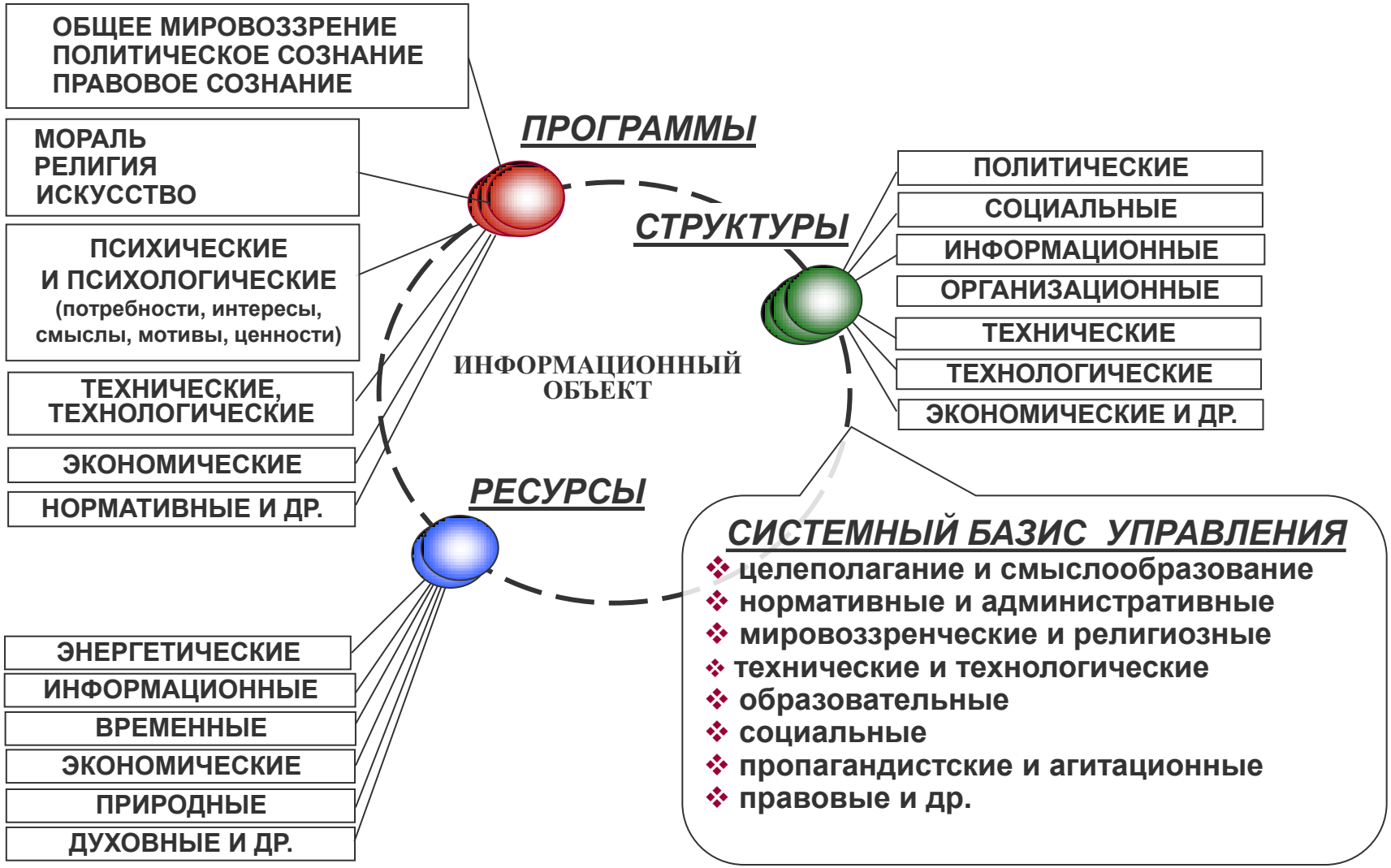
# 1.1.7. ТОПОЛОГИЯ ИНФОРМАЦИОННОГО ОБЪЕКТА



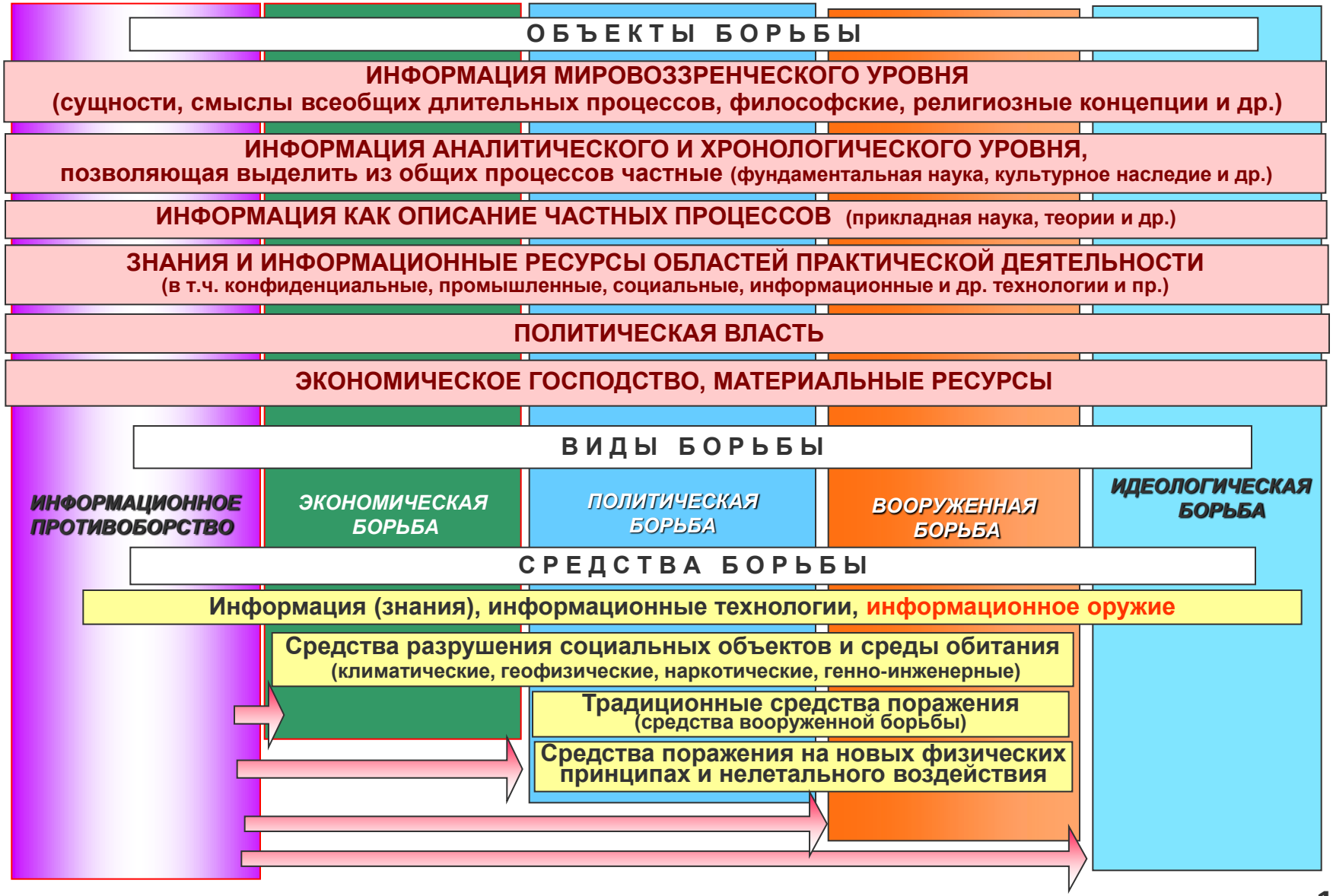
# 1.1.8. БАЗОВОЕ СОДЕРЖАНИЕ ЭЛЕМЕНТОВ ТОПОЛОГИИ ИНФОРМАЦИОННОГО ОБЪЕКТА

| ЭЛЕМЕНТЫ ТОПОЛОГИИ | ИНФОРМАЦИЯ | ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ ОБЪЕКТЫ | ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ ОБЪЕКТЫ |
|---|---|---|---|
| ***Структуры*** | Содержание информации (содержательность), логические структуры (последовательность), целостность | Конфигурация вычислительной сети, телекоммуникационные системы и пр. | Для индивидов: структура личности, психологическая структура, биологическая структура<br>Для социальных групп: политическая, социальная, психологическая, организационная и др. структуры |
| ***Программы*** | Смыслообусловленность и др. | Степень совершенства программного обеспечения, алгоритмов защиты информации, обеспечения информационной безопасности и др. | Духовные, культурные и материальные потребности, мировоззренческие, ценностно-смысловые аспекты, цели, задачи, планы, интересы, мотивы |
| ***Ресурсы*** | Объем, значимость (актуальность, новизна, важность, истинность) и др. | Объем и характеристика ресурсов: информационного, энергетического, ресурса технической надежности (защищенности) и пр. | Для индивидов: власть, социальный и профессиональный опыт, квалификация, компетенция, память, качество и объем знаний, социальный опыт, состояние физического здоровья и психологической устойчивости; мера удовлетворения потребностей.<br>Для социальных групп: экономические, психологические, моральные и др. ресурсы |
| ***Системный базис управления*** | Уровень обобщения (влияния), принадлежность к мировоззренческому, смысловому, мотивационному, хронологическому, фактологическому и др. уровням, отраслям знаний, конфиденциальность, доступность, достоверность, сохранность | Принадлежность, роль и место объекта, важность, устойчивость параметров, зависимость от человеческого фактора | Роль в обществе, важность, функции; моральные, нравственные и рационально-волевые качества, доминирующая идея, идеология, слаженность коллектива, дружба |
| ***Связи взаимодействия и иерархические связи*** | Логические связи: причины – следствия; посылки – выводы; аргументы – факты и др. | Системные связи | Подчиненность в структуре, политические и социальные отношения, коммуникабельность, гибкость. Факторы доминирующего влияния (противоборство, противостояние, конкуренция, сосуществование, сотрудничество) |

# 1.1.9. АНАЛИЗ ЭЛЕМЕНТОВ ТОПОЛОГИИ СОЦИОТЕХНИЧЕСКОГО ИНФОРМАЦИОННОГО ОБЪЕКТА

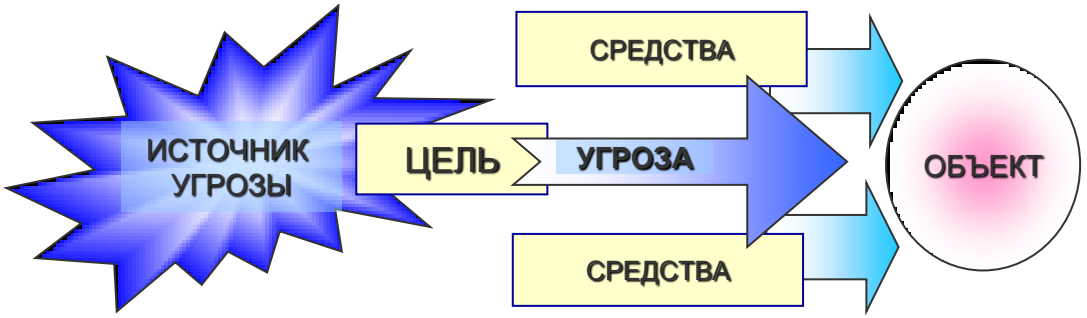


# 1.1.10. УНИВЕРСАЛЬНАЯ ВЗАИМОСВЯЗЬ ВИДОВ, ОБЪЕКТОВ И СРЕДСТВ БОРЬБЫ



# 1.1.11. СУЩНОСТЬ ПОНЯТИЙ «ОПАСНОСТЬ» И «БЕЗОПАСНОСТЬ»

**ИНФОРМАЦИОННАЯ ОПАСНОСТЬ** – состояние информационной обстановки, характеризуемое обострением угроз информационному объекту




Угрозы информационной безопасности объекта:

***утрата элементов его структуры;***

***нарушение его внешних и внутренних связей, а также программ и функций;***

***потеря способности к развитию***

**БЕЗОПАСНОСТЬ ПРЕДПОЛАГАЕТ**

**отсутствие опасности** для функционирования (безопасность как состояние)

надежную **защищенность** от воздействия угроз (безопасность как свойство)

**способность** преодолевать угрозы, избегать опасность (безопасность как система)

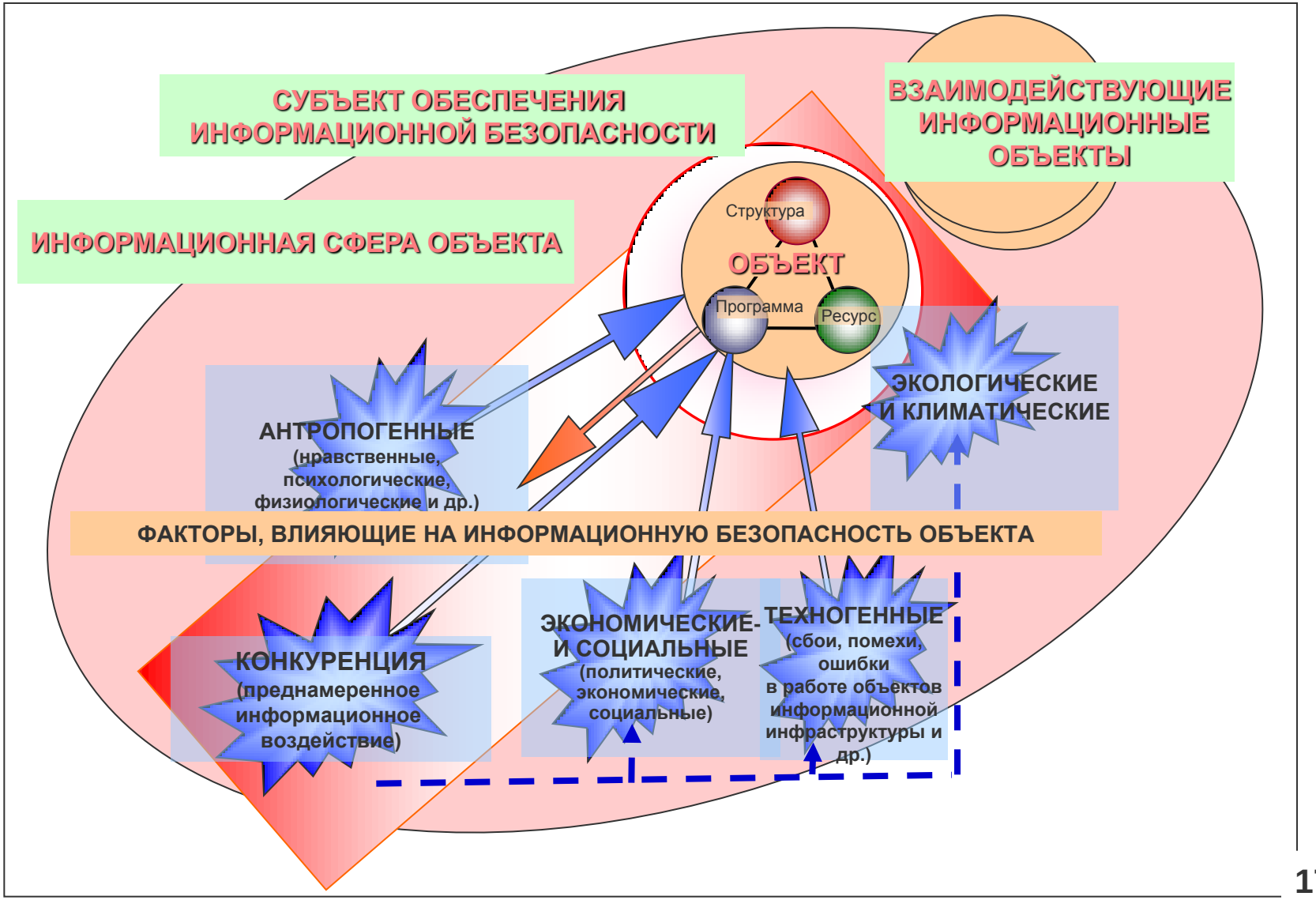
**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – состояние информационной обстановки, характеризуемое отсутствием опасности, надежной защищенностью от угроз и способностью их нейтрализовывать**

**ЦЕЛИ ДОСТИЖЕНИЯ БЕЗОПАСНОСТИ**

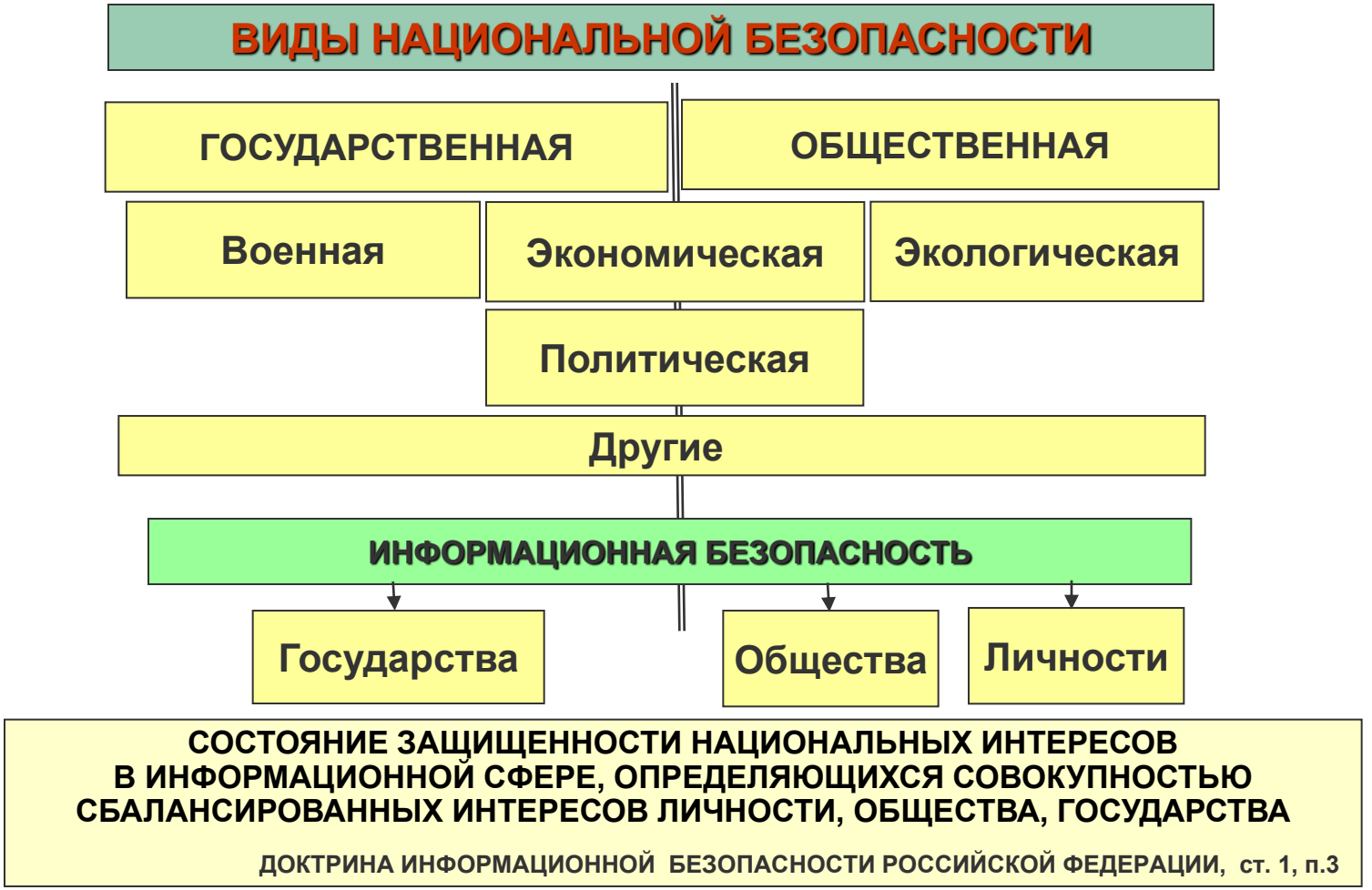
***Конфиденциальность, целостность и доступность: «модель CIA (Confidentiality-Integrity-Availability)»***

***Стандарты ISO 27001, ISO 27002***

# 1.1.12. ФАКТОРЫ, ОКАЗЫВАЮЩИЕ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

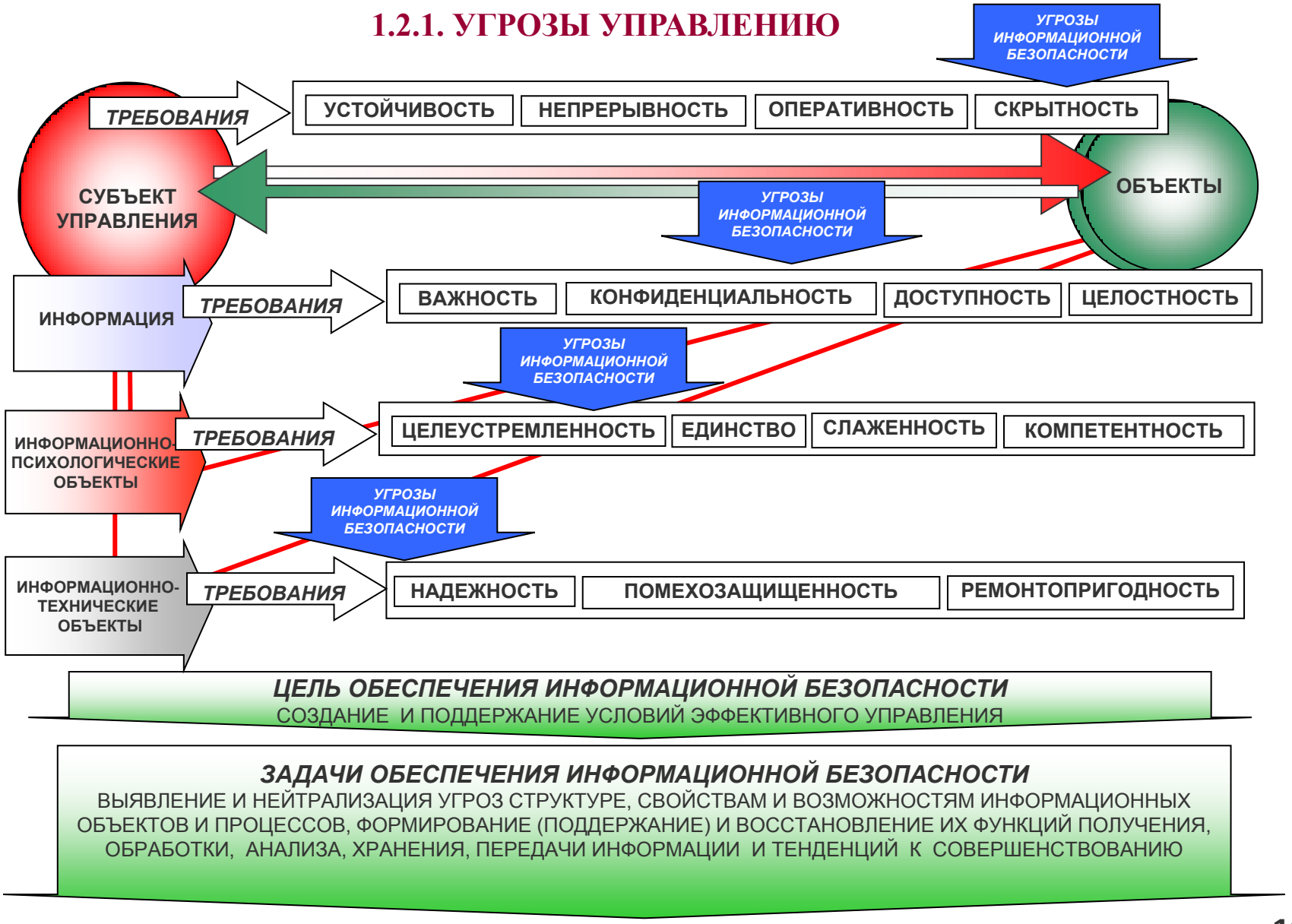


# 1.1.13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СТРУКТУРЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ



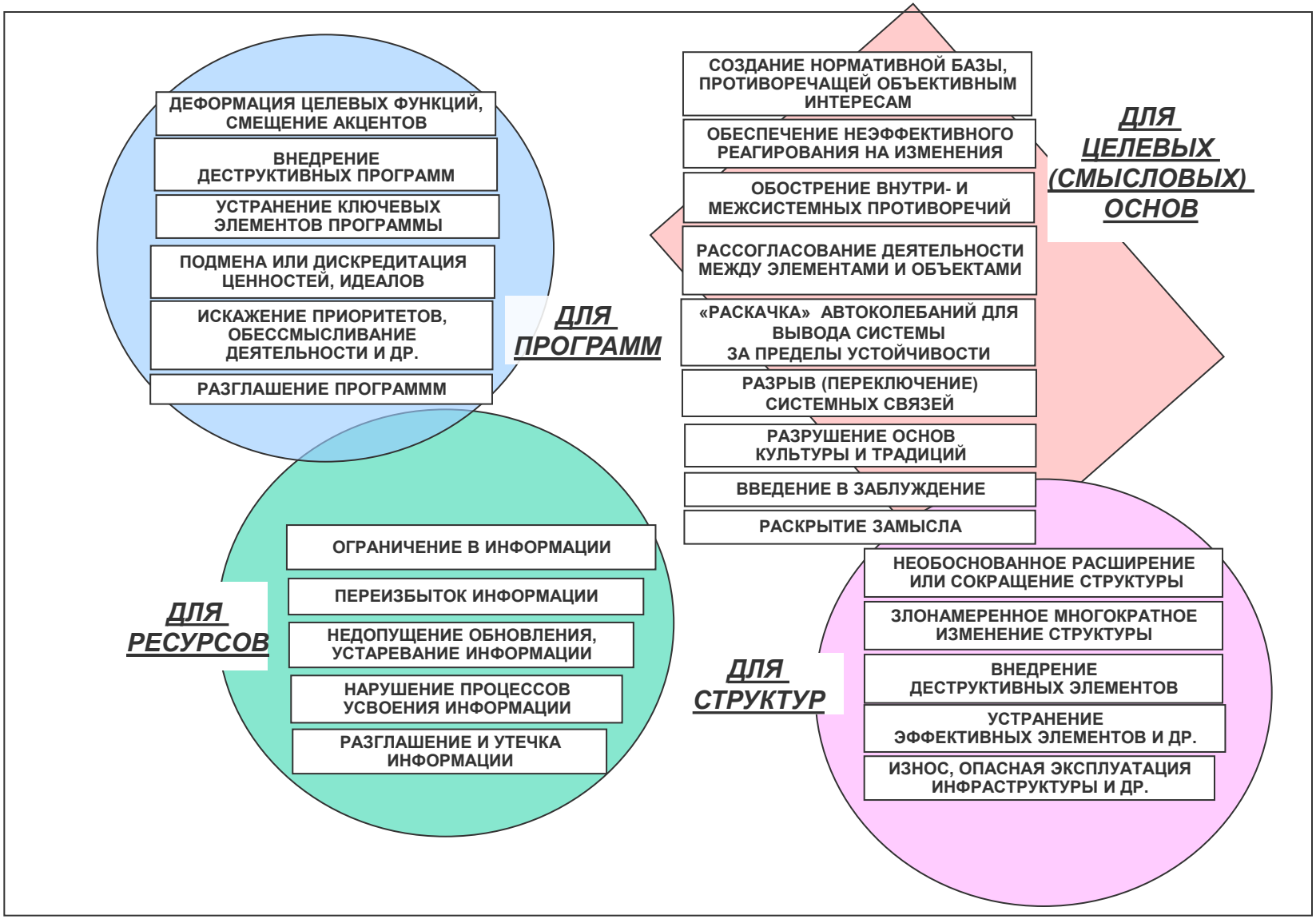
# 1.2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАДАЧИ ПО ИХ НЕЙТРАЛИЗАЦИИ

## 1.2.1. УГРОЗЫ УПРАВЛЕНИЮ

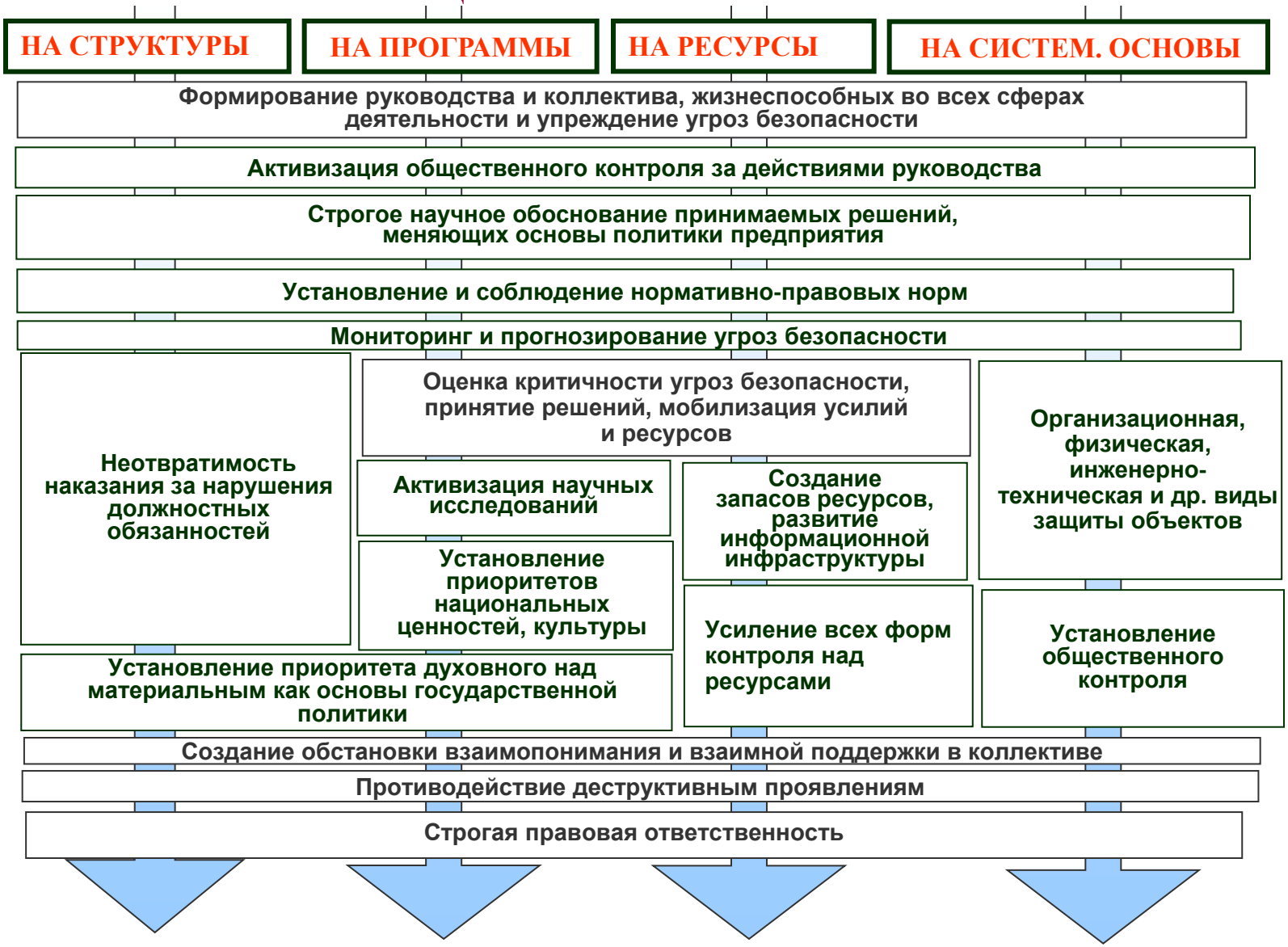


# 1.2.2. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА В ИНФОРМАЦИОННОЙ СФЕРЕ

# 1.2.3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕМЕНТОВ ИНФОРМАЦИОННОГО ОБЪЕКТА

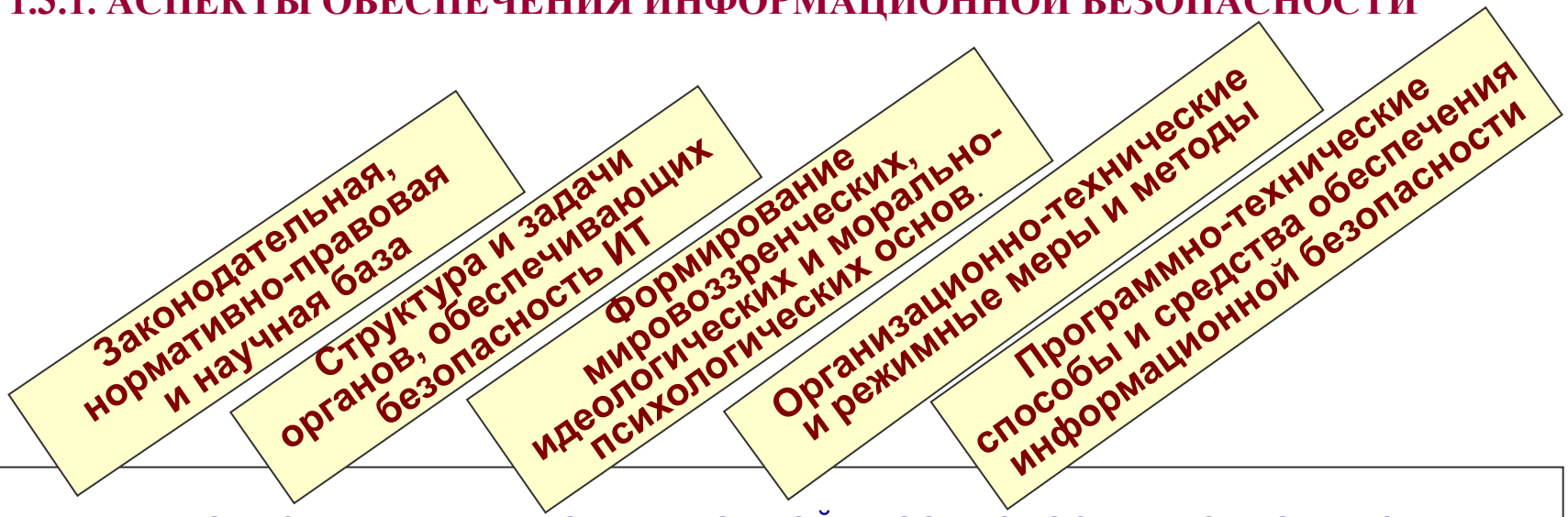


# 1.2.4. НАПРАВЛЕНИЯ НЕЙТРАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



# 1.3. СОДЕРЖАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 1.3.1. АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ




**ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕОБХОДИМО:**

- выявить требования безопасности, специфические для данного объекта;
- учесть требования национального и международного Законодательства;
- использовать наработанные практики (стандарты) построения СОИБ;
- определить подразделения, ответственные за реализацию и поддержку СОИБ;
- распределить области ответственности в осуществлении требований СОИБ;
- определить общие положения, технические и организационные требования, составляющие Политику информационной безопасности;
- реализовать требования Политики, внедрив соответствующие программно-технические способы и средства защиты информации;
- реализовать Систему менеджмента (управления) силами и средствами;
- организовать регулярный контроль эффективности и корректировку СОИБ

# 1.3.2. МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

## ПРАВОВЫЕ

1. Изменения в законодательстве в интересах системы обеспечения инф. безопасности
2. Законодательное разграничение полномочий между органами власти
3. Уточнение статуса иностранных информационных агентств
4. Законодательное закрепление приоритета развития национальных сетей связи

## ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ

1. Создание и совершенствование системы обеспечения информационной безопасности
2. Предупреждение и пресечение правонарушений в информационной сфере, привлечение к ответственности лиц, совершивших преступления
3. Совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности СПО
4. Создание систем и средств предотвращения НСД к обрабатываемой информации
5 Выявление технических устройств и программ, представляющих опасность
6. Предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты
7. Сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации
8. Совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации

## ЭКОНОМИЧЕСКИЕ

1. Разработка программ обеспечения информационной безопасности и определение порядка их финансирования
2. Совершенствование системы финансирования работ, по реализации правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков

# 1.3.3. СУБЪЕКТЫ, ОБЪЕКТЫ И СОДЕРЖАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

| | БЕЗОПАСНОСТЬ ИНФОРМАЦИОННОГО РЕСУРСА | БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИХ ОБЪЕКТОВ | БЕЗОПАСНОСТЬ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ОБЪЕКТОВ |
|---|---|---|---|
| | Разработка и реализация нормативно-правовых основ | | |
| РУКОВОДСТВО | Сохранность баз данных. Защита государственной тайны. Защита информационных коммуникаций от НСД. Защищенность информации, устойчивость управления | Нравственная чистота потребностей, интересов и мотивов деятельности руководства. Профессиональная компетентность. Психологическая устойчивость и др. | Обеспечение надежности работы и защищенности объектов информационной инфраструктуры. Развитие информационной инфраструктуры. Обеспеченность средствами информатизации. Обученность персонала. |
| КОЛЛЕКТИВ | Распространение научного мировоззрения, правосознания, всестороннее образование. Доступность информации, обусловливающей интересы коллектива. Сохранность корпоративных сведений от разглашения | Здоровые моральные и нравственные начала. Развитие социальных и духовных потребностей, интересов, ценностей. Реализация правовых норм. Сплоченность. | |
| ПЕРСОНАЛ | Адекватность представлений об окружающем мире, общая образованность. Профессиональная компетентность. Сохранность и неприкосновенность личных данных. Защита от дезинформации | Следование социальным нормам поведения. Идеалы, нравственное совершенствование, духовность. Духовная мотивация поведения и деятельности Способность к противодействию манипуляциям и др. | |

# 1.3.4. МЕТОДИЧЕСКИЙ АППАРАТ ФОРМИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# 3.3.4. ПУТИ РЕШЕНИЯ ПРОБЛЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# Глава 2.
# ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**2.1.** Принципы организационного обеспечения информационной безопасности и структура системы обеспечения

**2.2.** Силы и средства обеспечения информационной безопасности. Роль подразделения защиты информации в системе обеспечения информационной безопасности

**2.3.** Технологии обеспечения информационной безопасности и роли в системе ее обеспечения акционеров, высших корпоративных органов, менеджеров, сотрудников и внешних контролирующих органов

## Литература:


**1.** ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

**2.** ГОСТ Р ИСО/МЭК 13335-1-2006 «Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».

**3.** ОСТ 45.127-99 «Система обеспечения информационной безопасности взаимоувязанной сети связи РФ. Термины и определения».

**4.** http://asher.ru/security/book/its/09


Оглавление

# 2.1. ПРИНЦИПЫ ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И СТРУКТУРА СИСТЕМЫ ОБЕСПЕЧЕНИЯ

## 2.1.1. СИСТЕМА ОБЕСПЕЧЕНИЯ *(усл. – УПРАВЛЕНИЯ, МЕНЕДЖМЕНТА)* ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**СИСТЕМА ОБЕСПЕЧЕНИЯ (усл. – УПРАВЛЕНИЯ, МЕНЕДЖМЕНТА) ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ – модель создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов для достижения целей предприятия, основанную на оценке и принятии уровней риска для эффективного рассмотрения и управления ими**

**Включает в себя:**

**организационную структуру, политику, силы обеспечения, методы, процедуры, процессы и ресурсы (средства обеспечения).**

**Позволяет предприятию:**

**удовлетворять требования безопасности клиентов и др. заинтересованных лиц;**

**улучшать планы и действия организации;**

**соответствовать целям информационной безопасности организации;**

**выполнять регулирующие требования, требования законодательства и отраслевые нормативные документы;**

**организованно управлять информационными активами для облегчения непрерывного совершенствования организационных целей и внешних условий**

## 2.1.2. ПРИНЦИПЫ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**а) Вовлеченность высшего руководства Предприятия в процесс обеспечения информационной безопасности.**

Деятельность по обеспечению информационной безопасности инициирована и контролируется высшим руководством Предприятия. Координация деятельности по обеспечению информационной безопасности осуществляется в рамках действующего на предприятии комитета, в состав которого входят представители высшего руководства. Высшее руководство Предприятия выполняет те же правила по обеспечению информационной безопасности, что и все работники Предприятия.

**б) Законность обеспечения информационной безопасности.**

Предприятие реализует меры обеспечения информационной безопасности в строгом соответствии с действующим законодательством и договорными обязательствами.

**в) Согласованность действий по обеспечению информационной, физической и экономической безопасности.**

Действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений Предприятия и согласованы между собой по целям, задачам, принципам, методам и средствам.

**г) Экономическая целесообразность.**

Предприятие стремится выбирать меры обеспечения информационной безопасности с учетом затрат на их реализацию, вероятности возникновения угроз информационной безопасности и объема возможных потерь от их реализации.

**д) Знание своих работников.**

Предприятие стремится тщательно подбирать персонал (работников), вырабатывать и поддерживать корпоративную этику, что создает благоприятную среду для деятельности Предприятия и снижает риски информационной безопасности.

## 2.1.2а. ПРИНЦИПЫ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**е) Документированность требований информационной безопасности.**

Предприятие стремится, чтобы все требования в области информационной безопасности были зафиксированы во внутренних нормативных документах, утвержденных руководством Предприятия.

**ж) Осведомленность в вопросах обеспечения информационной безопасности.**

Документированные требования в области информационной безопасности доводятся до сведения работников Предприятия и контрагентов в части их касающейся. Предприятие на периодически осуществляет информирование, обучение и аттестацию работников по вопросам обеспечения информационной безопасности.

**з) Реагирование на инциденты информационной безопасности.**

Предприятие стремится выявлять, учитывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения информационной безопасности.

**и) Персональная ответственность.**

Работники Предприятия несут персональную ответственность за соблюдение требований информационной безопасности. Обязанности по обеспечению информационной безопасности включаются в трудовые договора и должностные инструкции работников, а так же в договора (соглашения) с контрагентами.

**к) Учет действий с информационными активами.**

Предприятие стремится вести учет всех действий работников Предприятия и контрагентов с информационными активами Предприятия**.**

**м) Учет требований информационной безопасности в проектной деятельности.**

Помимо операционной деятельности, Предприятие стремится учитывать требования информационной безопасности в проектной деятельности. Разработка и документирование требований по обеспечению информационной безопасности осуществляется на начальных этапах реализации проектов, связанных с обработкой, хранением и передачей информации.

## 2.1.3. ОРГАНИЗАЦИОННАЯ ЗАЩИТА ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

**ОРГАНИЗАЦИОННАЯ ЗАЩИТА** – это **регламентация** производственной **деятельности** и **взаимоотношений** исполнителей на нормативно-правовой основе, исключающей или существенно **затрудняющей неправомерное овладение конфиденциальной информацией** и проявление внутренних и внешних угроз, обеспечивающая: организацию **охраны, режима, работу с кадрами, документами**; использование **технических средств безопасности; информационно-аналитическую деятельность** по выявлению внутренних и внешних угроз предпринимательской деятельности.

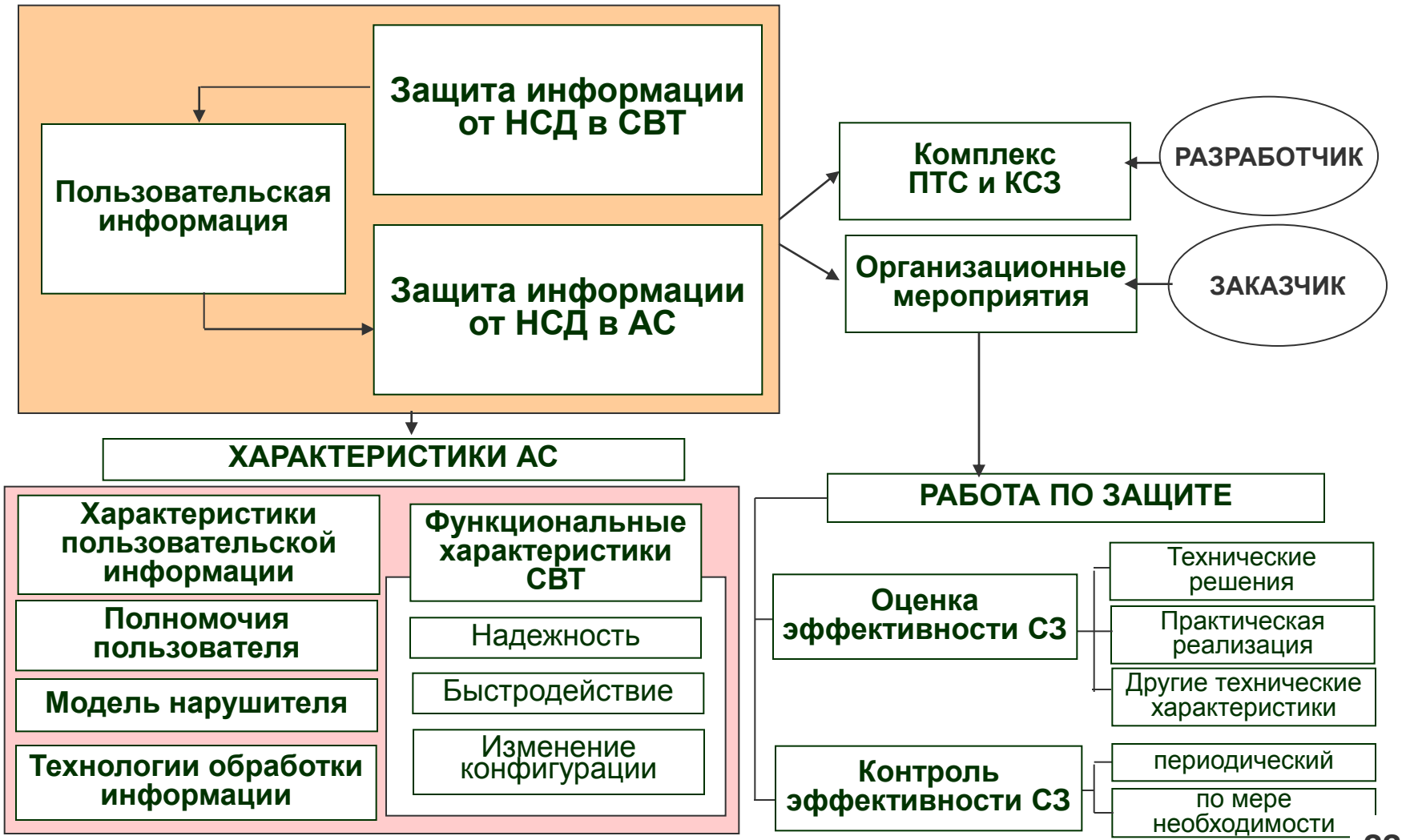
**К основным организационным мероприятиям следует отнести:**

- организацию **режима и охраны** с целью исключения возможности тайного проникновения на территорию и в помещения посторонних лиц;
- организацию **работы с сотрудниками**, предусматривающую подбор и расстановку персонала (ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и др.);
- организацию **работы с документами** и документированной информацией (разработка документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение);
- организацию **использования технических средств** сбора, обработки, накопления и хранения информации;
- организацию **работы по анализу** внутренних и внешних угроз информационной безопасности и выработке мер по обеспечению ее защиты;
- организацию работы по проведению **систематического контроля** за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей

# 2.1.4. НАПРАВЛЕНИЯ РАССМОТРЕНИЯ ПРОБЛЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В АСУ

**Защищенность СВТ** – свойство предотвращать или существенно затруднять НСД к информации при использовании СВТ в АС.

**НСД** – доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств СВТ или АС




*«Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». Утв. решением ГТК при Президенте РФ от 30 марта 1992 г.*

# 2.2. СИЛЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

## 2.2.1. СИЛЫ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

**ДЕПАРТАМЕНТ БЕЗОПАСНОСТИ**

- **Аналитическое подразделение**
- **Служба информационной безопасности**
  оценка состояния ИБ, разработка организационно-распорядительных документов
- **Служба экономической безопасности**

**ОТДЕЛ РЕЖИМА СЕКРЕТНОСТИ**

**ОТДЕЛ КАДРОВ**

**РУКОВОДСТВО**
цели и задачи функционирования СОИБ, направления ее развития, стратегические решения по вопросам безопасности, регламентация порядка

**ПОДРАЗДЕЛЕНИЯ**

- **Сотрудники (пользователи ИТ)**

**АКЦИОНЕРЫ**

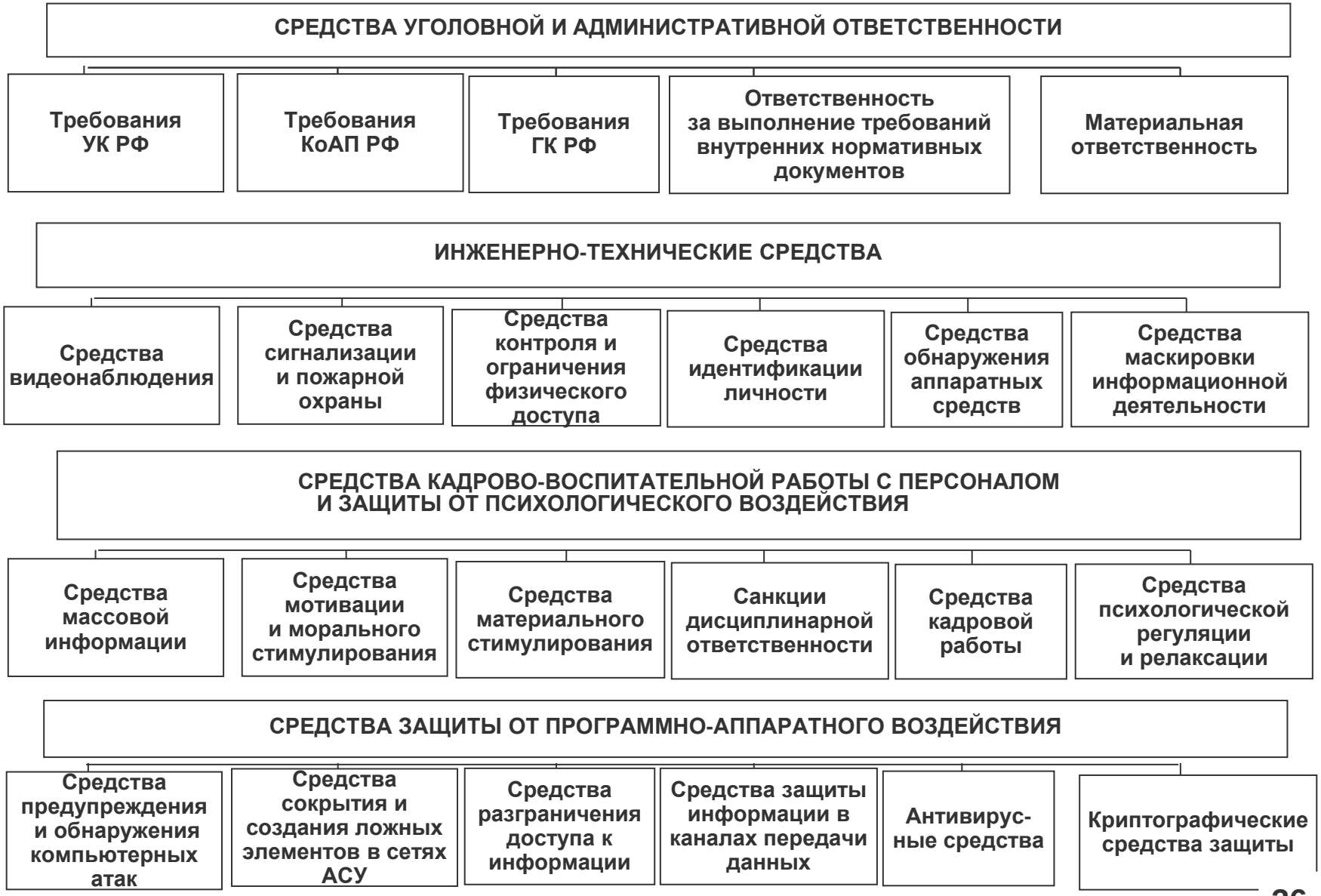
**ДЕПАРТАМЕНТ АВТОМАТИЗАЦИИ**

- **Программисты**
  разработка (приобретение и адаптацию) необходимых прикладных программ (задач)
- **Группа внедрения и сопровождения ПО**
  обеспечение функционирования и порядка инсталляции и модификации прикладных программ (задач)
- **Группа эксплуатации ТС**
  обеспечение нормальной работы и обслуживания технических средств обработки и передачи информации и СПО
- **Группа системных администраторов штатных средств защиты** (ОС, СУБД)
- **Группа защиты информации**
  требования к системе защиты, администрирование специальных дополнительных систем защиты

## 2.2.2. ЗАДАЧИ СЛУЖБЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- определение перечня сведений, составляющих коммерческую тайну, а также круга лиц, которые имеют к ним доступ;
- определение участков сосредоточения сведений, составляющих коммерческую тайну;
- формирование требований к системе защиты в процессе создания и участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы ЗИ;
- распределение между пользователями необходимых реквизитов защиты (установка паролей, управление средствами защиты коммуникаций и криптозащиту;
- координация действий с аудиторской службой, совместное проведение аудиторских проверок, контроль функционирования системы защиты и ее элементов;
- организация обучения сотрудников в соответствии с их функциональными обязанностями; обучение пользователей правилам безопасной обработки информации;
- определение круга предприятий, на которых возможен выход из-под контроля сведений, составляющих коммерческую тайну предприятия;
- выявление лиц на предприятии и предприятий (в том числе иностранных), заинтересованных в овладении коммерческой тайной;.
- расследование нарушений защиты, принятие мер реагирования на попытки НСД к информации и нарушениям правил функционирования системы защиты;
- выполнение восстановительных процедур после нарушения безопасности;
- анализ, оценка состояния и разработка предложений по совершенствованию СОИБ предприятия; внедрение достижений науки и техники, передового опыта;
- совместная работа с представителями других организаций по вопросам безопасности, непосредственный контакт или консультации с партнерами или клиентами;
- постоянная проверка соответствия принятых в организации правил безопасной обработки информации существующим правовым нормам

# 2.2.3. СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



# 2.3. ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**Под технологией обеспечения информационной безопасности в АС понимается определенное распределение функций и регламентация порядка их исполнения, а также взаимодействия подразделений и сотрудников по обеспечению комплексной защиты ресурсов АС в процессе ее эксплуатации.**

**Требования к технологии :**

- соответствие современному уровню развития информационных технологий;
- учет особенностей построения и функционирования различных подсистем АС;
- точная и своевременная реализация политики безопасности организации;
- минимизация затрат на реализацию самой технологии обеспечения безопасности.

**Для реализации технологии обеспечения безопасности в АС необходимо**:

- наличие полной и непротиворечивой правовой базы (системы взаимоувязанных нормативно-методических и организационно-распорядительных документов) по вопросам ОИБ;
- распределение функций и определение порядка взаимодействия подразделений и должностных лиц организации по вопросам ОИБ на всех этапах жизненного цикла подсистем АС, обеспечивающее четкое разделение их полномочий и ответственности;
- наличие специального органа (подразделения обеспечения информационной безопасности), наделенного необходимыми полномочиями и непосредственно отвечающего за формирование и реализацию единой политики информационной безопасности организации и осуществляющего контроль и координацию действий всех подразделений и сотрудников организации по вопросам ОИБ.

# 2.3.1. ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ЭКСПЛУАТАЦИИ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Эксплуатация СОИБ должна осуществляться в рамках согласованных мероприятий принятой политики и функционирования комплексной системы обеспечения информационной безопасности на основании разработанных регламентов, должностных инструкций обслуживающему персоналу и пользователям**

**Организационные меры должны охватывать следующие основные направления:**

- разработка системы документов, регламентирующих вопросы эксплуатации;
- назначение и подготовку должностных лиц, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации;
- инвентаризация, классификация и учет подлежащих защите ресурсов (информации, задач, каналов связи, серверов, автоматизированных рабочих мест и т.д.);
- организация и контроль процессов присвоения, внесения в систему разграничения доступа СОИБ, модификации и удаления полномочий пользователей по доступу к ИС;
- организация процессов изменения настроек средств защиты, в связи с подключением новых объектов, пользователей, IP-адресов, внедрением ИС и т.д.;
- организация процессов оперативного контроля за работой средств защиты и разработку мер своевременного реагирования на выявленные факты нарушения информационной безопасности;
- организация контроля работоспособности и технического обслуживания средств защиты;
- организация своевременного копирования и хранения информационных настроек средств защиты с целью возможности быстрого восстановления компонентов СОИБ при сбоях оборудования или возникновении нештатных ситуаций;
- организация процессов своевременного обновления программного и информационного обеспечения средств защиты;
- организация процесса обучения обслуживающего персонала правилам эксплуатации и технического обслуживания средств защиты;
- организация процесса обучения пользователей работе со средствами защиты;
- контроль эффективности и достаточности принимаемых мер защиты в связи с постоянным развитием средств информатизации и изменяющимися источниками угроз;
- организация процесса расследования инцидентов и нарушений установленных регламентов и инструкций по обеспечению информационной безопасности;
- организация сертификации средств защиты информации, контроль за использованием лицензионного программного обеспечения

## 2.3.2. РЕАЛИЗАЦИЯ ТЕХНОЛОГИЙ, ОБЕСПЕЧИВАЮЩИХ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

- назначение и подготовка должностных лиц, ответственных за организацию, реализацию функций и осуществление мероприятий;
- строгий учет всех подлежащих защите ресурсов системы (информации, ее носителей, процессов обработки) и определение требований к организационно-техническим мерам и средствам защиты;
- разработка реально выполнимых и непротиворечивых организационно-распорядительных документов по вопросам обеспечения ИБ;
- реализация технологических процессов обработки информации с учетом требований ИБ;
- принятие эффективных мер сохранности и обеспечения физической целостности технических средств и поддержку необходимого уровня защищенности компонентов АС;
- применение физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывную административную поддержку;
- регламентация всех процессов обработки информации и действий сотрудников на основе утвержденных организационно-распорядительных документов;
- четкое знание и строгое соблюдение всеми сотрудниками, использующими и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов;
- персональная ответственность за свои действия каждого сотрудника, участвующего в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС;
- эффективный контроль за соблюдением сотрудниками подразделений и обслуживающим АС персоналом требований по обеспечению ИБ;
- проведение постоянного анализа эффективности и достаточности принятых мер и применяемых средств защиты информации, разработку и реализацию предложений по совершенствованию системы обеспечения ИБ

## 2.3.3. СУЩНОСТЬ, РОЛЬ И МЕСТО ПОЛИТИК БЕЗОПАСНОСТИ

Основы безопасности
**информационно-телекоммуникационных технологий (ИТТ)**

| Общие цели | Стратегии (способы достижения цели) | Политика безопасности организации (правила, которые следует соблюдать при реализации стратегий) | Процедуры (методы осуществления политики) |
|---|---|---|---|

уточняются в детальных и специфических целях, политике и процедурах во всех сферах интереса организации (управление финансами, персоналом и безопасностью)

**Политика безопасности информации в организации** (англ. Organizational security policy) – совокупность документированных технических, организационных, административных, юридических, физических правил, процедур, практических приёмов или руководящих принципов, регламентирующих все вопросы обеспечения безопасности информации, которыми руководствуется организация в своей деятельности.

**Политика безопасности информационно-телекоммуникационных технологий (ИТТ)** (англ. ICT security policy) – правила и сложившаяся практика, которые определяют, как управлять активами организации, в том числе критичной информацией, защищать их и распределять в пределах информационно-телекоммуникационных технологий

*ГОСТ Р ИСО/МЭК 13335-1 - 2006*

# 2.3.4. СТРАТЕГИИ И ПОЛИТИКА БЕЗОПАСНОСТИ

Политика обеспечения информационной безопасности в рамках характеристик бизнеса, особенностей данной организации, ее расположения, ресурсов, технологий и эффективности процесса управления рисками:

- включает в себя основу для определения ее целей и осознание необходимости безопасности и повышение квалификации в области безопасности;
- устанавливает общее направление и принципы деятельности по отношению к ИБ;
- учитывает требования бизнеса и законодательной или нормативной базы, а также контрактные обязательства в области безопасности;

*ISO/IEC 27001:2005*

- объединяется со стратегическим контекстом управления рисками в организации, в котором будет происходить создание и сопровождение системы обеспечения ИБ;
- устанавливает критерии для оценивания рисков;
- утверждается руководством;
- позволяет оценивать, в какой мере бизнес организации зависит от ИТТ, учитывая:
  - **задачи бизнеса и их связь с безопасностью;**
  - **какие важные составляющие бизнеса не могут осуществляться без ИТТ;**
  - **какие задачи могут быть решены только при помощи ИТТ;**
  - **какие важные решения зависят от конфиденциальности, целостности, доступности, подотчетности, аутентичности и актуальности хранимой или обрабатываемой информации;**
  - **стратегию оценки риска и методы, адаптируемые в рамках организации;**
  - **комплексную политику безопасности ИТТ для каждой системы;**
  - **организационные методы безопасности для каждой системы;**
  - **схему классификации ИТТ систем;**
  - **стандартные схемы управления инцидентами информационной безопасности в рамках всей организации**

*ГОСТ Р ИСО/МЭК 13335-1 - 2006*

# 2.3.5. ИСХОДНЫЕ ДАННЫЕ ДЛЯ ФОРМИРОВАНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- общая характеристика и специализация организации (наименование, специализация, род деятельности, решаемые задачи, характер и объем работ), сведения о распределении обязанностей и инструкциях по обработке и защите информации);
- описание административной структуры и категорий зарегистрированных пользователей, технологии обработки информации, потенциальных субъектов и объектов доступа;
- общее описание рабочего процесса, технологическая схема операций при выполнении рабочего процесса, интенсивность с которой выполняется рабочий процесс, технологические ограничения, средства контроля и критерии качества результатов рабочего процесса, перечень проблемных вопросов подразделений по обеспечению защиты информации;
- информация которая подлежит защите, сведения конфиденциального характера, организация и структура информационных потоков и их взаимодействие;
- организация хранения данных;
- угрозы информационной безопасности, модель нарушителя и уязвимости;
- анализ рисков;
- общая характеристика автоматизированных систем организации, топология и расположение ЛВС, схема коммуникационных связей, структура и состав потоков данных (перечень входных и выходных информационных объектов, их источники и получатели, перечень внутренних информационных объектов);
- технические и программные средства ЛВС и доступа к ней из сетей общего доступа (физическая среда передачи, используемые протоколы, операционные системы, серверы баз данных, места хранения конфиденциальных данных, средства защиты информации);
- принадлежность и типы каналов связи;
- общее и специальное ПО (наименование и назначение, фирма разработчик, аппаратные требования, размещение);
- применяемые меры защиты (организационные меры, средства защиты ОС, средства защиты, встроенные в ПО, специализированные средства защиты)

# 2.3.6. ПЕРЕЧЕНЬ ВОПРОСОВ ПОЛИТИКИ БЕЗОПАСНОСТИ

**1. Введение**
1.1 Общий обзор
1.2 Область применения и цель политики обеспечения безопасности ИТ
**2. Цели и принципы обеспечения безопасности**
2.1 Цели
2.2 Принципы
**3. Организация и инфраструктура безопасности**
3.1 Ответственность
3.2 Основные направления политики обеспечения безопасности
3.3 Регистрация инцидентов нарушения безопасности
**4. Анализ риска и стратегия менеджмента в области обеспечения безопасности ИТ**
4.1 Введение
4.2 Менеджмент и анализ риска
4.3 Проверка соответствия мер обеспечения безопасности предъявляемым требованиям
**5. Чувствительность информации и риски**
5.1 Введение
5.2 Схема маркировки информации
5.3 Общий обзор информации в организации
5.4 Уровни ценности и чувствительности информации в организации
5.5 Общий обзор угроз, уязвимых мест и рисков
**6. Безопасность аппаратно-программного обеспечения**
6.1 Идентификация и аутентификация
6.2 Контроль доступа
6.3 Журнал учета использования ресурсов и аудит
6.4 Полное стирание
6.5 Программное обеспечение, нарушающее нормальную работу системы
6.6 Безопасность ПК
6.7 Безопасность компактных портативных компьютеров
**7. Безопасность связи**
7.1 Введение
7.2 Инфраструктура сетей
7.3 Интернет
7.4 Криптографическая аутентификация и аутентификация сообщений
**8. Физическая безопасность**
8.1 Введение
8.2 Размещение оборудования
8.3 Безопасность и защита зданий
8.4 Защита коммуникаций и систем обеспечения энергоносителями в зданиях
8.5 Защита вспомогательных служб
8.6 Несанкционированное проникновение в помещения
8.7 Доступность ПК и рабочих станций
8.8 Доступ к магнитным носителям информации
8.9 Защита персонала
8.10 Противопожарная защита
8.11 Защита от воды (жидкой среды)
8.12 Обнаружение опасностей и сообщение о них
8.13 Защита системы освещения
8.14 Защита оборудования от кражи
8.15 Защита окружающей среды
8.16 Управление услугами и ТО
**9. Безопасность персонала**
9.1 Введение
9.2 Условия найма персонала
9.3 Осведомленность и обучение персонала
9.4 Служащие
9.5 Контракты с лицами, проводящими самост.работу
9.6 Привлечение третьих сторон
**10. Безопасность документов и носителей информации**
10.1 Введение
10.2 Безопасность документов
10.3 Хранение носителей информации
10.4 Ликвидация носителей информации
**11. Обеспечение непрерывности деловой деятельности, включая ЧС и восстановлении после аварий**
11.1 Введение
11.2 Запасные варианты
11.3 Стратегия обеспечения бесперебойной работы
11.4 План (планы) обеспечения бесперебойной работы
**12. Надомная работа**
**13. Политика аутсортинга**
13.1 Введение
13.2 Требования безопасности
**14. Управление изменениями**
14.1 Обратная связь
14.2 Изменения в политике обеспечения безопасности
14.3 Статус документа

*ГОСТ Р ИСО/МЭК 13335-3 - 2006*

## 2.3.7. РОЛЬ АКЦИОНЕРОВ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Акционеры предприятия обязаны вникать в тонкости обеспечения информационной безопасности и предъявлять к ней не только бизнес-требования, но и специфические претензии к состоянию системы

Акционеры предприятия обязаны сохранять конфиденциальность по вопросам, касающимся деятельности предприятия

Акционеры предприятия обязаны извещать держателя реестра акционеров об изменениях своих реквизитов (места жительства), включая наименование (фамилию), номеров абоненткой связи и других данных. В случае непредставления ими информации об изменении своих данных держатель реестра акционеров не несет ответственности за причиненные в связи с этим убытки;

# 2.3.8. РОЛЬ ВЫСШИХ КОРПОРАТИВНЫХ ОРГАНОВ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Обеспечение собственного понимания, какая информация является защищаемой, где она рождается, где и кем изменяется, как перемещается внутри предприятия, в каком виде ее можно передавать регулирующим органам, контрагентам и клиентам, где она хранится и как уничтожается, а также того, что эта часть информационной безопасности имеет отдаленное отношение к безопасности информационных технологий

Обеспечить соблюдение баланса между доступностью, целостностью и конфиденциальностью информации, потенциальным ущербом от риска и реальными затратами на уменьшение вероятности риска, между удобством для бизнеса и требованиями регуляторов по защите информации

Обеспечить выполнение требований законодательства по защите информационных объектов в финансовом секторе – информации, составляющей банковскую тайну, персональных данных клиентов и сотрудников, данных пластиковых карт, описаний маркетинговых программ, планов развития, состава акционеров

Обеспечить непрерывность бизнеса и защиту информации от всех типов угроз при выполнении всех требований регуляторов

Помочь заказчику правильно поставить задачу, заложить надежный фундамент в систему защиты корпоративного содержания деятельности

Создать условия, чтобы деятельность службы обеспечения ИБ не мешала развитию компании и в минимальной степени подвергать изменениям принятые в компании бизнес-процессы

# 2.3.9. РОЛЬ ОРГАНОВ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ В ОБЕСПЕЧЕНИИ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Оценивают риски, влияющие на достижение поставленных целей, и принимают меры, обеспечивающие реагирование на меняющиеся обстоятельства и условия в целях обеспечения эффективности оценки рисков в информационной сфере

Обеспечивают участие во внутреннем контроле ИБ персонала в соответствии с их должностными обязанностями

Устанавливают порядок, при котором служащие доводят до сведения органов управления и руководителей структурных подразделений информацию обо всех нарушениях законодательства, учредительных и внутренних документов, случаях злоупотреблений, несоблюдения норм профессиональной этики в обращении с корпоративной и личной информацией

Утверждают документы по вопросам взаимодействия Службы информационной безопасности с другими подразделениями и персоналом и контролируют их соблюдение

Исключают принятие правил или осуществление практики, которые могут стимулировать совершение действий, противоречащих законодательству Российской Федерации и целям внутреннего контроля.

Осуществляют ежедневное повышение сознательного выполнения обязанностей и осведомленности сотрудников, обучение в сочетании с регулярной аттестацией, участие в корпоративных программах повышения лояльности в интересах повышения ответственности к обеспечению информационной безопасности

## Глава 3.
# ОСНОВЫ ОРГАНИЗАЦИОННОГО РЕГУЛИРОВАНИЯ ВЗАИМООТНОШЕНИЙ АДМИНИСТРАЦИИ И ПЕРСОНАЛА В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**3.1.** Направления и методы работы с персоналом, обладающим конфиденциальной информацией.

**3.2.** Проверочные мероприятия, обучение работе с конфиденциальной информацией и оформление допуска к ней при приеме на работу.

**3.3.** Мониторинг осведомленности персонала о тайнах работодателя.

**3.4.** Правовое регулирование взаимоотношений администрации и персонала при инцидентах нарушения информационной безопасности

**Литература:**

1. Федеральный закон № 5485-1 «О государственной тайне», 21 июля 1993 г. (с изм. от 11.12.2011 г.),

2. Федеральный закон № 98-ФЗ «О коммерческой тайне», 29 июля 2004 г.

3. Федеральный закон № 152-ФЗ «О персональных данных», 27 июля 2006 г.

Оглавление

# 3.1. НАПРАВЛЕНИЯ И МЕТОДЫ РАБОТЫ С ПЕРСОНАЛОМ, ОБЛАДАЮЩИМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

## 3.1.1. ПОНЯТИЕ О ПЕРСОНАЛЕ

**Понятие «персонал и окружающие фирму люди» включает :**

- всех сотрудников данной фирмы, ее персонал;
- сотрудников других фирм-посредников, изготовителей комплектующих деталей, торговых фирм, рекламных агентств и т.п.);
- сотрудников государственных учреждений, к которым фирма обращается в соответствии с законом: налоговых и иных инспекций, муниципальных, правоохранительных органов и т.д.;
- журналистов средств массовой информации, сотрудничающих с фирмой;
- посетителей фирмы, работников коммунальных служб, почтовых служащих, работников служб экстренной помощи и т.д.;
- посторонних лиц, работающих или проживающих рядом со зданием или помещениями фирмы, уличных прохожих;
- родственников, знакомых и друзей **всех** указанных выше лиц.

# 3.1.2. ПСИХОЛОГИЧЕСКИЕ ФАКТОРЫ РАБОТЫ С ПЕРСОНАЛОМ

## ВНЕШНИЕ ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛА

- **криминальные структуры,**
- **коррумпированные элементы,**
- **государственные институты,**
- **природные катаклизмы и техногенные катастрофы**

## ВНУТРЕННИЕ ИСТОЧНИКИ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛА

- **напряжения внутри коллектива из-за неправильных взаимоотношений по вертикали, горизонтали, неудовлетворенности результатами труда и его оценкой со стороны руководства;**
- **нездоровая конкуренция между отдельными сотрудниками или подразделениями;**
- **внутриролевые и межролевые конфликты;**
- **недостаточная управленческая компетентность;**
- **низкая профессиональная и личностная надежность персонала**

## КРУГ ЗАДАЧ ОБЕСПЕЧЕНИЯ ПСИХОЛОГИЧЕСКОЙ БЕЗОПАСНОСТИ

- профессиональный и психологический отбор персонала;
- профилактика, выявление и разрешение конфликтов;
- аттестация персонала;
- психологическое изучение партнеров, конкурентов, представителей криминальных структур;
- расследование чрезвычайных происшествий;
- подготовка и проведение ответственных переговоров различного уровня;
- психологическая защита информации;
- обучение персонала навыкам эффективной коммуникации;
- психотерапия и психокоррекция сотрудников, переживших стрессовые ситуации

## 3.1.3 КОРПОРАТИВНЫЕ ЦЕННОСТИ СОТРУДНИКА (выписка из уставных требований банковского учреждения)

***Преданность делу.*** Сотрудники преданны общему делу развития Банка.

***Законность.*** Сотрудники неукоснительно соблюдают принципы и нормы международного права, законодательства РФ, внутренние документы Банка.

***Профессионализм.*** Сотрудники стремятся к постоянному самосовершенствованию, ищут лучшие средства и возможности для более эффективной работы Банка.

Профессиональная этика сотрудника Банка предполагает:

- ✓отсутствие личной предвзятости, недоброжелательности;
- ✓отказ от прямого или косвенного использования положения сотрудника в Банке в частных целях, для преимущества личных интересов или получения преимуществ или выгоды;
- ✓отказ от использования непроверенной информации;
- ✓необходимость сохранения конфиденциальной информации;
- ✓верность своему делу, заботу о поддержании собственной деловой репутации.

***Открытость.*** Банк придерживается политики максимальной открытости и прозрачности в своей деятельности, Строит свои отношения с клиентами, партнерами, акционерами, сотрудниками Банка на условиях равноправия и открытости.

***Ответственность.*** Банк несет ответственность перед акционерами за результаты своей деятельности, перед клиентами – за качество предоставляемых услуг, перед деловыми партнерами – за добросовестное исполнение своих обязательств, перед обществом – за уважение личности, ее прав и свобод, за вклад в развитие экономики.

***Уважение личности.*** Банк уважает права и свободы человека независимо от национальности, социального положения, правового статуса и вероисповедания.

***Корпоративность.*** Сотрудники Банка строят взаимоотношения на основе взаимопонимания, взаимопомощи, доверия и солидарности.

***Безопасность.*** Банк принимает все необходимые меры для предотвращения любых противоправных действий в отношении имущества и ценностей Банка, клиентов, деловых партнеров, в отношении акционеров и сотрудников Банка.

***Прозрачность.*** Сотрудники Банка должны доходчиво и своевременно разъяснять каждому клиенту характеристики предлагаемых ими продуктов и услуг и возможные последствия их приобретения.

# 3.1.4. ПОДХОДЫ К РАБОТЕ С НОСИТЕЛЯМИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ИЗ ТЕОРИИ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

## 3.1.5. СРАВНИТЕЛЬНАЯ ОЦЕНКА ПОДХОДОВ К УПРАВЛЕНИЮ ПЕРСОНАЛОМ

| ПОДХОД (МЕТАФОРА) | КОНЦЕПЦИЯ УПРАВЛЕНИЯ ПЕРСОНАЛОМ | ОСНОВНЫЕ ЗАДАЧИ УПРАВЛЕНИЯ ПЕРСОНАЛОМ |
|---|---|---|
| **Экономический (механизм)** | **Использование человеческих ресурсов** | Отбор способных работников, стимулирование, нормирование труда |
| **Органический (личность, мозг)** | **Управление персоналом** | Изучение специфики потребностей, разработка различных программ, ориентированных на разные уровни потребностей (физиологический, потребность в безопасности, потребность в общении, потребности в получении профессионального признания, потребность в самореализации) |
| | **Управление человеческими ресурсами** | Обучение персонала – углубление как специализации, так и универсализации, создание условий для максимальной самоорганизации сотрудников |
| **Гуманистический (развитие личности)** | **Управление человеком** | Адаптация, развитие культуры организации – задание ценностей, формирование правил и норм, символизация |

## 3.1.6. ПРИНЦИПЫ КОНЦЕПЦИИ ИСПОЛЬЗОВАНИЯ ТРУДОВЫХ РЕСУРСОВ

- Обеспечение единства руководства
- Соблюдение строгой управленческой вертикали
- Фиксирование необходимого и достаточного объема контроля
- Соблюдение четкого разделения штабной и линейной структур организации
- Достижение баланса между властью и ответственностью
- Обеспечение дисциплины
- Достижение подчинения индивидуальных интересов общему делу
- Обеспечение равенства на каждом уровне организации
- Заслуженное вознаграждение

## 3.1.7. УСЛОВИЯ ЭФФЕКТИВНОСТИ И ЗАТРУДНЕНИЯ В РАМКАХ ЭКОНОМИЧЕСКОГО ПОДХОДА

| УСЛОВИЯ ЭФФЕКТИВНОСТИ | ОСОБЫЕ ЗАТРУДНЕНИЯ |
|---|---|
| Четкая задача для исполнения<br><br>Среда достаточно стабильна<br><br>Производство одного и того же продукта<br><br>Человек согласен быть деталью машины и ведет себя, как запланировано | Сложность адаптации к меняющимся условиям<br><br>Неповоротливая бюрократическая надстройка<br><br>Если интересы работников возьмут верх над целями организации, возможны нежелательные последствия<br><br>Дегуманизирующее воздействие на работников |

## 3.1.8. УСЛОВИЯ ЭФФЕКТИВНОСТИ И ЗАТРУДНЕНИЯ В РАМКАХ ОРГАНИЧЕСКОГО ПОДХОДА

| УСЛОВИЯ ЭФФЕКТИВНОСТИ | ОСОБЫЕ ЗАТРУДНЕНИЯ |
|---|---|
| Подчинение целей организации взаимодействию с окружающей средой | Неучет социальности организа-ции как продукта взглядов, идей, норм и верований |
| Улучшение управления за счет внимания к дифференцированным потребностям людей | Превращение людей в ресурс, который нужно развивать, в ущерб праву личности на выбор |
| Взгляд на организацию с точки зрения взаимодействия целей, стратегии, структуры и других измерений | Предположение о «функциональ-ном единстве», когда все органы работают на благо организма в целом |
| Выделение различных подсистем организации | Предположение о том, что работники должны удовлетворять все свои потребности через организацию |
| Учет естественных возможностей в процессе инновации | Опасность впасть в социальный дарвинизм |
| Повышенное внимание к «экологии» внутри- и между коллективных взаимодействий | Ответственность может перекла-дываться на внешние причины вместо изменения курса |

## 3.1.9. ФУНКЦИИ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

- планирование персонала
- определение способов привлечения персонала
- маркетинг персонала
- подбор, оценка, отбор и принятие сотрудников
- адаптация, обучение и повышение квалификации работников
- планирование карьеры
- мотивация персонала
- руководство персоналом
- управление расходами на персонал
- организация рабочего места
- обеспечение оптимального распорядка работы
- кадровое делопроизводство
- управление информацией
- оценка результатов деятельности
- контроль за персоналом
- управление конфликтами
- правовое регулирование трудовых отношений
- налаживание социальных отношений и сотрудничества
- обеспечение безопасности труда
- социальное обеспечение
- планирование и развитие организационной культуры
- обеспечение репутации фирмы
- освобождение персонала

## 3.1.10. ЭФФЕКТИВНОСТЬ УПРАВЛЕНИЯ ПЕРСОНАЛОМ

**эффективность результатов деятельности**
(общая экономическая эффективность: прибыль, рентабельность, производительность, рост оборота, качество удовлетворения спроса)

**материальная эффективность производственного процесса**
(индикаторы измерения: отклонения от плана, брак, рекламации, своевременность поставок, качество продукции)

**нематериальная эффективность производства**
(индикаторы измерения: точность и время решения проблемы, готовность к инновациям, преодоление, снятие неуверенности, определенность цели, точность и своевременность информации и др.)

**установки на труд**
(удовлетворенность трудом, инициатива, доля потерь рабочего времени, жалобы, способность брать на себя ответственность)

**установки на отношения с другими индивидами**
(восприятие влияния, готовность к кооперации, дружба, согласие, уважение, доверие, групповая сплоченность и др.)

## 3.1.11. НАПРАВЛЕНИЯ И МЕТОДЫ РАБОТЫ С ПЕРСОНАЛОМ

**Направления работы с персоналом, получающим доступ к конфиденциальной информации:**

• проведение усложненных аналитических процедур при приеме и увольнении;

• документирование добровольного согласия лица не разглашать конфиденциальные сведения и соблюдать правила обеспечения безопасности информации;

• инструктирование и обучение практическим действиям по защите информации;

• контроль за выполнением требований по защите информации, стимулирование ответственного отношения к сохранению конфиденциальных сведений.

**Сложности в работе с персоналом определяются:**

• большой ценой решения о допуске лица к тайне предприятия;

• наличием в фирме, как правило, небольшого контингента сотрудников, служебные обязанности которых связаны с использованием конфиденциальных сведений (руководители, ответственные исполнители, сотрудники режимной службы);

• разбиением тайны на отдельные элементы, каждый из которых известен определенным сотрудникам в соответствии с направлением их деятельности.

**Методы работы с персоналом:**

• обучение и систематическое инструктирование сотрудников, проведение регулярной воспитательной работы с персоналом;

• постоянный контроль за выполнением требований по защите информации;

• контрольную работу по изучению степени осведомленности персонала в области конфиденциальных работ фирмы;

• проведение служебных расследований по фактам утечки информации и нарушений персоналом требований по защите информации;

• совершенствование методики текущей работы с персоналом

# 3.1.12. ТРЕБОВАНИЯ К КОНФИДЕНЦИАЛЬНОСТИ В РАБОТЕ СОТРУДНИКА (выписка из устава банковского учреждения)

1. Сотрудники Банка обязаны соблюдать конфиденциальность информации о хозяйственной деятельности клиента и работодателя, полученной в процессе предоставления профессиональных услуг. Обязанность соблюдения конфиденциальности остается в силе даже после завершения отношений между сотрудником Банка и клиентом или работодателем.

2. Сотрудник Банка всегда должен соблюдать конфиденциальность, за исключением случаев, когда для раскрытия информации предоставлены специальные полномочия, или при наличии юридической или профессиональной обязанности такого раскрытия.

3. Конфиденциальность означает не только обязанность сохранения информации от раскрытия, но и требование к сотруднику Банка, получающему информацию в ходе выполнения профессиональных услуг, не использовать эту информацию в личных целях или в интересах третьей стороны.

4. Сотрудники Банка имеют доступ к большому объему конфиденциальной информации о хозяйственной деятельности клиента или работодателя, недоступной общественности при иных обстоятельствах. В связи с этим необходима уверенность в том, что сотрудник Банка в случае отсутствия полномочий не раскроет информацию третьим лицам. Это не относится к раскрытию информации в целях надлежащего выполнения профессиональных обязанностей сотрудника Банка в соответствии с требованиями действующего законодательства.

5. Раскрытие информации сотрудником Банка осуществляется в случаях, прямо предусмотренных действующим законодательством Российской Федерации. В случае, если прямого указания на раскрытие информации действующим законодательством не предусмотрено, информация может быть раскрыта при наличии соответствующего разрешения собственника информации, а при необходимости – и контролирующих органов, обеспечивающих ее конфиденциальность.

# 3.2. ПРОВЕРОЧНЫЕ МЕРОПРИЯТИЯ, ОБУЧЕНИЕ РАБОТЕ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ И ОФОРМЛЕНИЕ ДОПУСКА ПРИ ПРИЕМЕ НА РАБОТУ

## 3.2.1. ОСОБЕННОСТИ ПРИЕМА СОТРУДНИКОВ НА РАБОТУ, СВЯЗАННУЮ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

**ЭТАПЫ:**

• предварительно сформулировать, какие функции должен выполнять сотрудник, каков круг его ответственности, какие качества, знания и уровень квалификации необходимо иметь;

• составить перечень конфиденциальных сведений, с которыми будет работать специалист;

• составить перечень форм поощрения и стимулирования за хранение информации;

• составить перечни вопросов, которые необходимо будет решать специалисту, перечни его личных качеств, возрастных, профессиональных и иных характеристик;

• составить описание должности и требования к кандидату на должность.

**Направления активного поиска кандидатов на вакантную должность :**

1. Поиск кандидатов на вакантное место внутри фирмы, которое определяется высокими деловыми качествами работника, особенно руководителя или специалиста.

2. Поиск кандидатов среди студентов и выпускников учебных заведений, установление связей с подразделениями вузов, занятыми трудоустройством выпускников.

3. Обращение в государственные и частные бюро, агентства по найму рабочей силы, биржи труда, организации по трудоустройству лиц, уволенных по сокращению штатов, трудоустройству молодежи, бывших военнослужащих и т.п.

4. Рекомендации работающих в фирме сотрудников

## 3.2.2. ПРОВЕРОЧНЫЕ МЕРОПРИЯТИЯ В ХОДЕ ПРИЕМА НА РАБОТУ, СВЯЗАННУЮ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

- подбор кандидата для приема на работу или перевода, получение резюме;
- изучение резюме руководством фирмы, подразделения и службой персонала, беседа;
- информирование кандидатов, работающих в фирме, об их должностных обязанностях, связанных с владением тайной фирмы;
- предварительное собеседование руководства фирмы, подразделения и службы персонала с кандидатами, не работающими в фирме; уточнение отдельных положений резюме; ответы на вопросы о работе; изучение рекомендательных писем;
- заполнение кандидатами заявления о приеме, автобиографии, личного листка по учету кадров, копий документов об образовании, о наличии ученых степей, званий, передача в отдел кадров рекомендательных писем и характеристик;
- обновление материалов личного дела работающего в фирме сотрудника; получение представления о переводе от руководителя подразделения;
- собеседование кандидатов с работником отдела кадров по представленным документам, при необходимости подтверждение тех или иных сведений;
- опрос сотрудником отдела кадров авторитетных для фирмы лиц, лично знающих кандидата на должность, протоколирование опроса;
- собеседование экспертов с кандидатами с целью определения их личных и моральных качеств, а для неработающих в фирме сотрудников дополнительно – профессиональных способностей; рассмотрение медицинской справки;
- тестирование и анкетирование кандидатов;
- принятие решения руководством фирмы об отборе единственного претендента и возможности предложить ему работу, связанную с владением тайной фирмы;
- заключительное собеседование с претендентом на должность, получение от него принципиального согласия на работу с конфиденциальной информацией

## 3.2.3. ПРОЦЕДУРЫ ПРИЕМА СОТРУДНИКОВ, РАБОТА КОТОРЫХ СВЯЗАНА С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

- подписание претендентом обязательства о неразглашении тайны фирмы; информирование претендента о характере конфиденциальной информации, с которой он будет работать, наличии системы защиты этой информации и тех ограничениях, которые придется учитывать работнику в служебной и неслужебной обстановке;
- беседа-инструктаж руководителя подразделения, руководителя службы безопасности и сотрудника службы персонала с претендентом на должность; ознакомление претендента с должностной инструкцией, инструкцией по обеспечению ИБ фирмы;
- составление проекта контракта, содержащего пункт об обязанности работника не разглашать конфиденциальные сведения фирмы;
- подписание контракта о временной работе без права доступа к конфиденциальной информации;
- составление и подписание приказа о приеме на работу с испытательным сроком;
- заведение личного дела на вновь принятого сотрудника;
- заполнение на сотрудника необходимых учетных форм, личной карточки;
- внесение фамилии сотрудника в первичные учетные бухгалтерские документы;
- внесение соответствующей записи в трудовую книжку сотрудника;
- изучение качеств сотрудника в течение испытательного срока;
- обучение сотрудника правилам работы с конфиденциальной информацией, инструктажи, проверка знаний;
- оформление допуска сотрудника к конфиденциальной информации и документам
- анализ результатов работы сотрудника в течение испытательного срока, составление нового контракта и издание приказа или отказ сотруднику в работе

## 3.2.4. ПРОВЕРОЧНЫЕ МЕРОПРИЯТИЯ ПРИ РАБОТЕ С ДОКУМЕНТАМИ СОТРУДНИКОВ

❖ Предоставленные кандидатом персональные документы тщательно проверяются на достоверность: соответствие фамилий, имен и отчеств, других персональных данных, наличие необходимых отметок и записей, идентичность фотокарточки и личности гражданина (на фотографии очки, парик — только при постоянной носке), соответствие формы бланка годам их использования, отсутствие незаверенных подчисток, исправлений, попыток замены листов, фотографий, соответствие и качество печатей и т.п.

Сведения, включенные в характеристики, рекомендательные письма, списки научных трудов и изобретений, выданные и заверенные другими учреждениями, могут быть проверены путем обращения в эти учреждения. Документы, явно недостоверные, могут быть возвращены гражданину, и ему отказывается в рассмотрении вопроса о приеме на работу без объяснения причины отказа. Сведения, указываемые в резюме, не проверяются.

❖ Заявление о назначении (переводе) на должность, личный листок по учету кадров, автобиография пишутся или заполняются гражданином собственноручно, без использования пишущей машинки или принтера.

❖ Все записи, сделанные в личном листке по учету кадров, и текст автобиогра-фии сравниваются сотрудником отдела кадров с персональными документами. Исправления в указанных документах не допускаются.

❖ Копии с аттестатов, дипломов, свидетельств, грамот и т.п., которые приобща-ются к документам для решения вопроса о приеме на работу, снимаются с по-мощью копировальной техники в отделе кадров и заверяются сотрудником отде-ла. Копии, принесенные гражданином, внимательно сличаются с подлинником и также заверяются этим сотрудником. Нотариального заверения копий не требуется. Запрещается заверение копий с копии.

❖ Паспорт, военный билет, дипломы, аттестаты и др. персональные документы после работы с ними возвращаются (кроме трудовой книжки)

## 3.2.5. ЦЕЛИ СОБЕСЕДОВАНИЙ С КАНДИДАТОМ

**Собеседования с кандидатами на должность преследуют следующие цели:**

- выявить реальную причину желания работать в данной фирме;
- выявить возможных злоумышленников или попытаться увидеть слабости кандидата как человека, которые могут провоцировать преступные действия;
- убедиться, что кандидат не намерен использовать в работе секреты фирмы, в которой он раньше работал;
- убедиться в добровольном согласии кандидата соблюдать правила защиты информации и иметь определенные ограничения в профессиональной и личной жизни.

**Вопросники для собеседования составляются таким образом, чтобы выяснить:**

- причины увольнения кандидата с прежнего места работы;
- источник информации о вакансии в данной фирме – кто рекомендовал и т.п.;
- работал ли кандидат ранее с конфиденциальной информацией, подписывал ли обязательство о ее неразглашении;
- возникшие сомнения, появившиеся в связи с изучением документов кандидата;
- отношения в семье, уровень благосостояния кандидата, жилищные условия, культурный уровень и т.п.

**Ответы кандидата фиксируются, и те из них, которые вызвали сомнения, уточняются путем опроса знающих кандидата лиц, путем тестирования и другими способами (если это необходимо).**

**Одной из главных задач собеседования и тестирования** является выявление несоответствия мотиваций в различных логических группах вопросов. Например, несоответствие: хочет получать большую зарплату, но раньше он получал столько же, работал близко от дома, а хочет работать в фирме, находящейся на значительном расстоянии, и т.п.

## 3.2.6. ОТБОР КАНДИДАТОВ

**Цели психологического отбора:**

• выявление судимостей, преступных связей, криминальных наклонностей;
• определение возможных преступных склонностей, предрасположенности к совершению противоправных действий, дерзких и необдуманных поступков;
• установление факторов, свидетельствующих о морально-психологической ненадежности, неустойчивости, уязвимости кандидата и т.д.

**Основные личные качества, которыми должен обладать потенциальный сотрудник:**

• порядочность, честность, принципиальность и добросовестность, исполнительность, дисциплинированность;
• эмоциональная устойчивость, стремление к успеху и порядку в работе;
• самоконтроль в поступках и действиях;
• правильная самооценка собственных возможностей и способностей;
• умеренная склонность к риску;
• умение хранить секреты;
• тренированное внимание, хорошая память, способности к сравнительной оценке и т.д.

**Личные качества, не способствующие сохранению секретов:**

• эмоциональная неуравновешенность;
• разочарование в себе и своих способностях;
• отчуждение от коллег по работе;
• недовольство своим служебным положением;
• ущемленное самолюбие;
• крайне эгоистическое поведение;
• отсутствие достаточного благоразумия;
• нежелание и неспособность защищать информацию;
• нечестность;
• финансовая безответственность;
• употребление наркотиков, отрицательное воздействие алкоголя и т.д.

## 3.2.7. ОБЯЗАТЕЛЬСТВО (ПОДПИСКА) О НЕРАЗГЛАШЕНИИ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ

**Обязательство (подписка, соглашение) о неразглашении конфиденциальных сведений** представляет собой правовой документ, которым претендент добровольно и письменно дает согласие **на ограничение его прав** в отношении использования конфиденциальной информации и предупреждается об ответственности за ее разглашение.

***Пример:***

***ДОГОВОРНОЕ ОБЯЗАТЕЛЬСТВО***

***Обязуюсь:***

*1. В период оформления на работу и работы в ____ не разглашать сведения, составляющие ее коммерческую тайну, которые мне будут доверены или станут известны при исполнении обязанностей, собеседованиях, инструктировании и обучении.*

*2. Беспрекословно и аккуратно выполнять относящиеся ко мне требования приказов, инструкций и положений по защите коммерческой тайны, с которой я ознакомлен.*

*3. Не сообщать устно, письменно или иным способом кому бы то ни было сведений, составляющих тайну.*

*4. В случае отказа от работы, окончания работы или увольнения не разглашать и не использовать для себя и других лиц сведений, составляющих тайну.*

*Я предупрежден, что в случае нарушения данного обязательства должен возместить причиненный ____ ущерб или буду привлечен к дисциплинарной (вплоть до увольнения) или другой ответственности в соответствии с действующим законодательством.*

*Проинструктировал (подпись).*

*Подпись лица, принимающего обязательство.*

*Дата*

# 3.2.8 ОСОБЕННОСТИ ФУНКЦИОНИРОВАНИЯ РАЗРЕШИТЕЛЬНОЙ СИСТЕМЫ КОММЕРЧЕСКОГО ПРЕДПРИЯТЯИЯ

**Разрешительная система включает в себя допуск сотрудника к конфиденциальной информации и непосредственный доступ этого сотрудника к конкретным сведениям.**

**Допуск** – процедура оформления права сотрудника на доступ к сведениям ограниченного распространения и правовой акт согласия собственника информации на передачу ее для работы конкретному лицу.

Оформление допуска носит **добровольный характер**. Наличие допуска предоставляет сотруднику формальное право работать со строго определенным кругом конфиденциальных документов, баз данных и сведений.

В предпринимательских структурах **разрешение на допуск** дает первый руководитель фирмы. Разрешение оформляется соответствующим пунктом в контракте (трудовом договоре). Допуск может оформляться приказом первого руководителя с указанием типового состава сведений, с которыми разрешается работать данному сотруднику или группе сотрудников.

Допуск может носить временный характер на период выполнения определенной работы и пересматриваться при изменении профиля работы сотрудника

**Доступ** – практическая реализация каждым сотрудником предоставленного ему допуском права на ознакомление и работу с конфиденциальными сведениями, документами и базами данных. Санкционируется руководителем, его заместителем, руководителем подразделения, службы в отношении конкретной информации и конкретного сотрудника.

**Разрешение на доступ** к информации может быть дано при соблюдении условий:

- наличие подписанного приказа первого руководителя о приеме на работу (переводе, временном замещении, изменении должностных обязанностей и т.п.) или назначении на должность с данной информацией;
- наличие подписанного сторонами трудового договора имеющего пункт о сохранении тайны и подписанного обязательства о неразглашении сведений и соблюдении правил их защиты;
- соответствие функциональных обязанностей передаваемой информации;
- знание требований нормативно-методических документов по защите информации и сохранении тайны;
- наличие условий для работы с конфиденциальными документами и базами данных и систем контроля

## 3.2.10. ОБУЧЕНИЕ ПЕРСОНАЛА, ОБЛАДАЮЩЕГО КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

**Обучение сотрудников** предполагает приобретение и поддержание на высоком уровне производственных навыков работы с конфиденциальными сведениями, психологическое воспитание сотрудников и воспитание глубокой убежденности в необходимости выполнения требований по защите конфиденциальной информации.

**Задачи обучения включают в себя изучение:**

- характера и состава конфиденциальной информации;
- возможных угроз конфиденциальным сведениям, каналов их объективного распространения и каналов утраты, методов работы злоумышленников;
- структуры системы защиты, требований и правил защиты информации;
- порядка работы сотрудников с конфиденциальными сведениями и базами данных;
- действий персонала в конкретных экстремальных ситуациях.

**Методика обучения включает:**

- специализированные программы для обеспечения лекций и практических занятий;
- проведение лекций, семинаров и собеседований; тестирование сотрудников;
- решение ситуационных задач, связанных с выполнением требований по защите информации;
- практическую ситуационную учебу по действиям персонала в экстремальных ситуациях;
- проведение деловых игр, обучающих методам противодействия

# 3.2.11.ПРИНЦИПЫ ПОСТРОЕНИЯ И ЗАДАЧИ СОЗДАНИЯ СИСТЕМЫ ПОДГОТОВКИ И ПЕРЕПОДГОТОВКИ ПЕРСОНАЛА

**Принципы построения системы обучения:**

учет отраслевых особенностей построения и функционирования ИС и созданной системы защиты информации;

реализация единой организационно-технической политики при выборе методов подготовки персонала;

постоянный контроль нарушений в работе программно-технических средств ИС, персонала и пользователей для установления фактов появления угроз безопасности;

непрерывность и полнота охвата системой обучения персонала ИС и всех категорий пользователей;

централизованное управление системой обучения;

разумное сочетание различных форм обучения.

**Задачи системы подготовки персонала:**

1. Организация непрерывного сбора информации о нарушениях информационной безопасности в ИС предприятия.

2. Выработка совместно со специалистами подразделения защиты информации мер по устранению или локализации причин нарушений информационной безопасности.

3. Формирование дополнительных требований к уровню и объему знаний по организации защиты информации для каждой категории персонала в дополнение к общепринятым по данной специализации и разработка рекомендаций по их внедрению:

в учебные программы соответствующих отраслевых курсов подготовки или переподготовки для штатных работников предприятия по специализации ИТ, ЗИ, а также руководящего состава;

в учебные пособия для нештатных работников по специальности ИТ (администраторы ЛВС, серверов, специалисты по защите гостайны и др.);

в нормативно-методические документы, изучаемые пользователями при сдаче зачетов на самостоятельный допуск к исполнению служебных обязанностей с использованием СВТ.

4. Разработка конкретных организационно-методических материалов о действиях сотрудников в случаях нарушений ИБ и доведение их до пользователей всей ИС

# 3.2.12. СОДЕРЖАНИЕ БАЗОВЫХ ПРОГРАММ ПОДГОТОВКИ ПЕРСОНАЛА ПРЕДПРИЯТИЯ

**СПЕЦИАЛИСТЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ ДОЛЖНЫ:**

- иметь специальное базовое образование и практический опыт работы в этой области;
- периодически повышать квалификацию в Центрах безопасности информации, аккредитованных Гостехкомиссией России, по утвержденным программам, включающим широкий спектр вопросов защиты информации;
- обучаться внедрению и эксплуатации наукоемких технологий, систем и средств защиты информации в фирмах-разработчиках и дистрибьюторах таких продуктов при наличии у них лицензий Минобразования.

**ПОДГОТОВКА ПОЛЬЗОВАТЕЛЕЙ ДОЛЖНА ВКЛЮЧАТЬ СЛЕДУЮЩИЕ ВОПРОСЫ:**

- основные угрозы информационной безопасности при работе на персональном компьютере в корпоративной сети и Интернете;
- требования внутренних документов по ИБ, регламенты безопасности и т. д.;
- настройка и использование встроенных механизмов ЗИ операционных систем;
- работа с программно-аппаратными средствами ЗИ (аутентификации, разграничения доступа, криптографическими средствами) и антивирусной защиты;
- архивирование информации.
- изучение электронной рассылки информационных материалов по наиболее актуальным угрозам ИБ и методам их нейтрализации.

**Целесообразно создание специализированных учебных центров информационной безопасности для подготовки специалистов по ЗИ и ИТ и пользователей по программам различного уровня.**

# 3.3. МОНИТОРИНГ ОСВЕДОМЛЕННОСТИ ПЕРСОНАЛА
## 3.3.1. ОСОБЕННОСТИ РАЗГЛАШЕНИЯ ЦЕННОЙ ИНФОРМАЦИИ ПЕРСОНАЛОМ

**Информация от персонала легко переходит к злоумышленнику по причине:**

• слабого знания персоналом требований и правил защиты информации;

• злостного или безответственного невыполнения сотрудником этих правил;

• использования экстремальных ситуаций в помещениях фирмы и происшествий с персоналом: пожара, нападения, плохого самочувствия сотрудника в транспорте, отключения электропитания в помещении фирмы и т.п.;

• ошибочных или безответственных действий персонала.

**Ошибочные и безответственные действия персонала подразделяются:**

• на не провоцированные злоумышленником: взятие конфиденциальных документов на дом, оставление без надзора документа или загруженного компьютера, выбрасывание в мусорную корзину черновиков и копий конфиденциальных документов, использование конфиденциальной информации в открытых публикациях, ошибочная выдача конфиденциального документа сотруднику, не имеющему к нему доступа, и т.п.;

• на провоцированные злоумышленником: предоставление конфиденциальной информации на ложные социологические и другие опросы, прохождение сотрудником ложного анкетирования, обман сотрудника, выдающего документы, проход злоумышленника или его сообщника в режимное помещение, на территорию фирмы по фиктивным документам, общение сотрудника с легендированным злоумышленником по поводу сведений, составляющих тайну, и т.п.

**Результативность обмана зависит от подготовки, интуиции и сообразительности сотрудников, которых провоцируют на ошибочные действия. Сотрудники должны быть обучены и готовы к противодействию подобным действиям злоумышленника или его сообщников.**

## 3.3.2. МЕТОДЫ ДОБЫВАНИЯ ЦЕННОЙ ИНФОРМАЦИИ У ПЕРСОНАЛА

**А) осознанное сотрудничество со злоумышленником:**

• инициативное сотрудничество с целью мести руководству или коллективу, по причине подкупа, оплаты постоянных услуг и психической неустойчивости;

• формирование сообщества – злоумышленник и его сообщник, помощник, работающий на основе убеждения в справедливости взглядов злоумышленника, дружеских и иных отношений, взаимопомощи и т.п.

• сотрудничество на основе личного убеждения работника в противоправных действиях руководства фирмы или их моральном разложении;

• склонение к сотрудничеству обманными действиями, изменением взглядов или моральных принципов путем убеждения, вымогательства, шантажа с учетом отрицательных черт характера или физического насилия.

**Б) Использование сотрудника для неосознанного сотрудничества:**

• переманивание ценных и осведомленных специалистов обещанием лучшего материального вознаграждения, условий труда и иных преимуществ;

• ложная инициатива в приеме сотрудника на высокооплачиваемую работу в конкурирующую фирму, выведывание в процессе собеседования необходимых конфиденциальных сведений и затем отказ в приеме;

• выведывание ценной информации у сотрудника фирмы с помощью подготовленной системы вопросов на научных конференциях, встречах с прессой, на выставках, в личных беседах в служебной и неслужебной обстановке;

• подслушивание и записывание на диктофон разговоров сотрудников фирмы в служебных и неслужебных помещениях, в процессе переговоров и приеме посетителей, в транспорте, на банкетах, в домашней обстановке, при общении с друзьями;

• прослушивание служебных и личных телефонов сотрудников фирмы; перехват телексов, телеграмм, факсов, сообщений по электронной почте, ознакомление со служебной и личной корреспонденцией руководства фирмы сотрудников;

• получение злоумышленником от сотрудника нужной информации в состоянии алкогольного опьянения, под действием наркотиков, гипноза и приведения в иное состояние сознания, не позволяющее адекватно оценивать свои действия

## 3.3.3. МОНИТОРИНГ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ, ИЗВЕСТНОЙ КАЖДОМУ ИЗ СОТРУДНИКОВ

**1. Учет любых контактов** любого сотрудника с конфиденциальными сведениями, в том числе санкционированных, а также **случайного ознакомления** с информацией, к которой сотрудник не имеет доступа.

**2. Ведение карточной или электронной учетной формы с предметными зонами**, позволяющими сопоставлять функциональные обязанности сотрудника и состав конфиденциальной информации, полученной сотрудником:

- штатных функциональных обязанностей, при реализации которых используется конфиденциальная информация (по утвержденной должностной инструкции);
- изменений и дополнений, внесенных в обязанности сотрудника, с указанием документа-основания, его даты и руководителя, подписавшего документ;
- стандартного состава сведений, к которым допущен сотрудник в соответствии с должностной инструкцией (с указанием наименования документа о допуске, его даты, номера и фамилии руководителя, подписавшего документ);
- изменений и дополнений в составе конфиденциальных сведений, к которым допускается сотрудник в связи с пересмотром его должностных обязанностей;
- документированной информации, с которой знакомится или работает сотрудник, с указанием наименований документов, их дат и номеров, краткого содержания, целевого использования конфиденциальных сведений и их индексов по перечню, фамилий руководителей, разрешивших работу с документами;
- недокументированной конфиденциальной информации, которая стала известна, с указанием даты и цели ознакомления, фамилии руководителя, разрешившего ознакомление, состава конфиденциальных сведений и их индексов по перечню;
- обнаруженного несанкционированного ознакомления сотрудника с конфиденциальной информацией с указанием даты ознакомления, условий или причин ознакомления, фамилии виновного сотрудника, места ознакомления, состава сведений.

**3. Анализ сравнением содержания записей в зонах и индексов известной сотруднику конфиденциальной информации** (поиском несоответствий).

# 3.3.4. КОНТРОЛЬ КАЧЕСТВА РАБОТЫ СОТРУДНИКОВ

**Основные формы контроля качества работы в части защиты информации:**

- аттестация сотрудников;
- отчеты руководителей подразделений о работе подразделений и состоянии системы защиты информации;
- регулярные проверки руководителем фирмы или службой безопасности соблюдения сотрудниками требований по защите информации;
- самоконтроль сотрудников

**АТТЕСТАЦИЯ** – коллективная форма оценки профессиональной пригодности сотрудника и его соответствия занимаемой должности (ежеквартально, раз в год).

**РАССМАТРИВАЮТСЯ:**

✓трудовая дисциплина, исполнительность, трудолюбие,
✓ответственность, требовательность, принципиальность
✓организованность, качество и эффективность выполняемой работы, самостоятельность и инициатива,
✓творческая деятельность, прогрессивность профессиональных решений, профессиональный кругозор,
✓умение общаться, организаторские способности,
✓преданность делу фирмы;
✓знание нормативных документов по защите информации, умение применять требования этих документов в практической деятельности,
✓отсутствие нарушений в работе с документами,
✓умение общаться с посторонними лицами, не раскрывая секреты фирмы, и т.д.

По результатам издается **приказ**, в котором отражаются решения аттестационной комиссии о поощрении, переаттестации, повышении в должности или увольнении, об отстранении сотрудника от работы с информацией и документами, составляющими тайну

**ОТЧЕТЫ РУКОВОДИТЕЛЕЙ** структурных подразделений и руководителя службы безопасности на совещании у первого руководителя о состоянии системы защиты информации и выполнении ее требований сотрудниками.

**ПРОВЕРКИ ВЫПОЛНЕНИЯ** (плановые и внезапные): наличие у сотрудника числящихся за ним документов, дел, магнитных носителей информации; изделий и иных элементов, составляющих тайну

**САМОКОНТРОЛЬ** состоит в проверке исполнителями полноты и правильности выполнения действующих инструктивных положений, в немедленном информировании непосредственного руководителя и службы безопасности о фактах утери документов, утрате ценной информации, разглашении сотрудниками сведений, составляющих тайну, нарушении порядка защиты информации

# 3.2.11. ОСОБЕННОСТИ УВОЛЬНЕНИЯ СОТРУДНИКОВ, ВЛАДЕЮЩИХ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

**Технологическая цепочка увольнения сотрудника включает в себя:**

• написание сотрудником **заявления об увольнении** с подробным раскрытием причины увольнения и желательно указанием места предполагаемой работы;

• **передача заявления руководителю** структурного подразделения для оформления и передачи в отдел кадров или службу персонала;

• прием службой конфиденциальной документации от увольняющегося сотрудника **всех числящихся за ним документов, баз данных, носителей информации, изделий, материалов, с которыми он работал**, проверка их комплектности, полноты и оформление приема в описи исполнителя или актом;

• **сдача сотрудником пропуска** (идентификатора) для входа в рабочую зону, ключей и печатей, запрещение сотруднику входить в рабочее помещение с использованием знания шифра кодового замка;

• **проведение беседы с сотрудником** с целью напоминания ему об обязательстве сохранения в тайне тех сведений, которые ему были доверены по службе, предупреждение сотрудника о запрещении использования этих сведений в интересах конкурента или в личных целях, выяснение причины увольнения и места новой работы;

• **подписание сотрудником обязательства** о неразглашении им сведений после увольнения;

• **документальное оформление увольнения** в соответствии с общими правилами;

• **прием от сотрудника пропуска для входа в здание**, выдача ему трудовой книжки и расчета по заработной плате, сопровождение его до выхода сотрудником службы безопасности.

После сдачи всех документов и материалов сотруднику **запрещается входить в режимную рабочую зону**. При необходимости ему может быть выдан идентификатор посетителя с правом входа только в определенные административные помещения

# 3.4. ПРАВОВОЕ РЕГУЛИРОВАНИЕ ВЗАИМООТНОШЕНИЙ АДМИНИСТРАЦИИ И ПЕРСОНАЛА ПРИ ИНЦИДЕНТАХ

## 3.4.1. ПРИНЦИПЫ ЭФФЕКТИВНОЙ ПОЛИТИКИ РЕАГИРОВАНИЯ НА ИНЦИДЕНТЫ

| | |
|---|---|
| **1. Руководство организации должно способствовать созданию необходимых условий для внедрения процедуры расследования инцидентов информационной безопасности** | ❖ создание формализованной политики реагирования;<br>❖ разработка процедур обработки инцидентов;<br>❖ урегулирование юридических аспектов обращения информации в процессе расследования;<br>❖ утверждение структуры команды реагирования;<br>❖ налаживание внутриорганизационных контактов команды по расследованию инцидентов с профильными специалистами;<br>❖ определение зон ответственности команды расследования, обучение и техническое оснащение |
| **2. Документирование руководящих принципов и процедур расследования инцидентов ИБ для обеспечения внутриорганизационного взаимодействия и формирования представлений в органы государственной власти** | ❖ в процессе расследования инцидента потребуется общаться со сторонними организациями с целью доведения расследования до завершения (СМИ, органы правопорядка, пострадавшие);<br>❖ в случае несоразмерного разглашения конфиденциальной информации, связанной с результатами расследования инцидента, ущерб от может быть соизмерим или превышать ущерб, нанесённый вследствие самого инцидента;<br>❖ урегулированию проблемы несоразмерного разглашения служит создание контактных позиций, структура и правомочность которых оговаривается на этапе формирования политики расследования инцидентов и представляет собой юридически закреплённую доверительную среду участников информационного обмена |
| **3. Информирование о результатах расследования инцидента своих сотрудников и партнёров** | ❖ результаты расследования должны быть документированы и внесены в базу данных инцидентов ИБ;<br>❖ завершение расследования должно сопровождаться обсуждением его результатов со всеми привлечёнными сторонами;<br>❖ группа расследования инцидентов должна сделать выводы об уязвимостях, классифицировать их, принять меры к недопущению и обеспечить понимание причинно-следственных связей;<br>❖ решающим фактором проведения успешного расследования является консолидация действий сотрудников и внедрение практики ролевого управления расследованием |
| **4. Анализ инцидентов и обработка результатов с целью получения практического опыта** | |

## 3.4.3. НОРМАТИВНЫЕ АКТЫ, РЕГУЛИРУЮЩИЕ ВОЗМЕЩЕНИЕ МОРАЛЬНОГО ВРЕДА

**1. Гражданский кодекс РФ:**

ст. 151 - определяются основания возложения на нарушителя обязанности денежной компенсации морального вреда: причинение физических или нравственных страданий действиями, нарушающими личные неимущественные права либо посягающими на др. нематериальные блага;

ст. 152 (ч.5) - дает право гражданину, в отношении которого распространены сведения, порочащие его честь, достоинство или деловую репутацию требовать возмещения убытков и морального вреда;

ст. 1099-1101 - определяют общие положения, основания, способы и размер компенсации;

ст. 1123 – определяет право завещателя на компенсацию морального вреда в случае нарушения тайны завещания со стороны нотариуса, др. удостоверяющего завещание лица, переводчика, исполнителя, свидетелей, а также граждан, подписывающих завещание вместо завещателя.

**2. Трудовой кодекс РФ:** ст. 237 - право работника на возмещение морального вреда в случае неправомерных действий или бездействия работодателя.

**3. Уголовно процессуальный кодекс**: ст. 42, 44, 136 - устанавливают право потерпевшего на компенсацию морального вреда.

**4. ФЗ "О персональных данных":** ст. 17 - устанавливает право субъекта на компенсацию в судебном порядке в случае нарушения оператором обработки его персональных данных.

**5. ФЗ "Об информации, информационных технологиях и о защите информации":** ст. 17 – устанавливает компенсацию лицам, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа.

**6. ФЗ "О рекламе":** ст. 38 - устанавливает для лиц, права которых нарушены в результате распространения ненадлежащей рекламы, право обратиться в суд с иском.

**7. ФЗ "О средствах массовой информации":** ст. 62 - моральный вред, причиненный гражданину в результате распространения СМИ сведений, порочащих честь и достоинство гражданина либо причинивших ему иной неимущественный вред, возмещается СМИ, а также виновными.

**8. Постановление Пленума ВС РФ "О судебной практике по делам о защите чести и достоинства граждан, а также деловой репутации граждан и юридических лиц".** Компенсация осуществляется независимо от подлежащего возмещению имущественного вреда и от вины причинителя, если «…вред причинен распространением сведений, порочащих честь, достоинство и деловую репутацию». Компенсация осуществляется в денежной форме. При определении размера компенсации вреда должны учитываться требования разумности и справедливости. Характер физических и нравственных страданий оценивается судом с учетом фактических обстоятельств и индивидуальных особенностей потерпевшего

# Глава 4.
# ОСНОВЫ ВНУТРИОБЪЕКТОВОГО РЕЖИМА И ЕГО ОРГАНИЗАЦИЯ

**4.1.** Понятие и основы организации внутриобъектового режима.

**4.2.** Функциональные зоны: методика разграничения и методы обособления

**4.3.** Понятие и основы организации пропускного режима.

**4.4.** Охрана территории предприятия и функциональных зон от проникновения нарушителей

**4.5.** Охрана конфиденциальных документов и имущества при транспортировке

**Литература:**

1. Садердинов А.А. Информационная безопасность предприятия. Уч. пособие. – М.: Дашков и Ко, 2004 г.

2. Ярочкин В.И. Система безопасности фирмы. – М.: Ось-89, 2003 г.

Оглавление

# 4.1. ПОНЯТИЕ И ПРИНЦИПЫ ОРГАНИЗАЦИИ ВНУТРИОБЪЕКТОВОГО РЕЖИМА

## 4.1.1. ПОНЯТИЕ О ВНУТРИОБЪЕКТОВОМ РЕЖИМЕ

**Внутриобъектовый режим – основной элемент системы защиты информации** предприятия, организация и обеспечение которого направлены на соблюдение надлежащего **режима секретности – установленного нормативными актами единого порядка обеспечения защиты сведений**, составляющих государственную тайну, включающего систему административно-правовых, организационных, инженерно-технических и других мер

**Внутриобъектовый режим организуется в целях исключения:**

- **проникновения посторонних лиц** на охраняемую территорию и объекты предприятия, а также в служебные помещения, в которых проводятся работы с использованием сведений, составляющих государственную тайну;
- **посещения режимных помещений** без служебной необходимости сотрудниками предприятия, не имеющими к ним прямого отношения, а также командированными лицами, которым не предоставлено право на их посещение;
- **вноса (ввоза) на территорию** личных технических средств (кино-, фото-, видео-звукозаписывающей аппаратуры и других);
- **несанкционированного выноса (вывоза)** с территории предприятия носителей сведений, составляющих государственную тайну;
- **нарушений установленного регламента служебного времени**, распорядка работы структурных подразделений по защите государственной тайны, а также установленного порядка и режима работы сотрудников и командированных лиц с носителями сведений, составляющих государственную тайну

## 4.1.2. ПРИНЦИПЫ ОРГАНИЗАЦИИ ВНУТРИОБЪЕКТОВОГО РЕЖИМА

**ПОДХОДЫ К ОРГАНИЗАЦИИ ВНУТРИОБЪЕКТОВОГО РЕЖИМА:**

- определение **ответственности руководителей** подразделений и должностных лиц за защиту государственной тайны;
- четкое разграничение функций структурных подразделений (служба безопасности, режимно-секретное подразделение, подразделение противодействия иностранным техническим разведкам, служба охраны и др.);
- создание **эффективной системы контроля** за выполнением мероприятий по режиму секретности и обеспечению сохранности носителей сведений, составляющих государственную тайну.

**ПРИНЦИПЫ ФОРМИРОВАНИЯ СИСТЕМЫ ВНУТРИОБЪЕКТОВОГО РЕЖИМА:**

- **принцип персональной ответственности** руководителей структурных подразделений, других должностных лиц и сотрудников предприятия за выполнение задач в области защиты государственной тайны;
- **принцип комплексного использования** имеющихся сил и средств для решения задач по защите государственной тайны;
- **принцип полного охвата всех направлений** деятельности предприятия, в ходе работы по которым возможна утечка сведений, составляющих государственную тайну, или утрата носителей этих сведений

## 4.1.3. СОДЕРЖАНИЕ ОРГАНИЗАЦИИ ВНУТРИОБЪЕКТОВОГО РЕЖИМА

- обеспечение **охраны собственности** предприятия;
- **организация конфиденциального делопроизводства**, учета, хранения и уничтожения документов, содержащих конфиденциальную информацию;
- **защита конфиденциальной информации** при осуществлении внешнеэкономической деятельности предприятия;
- **контроль** выполнения требований нормативно-методических и внутренних организационно-распорядительных документов по защите информации;
- **выявление и закрытие возможных каналов утечки** конфиденциальной информации;
- **разработка системы организационных и технических мер**, регламентирующих внутриобъектовый режим предприятия, и контроль за их выполнением;
- **контроль за порядком изготовления, учета, хранения, использования бланков служебных удостоверений**, печатей, штампов предприятия, а также металлических и мастичных печатей с индивидуальными учетными номерами;
- **организация приема и передачи информации** с использованием различных технических средств связи;
- **разработка требований к режимным помещениям**, проведение их аттестации, установка и эксплуатация технических средств защиты информации;
- **участие в экспертизе материалов** для открытого опубликования;
- **организация и проведение служебных расследований** по фактам нарушений требований, касающихся внутриобъектового режима на предприятии;
- **осуществление взаимодействия** с правоохранительными и другими государственными органами по вопросам обеспечения безопасности предприятия

# 4.2. ФУНКЦИОНАЛЬНЫЕ ЗОНЫ:
## 4.2.2. МЕТОДИКА РАЗГРАНИЧЕНИЯ И МЕТОДЫ ОБОСОБЛЕНИЯ СУЩНОСТЬ И РАЗНОВИДНОСТИ ФУНКЦИОНАЛЬНЫХ ЗОН

**ФУНКЦИОНАЛЬНЫЕ ЗОНЫ – зоны, для которых документами территориального планирования определены границы и функциональное назначение**:

- **жилые,**
- **общественно-деловые,**
- **производственные,**
- **инженерной и транспортной инфраструктур,**
- **сельскохозяйственного использования,**
- **рекреационного назначения,**
- **особо охраняемых территорий,**
- **специального назначения,**
- **иные виды зон**

***ФЗ «О введении в действие Градостроительного кодекса РФ»***

**МЕТОДЫ ОБОСОБЛЕНИЯ ФУНКЦИОНАЛЬНЫХ ЗОН:**

1) установление препятствий (инженерные заграждения, ограды, барьеры, рвы);

2) установление контролируемых территориальных ограничений доступа (запреты, указатели и пр.);

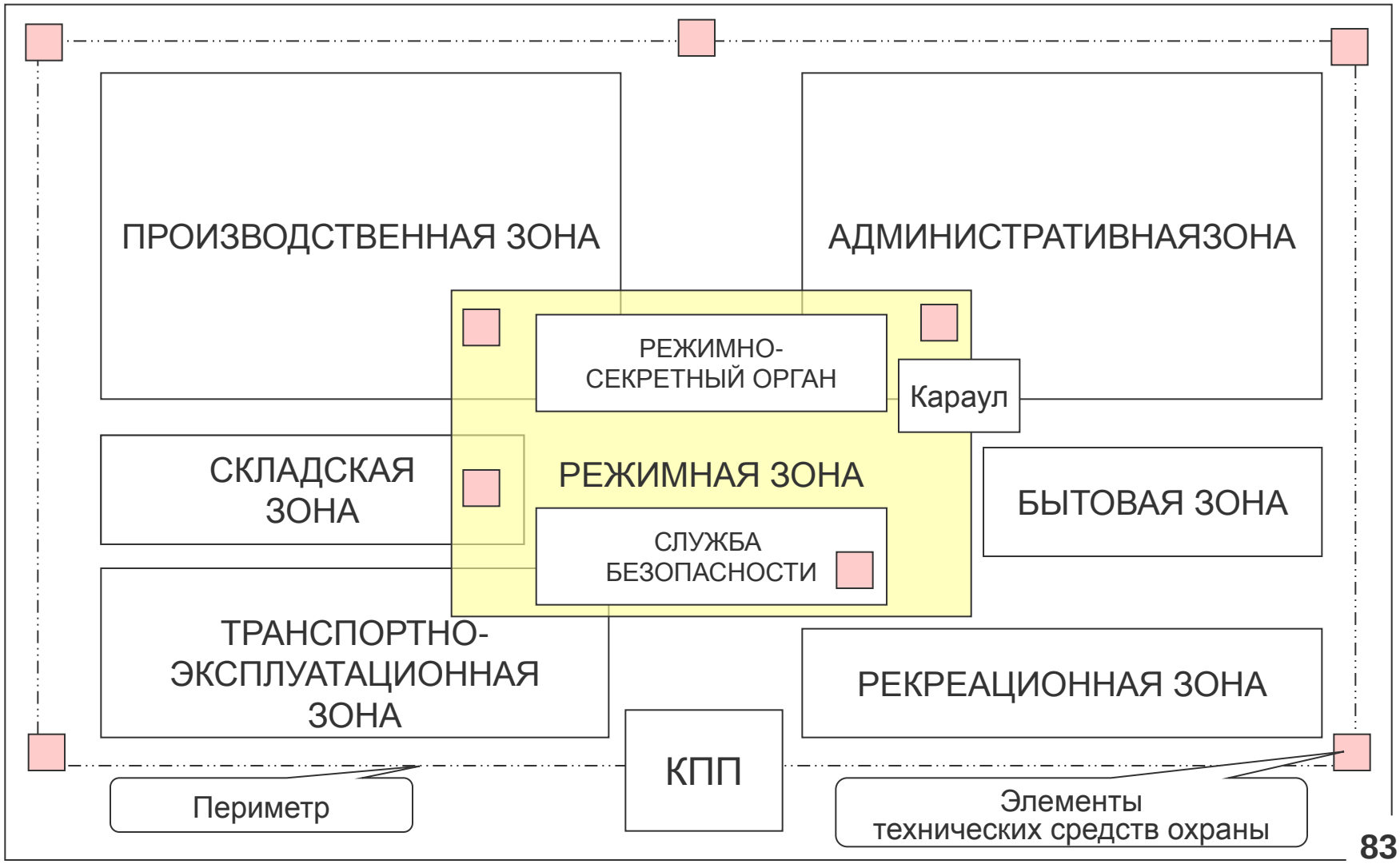
3) отделение объектов (здания, этажи, сектора, помещения, шкафы, двери и пр.);

4) распорядительный метод (инструкции, распоряжения);

5) визуальный метод (маскировка, ландшафт и пр.)

# 4.2.3. ФУНКЦИОНАЛЬНЫЕ ЗОНЫ И ИХ РАЗГРАНИЧЕНИЕ

- по производственной или бытовой функции;
- по классу оборудования для защиты информации;
- по степени ограничения доступа персонала;
- по функции системы защиты



## 4.2.4. СЕМИРУБЕЖНАЯ МОДЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ

**РУБЕЖ ЗАЩИТЫ – организованная совокупность всех средств, методов и мероприятий, используемых на соответствующем элементе для защиты информации в автоматизированных системах**

1) **территория**, занимаемая АСОД;

2) **здания**, расположенных на территории;

3) **помещения** внутри здания, в которых расположены ресурсы АСОД и защищаемая информация;

4) **ресурсы**, используемые для обработки и хранения информации, и самой защищаемой информации;

5) **линии связи**, проходящие в пределах одного и того же здания;

6) **линии (каналы) связи, проходящие между различными зданиями**, расположенными на одной и той же охраняемой территории;

7) **линии (каналы) связи, проходящие по неконтролируемой территории**

## 4.2.5. ТРЕБОВАНИЯ К ПОМЕЩЕНИЯМ, ПРЕДНАЗНАЧЕННЫМ ДЛЯ РАБОТЫ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ ИЛИ ХРАНЕНИЯ НОСИТЕЛЕЙ

**Исключение возможности бесконтрольного проникновения посторонних лиц и гарантирование сохранности носителей конфиденциальной информации обеспечиваются следующими мерами:**

входные двери оборудуются замками, гарантирующими надежное закрытие помещений в нерабочее время, в них также могут устанавливать-ся кодовые и электронные замки и автоматические турникеты;

оснащение охранной сигнализацией, связанной с караульным помеще-нием, пультом централизованного наблюдения за сигнализацией службы охраны и с дежурным;

оборудование в соответствии с требованиями по противодействию иностранным техническим разведкам и технической защите информации;

обследование комиссией, назначаемой руководителем предприятия перед началом эксплуатации, и аттестование на соответствие требованиям - не реже одного раза в 5 лет, а также перед началом эксплуатации, после их ремонта или реконструкции;

допуск строго ограниченного круга сотрудников, имеющих прямое отношение к ведущимся в них работам, а также руководителя предприятия, его заместителя, руководителя службы безопасности, руководителя режимно-секретного подразделения и их заместителей;

оборудование специальных окон, не выходящих в общий коридор, или выделение части рабочей комнаты с барьером

# 4.3. ПОНЯТИЕ И ОСНОВЫ ОРГАНИЗАЦИИ ПРОПУСКНОГО РЕЖИМА
## 4.3.1.СУЩНОСТЬ ПРОПУСКНОГО РЕЖИМА

**ПРОПУСКНОЙ РЕЖИМ – совокупность норм и правил, регламентирующих порядок входа на территорию предприятия и выхода лиц, въезда и выезда транспортных средств, вноса и выноса, ввоза и вывоза носителей сведений конфиденциального характера, а также мероприятий по реализации названных норм и правил с использованием имеющихся сил и средств.**

Сущность пропускного режима заключается в объединении усилий, а также сил и средств для достижения основной цели организации пропускного режима – обеспечения нормативных, организационных и материальных гарантий выявления, предупреждения и пресечения посягательств на законные права предприятия, его имущество, интеллектуальную собственность, производственную дисциплину и охраняемую информацию, исключения несанкционированного (бесконтрольного) пребывания на территории предприятия посторонних лиц и (или) транспорта.

**При организации пропускного режима используются основные понятия:**

- **посторонние лица или транспорт** – граждане или автомобильный и другой транспорт, не имеющие права посещения (даже разового) территории предприятия или пребывания на ней;
- **охраняемая территория** – территория предприятия, включающая его объекты и служебные помещения, на которой установлен и реализуется комплекс мероприятий пропускного и внутриобъектового режимов;
- **территория с особым режимом пропуска** – территория предприятия с расположенными на ней объектами и служебными помещениями, на которой устанавливаются дополнительные меры по обеспечению внутриобъектового и пропускного режимов;
- **пропуск** – оформленный в установленном порядке именной документ, подтверждающий право законного пребывания должностного лица или гражданина на территории предприятия, его объектах или в служебных помещениях

# 4.3.2. ЗАДАЧИ И ПРИНЦИПЫ ОРГАНИЗАЦИИ ПРОПУСКНОГО РЕЖИМА

**Основными задачами пропускного режима являются:**

- недопущение проникновения посторонних лиц на территорию (объекты) или в служебные помещения предприятия;
- исключение посещения служебных помещений предприятия без служебной необходимости сотрудниками предприятия и командированными лицами;
- предотвращение вноса (ввоза) на территорию предприятия личных технических средств (кино-, фото-, видео-, звукозаписывающей аппаратуры и др.);
- исключение несанкционированного выноса (вывоза) с территории предприятия носителей конфиденциальной информации;
- предотвращение хищения носителей конфиденциальной информации.

**Основные принципы организации пропускного режима:**

- централизация системы управления пропускным режимом;
- комплексный подход к использованию сил и средств для решения задач пропускного режима;
- максимальное использование элементов автоматизации;
- оперативное реагирование и принятие решений в чрезвычайных ситуациях

**ГАРАНТИИ ОБЕСПЕЧЕНИЯ ПРОПУСКНОГО РЕЖИМА:**

**НОРМАТИВНЫЕ** – заключаются в толковании и реализации норм права, уяснения пределов их действий, в формировании необходимых правоотношений; в определении и обеспечении правомерной деятельности подразделений и работников предприятия по поводу его безопасности использования ограничительных мер применением санкций к физическим и юридическим лицам, посягающим на законные интересы.

**ОРГАНИЗАЦИОННЫЕ** – формируются путем разработки, построения и поддержания высокой работоспособности организационной структуры управления процессом выявления и подавления угроз деятельности, использования эффективного механизма стимулирования функционирования предприятия и соответствующей подготовки кадров.

**МАТЕРИАЛЬНЫЕ** –за счет выделения и использования финансовых, технических, кадровых, интеллектуальных, информационных и иных ресурсов, обеспечивающих своевременное выявление, ослабление и подавление источников угроз, предотвращение и локализацию возможного ущерба и создание благоприятных возможностей и условий деятельности

## 4.3.3. ОСНОВНЫЕ ЭЛЕМЕНТЫ СИСТЕМЫ ОРГАНИЗАЦИИ ПРОПУСКНОГО РЕЖИМА

**Основными элементами системы организации пропускного режима являются:**

- **режимно-секретное подразделение;**
- **служба безопасности предприятия;**
- **бюро пропусков;**
- **контрольно-пропускные пункты.**

**Режимно-секретное подразделение и служба безопасности предприятия:**

**организуют выполнение комплекса мероприятий по обеспечении пропускного режима;**

**осуществляют постоянный контроль эффективности их реализации.**

**Основные задачи бюро пропусков:**

- **учет, хранение всех видов пропусков, печатей, штампов, в том числе используемых для проставления условных знаков (шифров);**
- **оформление, выдача, замена и уничтожение пропусков;**
- **обеспечение контрольно-пропускных пунктов образцами действующих пропусков;**
- **проведение проверок наличия бланков всех видов пропусков;**
- **контроль за работой контрольно-пропускных пунктов.**

В бюро пропусков находится список лиц, имеющих право подписи заявок на выдачу разовых пропусков, с образцами их подписей. Бюро пропусков оформляет постоянные и временные пропуска на основании заявок на их выдачу, подписанных должностными лицами, определенными распоряжением руководителя предприятия (его заместителя)

# 4.3.4. ИСХОДНЫЕ ДАННЫЕ ДЛЯ РАЗРАБОТКИ ПРОПУСКНОГО РЕЖИМА

1. Организационная структура, места расположения отдельных элементов и характер деятельности на них (объекты, площадки, здания, помещения, функции, персонал).
2. «Суточный объем» потоков транспортных средств, грузов, персонала и посетителей.
3. Территории по степени важности категорий объектов, транспортных средств и грузов, а также лиц, пересекающих установленные границы

| Категория зоны | Наименование зоны | Функциональное назначение | Условия доступа сотрудников | Условия доступа посетителей | Наличие охраны | Наличие технических средств охраны |
|---|---|---|---|---|---|---|
| 0 | Свободная | Места свободного посещения | Свободный | | Есть | Нет |
| 1 | Наблюдаемая | Комната приема посетителей | | | | Средства наблюдения |
| 2 | Регистрационная | Кабинеты сотрудников | Свободный | Свободный, с регистрацией, по документам, удостоверяющим личность | Усиленная охрана | Охранная сигнализация |
| 3 | Режимная | Секретариат, компьютерные залы, архивы | По служебным удостоверениям или идентификац. картам | По разовым пропускам | | Охранная сигнализация, система контроля доступа |
| 4 | Усиленной защиты | Кассовые операционные залы. Склады материальных ценностей | По специальным пропускам | | | Охранная сигнализация (2 рубежа), система контроля доступа, инженерные заграждения |
| 5 | Высшей защиты | Кабинеты высших руководителей, комнаты для ведения переговоров, спец. хранилища | | | | Охранная сигнализация (2 рубежа), система контроля доступа, технические СЗИ, инженерное усиление |

# 4.3.5. ЗАДАЧИ КОНТРОЛЬНО-ПРОПУСКНЫХ ПУНКТОВ

**ЗАДАЧИ КОНТРОЛЬНО-ПРОПУСКНЫХ ПУНКТОВ ВКЛЮЧАЮТ:**

- непосредственный контроль за входом граждан на территорию (объекты) предприятия и их выходом;
- учет транспорта, въезжающего на территорию предприятия и выезжающего с нее;
- контроль законности выноса (вывоза) с территории предприятия носителей конфиденциальной информации;
- контроль своевременности возврата посетителями предприятия разовых пропусков;
- оперативное реагирование в нештатных ситуациях, связанных с попытками проникновения посторонних лиц (транспорта) на территорию (объекты) предприятия;
- взаимодействие с караулом (подразделениями охраны) при решении задач обеспечения пропускного режима.

**НА КОНТРОЛЬНО-ПРОПУСКНОМ ПУНКТЕ ДОЛЖНЫ НАХОДИТЬСЯ:**

- выписка из инструкции по организации пропускного режима на предприятии;
- инструкции личному составу, несущему дежурство, в том числе по действиям в случае пожара, стихийного бедствия и в других чрезвычайных ситуациях;
- образцы действующих пропусков всех видов;
- списки должностных лиц, которым предоставлено право подписи всех видов пропусков, с образцами их подписей;
- номера телефонов для связи с оперативными службами (местных и городских автоматических телефонных станций).

# 4.3.6. ОБОРУДОВАНИЕ КПП

Оборудование КПП должно обеспечивать **необходимую пропускную способность и возможность тщательной проверки пропусков, документов у проходящих лиц, досмотра всех видов транспорта, провозимых грузов** и удовлетворять следующим требованиям:

- исключать возможность **несанкционированного проникновения через КПП**;
- **способствовать сокращению времени** на проверку документов, досмотр транспорта;
- способствовать **сведению к минимуму ошибок** при пропуске;
- обеспечивать **меры безопасности при досмотре** транспортных средств;

Все виды КПП должны быть оборудованы **необходимыми видами связи и тревожной сигнализации** для вызова резерва охраны.

А) **КПП для прохода людей** : комната для охраны, комната для досмотра, камера хранения, гардероб, проходы с техническими средствами охраны и физическими барьерами:

- средства механизации, автоматизации, системы контроля доступа, освещение;
- средства связи и тревожной сигнализации, системы видеоконтроля.
- электромеханические турникеты.

Б) **Автотранспортные КПП**: досмотровая площадка и служебные помещения.

Площадка должна:

- иметь достаточную площадь для размещения досматриваемого транспорта
- иметь **технические средства** для обеспечения нормальных условий работы;
- **исключать возможность проникновения на объект**;
- **обеспечивать досмотр** при установленной интенсивности движения;
- **быть изолированной** от других сооружений, не имеющих отношения к охране;
- обеспечивать **меры безопасности** при выполнении обязанностей.

На проезжей части площадки выделяется место остановки транспорта для досмотра. Автотранспортные КПП могут оборудоваться светофорами, весами для взвешивания автомобилей, досмотровой ямой или эстакадой для осмотра грузов, механизированными устройствами для автоматического открытия и закрытия ворот с фиксаторами.

## 4.3.7. ОСНОВЫ ОРГАНИЗАЦИИ ДЕЖУРСТВА

- **принятие решений, издание приказа и ввод инструкции;**
- **подбор и назначение персонала для несения дежурства;**
- **подготовка персонала: обучение и воспитание; вводный и текущий инструктаж, подготовка на рабочем месте;**
- **подготовка объектов для несения дежурства;**
- **контроль дежурства, режима и его совершенствование**

**На предприятии разрабатывается инструкция по организации пропускного режима, которая определяет:**

- **порядок организации и обеспечения пропускного режима,**
- **порядок и регламент работы бюро пропусков и контрольно-пропускных пунктов,**
- **обязанности должностных лиц и порядок их действий в различных ситуациях и другие вопросы.**

Инструкция утверждается руководителем предприятия и доводится до сведения каждого сотрудника предприятия в части его касающейся

# 4.3.8. ИНСТРУКЦИЯ О ПРОПУСКНОМ РЕЖИМЕ

**1. Общие положения:**

- нормативные документы, на основании которых составлялась инструкция;
- определение контрольно-пропускного режима и цель его установления;
- на кого возлагается руководство пропускным режимом, практическое его осуществление;
- санкции к нарушителям контрольно-пропускного режима;
- требования к оборудованию различных помещений.

**2. Порядок пропуска сотрудников предприятия, командированных лиц и посетителей**:

- перечислить все КПП и их назначение, описание, расположение и их единую нумерацию;
- изложить требования к оборудованию КПП;
- установить порядок прохода сотрудников и посетителей на территорию объекта и в категорированные подразделения;
- определить права и основные обязанности контролеров КПП;
- установить помещения, где запрещается принимать посетителей.

**3. Порядок допуска на объект транспорта и вывоза материальных ценностей:**

- порядок допуска на территорию автотранспорта, принадлежащего объекту;
- въезд и стоянка на территории объекта транспорта, принадлежащего сотрудникам;
- порядок пропуска автомашин сторонних организаций в рабочее и нерабочее время;
- порядок вывоза (ввоза) товарно-материальных ценностей;
- правила оформления документов на вывоз (вынос) материальных ценностей.

**4. Виды пропусков, порядок их оформления:**

- виды пропусков, их количество, статус и описание;
- порядок оформления, выдачи, общей замены и перерегистрации пропусков;
- мероприятия при утере пропуска сотрудником.

**5. Обязанности должностных лиц по поддержанию пропускного режима.**

**6. Учет и отчетность, порядок хранения пропусков, печатей.**

# 4.3.9. ВИДЫ ПРОПУСКОВ И ИХ ПРИМЕНЕНИЕ

**Основным средством обеспечения пропускного режима служат вводимые в установленном порядке и действующие в течение определенного срока пропуска на территорию и объекты предприятия**

**Используются следующие виды пропусков:**

- **постоянные** – выдаются штатному персоналу предприятия;
- **временные** – выдаются командированным на предприятие лицам – сотрудникам других организаций, а также вновь принятым на работу сотрудникам предприятия до оформления им постоянных пропусков;
- **разовые** – выдаются на одно посещение посетителям предприятия и действуют в течение рабочего дня;
- **материальные** – выдаются сотрудникам предприятия и предназначены для вноса (выноса), ввоза (вывоза) имущества (изделий) и др. предметов.

Право подписи всех видов пропусков устанавливается приказом руководителя предприятия.

**Должностным лицам, которым для выполнения их должностных обязанностей необходимо круглосуточное посещение всех объектов, выдаются соответствующие пропуска (проставляются отметки). Круг таких лиц строго ограничивается.**

Для ограничения входа на отдельные объекты (в помещения) на пропусках проставляются условные знаки (шифры). Распоряжением руководителя предприятия определяется перечень сотрудников, которым предоставляется право прохода через КПП с рабочими папками для переноски служебных документов. Наличие такого права удостоверяется проставлением в пропусках условных знаков.

**Изготовление бланков пропусков осуществляют организации, имеющие на это право. Образцы пропусков, условные знаки (шифры), период времени, в течение которого они действуют, должностные лица, которым предоставляется право подписи всех видов пропусков, утверждаются приказом руководителя предприятия.**

Въезд на территорию (выезд) транспортных средств осуществляется по пропускам, выдаваемым их водителям, или по спискам на КПП с фамилиями водителей, типами (марками) транспортных средств и их государственными регистрационными номерами.

# 4.3.10. ПРОПУСК НА ОБЪЕКТ ЛЮДЕЙ

❖ **Допуск** командированных (посетителей) производится по временным, разовым пропускам **в установленные и указанные в пропуске часы**, в исключительных случаях по утвержденным начальником службы безопасности спискам с предъявлением документов.

❖ **В нерабочее время, выходные и праздничные дни** допуск сотрудников на объект должен быть ограничен и производиться по предварительным заявкам (спискам) руководителей подразделений, завизированными начальником службы безопасности.

❖ **Дежурные специальных служб объекта** (электрики, сантехники, работники связи и т.д.), работающие посменно, допускаются на территорию объекта в нерабочее время, в выходные и праздничные дни по спискам, подписанным начальниками служб и утвержденными начальником службы безопасности.

❖ На основании действующего законодательства и решения администрации **отдельные категории лиц пользуются правом прохода на объект без пропуска**, при предъявлении служебного удостоверения. К ним относятся: работники прокуратуры; работники милиции по территориальности; инспектора труда, котлонадзора, Энергонадзора по территориальности; должностные лица и отдельные категории работников СЭС.

❖ В целях осуществления пропускного режима на территории объекта и в его структурных подразделениях приказом начальника предприятия утверждается **перечень категорированных подразделений (помещений), хранилищ**. В этих помещениях устанавливается специальный режим и повышенная ответственность за его соблюдение. Допуск осуществляется строго по списку, согласованному со службой безопасности.

❖ Во всех помещениях категорированных подразделений должны быть вывешены в застекленных рамках списки работников, имеющих допуск в эти помещения. Все помещения по окончании работ **осматриваются дежурными и лицами, ответственными за их противопожарное состояние**. Электроосветительная и электронагревательная аппаратура обесточивается, окна и форточки закрываются, двери запираются на замок и опечатываются ответственными лицами и сдаются под охрану караула.

❖ **Получение ключей, вскрытие помещений**, оборудованных охранной сигнализацией, производят лица, имеющие допуск на право вскрытия этих помещений с предъявлением постоянного пропуска. Списки лиц, имеющих право вскрывать (закрывать) указанные помещения с указанием номеров печатей, которыми опечатываются помещения и номеров служебных телефонов, подписываются начальником подразделения и утверждаются начальником службы безопасности

# 4.3.11. ПРОПУСК НА ОБЪЕКТ ТРАНСПОРТНЫХ СРЕДСТВ

- Допуск на территорию (с территории) предприятия транспортных средств, принадлежащих предприятию, производится при предъявлении водителем **личного пропуска со специальным шифром или транспортного пропуска и путевого листа**. Грузчики и сопровождающие лица, следующие с транспортом, пропускаются через КПП на общих основаниях.
- Все транспортные средства при проезде через КПП **подвергаются досмотру**. Въезд и стоянка на территории предприятия транспорта, принадлежащего сотрудникам на правах личной собственности разрешается по специальным спискам.
- **Автомашины сторонних организаций**, прибывшие с грузом в адрес предприятия в рабочее время, допускаются на территорию **по служебным запискам с досмотром на автотранспортном КПП**. Загон машин на территорию производится штатным водителем с представителем администрации.
- **Железнодорожный транспорт и обслуживающие его бригады** пропускаются на предприятие по пропускам установленного образца, по спискам или иным порядком установленным инструкцией о пропускном режиме. Для пропуска и досмотра железно-дорожного транспорта от подразделения охраны выделяется **досмотровая группа**. Опломбированные вагоны и контейнеры, пропускаются через КПП после их внешнего досмотра, если оттиски пломб соответствуют оттискам в препроводительных документах или накладных.
- **Вывоз и вынос** материальных ценностей с территории объекта осуществляется по материальным пропускам установленного образца. Убедившись в правильности оформления документов и их полном соответствии с вывозимыми ценностями, охранник **оставляет на КПП пропуск, ставит на пропуске дату и время вывоза груза, расписывается и дает разрешение** на вывоз материальных ценностей.
- Все документы на вывозимые (выносимые) с предприятия материальные ценности **регистрируются в бюро пропусков по книге учета и течение следующего дня передаются в бухгалтерию**. Бланки всех видов материальных пропусков хранятся в бухгалтерии, выдаются в подразделения предприятия по служебным запискам. Документы на вывоз (вынос) материальных ценностей должны быть выписаны только на то количество груза (мест, веса и т.п.), которое может быть вывезено (вынесено) одновременно и действительны только на дату, указанную в разрешительном документе.
- **Контроль за транспортными средствами**: работник охраны, убедившись в правильности оформления сопроводительных документов должен удостовериться в соответствии наименования и количества ввозимого (вывозимого) груза данным, а также проверить скрытые места транспортного средства (которые могут использоваться для хищения). Материальные ценности на транспортном средстве должны быть уложены в порядке, удобном для контроля. При пропуске опломбированных грузов охранник сверяет пломбы (печати) с указанными в накладных, после чего разрешается въезд (выезд) транспорта. Материальные пропуска, товаротранспортные накладные регистрируются в книге учета в строгом соответствии с порядком их поступления.

# 4.4. ОХРАНА ТЕРРИТОРИИ ПРЕДПРИЯТИЯ И ФУНКЦИОНАЛЬНЫХ ЗОН ОТ ПРОНИКНОВЕНИЯ НАРУШИТЕЛЕЙ

## 4.4.1. КЛАССИФИКАЦИЯ ОБЪЕКТОВ ОХРАНЫ

**В соответствии со ст. 1.1. Закона РФ от 11.03.1992 г. № 2487-I «О частной детективной и охранной деятельности в РФ» :**

**1. По состоянию объекта:** недвижимые вещи (здания, строения, сооружения), движимые вещи (транспортные средства, грузы, денежные средства, ценные бумаги), в том числе при их транспортировке.

**2. По размеру объекта, площади его территории:**

а) малые объекты (до 100 кв. м) - квартиры, малые офисы, торговые палатки и т.д.;

б) средние объекты (100-500 кв. м) - крупногабаритные квартиры, частные дома с надворными постройками и участком, отдельно стоящие или примыкающие к другим зданиям офисы со складами и производственными помещениями, автостоянки до 50-60 автомашин и т.д.;

в) большие стационарные объекты (0,5-4 тыс. кв. м) - средние предприятия до 300-400 человек, базы хранения продукции, крупные автомобильные стоянки, склады и т.д.;

г) очень большие стационарные объекты (более 4 тыс. кв. м) - крупные промышленные (акционированные) предприятия, фермерские хозяйства, крупные базы.

**3. По режиму работы персонала:** а) в одну смену; б) в 2-сменном режиме; в) круглосуточно.

**4. По району расположения охраняемого объекта:**

а) вне основной промышленной, производственной или охраняемой зоны;

б) в отдельно стоящих зданиях или занимающие часть др. помещения или территории: в производственной зоне; на охраняемой или вблизи от охраняемой территории; рядом с криминогенными объектами (рынки, вокзалы и др.).

**5. По технической укрепленности:**

а) очень хорошо укрепленные, практически не имеющие уязвимых мест;

б) хорошо укрепленные, имеющие незначительное число уязвимых мест, которые известны охране и контролируются ее сотрудниками;

в) слабо укрепленные, имеющие значительное число уязвимых мест, многие из которых охрана не контролирует.

**6. По типу охраны:** с простым (невооруженная охрана); с усложненным (охрана вооружена спецсредствами); с комбинированным (вооруженная охрана с собаками).

**7. По значимости и концентрации материальных, художественных, исторических, культурных и культовых ценностей на объекте, последствий от возможных преступных посягательств на них**

# 4.4.2. КЛАССИФИКАЦИЯ ОБЪЕКТОВ ОХРАНЫ ПО ЗНАЧИМОСТИ И КОНЦЕНТРАЦИИ МАТЕРИАЛЬНЫХ, ХУДОЖЕСТВЕННЫХ И ДРУГИХ ЦЕННОСТЕЙ

**АI и АII – объекты особо важные, повышенной опасности и жизнеобеспечения, противоправные действия на которых могут привести к крупному, особо крупному экономическому или социальному ущербу государству, обществу, предприятию и т.п.**

**БI и БII – объекты, хищения на которых, в соответствии с законодательством, могут привести к ущербу в размере до 500 МРОТ и свыше 500 МРОТ**

**ОБЪЕКТЫ ПОДГРУППЫ АI:**

- объекты особо важные, повышенной опасности и жизнеобеспечения, включенные в Перечень объектов, подлежащих государственной охране, согласно пост. Пр. РФ от 14.08.1992 г. № 587;
- объекты, включенные органами власти субъектов РФ или местного самоуправления в перечни объектов особо важных, повышенной опасности и жизнеобеспечения;
- объекты по производству, хранению и реализации радиоактивных, наркотических веществ, сильнодействующих ядов и химикатов, биологических, токсических и психотропных веществ;
- ювелирные магазины, базы, склады и объекты, использующие ювелирные изделия;
- помещения для хранения радиоизотопных веществ, предметов старины, искусства и культуры;
- объекты кредитно-финансовой системы (банки, пункты обмена валюты, банкоматы и пр.);
- кассы предприятий, организаций, учреждений, головные кассы торговых предприятий;
- сейфовые комнаты для хранения денег, ювелирных изделий, драгоценных металлов и камней.

**ОБЪЕКТЫ ПОДГРУППЫ АII (специальные помещения объектов АI):**

- хранилища и кладовые денег, ценных бумаг, ювелирных изделий, драгметаллов и камней;
- хранилища секретной документации;
- специальные хранилища взрывчатых, радиоактивных, наркотических, химических, бактериологических, токсичных и психотропных веществ и препаратов;
- специальные фондохранилища музеев и библиотек.

**ОБЪЕКТЫ ПОДГРУППЫ БI:**

- объекты хранения или размещения изделий технологического, санитарно-гигиенического и хозяйственного назначения, нормативно-технической документации, инвентаря и т.п.;
- объекты мелкооптовой и розничной торговли.

**ОБЪЕКТЫ ПОДГРУППЫ БII:**

- объекты хранения товаров, предметов повседневного спроса, продуктов питания, компьютерного оборудования, оргтехники, видео- и аудиотехники, кино- и фотоаппаратуры, натуральных и искусственных мехов, кожи, автомобилей и запасных частей к ним, алкогольной продукции с содержанием этилового спирта св. 13%.

# 4.4.3. ОХРАНА ОБЪЕКТОВ

**ПОД ОХРАНОЙ ОБЪЕКТА ПОДРАЗУМЕВАЕТСЯ комплекс мер, направленных на своевременное выявление угроз и предотвращение нападения на охраняемые объекты, совершения террористического акта, других противоправных посягательств в т.ч. экстремистского характера, а также возникновения чрезвычайных ситуаций**

**СИСТЕМА ОХРАНЫ ОБЪЕКТА – совокупность способов, сил и средств для выполнения задач по охране и обороне объекта.**

**Она должна соответствовать:**

технологическим особенностям охраняемого объекта,
уровню его оборудования инженерно-техническими средствами охраны,
обеспечивать эффективное и рациональное использование сил и средств,
строиться эшелонированно: на подступах к объекту, по его периметру и на КПП.

**ВИДЫ, СИСТЕМА И ПОРЯДОК ОХРАНЫ ОБЪЕКТОВ РЕГУЛИРУЮТСЯ :**

- № 116-ФЗ "О промышленной безопасности опасных производственных объектов» 21.07.97г.
- № 77-ФЗ "О ведомственной охране" от 14.04.99г.,
- № 2487-1 "О частной детективной и охранной деятельности в РФ" от 11.03.92г.,
- Пост. Пр. РФ от 14.08.1992 г. № 587 "Вопросы частной детективной и охранной деятельности",
- Рук. документом МВД РФ РД 78.36.003-2002 "Инженерно-техническая укрепленность. Технические средства охраны. Требования и нормы проектирования по защите объектов от преступных посягательств",
- ведомственными нормативными актами,
- условиями договора на охрану объекта.

## 4.4.4. РЕЖИМ ОХРАНЫ

**РЕЖИМ ОХРАНЫ ОБЪЕКТА – сочетание действий службы охраны, инженерно-технических средств и режимных мероприятий, направленных на обеспечение полной или частичной сохранности:**

- **материальных ценностей,**
- **персонала,**
- **интеллектуальной собственности,**
- **ценной информации о деятельности этого объекта**

**ОСНОВНЫЕ ЗАДАЧИ РЕЖИМА ОХРАНЫ:**

- защита охраняемых объектов, предупреждение и пресечение противоправных посягательств и административных правонарушений на объектах;
- обеспечение сохранности зданий и помещений, сохранности и контроля за перемещением материальных ценностей;
- обеспечение внутриобъектового и пропускного режима;
- обеспечение безопасности сотрудников и руководства фирмы;
- участие в локализации и ликвидации возникших ЧС, в т.чю. вследствие диверсионно-террористических акций, поддержание противопожарной безопасности (если этими вопросами не занимаются специальные службы).

**ВИДЫ РЕЖИМА ОХРАНЫ:**

**простой и усиленный, открытый и закрытый**

# 4.4.5. ТРЕБОВАНИЯ К СИСТЕМЕ ОХРАННЫХ МЕР

## СИСТЕМА ОХРАННЫХ МЕР ДОЛЖНА ПРЕДУСМАТРИВАТЬ:

- многорубежность построения охраны по нарастающей к наиболее ценному элементу;
- комплексное применение современных ТСО, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное документирование;
- надежное инженерно-техническое перекрытие вероятных путей вторжения;
- устойчивую (дублированную) систему связи и управления всех структур охраны;
- высокую подготовку и готовность основных и резервных сил охраны к оперативному противодействию преступным действиям;
- самоохрану персонала.

## СИСТЕМА РЕГУЛИРОВАНИЯ ДОСТУПА ДОЛЖНА ПРЕДУСМАТРИВАТЬ:

- объективное определение "надежности" лиц, допускаемых к работе;
- максимальное ограничение количества лиц, допускаемых на объекты;
- установление дифференцированного по времени, месту и деятельности права доступа;
- четкое определение порядка выдачи разрешений и оформления документов для входа;
- определение объемов контрольно-пропускных функций на каждом КПП;
- оборудование КПП ТС, обеспечивающими достоверный контроль проходящих, объективную регистрацию прохода и предотвращение проникновения (в т.ч. силового) посторонних лиц;
- высокую подготовленность и защищенность персонала КПП

## СИСТЕМА МЕР СОХРАННОСТИ ЦЕННОСТЕЙ И КОНТРОЛЯ :

- строго контролируемый доступ лиц в режимные зоны;
- максимальное ограничение посещений режимных зон лицами, не участвующими в работе;
- максимальное сокращение количества лиц, обладающих досмотровым иммунитетом;
- организацию и осуществление присутственного (явочного) и дистанционного - по техническим каналам (скрытого) контроля за соблюдением режима безопасности;
- организацию контроля любых предметов, перемещаемых за пределы режимных зон;
- обеспечение защищенного хранения документов и финансовых средств;
- соблюдение персональной и коллективной материальной и финансовой ответственности в процессе открытого обращения финансовых ресурсов и материальных ценностей;
- организацию тщательного контроля на каналах возможной утечки информации;
- оперативное выявление причин тревожных ситуаций в режимных зонах, пресечение их развития или ликвидацию во взаимодействии с силами охраны

# 4.4.6. ПРИНЦИПЫ РЕЖИМА И СПОСОБЫ ОХРАНЫ

## ПРИНЦИПЫ РЕЖИМА ОХРАНЫ:

- активность и предупредительный характер (заключается в опережающем выявлении признаков готовящейся криминальной акции);
- целесообразность организации режима охраны объекта, своевременность его усиления, рациональное использование сил и средств охраны;
- разумное сочетание возможностей охранного предприятия и сил правоохранитель-ных органов для обеспечения безопасности объектов;
- осуществление охраны объектов по единому плану и под общим руководством руководителя предприятия;
- неброскость или демонстративность охраны, в зависимости от ситуации;
- максимальная информированность сотрудников охраны о возможных инцидентах на охраняемых объектах и тех обстоятельствах, которые имеют непосредственное отношение к их функциональным обязанностям

## СИЛЫ ОХРАНЫ :

- милицейские, военизированные (ВОХР) и сторожевые подразделения вне- или ведомственной охраны;
- частные охранные предприятия (ЧОП)

## СПОСОБЫ ОХРАНЫ:

1. Охрана с помощью технических средств защиты с подключением на пульт централизованного наблюдения либо с установкой автономной сигнализации.
2. С использованием стационарных и обходных постов.
3. С использованием служебных собак.
4. Комбинированная охрана (сочетание всех видов охраны).

## 4.4.7. ФАКТОРЫ, ВЛИЯЮЩИЕ НА ВЫБОР СПОСОБОВ ОХРАНЫ

- принципы охраны;
- размер охраняемого объекта, режим и характер работы объекта, его технологические характеристики, имеющиеся ценности;
- режим охраны, используемый на объекте;
- количественные и качественные характеристики сил охраны, вооруженность и техническая оснащенность, наличие автотранспорта, средств связи, спец. средств.
- характеристика технической укрепленности охраняемого объекта;
- возможные способы преступных посягательств на объект;
- наличие (отсутствие) средств охранной и пожарной сигнализации;
- условия местности

**ЭФФЕКТИВНЫМ КОМПЛЕКСОМ МЕР ОХРАНЫ ОБЪЕКТА ЯВЛЯЕТСЯ:**

1. Создание на пути нарушителя физических препятствий с использованием ТСО с целью предупреждения проникновения на объект.
2. Раннее обнаружение злоумышленника (на дальних подступах к цели его движения) с использованием технических средств охраны.
3. Оценка ситуации.
4. Принятие немедленных мер по пресечению действий злоумышленника с использованием специальных средств или огнестрельного оружия.
5. Видеодокументирование обстановки.
6. Передача сигналов тревоги или сообщений о происшествии

## 4.4.8. ВИДЫ НАРЯДОВ ОХРАНЫ

**1. СТАЦИОНАРНЫЕ ПОСТЫ – НА КПП, А ТАКЖЕ НА ВХОДЕ В ЗДАНИЯ И ПОМЕЩЕНИЯ С ОГРАНИЧЕННЫМ ДОСТУПОМ.**

Допускается выставление одиночного поста на совмещенном КПП в нерабочее время, а также на объектах с незначительным количеством персонала и транспорта.

При наличии на объекте нескольких стационарных постов, один из них определяется как центральный. При невозможности совмещения функций пропускного режима и контроля на центральном посту техническими средствами выставляется парный стационарный пост, при этом все технические средства размещаются в отдельном помещении КПП или другом помещении (пост технического наблюдения).

**2. ОБХОДНЫЕ ПОСТЫ – ДЛЯ ОХРАНЫ НАИБОЛЕЕ УЯЗВИМЫХ УЧАСТКОВ ОГРАЖДЕНИЯ, ОТДЕЛЬНЫХ ЗДАНИЙ И ПОМЕЩЕНИЙ ОСОБОЙ ВАЖНОСТИ И ПОВЫШЕННОЙ ОПАСНОСТИ, КОНТРОЛЯ НАД СОБЛЮДЕНИЕМ ВНУТРИОБЪЕКТО-ВОГО РЕЖИМА.**

В целях повышения уровня защиты могут применяться служебные собаки. На участках со значительной протяженностью – мото- или автопатрули.

**3. ГРУППА БЫСТРОГО РЕАГИРОВАНИЯ – ГРУППА НА АВТОМОБИЛЕ, ОСУЩЕСТВЛЯЮЩАЯ ОПЕРАТИВНОЕ РЕАГИРОВАНИЕ НА СИГНАЛЫ ТРЕВОГИ ИЗ ОХРАНЯЕМЫХ ОБЪЕКТОВ**

**4. ГРУППА СОПРОВОЖДЕНИЯ ГРУЗОВ – ГРУППА НА АВТОМОБИЛЕ, НАРЯЖЕННАЯ ДЛЯ ОХРАНЫ И СОПРОВОЖДЕНИЯ ЦЕННЫХ ГРУЗОВ**

## 4.4.9. ОРГАНИЗАЦИЯ ОХРАНЫ

**ОРГАНИЗАЦИЯ ОХРАНЫ ВКЛЮЧАЕТ:**

- подбор личного состава на службу;
- общую специальную подготовку сотрудников;
- расстановку личного состава по охраняемым объектам;
- инструктаж и постановку конкретных задач личному составу непосредственно перед заступлением на службу;
- контроль за несением службы (суточным) нарядом, подведение итогов несения службы.

**РАСПРЕДЕЛЕНИЕ ЛИЧНОГО СОСТАВА ПО ОХРАНЯЕМЫМ ОБЪЕКТАМ ПРОВОДИТСЯ С УЧЕТОМ:**

- важности и особенностей охраняемого объекта;
- индивидуальных особенностей сотрудников охраны с учетом их образовательного, интеллектуального и возрастного цензов;
- физической подготовленности и огневой выучки, умения владеть специальными средствами самообороны;
- умения пользоваться инженерно-техническими средствами и средствами связи, имеющимися на охраняемых объектах

# 4.4.10. СРЕДСТВА СИГНАЛИЗАЦИИ В ОХРАНЕ СТАЦИОНАРНЫХ ОБЪЕКТОВ

## В ЗАВИСИМОСТИ ОТ ВИДА, СИГНАЛИЗАЦИИ ПОДРАЗДЕЛЯЮТСЯ НА:

- **технические средства охранной сигнализации;**
- **технические средства пожарной сигнализации;**
- **технические средства тревожной сигнализации.**

### ОХРАННО-ПОЖАРНАЯ СИГНАЛИЗАЦИЯ

предназначена для выдачи сигналов тревоги в охраняемое (нерабочее) время при попытках проникновения или возникновения пожаров на охраняемых объектах**.**

### ТРЕВОЖНАЯ СИГНАЛИЗАЦИЯ

предназначена для подачи сигналов тревоги при разбойных нападениях на сберегательные банки и на другие объекты и включается в действие персоналом путём воздействия на скрытно установленные датчики (кнопки, педали).

### АВТОНОМНАЯ

**- для выдачи местных звуковых и световых сигналов тревоги у доверенных лиц, в помещениях общественных организаций и учреждений.**

### ЦЕНТРАЛИЗОВАННАЯ

**- для выдачи сигналов тревоги на приборы, установленные на КПП, дежурных частей милиции или пунктов централизованной охраны**

## В СОСТАВ СИСТЕМЫ ОХРАННОЙ СИГНАЛИЗАЦИИ ВХОДЯТ:

- **средства обнаружения – датчики;**
- **средства передачи информации – каналы связи;**
- **средства приема и обработки информации;**
- **источники световых и звуковых сигналов.**

# 4.4.11. ДАТЧИКИ СИСТЕМ ОХРАННОЙ СИГНАЛИЗАЦИИ

**НАТЯЖНЫЕ** – несколько рядов стальной проволоки по периметру охраняемого объекта между вертикальными колоннами (стыковыми, промежуточными и сигнальными). В сигнальных колоннах установлены микровыключатели, которые срабатыва-ют как при обрыве, так и при натяжении проволоки в момент раздвигания её рядов при попытке нарушителя проникнуть на объект.

**МАГНИТОУПРАВЛЯЕМЫЕ** – для блокировки окон, форточек, дверей, люков и состоят из магнитоуправляемого контакта - геркона.

**ВИБРАЦИОННЫЕ** (контактные и бесконтактные) - для блокирования стеклянных и других легкоразрушаемых поверхностей (пластик, фанера и т.п.).

**ТЕПЛОВЫЕ** – основаны на их способности фиксировать повышение температуры в помещениях выше определённой величины.

**ЕМКОСТНЫЕ** – для блокирования мест возможного проникновения на объект (оконный, дверной проёмы), отдельных предметов (сейф, металлический шкаф, ящик), а также для охраны объектов по периметру. Принцип действия основан на регистрации изменения ёмкости антенны, вызванного приближением к ней какого-либо предмета, человека. В качестве антенны используется обычный провод, металлический корпус сейфа, шкафа, другие металлические предметы.

**УЛЬТРАЗВУКОВЫЕ** – для блокирования помещений по объёму; выдают сигнал тревоги как при появлении нарушителя, так и при возникновении пожара. Принцип их действия основан на регистрации изменения ультразвукового поля.

**ОПТИКО-ЭЛЕКТРОННЫЕ** (инфракрасные, активные и пассивные): активные – для блокирования помещений (контроль подступов через витрины, оконные, дверные проёмы; блокировка в помещении подходов к охраняемым участкам по перимет-ру, припотолочных пространств слабо укреплённых складских помещений и т.п.) и для охраны территории по периметру; пассивные – позволяют обнаруживать проник-новение человека в контролируемую зону путём регистрации изменения интенсив-ности принимаемого инфракрасного излучения от движущегося объекта, а также возникновения пожара.

**МИКРОВОЛНОВЫЕ** (частотные и амплитудные): обнаруживают проникновение человека в контролируемую зону путём регистрации допплеровского сигнала или регистрируют изменения напряженности поля на входе приёмника

## 4.4.12. СРЕДСТВА ПРИЁМА, ОБРАБОТКИ И ВОСПРОИЗВЕДЕНИЯ ИНФОРМАЦИИ СИСТЕМ ОХРАННОЙ СИГНАЛИЗАЦИИ

**ОДНОЛИНЕЙНЫЕ ПРИЁМО-КОНТРОЛЬНЫЕ ПРИБОРЫ**

**Для охраны объекта, все датчики на котором включены в один шлейф блокировки**

**МНОГОЛИНЕЙНЫЕ ПРИЁМНО-КОНТРОЛЬНЫЕ УСТРОЙСТВА**

**При наличии на объекте нескольких обособленных помещений и нескольких шлейфов блокировки (до 30-60) (Приёмно-контрольный прибор «Буг»)**

***Для приёма тревожных сообщений либо от объектовых однолинейных приёмо-контрольных приборов, либо непосредственно от датчиков, а также для включения местной световой и звуковой сигнализации и передачи сигнала тревоги на пульт централизованной охраны***

**АППАРАТУРА ЦЕНТРАЛИЗОВАННОГО НАБЛЮДЕНИЯ**

***Для централизованного приёма, обработки и воспроизведения информации с большого числа объектов охраны***

## 4.4.13. КОМБИНИРОВАННЫЕ СРЕДСТВА ОБНАРУЖЕНИЯ

**«МУРЕНА-К-02».**

Предназначено для блокирования периметров и объектов.

Используется в различных комбинациях с радиоволновыми двухпозиционными радиоволновыми линейными извещателями «Радон», «Радий» и др.

Один блок вибрационного извещателя применяется для участков периметра до 500 м, от - 40 до + 50°С, 10...30 В, 0,5 А.

Четыре входа для подключения вибрационных чувствительных элементов или шлейфов радиоволновых извещателей

**Технические характеристики.**

| | |
|---|---|
| Ширина зоны обнаружения, м | - до 1. |
| Длина зоны обнаружения (ЗО), м | - до 4000 |
| Номинальное напряжение, В | - 9-36 |
| Потребляемый ток при напряжении 12 В, мА | - не более 160 |
| Время технической готовности, с | - 60 |
| Длительность извещения о тревоге, с | - 2-4 |
| Габаритные размеры (БОС), мм | - 225х128х75 |
| Масса блока обработки (БОС), кг | - не более 0,4 |
| Средний срок эксплуатации, лет | - 8 |
| Гарантийный срок эксплуатации, мес. | - 12 |

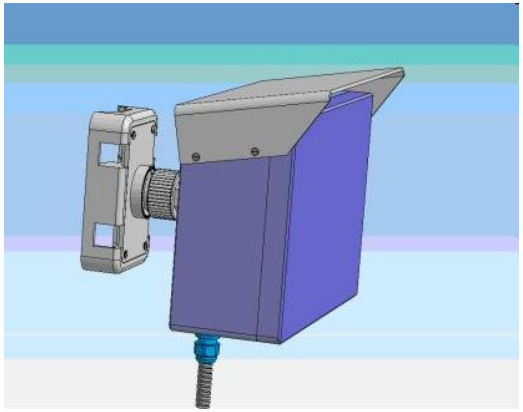
# 4.4.14а. ДВУХПОЗИЦИОННЫЕ РАДИОВОЛНОВЫЕ ИЗВЕЩАТЕЛИ

**РАДИЙ-7 РЭ**

Предназначен для охраны протяжённых периметров объектов со сложной помеховой обстановкой для городских условий эксплуатации

Обладает устойчивостью к движению групп пешеходов и автотранспорта параллельно границе ЗО за ее пределами и может использоваться в городских условиях эксплуатации.

Длина зоны обнаружения (ЗО), м - 20-300
Высота ЗО, м - не менее 1,8
Ширина зоны отчуждения, м - не более 3



**РЭ РМ-24-800**

Предназначен для установки на промышленных, транспортных и военных объектах вдоль заграждений и стен, а также по верху заграждений

Длина зоны обнаружения (ЗО), м - 20-800
Высота ЗО (при максимальной дальности), м - 1,8
Диапазон обнаруживаемых скоростей, м/с - 0,1-10,0.

# 4.4.14б. ДВУХПОЗИЦИОННЫЕ РАДИОВОЛНОВЫЕ ИЗВЕЩАТЕЛИ

## РЭ РМ-24-200

- Предназначен для установки по верху ограждений, вдоль ограждений и обеспечивает обнаружение нарушителя, пересекающего зону обнаружения (ЗО).

**ОСОБЕННОСТИ:**

ЭМС с другими извещателями.

Нечувствительность к движению одиночных мелких животных и птиц.

Отсутствие взаимного влияния между соседними извещателями (2 частотные литеры).

Автоматический и дистанционный контроль.

Повышенная устойчивость к электромагнитным помехам

## Радиоволновый двухпозиционный линейный извещатель "РАДОН-П"

Предназначен для работы в составе комплекса охраны периметра, построенного на базе контроллера "МУРЕНА-К". Включение извещателя в состав комплекса позволяет организовать второй рубеж охраны радиолучевым методом обнаружения нарушителя.

Питание осуществляется по двухпроводной линии от блока "Мурена-К".

Сигнал тревоги передается по линии питания.

ЭМС между соседними извещателями (4 литеры).

Автоматическая установка параметров.

## 4.4.15. СИСТЕМЫ IP-ВИДЕОНАБЛЮДЕНИЯ


**Уличный узел видеонаблюдения TFortis PSW-1**

Обеспечивает вынос четырёх IP-видеокамер по оптическому волокну до 20 км. и позволяет организовать работу системы при экстремально низких температурах за счет использования:

- схемы обогрева блока PSW-1;
- схемы обогрева термокожуха;
- режима сохранения тепла.

PSW-1 обеспечивает дополнительно предпусковой обогрев видеокамер

# 4.5. ОХРАНА КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ И ИМУЩЕСТВА ПРИ ТРАНСПОРТИРОВКЕ

## 4.5.1. БАЗОВЫЕ ПОНЯТИЯ

**ВИДЫ ОХРАНЫ ИМУЩЕСТВА :**

- техническая;
- физическая;
- охрана имущества по договорам при его транспортировке автомобильным, железнодорожным, водным или воздушным транспортом по территории РФ;
- смешаная (техническая и физическая).

**ТЕХНИЧЕСКАЯ ОХРАНА** по договорам организуется путем оборудования имущества ТСО, подключенными к пультам централизованного наблюдения пунктов централизованной охраны.

**ФИЗИЧЕСКАЯ ОХРАНА** имущества физических и юридических лиц по договорам в зависимости от характеристики охраняемого имущества, местности и других особенностей осуществляется путем выставления стационарных постов и (или) нарядов, групп задержания на маршрутах.

**ОХРАНА ИМУЩЕСТВА ПО ДОГОВОРАМ** при его транспортировке автомобильным, железнодорожным, водным или воздушным транспортом по территории Российской Федерации, а также других государств в соответствии с международными соглашениями, организуется путем выставления подвижных нарядов милиции, подразделений вневедомственной охраны численностью не менее двух сотрудников.

## 4.5.2. ПРИНЦИПЫ ОХРАНЫ ПРИ ТРАНСПОРТИРОВКЕ

1. Сопровождение грузов **осуществляется группами вооруженных сотрудников**, имеющими специальные средства защиты и связи. При необходимости группы укомплектовываются автомобилями повышенной проходимости. Сотрудники охраны проходят специальную подготовку и должны иметь опыт сопровождения грузов всеми видами транспорта.

2. Все сотрудники охраны обязаны иметь **разрешение на работу с огнестрельным оружием**, должны быть обеспечены мобильной радиосвязью, современными средствами защиты.

3. Лицами ответственными за документы должны быть приняты соответствующие **меры по их сохранности**, то есть защиту от внешних воздействий окружающей среды, таких, как влажность и возможные механические повреждения. С этой целью перевозка документов на бумажном носителе выполняется в специальных контейнерах, исключающих кроме того несанкционированный доступ к данным.

4. Транспортные и упаковочные средства для перемещения и перевозки документов **должны быть чистыми**.

5. **Транспортировка документов на электронных носителях требует особых мер защиты и сохранения информации**. Кроме защиты от механических повреждений должны быть приняты меры, исключающие потерю информации от воздействия магнитных полей или рентгеновского облучения. При прохождении через терминал сканирования в аэропортах, в процессе предпосадочного досмотра, необходимо передать электронные носители для спецдосмотра, при котором будут соблюдены условия сохранения данных.

6. При перемещении документов в пределах здания необходимо предусматривать наиболее рациональные пути и средства транспортирования, **исключая многократное перекладывание документов**

# 4.5.3. ОХРАНА ИМУЩЕСТВА ПРИ ЕГО ТРАНСПОРТИРОВКЕ НА АВТОМАШИНАХ

Охрана денежных средств при их транспортировке осуществляется на автомобилях, **специально предназначенных** для этих целей. При перевозке материальных ценностей автомашина должна быть в технически исправном состоянии, заправлена достаточным количеством топлива, укомплектована огнетушителем, буксировочным тросом, запасным колесом, аптечкой, знаком аварийной остановки и другими необходимыми предметами. Перевозимый груз должен быть надежно закреплен.

При поломке автомобиля в пути следования **перегрузка груза производится с разрешения и в присутствии представителя собственника**, сопровождающего груз, специально вызванными для этих целей грузчиками и только в исключительных случаях силами наряда, при этом принимаются меры к усилению охраны места происшествия.

При дорожно-транспортном происшествии, в результате которого целостность упаковки груза оказалась нарушенной, нарядом совместно с представителем собственника **принимаются меры к его сбору, складированию в безопасное место и усилению его охраны**. Обо всех происшествиях с грузом составляется акт.

Во время движения и остановки автомобиля с грузом, личный состав наряда несет службу **в автомобиле**, **либо по указанию старшего наряда – около автомобиля**, ведя наблюдение за подходами к нему со всех сторон

## 4.5.4. ОХРАНА ИМУЩЕСТВА ПРИ ЕГО ТРАНСПОРТИРОВКЕ ЖЕЛЕЗНОДОРОЖНЫМ И ВОЗДУШНЫМ ТРАНСПОРТОМ

### А. В купе пассажирского поезда:

при перемещении груза до вагона **старший наряда следует за представителем, а один из состава наряда – впереди представителя** собственника, несущего груз;

по прибытии в купе следует проверить, чтобы в нем не было **посторонних лиц и предметов**, исправность запоров двери, после чего убедиться в наличии и исправности упаковки охраняемого груза, **разместить его в удобном для охраны месте**; не допускать размещения груза в ящиках под нижней полкой;

дверь в купе держать постоянно **закрытой и запертой;**

**знать проводника в лицо** и допускать в купе для выполнения своих обязанностей, предварительно удостоверившись в его личности;

лицам наряда в пути следования **запрещается менять места** в вагоне;

по прибытии на станцию назначения организовать **выход из вагона наряда в первую или последнюю очередь**, исходя из складывающейся обстановки.

### Б. На воздушном транспорте:

переносить охраняемое имущество из автомашины в самолет **до посадки пассажиров**, если самолет пассажирский, при этом один работник следует впереди представителя собственника с охраняемым имуществом, старший наряда сзади;

перед посадкой в самолет старший наряда решает вопрос **о сдаче и хранении вооружения наряда, по возможности согласовывает с бортпроводником места посадки** личного состава наряда и представителя собственника;

в пути следования **запрещается оставлять охраняемый груз без присмотра**, один из состава наряда всегда находится вместе с грузом;

по прибытии в пункт назначения старший наряда **при передаче груза проверяет документы у встречающего, сличает государственные номерные знаки и марку машины** и только после этого передает груз согласно акту.

# 4.5.5. ОБЕСПЕЧЕНИЕ ОХРАНЫ ИМУЩЕСТВА ФИЗИЧЕСКИХ И ЮРИДИЧЕСКИХ ЛИЦ

**Организация охраны:**

- прием заявления на обеспечение охраны имущества физического или юридического лица;
- обследование имущества, мест хранения имущества физических и юридических лиц на предмет их инженерно-технической укрепленности и оснащенности техническими средствами охраны;
- заключение договора на охрану имущества физического или юридического лица;
- осуществление охраны имущества физических и юридических лиц по договорам, в том числе при его транспортировке;
- осуществление расчетов за охрану имущества физических и юридических лиц.

**Для рассмотрения вопроса о предоставлении организации государственной охраны подается заявление с обязательным приложением:**

а) свидетельства о регистрации юридического лица;

б) свидетельства о постановке на учет в территориальных органах ФНС;

в) учредительных документов организации (устав, положение, учредительный договор);

г) документов о праве собственности, оперативного управления, хозяйственного ведения организации на объект или договора аренды (субаренды), оформленного и зарегистрированного в установленном порядке;

д) документов, подтверждающих полномочия лица, подписывающего договор (приказ о назначении на должность руководителя – для государственных организаций; протокол собрания акционеров (участников и другие) или протокол заседания Совета директоров (Наблюдательного совета) об избрании президента общества (генерального директора) – для негосударственных организаций);

е) доверенности на право совершения юридических действий (в случае заключения договора доверенным лицом)

# 4.5.6. ОСНОВАНИЯ ДЛЯ ОТКАЗА В ОБЕСПЕЧЕНИИ ОХРАНЫ ИМУЩЕСТВА ЮРИДИЧЕСКИХ ЛИЦ

1. Предоставление заявителем **неполного пакета документов** либо отказ заявителя от предоставления необходимых документов
2. **Недостоверность информации**, указанной в заявлении или прилагаемых к нему документах либо признание их непригодными для использования.
3. Получение сведений (документов), подтверждающих **ограниченную дееспособность заявителя - физического лица** совершать юридические действия.
4. Установленный юридический **факт спора в отношении права собственности**, владения имуществом, передаваемым под охрану.
5. **Отсутствие необходимой штатной численности** подразделений, осуществляющих охрану имущества физических и юридических лиц по договорам.
6. **Отсутствие технической возможности охраны** имущества соответствующим подразделением вневедомственной охраны (расположение передаваемого под охрану имущества вне зоны действия пунктов централизованной охраны или отсутствие необходимых ТСО).
7. **Неустранимые противоречия** между заявителем, подразделением вневедомственной охраны, а также, при необходимости осуществления проектирования, монтажа и обслуживания технических средств охраны

# Глава 5.
# ОСНОВЫ ОРГАНИЗАЦИИ ПРОТИВОПОЖАРНОЙ ОХРАНЫ В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**5.1.** Основы противопожарной охраны и ее организации на предприятии

**5.2.** Средства противопожарной охраны

**Литература:**


1. Федеральный закон № 69-ФЗ «О пожарной безопасности»
2. Федеральный закон № 123-ФЗ «ТР о требованиях пожарной безопасности» от 22.07.08 г.;
3. Федеральный закон № 384-ФЗ «ТР о безопасности зданий и сооружений».
4. Правила пожарной безопасности (ППБ 01-03);
5. http://ru.wikipedia.org/wiki/Пожарная_безопасность, 2013 г.
6. http://www.sec4all.net/tolpa.html, 2013 г.


Оглавление

# 5.1. ОСНОВЫ ПРОТИВОПОЖАРНОЙ ОХРАНЫ И ЕЕ ОРГАНИЗАЦИИ НА ПРЕДПРИЯТИИ

## 5.1.1. БАЗОВЫЕ ОПРЕДЕЛЕНИЯ

**ПОЖАР** – неконтролируемое горение, причиняющее материальный ущерб, вред жизни и здоровью граждан, интересам общества и государства.

**ПОЖАРНАЯ БЕЗОПАСНОСТЬ** – состояние объекта, характеризуемое возможностью предотвращения возникновения и развития пожара, а также воздействия на людей и имущество опасных факторов пожара, обеспечиваемое защиты, в том числе организационно-техническими мероприятиями.

**ПОЖАРНАЯ ПРОФИЛАКТИКА** – обучение пожарной технике безопасности и комплекс мероприятий, направленных на предупреждение пожаров.

**ПРОТИВОПОЖАРНАЯ ЗАЩИТА** – комплекс мер и технологий, предназначенных для защиты от пожара, направленных на уменьшение ущерба в случае его возникновения, т. е. позволяющих снизить или полностью исключить возможность горения или повреждения огнем горючих материалов и объектов, построенных с их использованием.

**ПРОТИВОПОЖАРНЫЙ РЕЖИМ** – правила поведения людей, порядок организации производства, порядок содержания помещений и территорий, обеспечивающие предупреждение нарушений требований пожарной безопасности и тушение пожаров.

**ПОЖАРНАЯ ОХРАНА** – совокупность созданных в установленном порядке органов управления, подразделений и организаций, предназначенных для организации профилактики пожаров, их тушения и проведения возложенных на них аварийно-спасательных работ

## 5.1.2. СУЩНОСТЬ И СТАДИИ ПОЖАРА

**УСЛОВИЯ ВОЗГОРАНИЯ:**

наличие **горючей среды**.

наличие **источника зажигания** - открытого огня, химической реакции, электрического тока.

наличие **окислителя**, например, кислорода воздуха.

**СУЩНОСТЬ ГОРЕНИЯ**:

**а) нагревание источников зажигания горючего материала;**

**б) тепловое разложение** с образованием угарного газа, воды и большого количества тепла и сажи;

**в) воспламенение** (время от начала зажигания горючего материала до его воспламенения называется временем воспламенения - максимальное время воспламенения может составлять **несколько месяцев)**.

**г) пожар** (начинается с момента воспламенения)

**СТАДИИ ПОЖАРА В ПОМЕЩЕНИЯХ:**

**Фаза линейного распространения пожара** первые 10-20 мин. вдоль горючего материала. Помещение заполняется дымом: рассмотреть в это время пламя невозможно. Температура воздуха поднимается до 250-300$^{o}$C - температуры воспламенения основных горючих материалов.

**Фаза объёмного распространения пожара (**через 20 мин.); спустя ещё 10 мин. наступает разрушение остекления, увеличивается приток свежего воздуха, резко прогрессирует развитие пожара. Температура достигает 900$^{o}$C.

**Фаза выгорания**, при которой в течение 10 мин. скорость пожара – максимальна.

**Фаза стабилизации пожара** (от 20 мин. до 5 час.) после того, как выгорают основные вещества. Если огонь не может перекинуться на другие помещения, пожар идёт на улицу. В это время происходит обрушение выгоревших конструкций.

## 5.1.3. ПОЖАРНАЯ ПРОФИЛАКТИКА И ЗАЩИТА

**СОДЕРЖАНИЕ ПОЖАРНОЙ ПРОФИЛАКТИКИ:**

**проверка и утверждение проектов** строительства,
**контроль за выполнением норм** по пожарной безопасности,
**борьба с поджогами** (в т.ч. с пожароопасными играми подростков),
**сбор данных,**
**инструктаж и обучение** технике безопасности и мерам по предупреждению пожаров

**ЗАДАЧИ ПОЖАРНОЙ ПРОФИЛАКТИКИ**:

1) обучение, в т.ч. распространение знаний о пожаробезопасном поведении;
2) пожарный надзор, предусматривающий разработку государственных норм пожарной безопасности и строительных норм, а также проверку их выполнения;
3) обеспечение оборудованием и технические разработки.

**СФЕРА ПОЖАРНОГО НАДЗОРА**: нормы пожарной профилактики, строительные пожарные нормы и правила, стандарты изготовления и установки противопожарного оборудования, стандарты пожарной безопасности на товары широкого потребления.

**МЕТОДЫ И МЕРЫ ПРОТИВОПОЖАРНОЙ ЗАЩИТЫ:**

**методы противодействия пожару:**

уменьшающие вероятность возникновения пожара (профилактические, пассивные);
непосредственная защита и спасение людей от огня (активные);

**мероприятия по противопожарной защите:**

1) **контроль материалов, продуктов и оборудования;**
2) **активное ограничение распространения огня с использованием средств пожарной сигнализации, систем автоматического пожаротушения и переносных огнетушителей;**
3) **устройство пассивных систем, ограничивающих распространение огня, дыма, жара и газов за счет секционирования помещений;**
4) **эвакуация людей из горящего здания в безопасное место**

# 5.1.4. ДЕЙСТВИЯ ПО ТУШЕНИЮ ПОЖАРОВ

**ДЕЙСТВИЯ ПО ТУШЕНИЮ ПОЖАРОВ** начинаются с момента получения сообщения о пожаре пожарной охраной, считаются законченными по возвращении подразделения пожарной охраны на место постоянной дислокации и **включают в себя:**

- **прием и обработку сообщения о пожаре (вызове);**
- **выезд и следование к месту пожара (вызова);**
- **разведку места пожара;**
- **аварийно-спасательные работы, связанные с тушением пожаров;**
- **развертывание сил и средств;**
- **ликвидацию горения;**
- **специальные работы;**
- **сбор и возвращение к месту постоянного расположения.**

**ДЛЯ ВЫЗОВА ПОДРАЗДЕЛЕНИЙ ПОЖАРНОЙ ОХРАНЫ** в телефонных сетях населенных пунктов устанавливается единый номер - **01 (для моб. телефонов - 112).**

**НЕПОСРЕДСТВЕННОЕ РУКОВОДСТВО** тушением пожара осуществляется **руководителем тушения пожара** – прибывшим на пожар старшим оперативным должностным лицом пожарной охраны, которое управляет на принципах единоначалия личным составом пожарной охраны, участвующим в тушении пожара, а также привлеченными к тушению пожара силами. **Указания руководителя тушения пожара обязательны для исполнения всеми должностными лицами и гражданами на территории, на которой осуществляются боевые действия по тушению пожара.**

**ПРИ ТУШЕНИИ ПОЖАРОВ** проводятся необходимые действия по обеспечению безопасности людей, спасению имущества, в том числе:

- **проникновение в места распространения пожаров и их опасных проявлений;**
- **создание условий, препятствующих развитию пожаров и обеспечивающих их ликвидацию;**
- **использование на безвозмездной основе средств связи, транспорта, оборудования;**
- **ограничение доступа к местам пожаров и прилегающих к ним территориям;**
- **эвакуация с мест пожаров людей и имущества**

# 5.1.5. ТРЕБОВАНИЯ ПРИ ПРОВЕРКЕ ПОЖАРНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

1. Наличие ежегодного **приказа о противопожарном режиме.**
2. Наличие **приказа о назначении лица, ответственного** за пожарную безопасность.
3. Наличие **приказа об утверждении состава добровольной пожарной дружины**.
4. Наличие **инструкции по пожарной безопасности**.
5. Наличие **плана действий в случае возникновения пожара**.
6. Наличие **планов эвакуации**.
7. Наличие **инструкций для дежурного персонала** по безопасной и быстрой эвакуации.
8. Наличие ежегодного **плана проведения тренировки** по эвакуации людей в случае пожара.
9. Наличие **актов о результатах проведенных тренировок** по эвакуации людей.
10. Наличие **годового плана противопожарных мероприятий**.
11. Наличие журнала **регистрации противопожарного инструктажа**.
12. Наличие журнала **учета первичных средств пожаротушения**.
13. Наличие **акта технического обслуживания** и проверки **внутренних пожарных кранов (ПК)**.
14. Наличие **акта проверки пожарного гидранта** на водоотдачу.
15. Наличие **противопожарного уголка.**
16. Своевременность **ТО и проверки** внутренних ПК (в полгода)
17. Наличие **огнетушителей и своевременность их проверки** и перезарядки.
18. Наличие и ТО **автоматической пожарной сигнализации** и системы оповещения.
19. Состояние **эвакуационных проходов**, выходов, коридоров, тамбуров и лестниц.
20. Состояние **подвальных помещений**.
21. Наличие **знаков пожарной безопасности** и указателей путей эвакуации.
22. **Отсутствие глухих решеток на окнах**.
23. **Содержание территории** учреждения

# 5.1.6. СОДЕРЖАНИЕ ОСНОВНЫХ ДОКУМЕНТОВ ОРГАНИЗАЦИИ ПОЖАРНОЙ ОХРАНЫ

**ПРИКАЗ:** по-фамильно – ответственные за пожарную безопасность зданий и помещений; места и допустимое количество хранения лаков, красок, растворителей и др. легковоспламеняющихся жидкостей; порядок уборки помещений, горючих отходов и пыли; порядок обесточивания электрооборудования в случае пожара и по окончании рабочего дня; порядок проведения временных огневых и других пожароопасных работ; порядок осмотра и закрытия помещений после окончания работы; состав пожарного расчета из числа добровольной пожарной дружины; действия при обнаружении пожара; порядок и сроки прохождения противопожарного инструктажа; периодичность проведения тренировок по эвакуации, переосвидетельствования огнетушителей, осмотра наружных пожарных лестниц, проверки пожарных кранов и гидрантов а также назначение ответственных за их проведение. Приказ доводится под роспись

**ИНСТРУКЦИЯ для каждого структурного подразделения:** порядок содержания территории, зданий и помещений, в т.ч. эвакуационных путей; мероприятия по обеспечению пожарной безопасности при проведении работ, массовых мероприятий, эксплуатации оборудования, производстве пожароопасных работ; порядок и нормы хранения пожароопасных веществ и материалов; порядок сбора, хранения и удаления горючих веществ и материалов; обязанности и действия работников при пожаре, в т.ч.: правила вызова пожарной охраны, порядок аварийной остановки технологического оборудования, порядок отключения вентиляции и электрооборудования, правила применения средств пожаротушения и пожарной автоматики, порядок эвакуации горючих веществ и материальных ценностей

**ПЛАН ЭВАКУАЦИИ**: схема этажа с путями и направлениями эвакуации, условными знаками – местами расположения первичных средств пожаротушения и средств связи, а также текстовая часть – план действий в случае возникновения пожара и инструкция по пожарной безопасности

# 5.2. СРЕДСТВА ПРОТИВОПОЖАРНОЙ ОХРАНЫ
## 5.2.1. СУЩНОСТЬ СИСТЕМЫ ПОЖАРНОЙ СИГНАЛИЗАЦИИ

**СИСТЕМА ПОЖАРНОЙ СИГНАЛИЗАЦИИ** – совокупность технических средств, предназначенных для обнаружения факторов пожара, формирования, сбора, обработки, регистрации и передачи в заданном виде сигналов о пожаре, режимах работы системы, другой информации и, при необходимости, выдачи сигналов на управление техническими средствами противопожарной защиты, технологическим, электротехническим и другим оборудованием.

**СОСТАВ СИСТЕМЫ ПОЖАРНОЙ СИГНАЛИЗАЦИИ**:

- прибор приемно-контрольный,
- извещатели,
- оповещатели,
- соединительные линии
- исполняющие устройства.

**ТИПЫ СИСТЕМ ПОЖАРНОЙ СИГНАЛИЗАЦИИ:**

- радиальная;
- адресная;
- адресно-аналоговая

## 5.2.2. СРЕДСТВА ПРОТИВОПОЖАРНОЙ СИГНАЛИЗАЦИИ

**СПЕЦИАЛЬНАЯ СВЯЗЬ** обеспечивает передачу сообщений о пожаре персоналу пожарного управления по общей телефонной сети, от сигнализационной кнопки, предусмотренной вне здания, по громкоговорящему телефону, от радиостанции, от муниципальной системы пожарной сигнализации или от коммерческой системы автоматической сигнализации.

**ЗАЩИТНАЯ СИГНАЛИЗАЦИЯ** передает сигнал пожара, контрольный сигнал и сигнал неисправности (в речевой или цифровой форме) от места сигнализационной кнопки в др. части здания или на удаленную станцию контроля.

**БЫТОВЫЕ ИНДИКАТОРЫ ЗАДЫМЛЕННОСТИ И СИСТЕМЫ СИГНАЛИЗАЦИИ** (одно- и многоточечные): ионизационные, фотоэлектрические и комбинированные (ионизационно-фотоэлектрические). Индикатор задымленности должен давать сигнал с уровнем звукового сигнала не ниже 85 дБ на 3 м.

**АВТОМАТИЧЕСКАЯ ПОЖАРНАЯ СИГНАЛИЗАЦИЯ** с дымовыми, тепловыми, газоанализаторными или пламенными датчиками.

**Тепловые датчики** срабатывают по достижении определенной температуры (~60° С) или определенной скорости ее нарастания (7-8° С/мин).

**Пневмодатчики** – после нагревания воздуха в помещении и повышении давления газа в запаянной трубке.

**Термисторные датчики** генерируют сигнал, когда превышается установленное значение электросопротивления в помещении.

**В газоанализаторном датчике** полупроводниковый элемент или катализатор срабатывают, когда изменяется проводимость полупроводникового элемента или температура катализатора.

**Пламенные детекторы** реагируют на инфракрасное или ультрафиолетовое излучение.

**ДРУГИЕ СИСТЕМЫ:**

- контроля за работой системы пожаротушения, сигнализирующая о ее включении;
- сигнализации накопления больших концентраций газов (на производствах);
- контроля за работой охранной и пожарной сигнализации.

## 5.2.3. ПОЖАРНЫЕ ИЗВЕЩАТЕЛИ

**Извещатель пожарный дымовой оптико-электронный ИП 212-39/1 ”АГАТ”** предназначен для обнаружения загораний, сопровождающихся появлением дыма в закрытых помещениях. Применяется в составе автоматизированных систем обнаружения загораний (АСОЗ) совместно с приёмно-контрольными приборами (ПКП) или устройствами сигнально-пусковыми (УСП), обеспечивающими в шлейфе пожарной сигнализации напряжение 7-30 В. Имеет встроенную сирену и при срабатывании выдает громкий, 85 дБ, прерывистый звуковой сигнал.

**Извещатель пожарный пламени ИП 329-5 "АМЕТИСТ"** предназначен для обнаружения пламени, исходящего от очагов загораний и сопровождающегося ультрафиолетовым излучением. Устанавливается в помещениях и на открытом пространстве под навесом, например, для защиты автозаправочных станций, газовых станций, нефтебаз и т. п. Применяется в составе АЗОЗ совместно с ПКП или УСП, обеспечивающими в шлейфе пожарной сигнализации напряжение 12-30 В. В электрической схеме в качестве чувствительного элемента используется современный индикатор УФ излучения


**Извещатель пожарный ручной ИПР 513-2 "АГАТ"** предназначен для подачи сигнала тревоги на средства пожарной и охранно-пожарной сигнализации при воздействии на него человека. Применяется в составе АСОЗ совместно с ПКП или УСП, обеспечивающими в шлейфе пожарной сигнализации напряжение 9-30 В

# Глава 6.
# ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВЕЩАНИЙ ПО КОНФИДЕНЦИАЛЬНЫМ ВОПРОСАМ

**6.1.** Угрозы утечки конфиденциальной информации на совещаниях и заседаниях.

**6.2.** Подготовка и проведение совещаний и переговоров по конфиденциальным вопросам.

**6.3.** Мероприятия и средства предотвращения утечки информации

## Литература:


1. Садердинов А.А. Информационная безопасность предприятия. Уч. пособие. – М.: Дашков и К°, 2004 г.
2. Ярочкин В.И. Система безопасности фирмы. – М.: Ось-89, 2003 г.


Оглавление

# 6.1. УГРОЗЫ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА СОВЕЩАНИЯХ И ЗАСЕДАНИЯХ

## 6.1.1 ФАКТОРЫ, ВЛИЯЮЩИЕ НА ОСОБЕННОСТИ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЙ С УЧАСТИЕМ ПРЕДСТАВИТЕЛЕЙ СТОРОННИХ ОРГАНИЗАЦИЙ

- **величина ущерба** от утечки сведений по комплексным работам, в выполнении которых участвуют различные организации;
- присутствие на совещании, в том числе представителей заказчика и исполнителей, с **разным отношением к требованиям** по обеспечению безопасности информации;
- стремление части сотрудников сторонних организаций к **регистрации информации, в том числе на диктофоны**, с целью последующей обработки для доклада хода и результатов совещания руководству своих организаций;
- стремление некоторых сотрудников сторонних организаций **связаться с их начальством во время совещания** для проведения каких-либо оперативных мероприятий;
- выполнение участниками совещания **агентурных заданий**;
- **высокий уровень концентрации** и обобщения закрытых сведений в докладах выступающих, отображаемых на плакатах и находящихся на столах документах;
- **большая продолжительность совещания** по комплексным работам по сравнению с обсуждением внутренних вопросов головной организации;
- факт совещания и состав его участников **как информативный демаскирующий признак** хода выполнения комплексной работы.

# 6.1.2. ПОДСЛУШИВАНИЕ КАК КРИТИЧЕСКАЯ УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ХОДЕ СОВЕЩАНИЯ

**Непосредственное**

- *Прямое*
- *Через конструкции зданий и помещений*

**ПОДСЛУШИВАНИЕ - способ ведения разведки и промышленного шпионажа, применяемый агентами, наблюдателями, специальными постами подслушивания, разведывательными подразделениями и органами для подслушивания перегово-ров, а также сообщений, передаваемых по техническим средствам связи**

**С помощью технических средств**

- *С помощью микрофонов*
- *Посредством радиозакладок*
- *Лазерное*

**ЦИФРОВОЙ ДИКТОФОН EDIC-MINI TINY B22**

**ХАРАКТЕРИСТИКИ:**

**Металлический корпус, габаритные размеры 31х25х6 мм .**
**Вес не более 13 г (без элемента питания).**
**Время записи до 600 ч., режим записи - моно.**
**Питание: литиевая батарейка, время работы до 24 ч.**
**Комплект поставки:**

диктофон; USB-кабель; диск с программным обеспечением;
инструкция по эксплуатации с вкладышем;
элемент питания(батарейка CR 2016) - 2 шт.;
упаковочная коробка.

# 6.2. ПОДГОТОВКА И ПРОВЕДЕНИЕ СОВЕЩАНИЙ И ПЕРЕГОВОРОВ ПО КОНФИДЕНЦИАЛЬНЫМ ВОПРОСАМ
## 6.2.1а. ПЛАН МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЯ

**Планирование возглавляет руководитель предприятия, а его заместитель, в ведении которого находятся вопросы защиты информации и возлагается общая координация выполнения решений, непосредственно участвует в планировании. При отсутствии заместителя указанные задачи возлагаются на руководителя режимно-секретного подразделения (службы безопасности).**

**РАЗДЕЛЫ ПЛАНА:**

1. **Определение состава участников и их оповещение** – порядок формирования списка лиц, привлекаемых к участию в совещании, которым необходимо направить запросы с приглашениями; порядок подготовки и направления таких запросов, формирования их содержания.

2. **Подготовка служебных помещений**, в которых планируется проведение совещания, - работа по выбору служебных помещений и проверке их соответствия требованиям по защите информации; необходимость и целесообразность принятия дополнительных организационно-технических мер, направленных на исключение утечки информации; оборудование рабочих мест, в том числе средствами автоматизации, на которых разрешена обработка конфиденциальной информации; порядок использования звукоусиления, кино- и видеоаппаратуры.

3. **Определение объема обсуждаемой информации** – порядок определения перечня вопросов и очередности их рассмотрения, оценки степени их конфиденциальности; выделение вопросов, к которым допускается узкий круг лиц, участвующих в совещании.

4. **Организация пропускного режима** на территории и в служебных помещениях – виды пропусков и проставляемых на них условных знаков или шифров; порядок их учета, хранения, выдачи и выведения из действия, сроки уничтожения; режим прохода, посещения и пребывания в помещениях участников в совещания; количество и регламент работы основных и дополнительных КПП для прохода на территорию и в служебные помещения.

5. **Организация допуска участников совещания** к рассматриваемым вопросам с учетом порядка их обсуждения и степени конфиденциальности информации.

6. **Осуществление записи, фото-, кино-, видеосъемки** совещания – порядок и возможные способы записи, съемки, стенографирования обсуждаемых вопросов с учетом их конфиденциальности; должностные лица или подразделения, отвечающие за техническое обеспечение данных процессов.

# 6.2.1б. ПЛАН МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ СОВЕЩАНИЯ

7. **Меры по защите информации** – порядок и способы охраны служебных помещений, меры по исключению проникновения в них посторонних лиц, а также участников совещания, не участвующих в рассмотрении конкретных вопросов; мероприятия по предотвращению утечки информации по техническим каналам, силы и средства; конкретные меры, исключающие визуальный просмотр и прослушивание ведущихся переговоров и обсуждения участниками совещания вопросов конфиденциального характера

8. **Организация учета, хранения, выдачи и рассылки материалов совещания** – порядок учета, хранения, размножения, выдачи, рассылки и уничтожения материалов, рабочих тетрадей или блокнотов; порядок обращения с носителями информации, зафиксированных на магнитных носителях (исполненных в электронном виде) в ходе совещания и после его окончания; порядок учета, хранения, размножения и использования материалов.

9. **Оформление документов** лиц, принимавших участие в совещании, – порядок и сроки оформления документов, подтверждающих право доступа участников совещания к конфиденциальной информации, предписаний или доверенностей на участие в совещании, командировочных удостоверений и иных документов командированных лиц.

10. **Проверка и обследование места проведения совещания после его окончания** – мероприятия по организации и проведению визуальной проверки, а также с использованием специальных технических средств помещений в целях выявления забытых участниками технических устройств, носителей информации и личных вещей.

11. **Организация контроля за выполнением требований по защите информации** – порядок, способы и методы контроля полноты и качества проводимых мероприятий, утрат хищений носителей информации; структурные подразделения или должностные лица, отвечающие за осуществление контроля; порядок и сроки представления ответственными должностными лицам докладов о наличии носителей конфиденциальной информации, выявленных нарушениях.

12. В**ремя и место проведения совещания, состав участников, перечень предприятий**, участвующих совещании. Для каждого мероприятия плана определяется срок (время) его проведения и ответственное за его выполнение должностное лицо (подразделение).

**После утверждения план под подписку доводится до сведения руководителей подразделений и ответственных за выполнение в части, касающейся. Контроль осуществляется режимно-секретным подразделением (службой безопасности).**

# 6.2.2. ТРЕБОВАНИЯ ПО ЗАЩИТЕ РЕЧЕВОЙ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В ЗАЩИЩЕННОМ ПОМЕЩЕНИИ (ЗП)

1. Определить перечень ЗП и ответственных лиц, а также составить технический паспорт на ЗП.

2. Защищаемые помещения оснащать сертифицированными средствами, прошедшими специальные исследования и имеющими предписание на эксплуатацию.

3. По решению руководителя провести специальную проверку (аудит) ЗП и оборудования с целью выявления электронных устройств перехвата информации.

4. Запретить использование в ЗП радиотелефонов, устройств сотовой связи, магнитофонов и других средств аудио и видеозаписи. При установке в ЗП телефонных и факсимильных аппаратов с автоответчиком и АОН отключать их из сети при проведении мероприятий.

5. Для исключения утечки информации за счет электроакустического преобразования использовать в ЗП в качестве оконечных устройств телефонной связи, имеющих прямой выход в городскую АТС, ТА, прошедшие специальные исследования, оборудовать их сертифицированными СЗ.

6. Для исключения возможности скрытного прослушивания разговоров не устанавливать в ЗП цифровые ТА цифровых АТС, имеющих выход в городскую АТС или к которой подключены посторонние абоненты, а использовать сертифицированные ЦАТС либо аналоговые аппараты.

7. Ввод системы городского радиотрансляционного вещания на территорию учреждения (предприятия) осуществлять через радиотрансляционный узел (буферный усилитель).

8. В случае размещения электрочасовой станции внутри КЗ использовать в ЗП электровторичные часы (ЭВЧ) без СЗИ. При установке электрочасовой станции вне КЗ в линии ЭВЧ, имеющие выход за пределы КЗ, устанавливать сертифицированные СЗИ.

9. Системы пожарной и охранной сигнализации ЗП строить только по проводной схеме сбора информации, как правило, в пределах одной с ЗП КЗ из сертифицированных изделий.

10. Звукоизоляцией ограждающих конструкций ЗП, систем вентиляции и кондиционирования обеспечить невозможность прослушивания разговоров. Проверку звукоизоляции осуществлять аттестационной комиссией. Для обеспечения необходимого уровня звукоизоляции помещений оборудовать: дверные проемы тамбурами с двойными дверями, дополнительные рамы, уплотнительные прокладки в дверях и окнах и шумопоглотители на выходах вентиляционных каналов.

11. Для снижения вероятности перехвата информации по виброакустическому каналу исключить установку посторонних предметов на внешней стороне ограждающих конструкций ЗП и выходящих из них инженерных коммуникаций (систем отопления, вентиляции, кондиционирования). Для снижения уровня виброакустического сигнала элементы инженерно-технических систем отопления, вентиляции оборудовать звукоизолирующими экранами.

12. Если указанные меры недостаточны, применять метод активного маскирующего зашумления.

13. Предусматривать организационно-режимные меры исключения НСД в ЗП

# 6.2.3. ТРЕБОВАНИЯ ПО ЗАЩИТЕ РЕЧЕВОЙ ИНФОРМАЦИИ, ЦИРКУЛИРУЮЩЕЙ В СИСТЕМАХ ЗВУКОУСИЛЕНИЯ И ЗВУКОВОГО СОПРОВОЖДЕНИЯ

**1. Здание, где размещаются ЗП, должно иметь круглосуточную охрану и систему сигнализации, а ЗП – располагаться на верхних этажах, в центре здания, рядом с кабинетами руководства.**

**2. ЗП не должны иметь окон с балконами и выходящих на соседние здания. Они должны смотреть на внутренний двор или закрываться глухими ставнями. Форточки должны закрываться, шторы – задвигаться. ЗП должно содержать минимальное количество мебели, конструкция которой должна быть приспособлена для работы по поиску техники подслушивания.**

**3. В качестве оборудования систем звукоусиления, предназначенных для обслуживания проводимых в ЗП закрытых мероприятий, и систем звукового сопровождения кинофильмов использовать оборудование, удовлетворяющее требованиям стандартов по ЭМС России (ГОСТ 22505-97), Евросоюза и США, применять оборудование, сертифицированное или прошедшее специальные исследования и имеющее предписание на эксплуатацию.**

**4. Системы звукоусиления должны выполняться по проводной схеме передачи информации экранированными проводами и располагаться в пределах КЗ. С целью уменьшения ПЭМИН следует использовать систему звукоусиления с рассредоточенной системой звукоизлучателей, т.е. отдавать предпочтение системам с большим количеством оконечных устройств малой мощности перед системами с малым количеством оконечных устройств большой мощности. Использовать звуковые колонки в защищенном исполнении или экранировать их по электрическому полю металлической сеткой до 1 мм$^2$, заземляемой через экранирующую оплетку кабеля.**

**5. Использовать усилители только в металлических экранах с возможностью их заземления.**

**6. Коммутационное и распределительное оборудование (распределительные, входные и выходные щитки подключения) размещать в металлических шкафах (коробках) с клеммами для их заземления и приспособлениями для опечатывания. Усилительное и оконечное оборудование систем звукоусиления размещать на возможно большем расстоянии относительно границы КЗ.**

**7. Обеспечить соответствие системы электропитания и заземления требованиям «Правил устройства электроустановок».**

# 6.2.4. АУДИТ БЕЗОПАСНОСТИ КАК МЕРА ПРЕДОТВРАЩЕНИЯ УТЕЧКИ ИНФОРМАЦИИ

**1. АТТЕСТАЦИЯ ОБЪЕКТОВ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ:**

- аттестация АСУ, средств связи, обработки и передачи информации;
- аттестация помещений, предназначенных для конфиденциальных переговоров;
- аттестация технических средств, установленных в выделенных помещениях.

**2. КОНТРОЛЬ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА:**

- выявление технических каналов утечки информации и способов НСД к ней;
- контроль эффективности применяемых средств защиты информации.

**3. СПЕЦИАЛЬНЫЕ ИССЛЕДОВАНИЯ ТЕХНИЧЕСКИХ СРЕДСТВ НА НАЛИЧИЕ ПЭМИН:**

- персональные ЭВМ, средства связи и обработки информации;
- локальные вычислительные системы;
- оформление результатов исследований в соответствии с требованиями ГТК.

**4. ПРОЕКТИРОВАНИЕ ОБЪЕКТОВ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ:**

- разработка концепции информационной безопасности;
- проектирование автоматизированных систем, средств связи, обработки и передачи информации в защищенном исполнении;
- проектирование помещений, предназначенных для ведения конфиденциальных переговоров, защищенных программных средств обработки, защиты информации и контроля ее защищенности.

**5. ПРОВЕДЕНИЕ РАБОТ ПО ВЫЯВЛЕНИЮ ЭЛЕКТРОННЫХ УСТРОЙСТВ ПЕРЕХВАТА ИНФОРМАЦИИ В ПОМЕЩЕНИЯХ**

**6. ПРОВЕДЕНИЕ РАБОТ ПО ВЫЯВЛЕНИЮ ЭЛЕКТРОННЫХ УСТРОЙСТВ ПЕРЕХВАТА ИНФОРМАЦИИ В ТЕХНИЧЕСКИХ СРЕДСТВАХ**

**7. ПОДГОТОВКА И ПЕРЕПОДГОТОВКА КАДРОВ В ОБЛАСТИ ЗАЩИТЫ ИНФОРМАЦИИ**

# 6.2.6. ПОДГОТОВИТЕЛЬНЫЙ ЭТАП АУДИТА ПОМЕЩЕНИЙ

1. **Уточнение границ и ранжирование по степени важности информации, относимой к конфиденциальной.**
2. **Уточнение вероятного злоумышленника, оценка его возможностей, тактики внедрения средств НСИ и их использования («модель злоумышленника»).**
3. **Разработка замысла проведения аудита помещений:**
   - выработка целевой установки;
   - определение масштаба, места, времени поисковых мероприятий,
   - разработка легенды, под прикрытием которой будет проводиться аудит;
   - выработка замысла активации внедренных средств НСИ;
   - выбор вариантов действий в случае обнаружения средств НСИ.
4. **Изучение планов помещений, схем технических коммуникаций, связи, организации охраны, доступа и др.**
5. **Предварительный осмотр объекта.**
6. **Разработка перечня аппаратуры, необходимой для проведения проверки**
7. **Разработка дополнительных мер по активации внедренных средств НСИ**
8. **Распределение привлекаемых сил и средств по объектам и видам работ.**
9. **Уточнение частных методик использования привлекаемой аппаратуры**
10. **Оформление плана проведения комплексной проверки помещений и объектов**
11. **Подготовка аппаратуры для проведения поисковых работ**
12. **Предварительный сбор данных и анализ радиоэлектронной обстановки в районе обследуемых объектов и помещений**
13. **Подготовка документов прикрытия работ в соответствии с выбранной легендой прикрытия.**
14. **Подготовка бланков, схем, заготовок документов, необходимых для проведения работ на последующих этапах**

## 6.2.7. НЕПОСРЕДСТВЕННОЕ ПРОВЕДЕНИЕ АУДИТА ПОМЕЩЕНИЙ

1. **Визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера**
2. **Проверка элементов строительных конструкций, мебели с использованием специальных поисковых технических средств**
3. **Выполнение мер по активации внедренных средств НСИ.**
4. **Проверка линий и оборудования проводных коммуникаций:**
   - линий силовой и осветительной электросети;
   - линий и оборудования офисной и абонентской телефонной сети;
   - линий селекторной связи;
   - линий радиотрансляционной сети;
   - линий пожарной и охранной сигнализации;
   - линий системы часофикации и других проводных линий.
5. **Исследование радиоэлектронной обстановки для выявления сигналов радиопередающих средств НСИ и их локализации.**
6. **Поиск средств негласного съема и передачи информации, внедренных в электронные приборы.**
7. **Исследование звукопроницаемости элементов конструкций, проверка трубопроводных и других технологических коммуникаций на наличие в них акустических и виброакустических сигналов из проверяемого помещения.**
8. **Исследование ПЭМИН компьютеров, оргтехники и другого оборудования для выявления в них информативных сигналов.**

## 6.2.8. ПРОПУСК УЧАСТНИКОВ СОВЕЩАНИЯ

1. На совещание приглашаются работники, имеющие **непосредственное отношение к рассматриваемым вопросам и имеющие допуск** по соответствующей форме. При рассмотрении вопросов, отнесенных к иным видам конфиденциальной информации, участники совещания должны иметь оформленное в уставленном порядке решение руководителя предприятия о допуске данной категории информации.

2. Должностное лицо, ответственное за проведение совещания, по указанию руководителя предприятия (подразделения) формирует **список лиц, участвующих в совещании** на основании письменных обращений руководителей предприятий, приглашенных участвовать в совещании, и решений руководителей подразделений предприятия-организатора о привлечении к участию в совещании сотрудников этих подразделений.

В списке указывают фамилию, имя, отчество каждого участника, его место работы и должность, номер допуска к сведениям составляющим государственную тайну или номер решения руководителя о допуске к иной конфиденциальной информации, мера вопросов совещания, к обсуждению которых допущен участник и другие сведения.

3. Подготовленный список участников **согласовывается с режимно-секретным подразделением (службой безопасности) предприятия-организатора совещания** и утверждается руководителем предприятия, давшим разрешение на проведение совещания.

Включенные в список участники совещания проходят в служебные помещения, в которых оно проводится, предъявляя сотрудникам службы охраны (безопасности) **документ, удостоверяющий личность**. Проход участников совещания в эти помещения может быть организован по пропускам, выдаваемы им исключительно на период проведения совещания и отличающимся от других используемых предприятием-организатором пропусков. Участники совещания имеют право посещения только тех служебных помещений, в которых будут обсуждаться вопросы, к которым эти участники имеют непосредственное отношение.

4. **Проверку документов, подтверждающих наличие у участников совещания допуска и разрешений на ознакомление с конфиденциальной информацией осуществляет служба безопасности** (режимно-секретное подразделение) предприятия-организатора совещания

## 6.2.9а. ПРОВЕДЕНИЕ СОВЕЩАНИЯ И ИСПОЛЬЗОВАНИЕ ЕГО МАТЕРИАЛОВ

- **Непосредственно перед началом совещания его руководитель или должностное лицо, ответственное за его проведение, обязаны проинформировать участников совещания о степени конфиденциальности обсуждаемых вопросов.**
- **В ходе совещания, в том числе и во время перерывов, сотрудник, ответственный за его проведение, совместно со службой безопасности осуществляет необходимые организационные мероприятия по исключению утечки информации.**
- **Во время перерывов в совещании, а также после завершения обсуждения одного вопроса и перехода к обсуждению следующего, сотрудники службы безопасности (службы охраны) организуют контроль посещения служебных помещений, в которых проводится совещание, его участниками в соответствии с утвержденным списком.**
- **На все время проведения совещания запрещается пронос в служебные помещения, в которых оно проводится, индивидуальных видео- и звукозаписывающих устройств, а также средств связи (в т.ч. мобильных телефонов). В целях обеспечения их сохранности организуется камера хранения личных вещей.**
- **Звуко- и видеозапись хода совещания проводятся с разрешения руководителя предприятия – организатора совещания только на учтенных в режимно-секретном подразделении носителях.**
- **Участникам совещания не разрешается:**

информировать о факте, месте, времени проведения совещания, повестке дня, вопросах и ходе их обсуждения любых лиц, не принимающих участия в совещании;

производить выписки из документов и иных носителей конфиденциальной информации, используемых при обсуждении, на неучтенные носители;

обсуждать вопросы, вынесенные на совещание, в местах общего пользования во время перерывов в совещании и после его завершения;

расширять объем конфиденциальной информации, используемой в выступлениях, а также при обмене мнениями и обсуждении рассматриваемых вопросов.

**Носители конфиденциальной информации, рабочие тетради или блокноты выдаются режимно-секретным подразделением под расписку, а после окончания совещания возвращаются.**

# 6.2.9б. ПРОВЕДЕНИЕ СОВЕЩАНИЯ И ИСПОЛЬЗОВАНИЕ ЕГО МАТЕРИАЛОВ

- **Аудио- и видеозаписьведется только по письменному указанию руководителя** одним из сотрудников, готовивших совещание. Чистый магнитный носитель для этих целей выдается под роспись и возвращается после совещания.
- **Доступ участников совещания** в помещение, в котором оно будет проводиться, **осуществляет ответственный организатор совещания** под контролем службы безопасности в соответствии с утвержденным списком и предъявляемыми персональными документами. Перед началом обсуждения каждого вопроса состав присутствующих корректируется.
- Целесообразно, чтобы при открытии совещания организовавший его руководитель **напомнил о необходимости сохранения тайны**, уточнил, какие сведения являются конфиденциальными.
- Ход совещания **документируется одним из готовивших его сотрудников**. Протокол должен иметь гриф и оформляться в зарегистрированной тетради.
- Целесообразность записи участниками хода совещания определяется руководителем, организовавшим совещание. **Руководитель имеет право не разрешить вести какие-либо записи**.
- При необходимости вызова на совещание **дополнительных лиц (экспертов, консультантов, представителей других организаций) факт их участия фиксируется в протоколе с указанием мотивов вызова.**
- Участники совещания, замеченные в несанкционированной аудио или видеозаписи, использовании средств связи, фотографировании, **лишаются права дальнейшего присутствия на совещании**. По факту составляется акт, копия которого направляется руководству представителя.
- Итоговые документы совещания, а также материалы выступлений участников, в том числе и оформленные в электронном виде, **в установленном порядке высылаются в организации**, направлявшие на совещание своих представителей, а также в вышестоящие организации.
- Лицам, принимавшим участие в совещании, без письменного разрешения предприятия-организатора совещания **запрещается использовать материалы совещания при взаимодействии с организациями, представители которых на него не приглашались**

## 6.2.10. НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПРОВЕДЕНИИ ПЕРЕГОВОРОВ

***Выбор оптимального расположения средств документирования, размножения и отображения (экра-ны ПЭВМ, экраны общего пользова-ния и др.) информации с целью исключения прямого или дистанци-онного наблюдения (фотографиро-вания)***

***Выбор помещений, обращен-ных окнами в безопасные зоны (направления)***

***Использование светонепрони-цаемых стекол, занавесок, драпи-ровок, пленок и других защитных материалов (жалюзи, ставни и пр.)***

***Использование средств гашения экранов ЭВМ и табло коллективного пользования после определенного времени работы (работа по режиму времени)***

***Применение электронных средств, выявляющих звукозапи-сывающие и подавляющих радиопередающие устройства***

***Лицензирование деятельности предприятия для ведения работ и обращения сведений, составляющих государственную тайну как исходная мера обеспечения информационной безопасности***

# 6.2.11. ОСОБЕННОСТИ ПРОВЕДЕНИЯ ПЕРЕГОВОРОВ

- В процессе подготовки переговоров первоначально необходимо **выяснить намерения организации** или фирмы, с которой предполагаются переговоры: целесообразно получить о ней подробную информацию, чтобы избежать ошибочного выбора партнера или клиента.
- Подготовительная работа к проведению переговоров предполагает выработку **плана переговоров и определение на этой основе дозированного состава ценной информации**, которую допускается использовать в общении с участниками переговоров, динамики ее оглашения и условий возникновения в этом рабочей необходимости. Сообщаемые на этом этапе сведения, не должны содержать производственную или коммерческую тайну.
- Сотрудникам фирмы, участвующим в переговорах, **не разрешается использовать в дискуссии конфиденциальную информацию и раскрывать желаемые результаты переговоров**, итоги аналогичных переговоров с другими партнерами. В процессе неофициальной части переговоров обсуждение вопросов, связанных с содержанием дискуссии, не допускается.
- При ведении переговоров **не следует сразу же передавать партнеру всю запрашиваемую им информацию в полном объеме**, следует выяснить, с какой целью ему необходимы эти сведения и как знание этих сведений отразится на ходе дальнейшего сотрудничества. На этом этапе переговоров при выяснении сути взаимных намерений целесообразно строить дискуссию таким образом, чтобы ответы на вопросы были максимально лаконичными («да и нет», «можем и не можем»).
- После юридического оформления взаимоотношений и подписания обязательства о неразглашении ценных сведений, партнеры могут быть более подробно ознакомлены с предметом договора. В договоре по итогам переговоров должно найти отражение **взаимное обязательство сторон о защите ценных и особенно конфиденциальных сведений, недопустимости передачи их без предварительного согласия сторон третьему лицу**, необходимости ознакомления с предметом договора ограниченного числа сотрудников, которые должны подписать обязательства о сохранении в тайне полученных сведений.
- В коммерческой практике местом проведения переговоров становятся часто **постоянно действующие и периодические торговые или торгово-промышленные выставки и ярмарки**. Секретарь-референт должен **знать порядок защиты ценной информации фирмы в ходе этих переговоров, инструктировать их участников и контролировать соблюдение** ими установленных правил

# 6.3. МЕРОПРИЯТИЯ И СРЕДСТВА ПРЕДОТВРАЩЕНИЯ УТЕЧКИ ИНФОРМАЦИИ

## 6.3.1. СРЕДСТВА ОБНАРУЖЕНИЯ РАБОТАЮЩИХ ЭЛЕКТРОННЫХ СРЕДСТВ

**ИНДИКАТОР ПОЛЯ-ЧАСТОТОМЕР SEL SP-71R RAKSA предназначен для обнаружения в ближней зоне и определения местоположения радиопередающих устройств, использующихся для негласного съёма аудио- и видеоинформации.**

**Позволяет обнаруживать:**

- сотовые телефоны стандартов GSM900/1800, UMTS(3G), CDMA450;
- беспроводные телефоны стандарта DECT;
- устройства Bluetooth и Wi-Fi;
- беспроводные видеокамеры;
- радиопередатчики: с аналоговой модуляцией (АМ, ЧМ, ФМ); с цифровой модуляцией и непрерывной несущей (FSK, PSK и др.); с широкополосной модуляцией с полосой до 10 МГц.

**Технические характеристики:**

- диапазон принимаемых частот 50-3300 МГц
- типовая чувствительность 70 мВ/м
- динамический диапазон 50 дБ
- время работы в режиме охраны 4-12 ч., время работы в остальных режимах 3 ч
- размеры 77 х 43 х 18 мм, вес 35 г


**НЕЛИНЕЙНЫЙ ЛОКАТОР предназначен для поиска радиоэлектронных (прослушивающих) устройств, содержащих полупроводниковые элементы, а также отдельных полупроводниковых элементов, вне зависимости от места их расположения – в кирпичных и железобетонных стенах, в мебели или металлических шкафах, на теле человека (под одеждой), в головном уборе, обуви или в личных вещах – как во включенном, так и в выключенном состояниях: диктофоны и активные проводные микрофоны, системы с накоплением и последующей импульсной передачей информации**



## 6.3.2. СРЕДСТВА ЗАЩИТЫ ОТ ЗАКЛАДОК РАЗВЕДЫВАТЕЛЬНЫХ ЭЛЕКТРОННЫХ УСТРОЙСТВ

**Для защиты звонковой цепи телефонных аппаратов с дисковым номеронабирателем:**

**фильтр «Корунд-М»,** обеспечивающий затухание сигнала утечки до 80 дБ.

**Для защиты от проводных микрофонов, использующих сеть 220 В:**

**генератор типа «Соната-С1».**

**Для защиты переговорных от специальных технических средств :**

**а) генератор виброакустического шума «Соната-АВ»**

от непосредственного подслушивания в условиях плохой звукоизоляции;

от применения радио- и проводных микрофонов в полостях стен, надпотолочном пространстве, в вентиляционных проходах и т.д.;

от использования стетоскопов на стенах, потолках, полах, трубах водо- и теплоснабжения и т.д.;

применения лазерных и других типов направленных микрофонов.

**б) генератор радиошума «Баррикада-1»:**

обеспечивает защиту переговоров от всех радиозакладок, создавая в точке приема злоумышленником превышающий уровень помехи над уровнем излучаемого радиозакладкой сигнала.

# 6.3.3а. СРЕДСТВА ПРЕДОТВРАЩЕНИЯ ПОДСЛУШИВАНИЯ

**ГЕНЕРАТОРЫ ШУМА «ПОРОГ-2М», «БАРОН» НИИСТ МВД РОССИИ, «КАБИНЕТ» СНПО «ЭЛЕРОН»** предназначены для защиты служебных помещений от подслушивания при помощи радиотехнических, лазерных, акустических и других средств. Позволяют защищать от утечки информации через стены, окна, трубы отопления и водоснабжения, вентиляционные колодцы и т. п. Работают в режиме «дежурного приема», включаются только в случае, если в защищенном помещении начинается разговор.

Принцип действия основан на создании маскирующего вибрационного шума в ограждающих конструкциях и акустического шума в объеме помещения и вне его

**ГЕНЕРАТОР ЗВУКОВОЙ РЕЧЕПОДОБНОЙ ПОМЕХИ «ШАМАН»**

**ПЕРЕНОСНОЙ ГЕНЕРАТОР РАДИОШУМА «БРИЗ»**

**АППАРАТУРА ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ПЕРЕГОВОРОВ TF-012N**

Предназначен для защиты переговоров от любых методов подслушива-ния и звукозаписи постановкой маскирующей акустической помехи в месте переговоров. Проведение переговоров обеспечивается с помощью теле-фонных гарнитур. Гарантируется конфиденциальность переговоров, прово-димых в любых помещениях и в салоне автомобиля.

**Комплектность:**

блок генерации шумовой помехи и обработки речевых сигналов;
телефонные гарнитуры;
штатная упаковка.

**Технические характеристики :**

Уровень создаваемой акустической помехи 90, дБА
Количество участников переговоров 2...4 чел
Класс качества связи не ниже 2.
Питание (электросеть / бортовая сеть автомобиля) ~220 В / 12 В
Габариты 250х165х70 мм, масса 5,9 кг

# 6.3.3б. СРЕДСТВА ПРЕДОТВРАЩЕНИЯ ПОДСЛУШИВАНИЯ

## АКУСТИЧЕСКИЙ СЕЙФ SEL SP-125 "СВЕРЧОК"

Предназначен для защиты речевой информации, циркулирующей в местах пребывания владельца мобильного телефона, в случае негласной дистанционной активизации телефона с целью прослушивания через каналы сотовой связи на основе постоянного мониторинга излучения сотового телефона и включении акустической помехи в случае изменения напряжённости электромагнитного поля рядом с устройством (что свидетельствует о несанкционированном включении передатчика сотового телефона). Создаёт на входе микрофона трубки сотового телефона такой уровень шума, который обеспечивает гарантированное закрытие канала утечки информации через включённый микрофон мобильного телефона.

Отличительные особенности: интеллектуальный режим работы; имеет размеры банковской карточки толщиной 3 мм, что позволяет разместить его рядом с телефоном в кармане одежды; автоматическое выключение помехи при изъятии телефона из кармана.

**Технические характеристики:**

Эффективный спектр шумового сигнала 250 – 4000 Гц.

Напряжение питания 3 В (CR 2032).

Время непрерывной работы от одного комплекта батарей 3 мес.

## ЛАДЬЯ. АКУСТИЧЕСКИЙ СЕЙФ

Гарантирует защиту от негласного прослушивания через каналы сотовой связи путем несанкционированной активации его аппарата в режиме удаленного информационного доступа путем автоматического акустического зашумления тракта передачи речевой информации при попытке дистанционного включения микрофона трубки сотового телефона.

В случае негласной дистанционной активации телефона в режиме прослушивания единственным демаскирующим признаком является изменение напряженности электромагнитного поля. Это изменение фиксируется индикатором поля, входящим в состав устройства, который дает команду на автоматическое включение акустического шумогенератора, расположенного внутри объема изделия.

# 6.3.3в. СРЕДСТВА ПРЕДОТВРАЩЕНИЯ ПОДСЛУШИВАНИЯ

## МАСКИРАТОР ПЕРЕГОВОРОВ «БУКЕТ».

Предназначен для маскирования речи двух или более собеседников методом акустического зашумления помещения, в котором ведутся переговоры.

В зоне разговора располагается микрофон. В двух-пяти метрах - блок обработки со встроенными громкоговорителями. При попадании в него речевого сигнала опре-деляется мощность каждой его спектральной составляющей. Блок вырабатывает сигнал зашумления, поступающий в громкоговорители, спектральный состав и мощность которого соответствуют спектральному составу и мощности речи собеседников. В паузах разговора зашумление отсутствует.

**Технические характеристики.**

Питание от сети переменного тока 220В/ 50 Гц.

Максимальная потребляемая мощность (в режиме зарядки) - 10 Вт.

Время работы устройства - до 60 мин.

Масса прибора - не более 4 Кг.

## ГЕНЕРАТОР ВИБРОАКУСТИЧЕСКИХ ПОМЕХ «КЕДР»

Предназначен для защиты помещений от утечки акустической информации по вибрационному и акустическому каналам путем маскировании речи шумовой помехой, которая создаётся с помощью виброизлучателей.

Предотвращает возможность прослушивания переговоров с помощью акустических, вибрационных датчиков, лазерных устройств съёма информации, аппаратуры прослушивания через стены, потолки, перекрытия, окна, воздуховоды, трубы отопления, анализируя акустическую обстановку, по встроенному алгоритму формируя сигнал управления, функционально связанный с огибающей акустического (речевого) сигнала.


**Технические характеристики**

Полоса частот сигнала защиты: 200 Гц - 15 кГц

Количество каналов: 3

Макс. количество виброизлучателей, подключаемых на 1-й и 2-й канал: 20

Максимальное количество акустоизлучателей: 4

Радиус действия одного вибродатчика: 1,5 м

Количество подключаемых микрофонов: 2

Потребляемая мощность: не более 20 ВА

Габаритные размеры: 160 х 220 х 54

# 6.3.3г. СРЕДСТВА ПРЕДОТВРАЩЕНИЯ ПОДСЛУШИВАНИЯ

## ГЕНЕРАТОР РАДИОПОМЕХ ЛГШ-501

Предназначен для работы в составе системы активной защиты информации (САЗ), обрабатываемой на объектах ЭВТ второй и третьей категорий. САЗ обеспечивает защиту информации от утечки по каналам ПЭМИН путем создания широкополосной шумовой электромагнитной помехи в диапазоне частот от 0,01 до 1800 МГц.

Принцип работы САЗ на базе генератора ЛГШ-501: создание на границе КЗ шумовой помехи, которая зашумляет побочные излучения защищаемого объекта. Генератор может работать на две телескопические антенны и (или) на внешние антенны, смонтированные как три короткозамкнутых контура в виде петель из провода, уложенных по периметру трех взаимно перпендикулярных граней.

ЛГШ-501 питается от сети переменного тока напряжением 220 В и частотой 50 Гц. Устройство может эксплуатироваться круглосуточно.

## ЛГШ-701 БЛОКИРАТОР СВЯЗИ

Для блокирования работы устройств несанкционированного прослушивания и радиоисполнительных устройств, созданных с использованием стандартов сотовой связи.

Принцип работы заключается в генерации шумового сигнала, который подается на выходы антенн. В приборе имеются три выхода и, соответственно, три антенны. По каждому из выходов возможна плавная регулировка мощности излучения.

### Технические характеристики

Диапазон рабочих частот:

стандарт IMT-MC-450 (NMT-450i)

стандарт CDMA2000 1x  не менее 462,5...467,475 МГц

стандарт GSM900  не менее 935...960 МГц

стандарт DSC/GSM1800  не менее 1805...1900 МГц

Эффективный радиус подавления  3...50 м

Питание  однофазная сеть переменного тока с напряжением от 85 до 264 V частотой 47...63 Hz

Мощность, потребляемая от сети 220 V 50 Hz  до 20 W

Габаритные размеры (без антенн)  256×128×36 мм

# 6.3.4. СРЕДСТВА РАДИОКОНТРОЛЯ

## МНОГОКАНАЛЬНЫЙ МОБИЛЬНЫЙ КОМПЛЕКС РАДИОКОНТРОЛЯ ЗДАНИЙ RS TURBO MOBILE M.

Предназначен для защиты объекта – нескольких пространственно разнесенных помещений или здания – от угроз, связанных с несанкционированной передачей информации подслушивающими устройствами или другими радиоэлектронными средствами.

Комплекс проводит автоматизированное сравнение сигналов в контролируемых помещениях и на внешней антенне. Из всех внутренних сигналов выбирается сигнал с максимальным уровнем и указывается его разница относительно опорного сигнала на внешней антенне. Если вновь обнаруженный сигнал превышает уровень во внешней антенне, он заносится в графу "тревога" и может быть блокирован встроенным в систему генератором RS/N.

Автоматическое блокирование может включаться и выключаться программно по желанию оператора.

Комплекс контролирует до 25 каналов в радиодиапазоне и проводных линиях и допускает подключение удаленных устройств: конверторов, генераторов, акустических систем и т.д.

Вся информация о сигналах помещается в компьютерную базу данных, которая в процессе эксплуатации системы заполняется автоматически без участия оператора. Имеется возможность визуального наблюдения в реальном времени одновременно до 8-ми каналов в широкой и узкой полосах.

В состав комплекса входят:

приемник AR5000;

контроллер RS turbo M с программой под Windows 9x/2000/NT/XP;

антенный 8-ми входовый коммутатор RS/K диапазона 2,6 ГГц;

антенна RS/A - 6 шт.; внешняя антенна.

Все устройства комплекса вмонтированы в ударопрочный кейс "Pelican 1520-000"

# Глава 7.
# ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РАБОТЕ СО СРЕДСТВАМИ МАССОВОЙ ИНФОРМАЦИИ

**7.1.** Условия, способствующие нежелательной публикации в СМИ конфиденциальной информации.

**7.2.** Роль органов управления, пресс-службы и службы защиты информации в недопущении утечки конфиденциальной информации через СМИ

**Литература:**

1. Викентьев И.Л., Приемы рекламы и Public Relations, СПб, 1998, с. 14-15, 176-187.

2. Wilcox D.L., Nolte L.W. Public Relations writing and media techniques. - New York, 1995. - P. 232-233).

Оглавление

# 7.1. УСЛОВИЯ, СПОСОБСТВУЮЩИЕ НЕЖЕЛАТЕЛЬНОЙ ПУБЛИКАЦИИ В СМИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

## 7.1.1. УСЛОВИЯ ФОРМИРОВАНИЯ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЧЕРЕЗ СМИ

**1.** Внешние (технико-физические, средовые и т.п.) факторы информационно-коммуникативных ситуаций

**2.** Неудовлетворительный уровень обеспечения информационной безопасности и защиты конфиденциальной информации на предприятии, при котором высока вероятность съема, разглашения и утечки информации с последующим попаданием в СМИ

**3.** Наличие криминальных, асоциальных или аморальных аспектов в деятельности предприятия, его руководства и персонала

**4.** Конфликт интересов с конкурентами и партнерами

**5.** Конфликтная обстановка в коллективе

**6.** Ошибки руководства в подборе персонала, его подготовке и индивидуальной работы с ним

**7.** Применение специальных технологий психологического воздействия при подготовке материалов

## 7.1.2. НОРМАТИВНЫЕ АСПЕКТЫ ФОРМИРОВАНИЯ ВНЕШНИХ ФАКТОРОВ ИНФОРМАЦИОННО-КОММУНИКАТИВНЫХ СИТУАЦИЙ В РАБОТЕ СО СМИ

1. В Российской Федерации цензура СМИ не допускается.

2. Не допускается использование СМИ для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну. В случае разглашения указанных сведений деятельность СМИ по решению учредителя либо судом в порядке гражданского судопроизводства по иску регистрирующего органа может быть прекращена или приостановлена. Редакция СМИ имеет право запрашивать информацию о деятельности государственных органов, общественных объединений, их должностных лиц.

3. Руководители органов, организаций и объединений, их заместители, работники пресс-служб либо другие уполномоченные лица обязаны предоставить СМИ запрашиваемую информацию. Отказ в ее предоставлении возможен, если она содержит сведения, составляющие государственную, коммерческую или иную охраняемую законом тайну. В этом случае руководители в направляемом в СМИ уведомлении обязаны указать причины, по которым запрашиваемая информация не может быть от этих сведений отделена.

4. Журналист имеет право:

искать, запрашивать, получать и распространять информацию;

посещать государственные органы и организации, предприятия и учреждения, органы общественных объединений либо их пресс-службы;

быть принятым должностными лицами в связи с запросом информации;

получать доступ к документам и материалам, за исключением их фрагментов, содержащих сведения, составляющие государственную, коммерческую или иную специально охраняемую законом тайну.

5. Журналист обязан сохранять конфиденциальность полученной информации.

6. В целях реализации прав журналистов редакция СМИ имеет право подать заявку в государственный орган, организацию, учреждение, орган общественного объединения на аккредитацию при них своих журналистов в целях осуществления корреспондентами своей профессиональной деятельности и обеспечения доступа к источникам информации

***Ст. 3, 47-49 Закона РФ «О средствах массовой информации»***

## 7.1.3. ТЕХНОЛОГИИ ВОЗДЕЙСТВИЯ ЧЕРЕЗ СМИ

Формируются и распространяются заранее «сконструированные» образы конкретных лиц, фирм и организаций, идей, программ, товаров и т.п., которые, как правило, неадекватно отражают реальные существенные их характеристики и дезориентируют людей:

*1. Облегчение восприятия последующих пропагандистских материалов: создание атмосферы доверия между коммуникатором (источником информации) и аудиторией*

*2. Привлечение внимания и возбуждения интереса к передаваемым сообщениям, на основании некритического восприятия и усвоения аудиторией получаемой информации: увеличение внушающего эффекта воздействия информации в ущерб ее рациональной оценке*

Информационные сообщения готовятся специалистами, прошедшими подготовку и ориентирующимися на особенности восприятия той или иной информации

Время сообщения информации, канал ее распространения и другие особенности «доставки» адресату, не являются случайными, а диктуются определенным расчетом

Лицо, непосредственно излагающее информацию (диктор, ведущий, комментатор) подбирается и подается таким образом, чтобы вызвать у аудитории симпатию

Подбор приемов привлечения человека сделать выбор источника информации

## 7.1.4. ПРИЕМЫ ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ И ТЕХНИКА ФОРМИРОВАНИЯ ДОВЕРИЯ К КОММУНИКАТОРУ

**ФАЛЬСИФИКАЦИЯ** – намеренное смещение акцентов в показе событий.

**ДЕЗИНФОРМАЦИЯ** – распространение заведомо ложных сведений.

**ДИСКРЕДИТАЦИЯ** – оглашение сведений через СМИ, порочащих государство (общество, личность) и подрывающих доверие к нему.

**НАКЛЕИВАНИЕ ЯРЛЫКОВ** – заключается в подборе эпитетов и такой терминологии, которые дают объекту показа четкую негативную оценку

| | |
|---|---|
| ФОРМИРОВАНИЕ ИМИДЖА «ОСОБОЙ ОСВЕДОМЛЕННОСТИ | «ПСЕВДООБЪЕКТИВНОСТЬ» «АЛЬТЕРНАТИВНЫЙ ГОЛОС» |
| ПЕРЕДАЧА ДОСТОВЕРНЫХ СВЕДЕНИЙ | ВКЛЮЧЕНИЕ В СООБЩЕНИЯ ЭЛЕМЕНТОВ САМОКРИТИКИ |
| ЭКСПЛУАТАЦИЯ БАЗОВЫХ ПОТРЕБНОСТЕЙ ЧЕЛОВЕКА | ПРИМЕНЕНИЕ «ЗАКОНА ПРЕДШЕСТВОВАНИЯ» |
| СОЗДАНИЕ «ЭФФЕКТА ПРИСУТСТВИЯ» | ПРИДАНИЕ СООБЩЕНИЮ ВИДИМОСТИ СЕНСАЦИОННОСТИ |
| «ЗАТРАГИВАНИЕ ЗАПРЕТНЫХ ИЛИ НЕЖЕЛАТЕЛЬНЫХ ТЕМ | ПРЕДСКАЗАНИЕ СОБЫТИЙ |

# 7.1.4а. АЗБУКА ПРОПАГАНДЫ В СМИ

**«Приклеивание или навешивание ярлыков» -** выбор оскорбительных эпитетов, метафор, названий, имен для именования человека, идеи, вызывающих эмоционально негативное отношение окружающих.

**«Сияющие обобщения» -** замена названия, обозначения социального явления, идеи, организации, человека более общим родовым именем, которое имеет положительную эмоциональную окраску и вызывает доброжелательное отношение окружающих для протаскивания решений и взглядов, оценок и действий, выгодных для конкретного лица, группы или организации.

**«Перенос» -** искусное, ненавязчивое и незаметное для большинства людей распространение авторитета или негатива того, что ими ценится или не приветствуется на то, что преподносит источник коммуникации**.**

**«Ссылка на авторитеты» -** приведение высказываний личностей, обладающих высоким авторитетом или таких, которые вызывают отрицательную реакцию тех, на кого направляется манипулятивное воздействие.

**«Свои ребята», или «игра в простонародность» -** установление доверительных отношений с аудиторией, как с близкими по духу людьми на основании того, что коммуникатор, его идеи, предложения, высказывания хороши, так как принадлежат простому народу.

**«Перетасовка» или «подтасовка карт» -** отбор и тенденциозное преподнесение только положительных или только отрицательных фактов и доводов при одновременном замалчивании противоположных.

**Мультипликативность -** дробление подачи информации, избыточность, высокий темп.

**«Общий вагон» -** подбор суждений, высказываний, фраз, требующих единообразия в поведении, создающих впечатление, будто так делают все, хороши, так как принадлежат простому народу.

**«Осмеяние»** как конкретных лиц, так и взглядов, идей, программ, организаций и их деятельности, против которых идет борьба.

**«Метод отрицательных групп отнесения**». Утверждается, что данная совокупность взглядов является единственно правильной. Все те, кто разделяют эти взгляды, обладают какими-то ценными качествами и лучше тех, кто разделяет другие

**«Повторение лозунгов (шаблонных фраз)» -** применение относительно краткого высказывания таким образом, чтобы привлекать внимание и воздействовать на воображение и чувства читателя или слушателя.

**«Эмоциональная подстройка» -** способ создания настроения с помощью различных средств (внешнее окружение, определенное время суток, освещение, легкие возбуждающие средства, театрализованные формы, музыка, песни) с одновременной передачей определенной информации.

**«Мнимый выбор»** - слушателям или читателям сообщается несколько разных точек зрения по определенному вопросу, но так, чтобы незаметно представить в наиболее выгодном свете ту, которую хотят, чтобы она была принята аудиторией.

«**Инициирование информационной волны**» - проведение пропагандистской акции такого характера, когда не содержание самой акции, а ее освещение заставляет значительно большее количество СМИ комментировать первоначальные сообщения, тем самым многократно усиливая мощность психологического воздействия

# 7.2. РОЛЬ ОРГАНОВ УПРАВЛЕНИЯ, ПРЕСС-СЛУЖБЫ И СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ В НЕДОПУЩЕНИИ УТЕЧКИ ИНФОРМАЦИИ ЧЕРЕЗ СМИ

## 7.2.1. РОЛЬ ОРГАНОВ УПРАВЛЕНИЯ В ФОРМИРОВАНИИ УСЛОВИЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННННОЙ БЕЗОПАСНОСТИ

1. Анализ внешних факторов информационно-коммуникативных ситуаций, повышающих или снижающих действенность психологического воздействия

2. Поддержание информационной безопасности и уровня защиты конфиденциальной информации на предприятии, при котором обеспечивается снижение вероятности съема, разглашения и утечки информации с последующим попаданием в СМИ

3. Устранение криминальных, асоциальных и аморальных аспектов в деятельности предприятия, его руководства и персонала

4. Своевременное разрешение конфликтов с конкурентами и партнерами

5. Управление моральной обстановкой в в коллективе и управление конфликтами

6. Тщательный подбор персонала, его подготовка и индивидуальная работа с ним

7. Оценка и нейтрализация специальных технологий психологического воздействия в материалах СМИ

## 7.2.2. ОСНОВНЫЕ НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ РАБОТЫ СО СМИ

**проведение оценки материалов**, передаваемых журналистам, на предмет отсутствия в них конфиденциальной информации;

**соблюдение установленных требований** режима конфиденциальности информации при проведении на территории предприятия (его объектах) **мероприятий с участием представителей СМИ**;

**регламентация проведения посещений**, встреч, интервью и других мероприятий, организуемых по инициативе СМИ;

исключение утечки конфиденциальной информации в ходе мероприятий, проводимых с участием журналистов **по инициативе предприятия;**

подготовка официальных сообщений, не содержащих конфиденциальной информации, **в целях информирования СМИ о деятельности предприятия.**

# 7.2.3. ЗАДАЧИ РУКОВОДСТВА ПРЕДПРИЯТИЯ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕШАЕМЫЕ С ПРИМЕНЕНИЕМ СМИ

***ЗА ПРЕДЕЛАМИ ПРЕДПРИЯТИЯ:***

- навязывание конкуренту принятия и реализации решений, выгодных для обеспечения интересов предприятия;
- содействие разрешению противоречий между партнерами без открытого (прямого) конфликта;
- информационная поддержка мероприятий, проводимых руководством в целях укрепления своей позиции, совершенствования организации, укрепления и всестороннего обеспечения деятельности предприятия;
- убеждение общественного мнения в правильности и необходимости деятельности предприятия;
- создание обстановки неуверенности и беспокойства среди конкурентов;
- противодействие негативному психологическому воздействию, нацеленному на дискредитацию учреждения;

***ВНУТРИ ПРЕДПРИЯТИЯ:***

- разъяснение персоналу политики предприятия;
- демонстрация высокого потенциала предприятия, решимости руководства достичь успеха в конкурентной борьбе;
- воспитание персонала моральных ценностей, норм и принципов поведения, направленных на укрепление коллектива и повышение эффективности деятельности;
- разъяснение существующих угроз информационной безопасности предприятия;
- противодействие акциям, направленным на снижение престижа предприятия, авторитета руководства

# 7.2.4. НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ ПУБЛИКАТОРСКОЙ ДЕЯТЕЛЬНОСТИ

**ОПРЕДЕЛЕНИЕ ТЕМАТИКИ ИЗДАВАЕМЫХ МАТЕРИАЛОВ** в целях исключения из них тематик, содержащих конфиденциальную информацию, подготовки рекомендаций по исключению из них иной актуальной информации, распространение которой может нанести ущерб предприятию.

**ПИСЬМЕННОЕ СОГЛАСОВАНИЕ СОДЕРЖАНИЯ МАТЕРИАЛОВ И ВОЗМОЖНОСТИ ИХ ИЗДАНИЯ С ОРГАНИЗАЦИЯМИ-ОБЛАДАТЕЛЯМИ ИНФОРМАЦИИ.**

**ПРЕДВАРИТЕЛЬНАЯ ЭКСПЕРТИЗА МАТЕРИАЛОВ, ГОТОВЯЩИХСЯ К ИЗДАНИЮ, ЭКСПЕРТНОЙ КОМИССИЕЙ ПРЕДПРИЯТИЯ** (ст.5 Закона РФ «О государственной тайне», Перечень сведений, отнесенных к государственной тайне, перечень сведений, составляющих коммерческую тайну предприятия).

**ОКОНЧАТЕЛЬНАЯ ВЫБОРОЧНАЯ ЭКСПЕРТИЗА ПОДГОТОВЛЕННЫХ К ИЗДАНИЮ МАТЕРИАЛОВ, ОПРЕДЕЛЕНИЕ ТИРАЖА И СПОСОБА ИХ РАСПРОСТРАНЕНИЯ.**

**КОНТРОЛЬ ЗА ВЫПОЛНЕНИЕМ РАБОТ ПО ИЗДАНИЮ** (тиражированию, размеще-нию) материалов непосредственно в типографии или иной организации в зависи-мости от выбранного способа распространения.

**ОРГАНИЗАЦИЯ ПОДГОТОВКИ МАТЕРИАЛОВ К ОТКРЫТОМУ ОПУБЛИКОВАНИЮ**

# 7.2.5. МЕРЫ, ИСКЛЮЧАЮЩИЕ ОТКРЫТОЕ ОПУБЛИКОВАНИЕ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ В ПЛАНЕ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

- разработка и **утверждение руководителем предприятия организационно-распорядительных документов**, определяющих порядок и особенности работы по подготовке материалов к открытому опубликованию;
- **предварительный анализ материалов и их согласование** с руководителями структурных подразделений предприятия, сотрудники которых осуществляют их подготовку к открытому опубликованию;
- **анализ материалов**, готовящихся к открытому распространению, службой безопасности (режимно-секретным подразделением) предприятия;
- **выборочный контроль** изданных (опубликованных) материалов;
- проведение занятий с сотрудниками предприятия по изучению положений нормативных правовых актов и внутренних организационных документов предприятия;
- **взаимодействие с должностными лицами издательств,** типографий, СМИ;
- **определение состава экспертной комиссии предприятия** по оценке возможности опубликования материалов и осуществление ее деятельности;
- **взаимодействие с другими предприятиями** по вопросам открытого опубликования материалов, содержащих информацию о проводимых этими предприятиями совместных и других работах, а также с органами государственной власти и предприятиями, являющимися заказчиками работ и обладателями информации, которую планируется открыто опубликовать, получение письменного согласия этих органов (предприятий) на открытое опубликование материалов;
- **проведение периодического анализа эффективности проводимых мероприятий** по исключению открытого опубликования конфиденциальной информации и совершенствование этой работы на предприятии.

## 7.2.4. ЗАДАЧИ ПРЕСС-СЛУЖБЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

- информационное обеспечение деятельности руководства в части, касающейся связей с общественностью и средствами массовой информации;
- подготовка и распространение в средствах массовой информации официальных заявлений и сообщений;
- планирование и организация выступлений руководства в средствах массовой информации;
- подготовка и проведение пресс-конференций, брифингов, заседаний пресс-клуба с участием руководства;
- распространение материалов в средствах массовой информации;
- поддержание постоянных связей со средствами массовой информации, информационными структурами органов государственной власти, общественных организаций;
- систематический анализ и прогнозирование информационной ситуации вокруг предприятия, выработка предложений по ее улучшению;
- организация размещения информации о жизни и деятельности предприятия и его персонала на сайте в Интернете;
- разработка и контроль за реализацией плана информационного сопровождения мероприятий повседневной деятельности;
- обеспечение информационной безопасности в средствах массовой информации в порядке, установленном нормативными правовыми актами РФ

## 7.2.5. ФОРМЫ РАБОТЫ СО СМИ

### *ОБЩИЕ*

- Подготовка сообщений и пресс-релизов
- Проведение пресс-конференций и брифингов
- Посещение объектов журналистами
- Присутствие журналистов на мероприятиях
- Официальные комментарии
- Организация встреч с представителями СМИ

### *СПЕЦИАЛЬНЫЕ*

- «Вброс» или «утечка» информации
- Неформальные контакты с представителями СМИ
- Беседы «для фона»
- Размещение материалов в СМИ на правах рекламы
- Организация информационных поводов

ПОДГОТОВКА СООБЩЕНИЙ (МАТЕРИАЛОВ, ПРОГРАММ) – форма распространения специально подготовленной информации в виде материалов для опубликования в печати (выхода в эфир) в теле-, радио-передачах и в Интернет

ПРЕСС-РЕЛИЗ – документ для СМИ (1-2 машинописные страницы), содержащий акту-альную информацию

ПРЕСС-КОНФЕРЕНЦИИ – встречи представителей с журналистами, предполагающие выступление должностных лиц с целью предоставления информации по заранее заявленной теме

БРИФИНГ – односторонне доведение информации, не предполагающее высказывания мнений, оценок, вопросов и т.д. Официальный представитель сообщает или зачитывает информацию

# 7.2.6. ТЕХНИКА РАБОТЫ С ПРЕССОЙ

## В области "демонстрации статуса":

заполненное расписание, куда невозможно попасть;
переполненная приемная;
набор секретарей, охранников, водителей.

## Для эффективной работы с прессой:

1. ***Знайте ваши масс-медиа***, публикации, аудиторию.
2. ***Сократите рассыл материалов*** (многочисленные пресс-релизы дороги и неэффективны).
3. ***Вводите местную специфику*** (наиболее эффективные материалы связаны с ней).
4. ***Шлите новостную информацию*** (не рассылайте то, что не представляет интереса).
5. ***Пишите хорошо*** (новости должны быть изложены качественно и кратко).
6. ***Избегайте трюков*** (не пересылайте подарков, чтобы привлечь внимание журналистов).
7. ***Будьте доступным для журналистов,*** если вы отвечаете за связи с прессой.
8. ***Возвращайтесь к проблемам*** (если вы говорите репортерам, что сообщите дополнительную информацию, поскольку сейчас вы ее не имеете, обязательно сделайте это).
9. ***Отвечайте на звонки*** (репортеры не любят электронных автоответчиков).
10. ***Будьте искренни*** (давайте полную информацию, даже если она не совсем приятна).
11. ***Отвечайте на вопросы*** (Три вида принятых ответов: "Вот он", "Я не знаю, но я перезвоню вам в течение часа" и "Я знаю, но сейчас не могу сказать вам, потому что ...").
12. ***Сохраняйте эксклюзивность*** (Если вы дали информацию, не отдавайте ее кому-то).
13. Будьте справедливы (Конкурирующие масс-медиа заслуживают равные возможности)
14. ***Помогайте фоторепортерам*** (собирая людей, предоставляя точные имена и названия).
16. ***Объясняйте*** (Давайте репортерам материалы для понимания вашей организации, как и почему принимаются те или иные решения).
17. ***Помните о сроках*** (Информация должна поступать заранее, чтобы успеть написать статью).
18. ***Хвалите хорошую работу*** (Если журналист написал хорошую статью, пошлите ему благодарственное письмо).
19. ***Исправляйте вежливо ошибки*** (На небольшие ошибки обращать внимания не стоит).

# Глава 8.
# ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ В РЕКЛАМНО-ВЫСТАВОЧНОЙ ДЕЯТЕЛЬНОСТИ

**8.1.** Условия, способствующие утечке конфиденциаль-ной информации в рекламной деятельности.

**8.2.** Роль органов управления, рекламной службы и службы защиты информации в недопущении утечки конфиденциальной информации в рекламной деятельности.

**8.3.** Противодействие манипуляции в ходе восприятия потребительской рекламы

**Литература:**

1. Викентьев И.Л. Приемы рекламы и Public Relations, СПб, 1998, с. 14-15, 176-187.

2. http://all-ib.ru/content/zashita-replami/zashita_replami_part_13.html

# 8.1. УСЛОВИЯ, СПОСОБСТВУЮЩИЕ УТЕЧКЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

## 8.1.1. БАЗОВЫЕ ПОНЯТИЯ

**РЕКЛАМА – информация, распространенная любым способом, в любой форме и с использованием любых средств, адресованная неопределенному кругу лиц и направленная на привлечение внимания к объекту рекламирования, формирование или поддержание интереса к нему и его продвижение на рынке (например, продвижение сайта в ИНТЕРНЕТе).**

**ОБЪЕКТ РЕКЛАМИРОВАНИЯ – товар, средство его индивидуализации, изготовитель или продавец товара, результаты интеллектуальной деятельности либо мероприятие (в т. ч. спортивное соревнование, концерт, конкурс, фестиваль, основанные на риске игры, пари), на привлечение внимания к которым направлена реклама.**

**НЕНАДЛЕЖАЩАЯ РЕКЛАМА – реклама, не соответствующая требованиям законодательства.**

**РЕКЛАМОДАТЕЛЬ – изготовитель или продавец товара, либо иное определившее объект рекламирования и (или) содержание рекламы лицо.**

**РЕКЛАМОПРОИЗВОДИТЕЛЬ – лицо, осуществляющее полностью или частично приведение информации в готовую для распространения в виде рекламы форму.**

**РЕКЛАМОРАСПРОСТРАНИТЕЛЬ – лицо, осуществляющее распространение рекламы любым способом, в любой форме и с использованием любых средств.**

**ПОТРЕБИТЕЛИ РЕКЛАМЫ – лица, на привлечение внимания которых к объекту рекламирования направлена реклама**

## 8.1.2. ВИДЫ РЕКЛАМЫ

**НАРУЖНАЯ РЕКЛАМА** - реклама, размещаемая на рекламных конструкциях (щитах, стендах, строительных сетках, перетяжках, электронных табло и иных технических средствах стабильного территориального размещения, монтируемых и располагаемых на внешних стенах, крышах и т.п., а также на остановочных пунктах движения общественного транспорта) – в местах общего пользования.

**РЕКЛАМА НА ТЕЛЕВИДЕНИИ И РАДИО, А ТАКЖЕ В ПЕРИОДИЧЕСКИХ ПЕЧАТНЫХ ИЗДАНИЯХ.**

**РЕКЛАМА, РАСПРОСТРАНЯЕМАЯ ПО СЕТЯМ ЭЛЕКТРОСВЯЗИ И РАЗМЕЩАЕМАЯ В ПОЧТОВЫХ ОТПРАВЛЕНИЯХ.**

**РЕКЛАМА НА ТРАНСПОРТНЫХ СРЕДСТВАХ** (маршрутное такси, автобусы, электротранспорт) и с их использованием.

**РЕКЛАМА В ХОДЕ ПРОВЕДЕНИЯ КОНФЕРЕНЦИЙ, СИМПОЗИУМОВ,** организуемых и проводимых вне предприятия.

**РЕКЛАМА, РАЗМЕЩАЕМАЯ В ГЛОБАЛЬНЫХ ИНФОРМАЦИОННЫХ СЕТЯХ ОБЩЕГО ПОЛЬЗОВАНИЯ.**

**РЕКЛАМА В ХОДЕ ПРОВЕДЕНИЯ ВНУТРЕННИХ МЕРОПРИЯТИЙ С ПРИВЛЕЧЕНИЕМ (ПРИГЛАШЕНИЕМ, УЧАСТИЕМ) ПРЕДСТАВИТЕЛЕЙ СТОРОННИХ ОРГАНИЗАЦИЙ И СМИ.**

## 8.1.3. УСЛОВИЯ ФОРМИРОВАНИЯ УГРОЗ ЗАЩИТЕ ИНФОРМАЦИИ В РЕКЛАМНО-ВЫСТАВОЧНОЙ ДЕЯТЕЛЬНОСТИ

**1.** Внешние (технико-физические, средовые и т.п.) факторы информационно-коммуникативных ситуаций и высокая вероятность анализа конкурентом рекламно-выставочного материала

**2.** Слабый уровень обеспечения информационной безопасности и защиты конфиденциальной информации на предприятии, при котором высока вероятность безответственного разглашения информации в ходе рекламно-выставочной деятельности

**3.** Бесконтрольность деятельности и халатность руководства предприятия, рекламной службы и персонала

**4.** Слабая подготовленность персонала в области обеспечения информационной безопасности и недостаточная индивидуальная работа с ним со стороны руководства

**5.** Неудовлетворительное противодействие силам и средствам шпионажа

# 8.2. РОЛЬ ОРГАНОВ УПРАВЛЕНИЯ, РЕКЛАМНОЙ СЛУЖБЫ И СЛУЖБЫ ЗАЩИТЫ ИНФОРМАЦИИ В НЕДОПУЩЕНИИ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ

## 8.2.1. НАПРАВЛЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ХОДЕ РЕКЛАМНО-ВЫСТАВОЧНОЙ ДЕЯТЕЛЬНОСТИ

- **ПОДГОТОВКА И ЭКСПЕРТИЗА МАТЕРИАЛОВ, ПРЕДНАЗНАЧЕННЫХ ДЛЯ ПОЛЬЗОВАНИЯ В РЕКЛАМНОЙ ДЕЯТЕЛЬНОСТИ, НА ПРЕДМЕТ ОТСУТСТВИЯ НИХ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ.**

- **АНАЛИЗ МАТЕРИАЛОВ В ПРОЦЕССЕ ИХ ПОДГОТОВКИ РЕКЛАМО-ПРОИЗВОДИТЕЛЕМ И РЕКЛАМОРАСПРОСТРАНИТЕЛЕМ К РАЗМЕЩЕНИЮ В СРЕДСТВАХ РЕКЛАМЫ.**

- **ПОСТОЯННЫЙ КОНТРОЛЬ ПОРЯДКА РАСПРОСТРАНЕНИЯ И СОДЕРЖА-НИЯ РЕКЛАМНЫХ МАТЕРИАЛОВ НЕЗАВИСИМО ОТ СПОСОБА, ФОРМЫ И ПЕРИОДИЧНОСТИ ИХ РАСПРОСТРАНЕНИЯ.**

- **ПРОВЕДЕНИЕ КОМПЛЕКСА МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ:**

проведение комиссией предприятия экспертизы подготовленных к распространению материалов:

анализ возможных форм, способов распространения рекламных материалов и непосредственное взаимодействие в процессе подготовки и распространения материалов с рекламопроизводителем и рекламораспространителем;

оценка комиссией предприятия, состоящей из компетентных специалистов, содержания рекламных материалов на предмет возможности их распространения

# 8.2.2. ОЦЕНКА МАТЕРИАЛА, ПОДЛЕЖАЩЕГО ПУБЛИКАЦИИ, ЭКСПЕРТНОЙ КОМИССИЕЙ

**Экспертная комиссия создается сроком на один календарный год.**

**Состав экспертной комиссии** – сотрудники предприятия-специалисты в различных областях деятельности, в необходимых случаях, с допуском к государственной тайне.

**Могут привлекаться**: руководитель структурного подразделения, в котором работает автор подготовленного материала; представители других предприятий, имеющих отношение к рассматриваемым материалам (являющихся собственниками информации, заказчиками а также к иным видам конфиденциальной информации), составители, руководители или редакторы работы (материалов). Вопрос о привлечении этих специалистов к работе в составе комиссии письменно согласовывается с руководителями соответствующих предприятий.

**Не могут входить в состав комиссии:**

сотрудники службы безопасности и режимно-секретного подразделения.

**При подготовке и проведении экспертизы члены экспертной комиссии обязаны**:

- знать перечни сведений, запрещенных к открытому опубликованию на предприятии, и строго руководствоваться ими при проведении экспертизы;
- при обнаружении в рассматриваемых материалах сведений, составляющих государственную, коммерческую, служебную тайну, вынести заключение, запрещающее их открытое опубликование;
- проверять наличие письменного согласия руководителей предприятий-заказчиков работ на опубликование материалов или контролировать выполнение рекомендаций (заключений) этих руководителей;
- рассматривать материалы с учетом ранее опубликованных работ, имеющих отношение к этим материалам, с тем, чтобы готовящаяся публикация не привела к разглашению конфиденциальной информации и нанесению, таким образом, ущерба предприятию;
- при рассмотрении сборников материалов (статей) принимать решение о возможности опубликования (издания) как всего сборника в целом, так и его отдельных статей (материалов).

## 8.2.3. ЭКСПЕРТИЗА МАТЕРИАЛА, ПОДЛЕЖАЩЕГО ПУБЛИКАЦИИ

**Члены экспертной комиссии имеют право:**

получать от автора (авторов) письменное подтверждение об источниках, использованных им при подготовке материалов к опубликованию, а также иную информацию, необходимую для подготовки заключения;

обращаться в установленном порядке за консультацией (разъяснениями) на другие предприятия, в органы государственной власти и к их должностным лицам.

**Экспертная комиссия готовит заключение** о возможности (невозможности) их открытого опубликования. Экспертное заключение подписывается всеми членами комиссии, ее руководителем (председателем) и утверждается руководителем предприятия - организатора экспертизы.

**При отсутствии единого мнения** экспертов и невозможности формулирования вывода по результатам изучения материалов вопрос о возможности опубликования **решается руководителем вышестоящей организации** (органа государственной власти). В исключительных случаях, при отсутствии вышестоящей организации (органа государственной власти) решение о возможности открытого опубликования материалов выносится руководителем предприятия самостоятельно либо совместно с руководителем предприятия-заказчика проводимых совместных работ.

**Если заключение экспертной комиссии о возможности открытого опубликования материалов – положительное**, оно в установленном порядке вместе с рассмотренными материалами передается в службу безопасности (режимно-секретное подразделение) предприятия или уполномоченному должностному лицу для принятия окончательного решения.

После получения разрешения подготовленные материалы **в установленном порядке передаются в издательство** (редакцию, представителям СМИ) для их опубликования (открытого распространения).

# 8.2.4. ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ В РЕКЛАМНО-ВЫСТАВОЧНОЙ ДЕЯТЕЛЬНОСТИ

**Утрата ценной информации на выставке происходит за счет:**

общения специалистов родственных профессий, но разных фирм;

наличия в выставочной экспозиции нового продукта;

проведения параллельно с выставочными мероприятиями пресс-конференций и пр.

**Источники ценных сведений в процессе выставочной деятельности:**

экспозиция, персонал фирмы и рекламно-выставочные материалы.

**Требования к действиям организаторов при подготовке и проведении выставки:**

1. Работа с посетителями выставки должна быть строго регламентирована, прежде всего, в части состава оглашаемых сведений о продукции и всех новшествах.

2. Состав сведений дифференцируется в зависимости от категории посетителей – посетителя-дилетанта (“любителя”) и посетителя-специалиста (“эксперта”).

3. Посетителю сообщается все, что касается назначения продукции и ее потребительских качеств, но остаются в тайне технология и способы, которыми достигнуты эти качества, и технические возможности продукции. Персоналу, обслуживающему экспозицию, не следует знать сведения о продукции, отнесенные к производственной или коммерческой тайне. Специалисты, осведомленные в секретах, не должны участвовать в работе выставки.

4. Рекламно-выставочные материалы (проспекты, прайс-листы, брошюры) рассматриваются как канал распространения сведений, который тщательно анализируется конкурентом с целью выявления сведений, которые составляют тайну фирмы.

5. В ходе защиты информации предусмотреть: заблаговременный анализ в целях обнаружения в содержании или элементах отображения (таблицах, формулах и пр.) конфиденциальных сведений; последующий контроль всех опубликованных материалов, сообщений СМИ, рекламных изданий и проспектов; анализ материалов других фирм для определения возможной утраты сведений.

6. В целях предотвращения разглашения сведений следует заблаговременно:

проанализировать все материалы с точки зрения возможности извлечения из них ценных, конфиденциальных сведений при сопоставлении показателей и обобщений сведений;

осуществить дробление информации между разными рекламно-выставочными материалами для массового посетителя и специалистов и издание серии дополнений к основному проспекту для специалистов разного профиля;

осуществить разбиение информации по видам и средствам рекламы – бумажным изданиям, электронной рекламе, Web-странице, рекламе в средствах массовой информации и др.

# 8.3. ПРОТИВОДЕЙСТВИЕ МАНИПУЛЯЦИИ В ХОДЕ ВОСПРИЯТИЯ ПОТРЕБИТЕЛЬСКОЙ РЕКЛАМЫ

## 8.3.1. ОТНОШЕНИЯ ВЗАИМОЗАВИСИМОСТИ МЕЖДУ РЕКЛАМОЙ И ЧЕЛОВЕКОМ

- **реклама способствует получению новой информации,** которая может помочь при разрешении жизненных или бытовых проблем;
- **реклама поддерживает и утверждает индивидуальные и социальные ценности**, способствуя укреплению или возникновению позиций и убеждений;
- реклама **предлагает человеку пережить те или иные психологические эмоции;**
- реклама **позволяет пережить эстетические эмоции**, способствует возникновению или усилению различных эстетических предпочтений;
- реклама **способствует возникновению состояния комфорта**

## 8.3.2. УГРОЗА МАНИПУЛИРОВАНИЯ В РЕКЛАМНОМ СООБЩЕНИИ

## 8.3.3. ТИПЫ МАНИПУЛЯТИВНОЙ РЕКЛАМЫ И ВИДЫ КОММУНИКАТИВНЫХ ИСКАЖЕНИЙ

**ПРЯМАЯ ДЕЗОРИЕНТАЦИЯ, ЛОЖЬ**
(признаки: слова «лучший», «самый», «исключительный»)

**КОСВЕННАЯ ДЕЗОРИЕНТАЦИЯ, ВВЕДЕНИЕ В ЗАБЛУЖДЕНИЕ**
(предоставление части информации о товаре, например, о лечебном эффекте от лекарств, с утаиванием противопоказаний и побочных эффектов)

**НАРУШЕНИЕ ЛОГИЧЕСКИХ СВЯЗЕЙ, ПОДМЕНА ПРИЧИНЫ СЛЕДСТВИЕМ** (ложный силлогизм: «С тех пор, как она пользуется этим стиральным порошком, ее белье выглядит всегда безупречно»)

**ВОЗДЕЙСТВИЕ НА ПОДСОЗНАНИЕ ПОТРЕБИТЕЛЯ**

**ВИДЫ КОММУНИКАТИВНЫХ ИСКАЖЕНИЙ В РЕКЛАМЕ:**

НАИВНЫЙ РЕАЛИЗМ: убежденность в том, что рекламная информация – есть истина в последней инстанции, что цель рекламы – только расширить представления потребителей и помочь им точнее ориентироваться в мире товаров и услуг

ЛОГИЧЕСКИЙ СУБЪЕКТИВИЗМ: выработка собственных критериев объективности рекламного сообщения, построенного на сравнении разных рекламных сообщений об одном и том же товаре

СКЕПТИЧЕСКИЙ СУБЪЕКТИВИЗМ: негативная оценка любого рекламного сообщения в случае несовпадения ее с имеющимися убеждениями или установками личности

## 8.3.4. ТИПИЧНЫЕ МАНИПУЛЯТИВНЫЕ ПРИЕМЫ В РЕКЛАМЕ

## 8.3.5. ЗАДАЧИ И МЕТОДЫ НЕЙТРАЛИЗАЦИИ МАНИПУЛЯТИВНОГО ВОЗДЕЙСТВИЯ

1. Своевременное **обнаружение факта** манипулятивного воздействия и его направленности

2. **Прогнозирование вероятной цели** и последствий воздействия (изменение поведения, взглядов, оценок, возможный ущерб и т.п.)

3. **Формирование адекватной ответной реакции**, собственного поведения в ситуации манипулятивного воздействия

**МЕТОДЫ:**

**физический:** регулярные занятия спортом, любая физическая сосредоточенная работа

**эмоциональный:** заполнение своего досуга после работы хорошей музыкой, фильмами, общением с друзьями – всем, что несет живые положительные эмоции

**интеллектуальный:** приобретение и наличие элементарных знаний о том, что такое манипуляции, и как распознать негативную рекламу

# Глава 9.
# МЕТОДИКА ОЦЕНКИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**9.1.** Источники и методы сбора информации об уровне информационной безопасности.

**9.2.** Оценка достоверности сведений.

**9.3.** Аналитическое выявление угроз информационной безопасности

**9.4.** Алгоритмы анализа информационной обстановки в интересах обеспечения информационной безопасности.

**Литература:**

1. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Фонд «Мир», 2003. – 640 с.

2. Курносов Ю.В., Конотопов П.Ю. Аналитика: методология, технология и организация информационно-аналитической работы. – М.: Издательство «Русаки», 2004 г. – 550 с.

3. Герасименко В.А., Малюк А.А. Основы защиты информации. Учебник. – М.: МИФИ, 1997. – 537 с.

# 9.1 ИСТОЧНИКИ И МЕТОДЫ СБОРА ИНФОРМАЦИИ ОБ УРОВНЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
## 9.1.1. БАЗОВЫЕ ПОНЯТИЯ

**Данные (факты) –** совокупность знаков (текстов, изображений и т.д.) фиксирующая явления окружающей деятельности.

**Сведения (мнения)** – представления, личностные предложения, которые возникают у субъекта в результате восприятия и анализа данных.

**Информация** – это новое в сведениях. Количество информации в данных – степень их новизны.

**Информационная характеристика** такого объекта как информация может содержать классификационные признаки информации, принадлежность к мировоззренческий, смысловой, мотивационный, хронологический, фактологический и др. видам информации, а также отраслям знаний и отражать такие ее свойства, как качество, содержательность, т.е. значимость (актуальность, новизна, важность, идентичность, истинность); достоверность (помехоустойчивость, помехозащищенность), сохранность (целостность, готовность) и конфиденциальность (доступность, скрытность).

**Носитель данных –** предмет, компоненты которого используются в качестве знаков.

**Источник данных –** обладатель или производитель носителей данных.

**Канал передачи данных –** путь поступления данных к их потребителю.

**Документ –** носитель визуально воспринимаемых данных, составляющих целостный набор.

**Значимость информации**. Информация может быть одновременно и важной и бесполезной, поскольку ее может оказаться недостаточно для понимания сущности процесса, единичного события или явления в целом.

**Важность информации**: информация является важной, если она *релевантна* (имеет связь с решением проблемы), и если ее использование может внести вклад в текущую или планируемую деятельность.

**Критерии достоверности информации**:

*обоснованности* (наличие подтверждений полученной информации в ряде независимых источников);

*непротиворечивости* (отсутствие противоречий между отдельными утверждениями; отсутствие противоречий внутри группы сообщений, поступивших одного и/или группы источников за некий промежуток времени; отсутствие противоречий с имеющимися моделями интерпретации и моделями предметной области;

*авторитетности источника* и/или степени защищенности носителя (документа).

# 9.1.2. ИСТОЧНИКИ ИНФОРМАЦИИ И СПОСОБЫ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

| № п/п | ИСТОЧНИКИ | СПОСОБЫ | | | | | | | | | | | | | | ОБЩЕЕ КОЛ-ВО ПО ИСТОЧНИКУ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Инициативное сотрудничество | Склонение к сотрудничеству | Выпытывание | Подслушивание | Наблюдение | Хищение | Копирование | Подделка (модификация) | Уничтожение (порча) | Незаконное подключение | Перехват | Негласное ознакомление | Фотографирование | Сбор и аналитич. обработка | |
| 1 | **Люди** | v | v | v | v | v | v | | | | | | | v | | 7 |
| 2 | **Документы** | | | | | v | v | v | v | v | | | v | v | v | 8 |
| 3 | **Публикации** | | | | | | | | v | | | | | | v | 2 |
| 4 | **Технические носители** | | | | | | v | v | v | v | | | v | | | 5 |
| 5 | **Технические средства АСОД, СПД** | | | | | | v | v | v | v | v | v | v | | | 7 |
| 6 | **Продукция** | | | | | v | v | v | v | v | | | v | v | | 7 |
| 7 | **Отходы** | | | | | v | v | | | | | | | v | v | 4 |
| | **ИТОГО** | 1 | 1 | 1 | 1 | 4 | 6 | 4 | 5 | 4 | 1 | 1 | 4 | 4 | 3 | 40 |

# 9.1.3. ЭТАПЫ И МЕТОДЫ СБОРА ИНФОРМАЦИИ ОБ УЯЗВИМОСТЯХ СИСТЕМЫ ЗАЩИТЫ

**ПРЕДВАРИТЕЛЬНЫЙ**
Организационные и технологические мероприятия по сбору данных

**ОСНОВНОЙ**
Аналитическая обработка данных
Формулирование выводов
Прогнозирование

**ЗАКЛЮЧИТЕЛЬНЫЙ**
Оформление и доклад полученных результатов

**МЕТОДЫ АНАЛИЗА**

- графический,
- морфологический,
- системный,
- математический (теоретико-вероятностный, статистический, временных рядов, теоретико-игровое моделирование и др.)
- логический,
- экспертный,
- концептуальный,
- структурный (кластерный),
- ресурсный,
- корреляционный,
- факторный (причинно-следственный),
- ретроспективный,
- семантический,
- показателей эффективности,
- логико-лингвистический,
- анализ вариаций,
- сравнительный и др.

**Анализ**

**Синтез**

**Сравнение**

**Обобщение**

**Аналогирование**

**Построение структурных моделей информационной обстановки**

**Исследование структурных моделей информационной обстановки**

**Формирование итоговой модели и выводов из оценки информационной обстановки**

**Прогноз развития информационной обстановки**

# 9.1.4. СБОР ИНФОРМАЦИИ ОБ УЯЗВИМОСТИ КАНАЛОВ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

**Обнаружение канала или каналов несанкционированного доступа к ценной информации включает в себя:**

- анализ источников конфиденциальной информации;
- анализ каналов объективного распространения информации;
- аналитическую работу с источником угрозы информации.

**Аналитическое исследование источников конфиденциальной информации предусматривает:**

- выявление и классификацию существующих и возможных конкурентов и соперников фирмы, криминальных структур и отдельных элементов, интересующихся фирмой;
- выявление и классификацию максимально возможного числа источников конфиденциальной информации фирмы;
- выявление, классификацию и ведение перечня (учетного аппарата) реального состава циркулирующей в фирме конфиденциальной информации в разрезе источников, обеспечиваемых функций и видов работы, с указанием носителей;
- изучение данных учета осведомленности сотрудников в тайне фирмы, т.е. изучение степени и динамики реального владения сотрудниками конфиденциальной информацией;
- изучение состава конфиденциальной информации в разрезе документов, т.е. изучение правильности расчленения тайны (конфиденциальной информации) между документами и определение избыточности ценной информации в документах;
- учет и изучение выявленных внутренних и внешних, потенциальных и реальных (пассивных и активных) угроз каждому отдельному источнику информации, контроль процесса формирования канала несанкционированного доступа к информации;
- ведение и анализ полноты перечня защитных мер, предпринятых по каждому источнику, и защитных мер, которые могут быть использованы при активных действиях злоумышленника.

# 9.1.5. ПРИНЦИПЫ ИНФОРМАЦИОННОЙ РАБОТЫ

1. **Цель** – подход к решению любой информационной задачи зависит от того, в каких целях будут использованы полученные результаты, чем определяется масштаб, формы и методы работы.
2. **Определение понятий** – установить с помощью подходящего определения точный смысл каждого термина (тип конкуренции, инфраструктуры – социальной, промышленной, криминальной т.д.)
3. **Использование всех возможных источников** – тщательное исследование источников, из которых можно почерпнуть сведения, выяснение вероятных возможностей и пределов использования каждого источника, в какой степени содержащиеся в них данные подтверждают или опровергают друг друга.
4. **Раскрытие значений фактов или повышение их полезности** – смысл фактов, сравнение данных с аналогичными данными раннего периода или с данными того же рода в отношении аналогичной организации.
5. **Установление причинно-следственных связей** – уяснение движущих сил событий.
6. **Определение тенденции развития** – возможное направление развития событий в будущем.
7. **Степень достоверности** (высокая, средняя, низкая) – точность цифрового материала и правильность оценок и выводов
9. **Выводы** – определяются той целью, которая была поставлена, в форме ответа на вопрос "Что означает данное явление?".

# 9.2. ОЦЕНКА ДОСТОВЕРНОСТИ СВЕДЕНИЙ
## 9.2.1. АНАЛИЗ И ОЦЕНКА ДАННЫХ

**КАТЕГОРИИ ДАННЫХ:**

**1) базовая информация - для сравнения;**
**2) текущая информация о фактах;**
**3) умозрительно-оценочные категории с оценками и предупреждениями.**

**АНАЛИТИЧЕСКИЕ ИНСТРУМЕНТЫ АНАЛИЗА И ОЦЕНКИ:**

**1) Надежность источника:**
а) совершенно надежный;
б) обычно надежный;
в) довольно надежный;
г) не всегда надежный;
д) ненадежный;
е) надежность не может быть определена.

**2) Достоверность информации:**
а) достоверность подтверждена;
б) вероятно (возможно) правдивая;
в) сомнительная;
г) неправдоподобная;
д) достоверность не может быть определена.

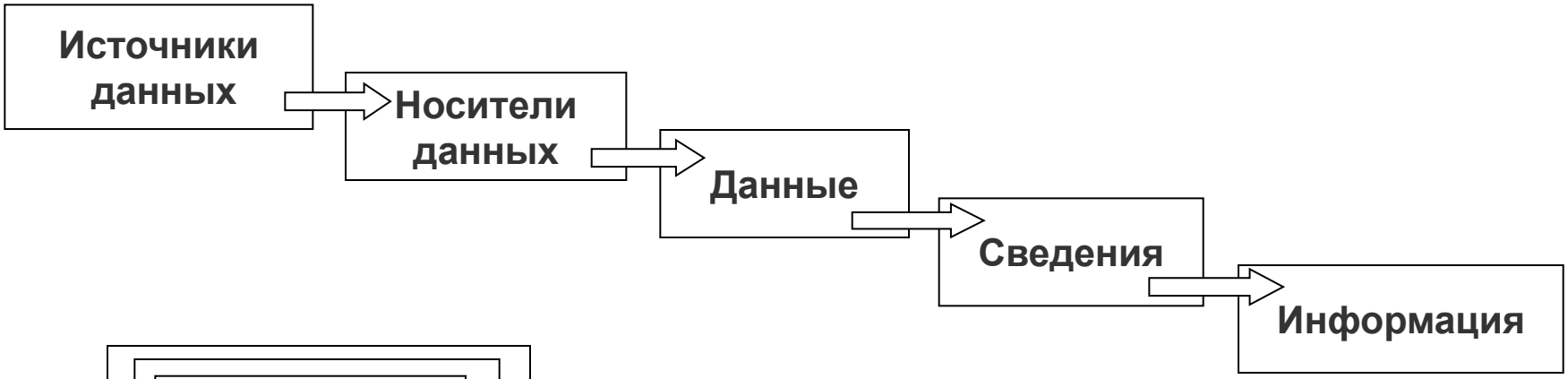
**3) Направленность информации:**
а) обзорные, апологетические статьи;
б) статьи дискредитационного плана;
в) заказные рекламные статьи;
г) статьи, разглашающие коммерческую тайну.

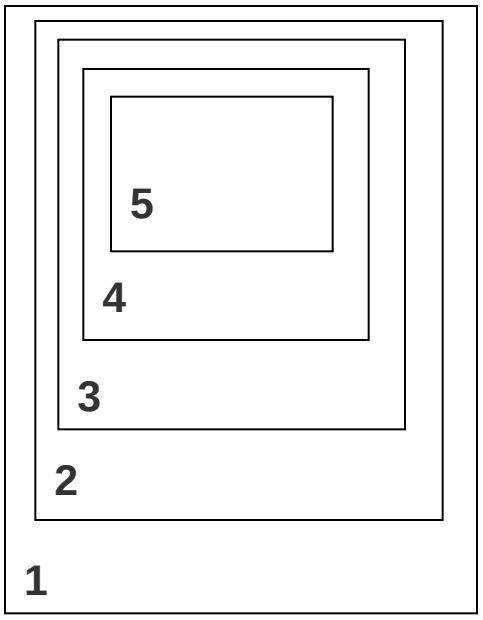
**4) Виды учетов:**
а) указатель имен;
б) указатель связей объекта;
в) картотека рекламы;
г) анкета статьи (организации, лица): источник, заказчики, финансирование, маршруты поездок и контакты, данные сравнения с материалами объективного характера, сведения о лицах, в чьем ведении находилась служебная информация и пр.

***Достоверность информации может оцениваться :***
*свободная беседа с консультантом- специалистом – 90-95 %;*
*вопросно-ответная форма опроса партнера – 40-70 %;*
*свободный рассказ о событиях – 25-30 %.*

***Достоверность сообщений, полученных от источников информации, не должна оцениваться выше:***
*от одного – 33 %;*
*от двух – 66 %,*
*от трех – 94-99 %.*

## 9.2.2. СХЕМЫ СООТНОШЕНИЙ ОБЪЕМА ИНФОРМАЦИИ, ОСТАЮЩЕГОСЯ В ПОЛЕ ЗРЕНИЯ ПО МЕРЕ ЕЕ ОБРАБОТКИ




1. Данные, имеющиеся в источнике.
2. Данные источника, попавшие в поле зрения наблюдателя.
3. Воспринятые данные из совокупности попавших в поле зрения.
4. Понятые данные из совокупности воспринятых.
5. Данные, оцененные как значимые, то есть содержащие информацию.

## 9.2.3. ФАКТОРЫ ИСКАЖЕНИЯ ИНФОРМАЦИИ И ДЕЗИНФОРМАЦИИ

1. **Поступающая фактура** может быть:
- представлена источнику как дезинформация;
- искажена им преднамеренно;
- изменена – произвольно или непроизвольно – в ходе ее передачи.

2. **Устные сообщения**, циркулирующие по горизонтальным и неформальным каналам, менее подвержены искажениям, а информация, поставляемая наверх, приукрашивается.

3. **При намеренной дезинформации** применяют как заведомую ложь, так и утонченную полуправду, подталкивающую воспринимающих к ложным суждениям.

Приемы:
- прямое сокрытие фактов;
- тенденциозный подбор данных;
- нарушение логических и временных связей между событиями;
- преподание правды в таком контексте (добавлением ложного факта или намека), чтобы она воспринималась как ложь;
- изложение важнейших данных на ярком фоне отвлекающих внимание сведений;
- смешивание разнородных мнений и фактов;
- сообщение информации словами, которые можно истолковывать по-разному;
- умолчание ключевых деталей факта.

4. **Искажения в процессе ретрансляции исходных данных, происходят из-за**:
- передачи только части сообщения;
- пересказа услышанного своими словами ("испорченный телефон");
- пропуска фактуры через призму субъективно-личностных отношений.

5. **Для успешности борьбы с дезинформацией следует**:
- различать факты и мнения;
- понимать, способен ли информатор по своему положению иметь доступ к сообщаемым фактам;
- учитывать субъективные (самомнение, фантазийность) характеристики источника и его предполагаемое отношение к выдаваемому сообщению;
- применять дублирующие каналы информации;
- исключать все лишние промежуточные звенья;
- помнить, что особенно легко воспринимается та дезинформация, которую вы предполагаете, или желаете услышать.

# 9.2.4. ТЕХНИКА ИНТЕРПРЕТАЦИИ ДАННЫХ

**1.** Истина обычно раскрывается не в исходных данных, а **в их точном истолковании**, ибо конкретный факт можно уяснить лишь в сочетании с другими фактами.

**2. Переработка информации после предварительного собирания фактуры** и конкретной постановки проблемы подразумевает:

а) систематизацию фактов, которые сортируют по степени их отношения к тому или иному вопросу;

б) выявление, основываясь на интуиции, ключевых моментов;

в) построение предположений, объясняющих основные факты;

г) получение, при необходимости, дополнительных данных;

д) оформление выводов и их проверка на соответствие другим фактам.

**3.** На отдельные вопросы часто удается получить прямой и вполне определенный ответ, а в отношении других вынужденно ограничиваются одними предположениями. Следует интуитивно понимать, **каковые из моментов являются важнейшими**, а не концентрировать внимание сразу на многих.

**4. Предположение тщательно проверяют на согласованность** со всеми данными, и когда обнаружится значительная неувязка, а факты явно правдивы, - требуется изменить суждение.

**Ложная интерпретация фактуры вероятна, если**:

- представлены не все материалы,
- некоторые из имеющихся под рукой фактов сомнительны,
- все внимание сосредотачивается лишь на тех сообщениях, кои подтверждают ожидания и предположения аналитика.

**Чтобы выявить возможные пути развития исходной ситуации, надо четко представлять:**

- ключевых персон конкурента;
- то, к чему он стремится (как по максимуму, так и по минимуму);
- есть ли некая система в его действиях;
- чего в них больше: логики, эмоций, традиций или случайностей;
- существует ли такой союзник, с которым конкурент не разорвет отношения;
- явные границы допустимости в его деяниях;
- уязвимые места;
- то, как конкурент оценивает ситуацию и вероятные реакции на действия.

# 9.3. АНАЛИТИЧЕСКОЕ ВЫЯВЛЕНИЕ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
## 9.3.1. БАЗОВЫЕ ПОНЯТИЯ

**Аналитическая информация** – осмысленные сведения, полученные из оцененных, истолкованных и соотнесенных фактов, изложенных таким образом, что ясно видно их значение для решения конкретной текущей задачи. К элементам аналитической информации относят сведения: о возможностях; уязвимых местах; достоверном курсе действий объекта.

**Структура аналитической информации** в виде типовой формы прогнозов:

1) последовательно описанные благоприятные и неблагоприятные факторы и оценка результатов их взаимодействия;

2) сравнение положения объектов с известным положением аналогичного;

3) определение верхних и нижних пределов развития объекта с учетом постоянно действующих факторов и разделения воздействующих и временных факторов.

**Уязвимость объекта** – наличие малозащищенных мест, воздействие на которые приводит к разрушению всей структуры.

**Индикаторы угрозы** - слова или существенные элементы информации в контексте статьи на ту или иную тему, имеющие прямое или косвенное отношение к профилю работы защищаемой организации, указывающие на то, что может случиться, и являющиеся признаком вероятности наступления событий, замаскированной угрозы или замаскированного предупреждения кому-либо

## 9.3.2. СУЩНОСТЬ И СОДЕРЖАНИЕ АНАЛИТИЧЕСКОЙ РАБОТЫ

**Аналитическая работа** представляет собой комплексное исследование различной целевой направленности в целях выявления, структуризации и изучения опасных ситуаций, которые могут создать риск для экономической и информационной безопасности, ее деятельности или персонала, привести к материальным, финансовым или иным убыткам, падению престижа или продукции:

- изучение существующего положения («изучать и считать») только через факты, подо-бранные так, чтобы они указывали на определенные закономерности или тенденции;
- изучение возможностей («что могут сделать» без учета противодействия - «общие возможности», а с учетом противодействия - «чистые возможности»);
- изучение намерений («что намеревается сделать объект»).

**Задачи аналитической работы:**

- обеспечить своевременное поступление надежной и всесторонней информации по интересующим вопросам;
- описать сценарии действий конкурентов, которые могут затрагивать текущие интересы;
- осуществлять постоянный мониторинг событий во внешней конкурентной среде и на рынке, которые могут иметь значение для интересов предприятия;
- обеспечить безопасность собственных информационных ресурсов;
- обеспечить эффективность и исключить дублирование при сборе, анализе и распространении информации.

**Основные направления аналитической работы:**

- анализ объекта защиты,
- анализ угроз,
- анализ каналов несанкционированного доступа к информации,
- анализ комплексной безопасности фирмы,
- анализ нарушений режима конфиденциальности,
- анализ подозрений утраты конфиденциальной информации и т.д.

# 9.3.3. ВИДЫ АНАЛИЗА ИНФОРМАЦИОННЫХ ОБЪЕКТОВ

**Структурный анализ**

- оценка и определение рационального числа уровней управления;
- корректировка состава элементов, отношений и связей между ними;
- определение предельного числа элементов в иерархиях и установление рациональной численности управленческого персонала системы при заданном количестве непосредственных исполнителей;
- оценка и определение мест размещения элементов для обеспечения устойчивости и оперативности управления

**Функциональный анализ**

- определение целей управления и построение дерева целей, соответствующего иерархической структуре системы управления;
- определение перечня и содержания основных задач управления, установление их взаимосвязи по входной и выходной информации;
- анализ и рациональное распределение функций управления между органами и отдельными руководителями;
- анализ и определение обязанностей, прав, ответственности и подчиненности органов и отдельных должностных лиц;
- исследование и разработку эффективных методов решения задач управления;
- обобщение и применение принципов управления, разработанных в ходе исторического развития и совершенствования исследуемых систем

**Информационный анализ**

- определение перечня и содержания документов, порядок их оформления, учета и доставки;
- методы сбора и обработки неформализованных сообщений;
- организация информационного взаимодействия должностных лиц и органов управления в процессе принятия решений и их выполнения.

## 9.3.4. СИСТЕМНЫЙ АНАЛИЗ

**СИСТЕМНЫЙ АНАЛИЗ – научный метод познания, представляющий собой последовательность действий по установлению структурных связей между переменными или элементами исследуемой системы.**

Опирается на **комплекс общенаучных, экспериментальных, естественно-научных, статистических, математических методов и процедур**:

- абстрагирование и конкретизация;
- анализ и синтез, индукция и дедукция;
- формализация и конкретизация;
- композиция и декомпозиция;
- линеаризация и выделение нелинейных составляющих;
- структурирование и реструктурирование;
- макетирование;
- реинженеринг;
- алгоритмизация;
- моделирование и эксперимент;
- программное управление и регулирование;
- распознавание и идентификация;
- кластеризация и классификация;
- экспертное оценивание и тестирование;
- Верификация и др.

# 9.3.5. СПЕЦИАЛЬНЫЕ МЕТОДЫ АНАЛИЗА

**А) ГРАФИЧЕСКИЕ (ТАБЛИЧНЫЕ, МАТРИЧНЫЕ):**

**Диаграммы связей:** выявляется наличие связи между субъектами, вовлеченными в ситуацию, подвергающуюся анализу, а также области соприкосновения этих субъектов.

**Матрицы связей:** в дополнение к диаграммам отражают частоту взаимодействия субъектов за определенный период времени и позволяют оценить характер взаимодействий между субъектами через частоту взаимодействий.

**Схемы потоков информации:** позволяют оценить то, каким образом происходят события, анализировать пути движения информации среди субъектов анализа, т.е. оценивать положе-ние каждого субъекта в общей группе и выявлять неустановленные связи между ними, особенно в физических процессах и при взаимодействиях юридических и физических лиц.

**Временные графики:** используются для регистрации событий и помогают эффективнее их анализировать и рационально планировать противодействия.

**Графики анализа визуальных наблюдений** (VIA – Visual Investigative Analysis – схема визуальных наблюдений в процессе одиночного события), составная часть графиков оценки результатов PERT (Program Evaluation Review Technique – схемы общего хода событий) – составляются по принципу разбивки сложной операции на составные элементы и позволяют наглядно отражать ход событий для повышения эффективности работы предприятий и служб безопасности. События представлены треугольниками и кругами: треугольники отмечают начало, конец события и его наиболее важные моменты.

**Б) ЭКСПЕРТНЫЕ СИСТЕМЫ** – класс компьютерных программ, которые проводят анализ, выполняют классификацию, дают консультации и ставят диагноз, в зависимости от развития:

**1) ассистент** – система освобождает аналитика от рутинной работы, позволяя заниматься только наиболее важными вопросами;

**2) коллега** – система участвует в решении проблемы на равных с человеком в виде постоянного диалога;

**3) эксперт** – уровень знаний системы как пополняемая совокупность знаний многих ведущих экспертов в этой области во много раз превосходит уровень знаний человека

## 9.3.6. МЕТОД КОНТЕНТ-АНАЛИЗА

- выявление смысловых единиц - понятий и терминов;
- установление частоты применения понятий, связанных с критикой объекта;
- установление, в какой мере источник информации ориентирован на те или иные позиции и осведомлен о них;
- анализ тематики - определение содержания, показательных сюжетов, свидетельствующих об определенной направленности взглядов, интересов, ценностной ориентации журналистов, пишущих по проблемам, затрагивающим интересы организации;
- выяснение частоты употребления определенных имен, ссылки на авторитетных в той или иной области специалистов, свидетельствующей о влиянии отдельных лиц или представляемых ими организаций на журналиста, а также частоты упоминания организаций

## МЕТОД СЕТИ СВЯЗЕЙ (ПОСТРОЕНИЯ МАТРИЦЫ АССОЦИАЦИЙ)

1) **Подбор информации, выделение данных, касающихся индивидуумов и связей, разработка матрицы ассоциаций и предварительной схемы связей, включение в схему организационных наложений и уточнение схемы** (прочность ассоциации: сильная ассоциация или связь, умеренная, слабая и отсутствие какой-либо связи).

2) **Построение матрицы для регистрации оцененных ассоциаций** :

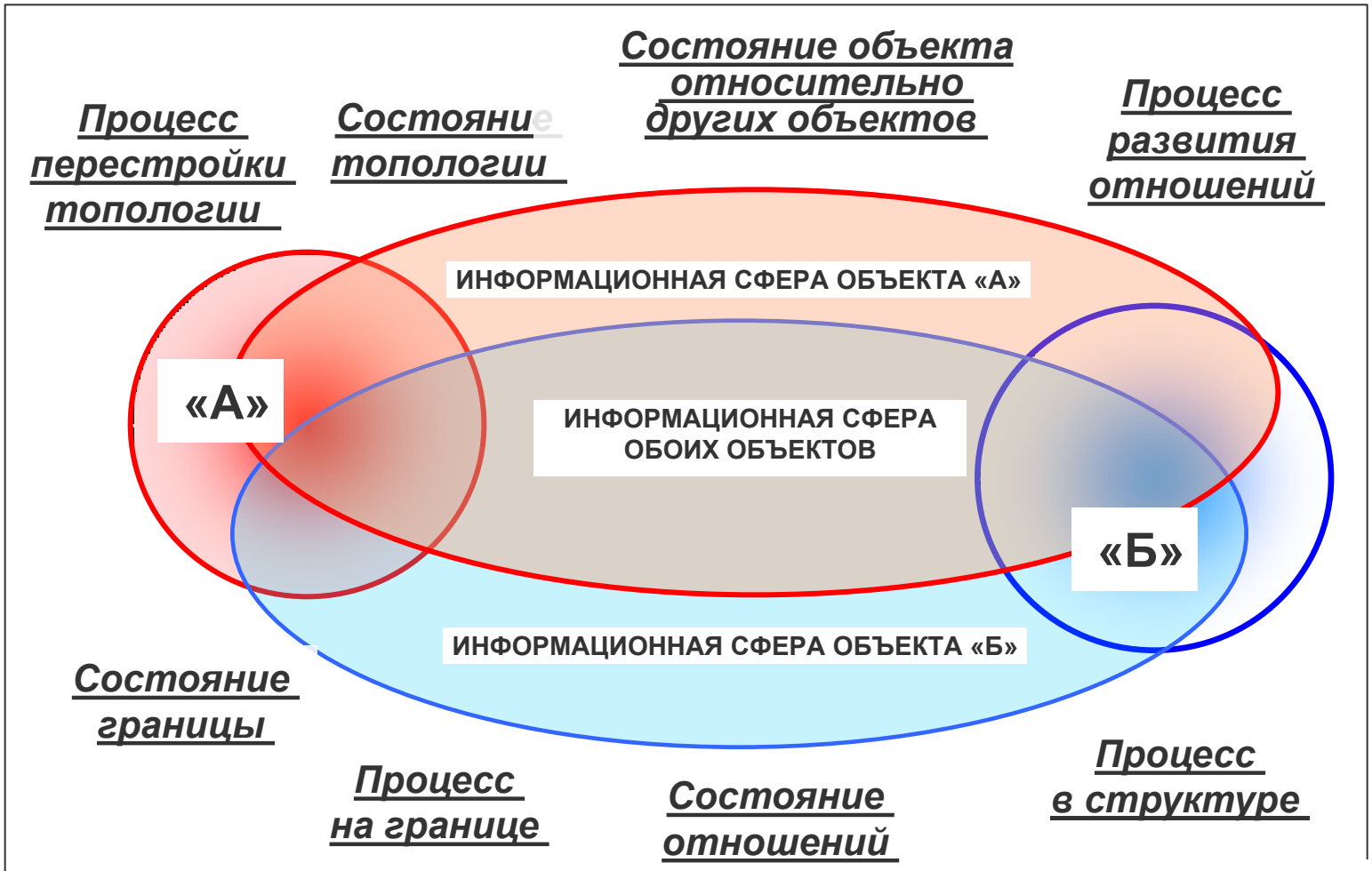
перечисляют индивидуумов вдоль горизонтальной оси в алфавитном порядке слева направо, а вдоль вертикальной - сверху вниз;

в каждой ячейке, в месте перекрещивания имен индивидуумов по горизонтальной и вертикальной осям, графически отображаются полученные оценки прочности ассоциаций: сильная (бесспорная), умеренная, слабая (вероятная) или отсутствие связи;

подсчитывают число клеточных ассоциаций и проставляют его по горизонтальной оси под именем каждого индивидуума.

3) **Графическое построение схемы сети связей** (**графические приемы**: лиц изобра-жают кружочками, организации – квадратиками, ассоциации (связи) – линиями; сильные связи изображают сплошными линиями, умеренные – пунктирными, слабые – точечными, отсутствие связей – отсутствием линий.

## 9.3.7. СХЕМА ЭЛЕМЕНТОВ МОРФОЛОГИЧЕСКОГО АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТА (методика Johary)



## 9.3.8. СОДЕРЖАНИЕ МОРФОЛОГИЧЕСКОГО АНАЛИЗА

**Морфология –** представление о внутренней организации системы (сочетание и взаимное расположение элементов, их топология или пространственная структура, информация, передаваемая в них).

**Морфологический анализ** – систематизированное изучение объекта с целью выявления его **структуры и основных закономерностей развития**.

**Особенность морфологического анализа**: исходит из постулата единства формы и содержания (если система выглядит как нечто известное снаружи и ведет себя аналогичным образом, то внутреннее ее строение и состояние ее элементов подобно известному или наоборот – если известно строение, то может быть предсказано поведение и внешний вид).

**СОДЕРЖАНИЕ АНАЛИЗА**

**Состояние топологии** информационного объекта позволяет описывать его структуру, внутреннее строение и содержание. Характеристики: для информации – факт своего объективного наличия, отражение в виде материальной формы знака (символа) своего предметного и смыслового значения, имеющиеся противоречия и количество (объем информационного ресурса); для информационно-психологического объекта – его социальную структуру, место и роль в социальной группе, построение информационной модели мира и его программы (психологические потребности, мотивационный комплекс и пр.); для информационно-технического объекта – структуру его программно-аппаратного комплекса (конфигурацию сети, операционные системы, программы администрирования, программные и аппаратные устройства защиты информации и др.) и информационный ресурс.

**Процесс перестройки топологии** описывает процесс перестройки структуры (строения), программ и ресурсов рассматриваемого объекта как целого: для информации – ее лексическую модификацию и изменение смыслообразующих элементов; для информационно-психологического объекта – осознание им своей причастности к изменениям окружающего мира, трансформации мотивационных и смысловых структур; для информационно-технического объекта – процесс совершенствования структуры и программного обеспечения.

**Состояние границы** между объектом и его окружением позволяет описывать место рассматриваемого объекта и его способность противостоять «внешнему»: для информации – формирование новых смыслов и знания; для информационно-психологического объекта – разграничение на «свое» и «чужое», наличие условий взаимодействия (сотрудничество, дружба, вражда), условности сосуществования и др.; для информационно-технического объекта – его «внутреннее» и «внешнее», объем, границы занимаемого пространства, досягаемость воздействий.

## 9.3.8б. СОДЕРЖАНИЕ МОРФОЛОГИЧЕСКОГО АНАЛИЗА

СОДЕРЖАНИЕ АНАЛИЗА

**Описание процесса на границе между объектом и его окружением** – касается изменений данной границы: для информации – влияние иной информации на первоначальную, устаревание сведений; распространение информации на другие виды объектов, появление сведений, противоречащих старым, увеличение информационного ресурса; для информационно-психологического объекта – изменения во взаимоотношениях с другими, увеличение объема знаний; для информационно-технического объекта – подключения внешних источников и потребителей и др.

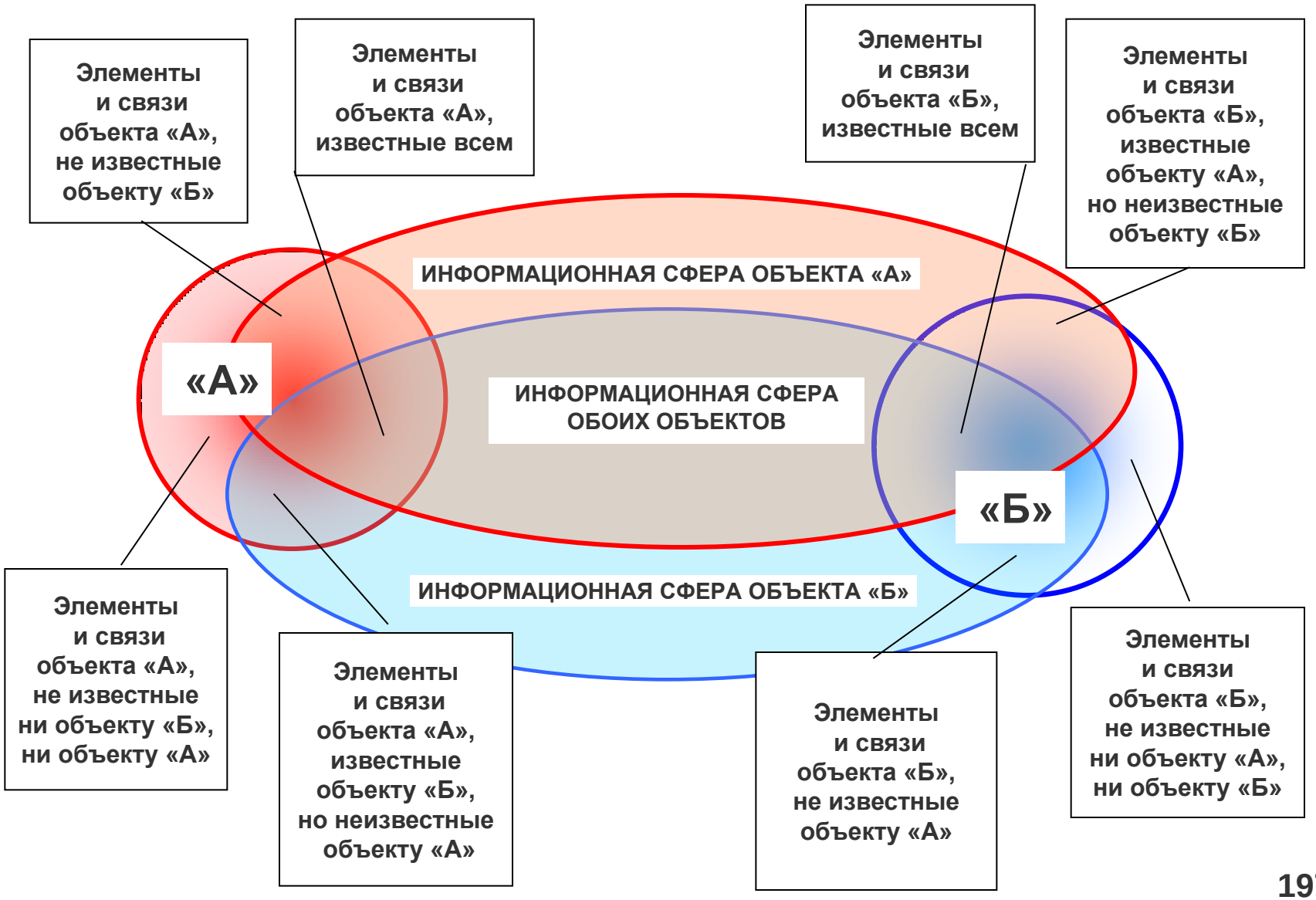
**Описание состояния объекта относительно других объектов** – пространственное и смысловое позиционирование других объектов относительно рассматриваемого: для информации – наличие альтернативных взглядов и знаний; для информационно-психологического объекта – его представления об объектах окружающего мира типа «знает - не знает» и т.п.; для информационно-технического объекта – его роль и место в информационной инфраструктуре системы.

**Описание процесса в структуре системы** – выделяется весь комплекс информации о процессах, происходящих со структурой объекта :для информации – возрастание противоречивости и старение данных, трансформацию смыслов; для информационно-психологического объекта – процессы совершенствования знаний или их утраты, наличие возможностей и способов изменения своих информационных характеристик (психологических черт личности, сплоченности коллектива и т.д.) или управления ими; для информационно-технического объекта – износ аппаратных средств, выход из строя элементов, сбои в работе и др.

**Состояние отношений между объектами** - касается всего комплекса информации о взаимосвязях между объектами данного множества на данном этапе: для информации – ее важность (уровень влияния), согласуемость полученных данных с ранее имевшимися, устойчивость базовых программ от воздействия программ вредоносных; для информационно-психологического объекта – эмоциональные проявления как фиксацию отношений в коллективах, включая также возможность управления человеком эмоциональным состоянием в конкретных условиях; для информационно-технического объекта – совместимость, в т.ч. электромагнитная, с другими объектами и пр.

**Процесс развития отношений между информационными объектами** охватывает весь комплекс информации о процессах установления и реструктурирования отношений между конкретными объектами данного уровня: для информации – согласование новых данных с ранее имевшимися, борьба антивирусных программ с вредоносными; для информационно-психологического объекта – тенденции развития отношений в коллективах и между коллективами, о потребностях одних объектов в других, о необходимости или вредоносности одного объекта для другого; для информационно-технического объекта – совершенствование совместимости технических устройств систем управления различного назначения.

# 9.3.9. ВАРИАНТ МОРФОЛОГИЧЕСКОГО АНАЛИЗА ОБЪЕКТА

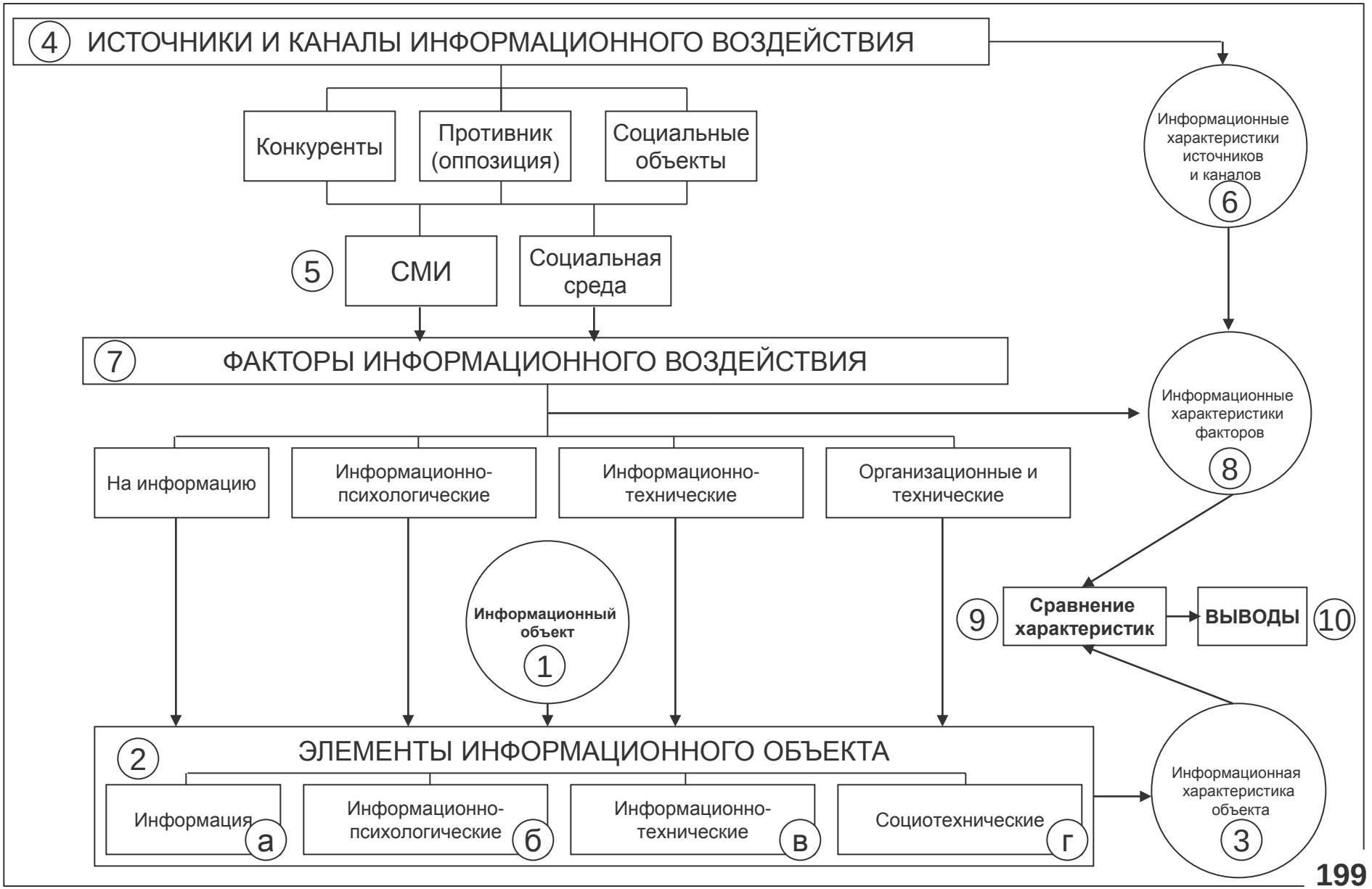


## 9.3.10. ФОРМИРОВАНИЕ ВЫВОДОВ ИЗ МОРФОЛОГИЧЕСКОГО АНАЛИЗА

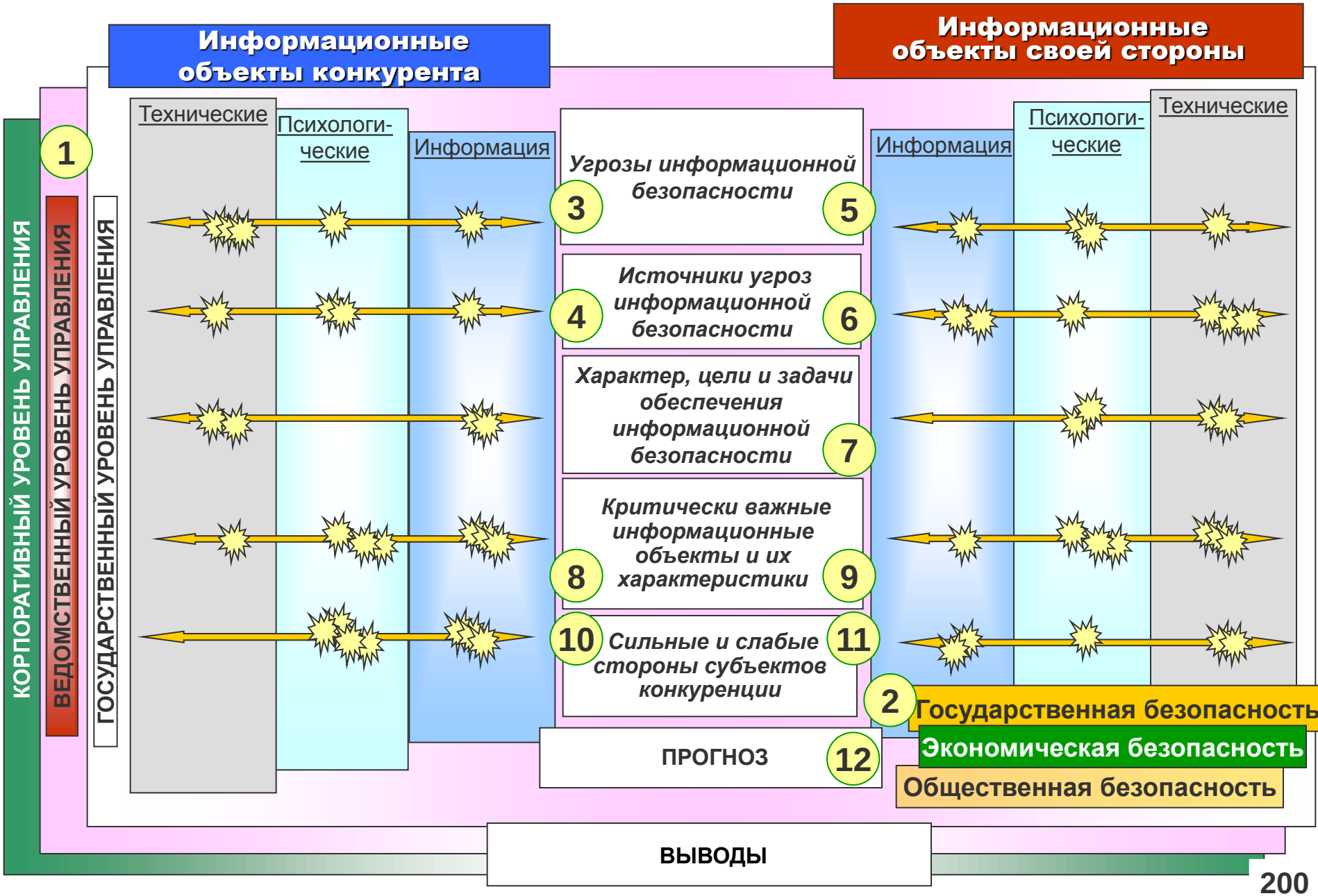
| РАССМАТРИВАЕМЫЕ ЭЛЕМЕНТЫ ИНФОРМАЦИОННОЙ СФЕРЫ ОБЪЕКТОВ | | СОДЕРЖАНИЕ ЗАДАЧ |
|---|---|---|
| «А» | Элементы и связи объекта «А», известные всем | Поддержание неизменности картины и ее демонстративный показ |
| | Элементы и связи объекта «А», не известные объекту «Б» | Скрытие от конкурента |
| | Элементы и связи объекта «А», не известные ни объекту «Б», ни объекту «А» | Упреждение в выявлении и анализе элементов, отношений и связей |
| | Элементы и связи объекта «А», известные объекту «Б», но неизвестные объекту «А» | Рефлексирование |
| Общие элементы информационной сферы обоих объектов «А» и «Б» | | Защита от воздействия своих информационных объектов и воздействие на конкурента |
| «Б» | Элементы и связи объекта «Б», известные всем | Сбор и добывание данных об изменениях обстановки на рынке производства и сбыта |
| | Элементы и связи объекта «Б», не известные объекту «А» | Добывание, сбор, анализ обстановки и прогнозирование тенденций |
| | Элементы и связи объекта «Б», известные объекту «А», но неизвестные объекту «Б» | Скрытие сведений, использование их для формирования деструктивных процессов у конкурента. |
| | Элементы и связи объекта «Б», не известные ни объекту «А», ни объекту «Б» | Формирование новых условий для контроля за конкурентом, упреждение в выявлении и анализе элементов и связей |

# 9.4. АЛГОРИТМЫ АНАЛИЗА ИНФОРМАЦИОННОЙ ОБСТАНОВКИ В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## 9.4.1. СТРУКТУРА АЛГОРИТМА ОЦЕНКИ ИНФОРМАЦИОННОЙ ОБСТАНОВКИ



# 9.4.2. АЛГОРИТМ МЕТОДИКИ ОЦЕНКИ ИНФОРМАЦИОННОЙ ОБСТАНОВКИ



# 9.4.3. ОЦЕНКА БЕЗОПАСНОСТИ ИНФОРМАЦИИ С УЧЕТОМ УГРОЗ ВОЗДЕЙСТВИЯ

**Объект – информация (сообщение)**

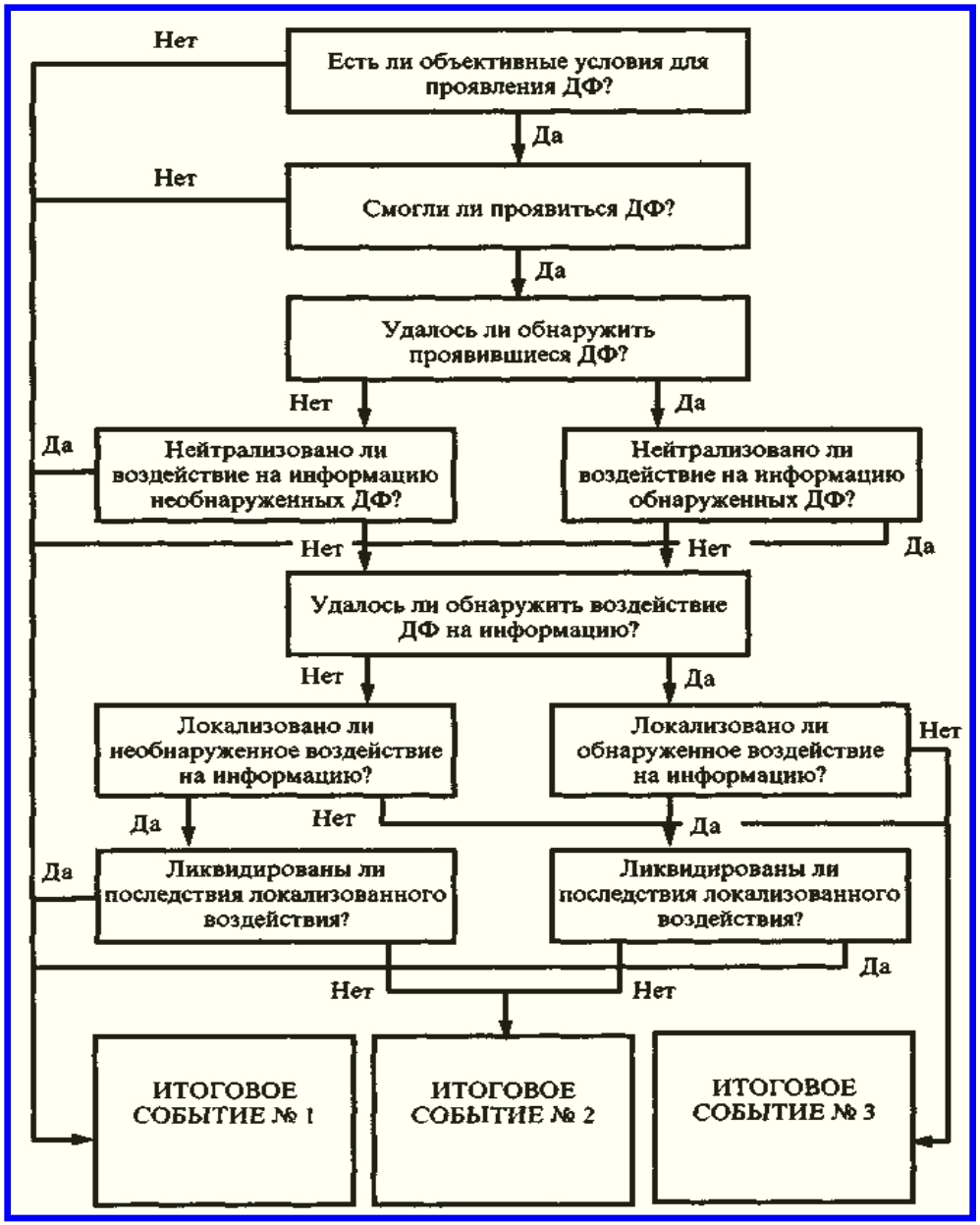
| Показатели информационной характеристики объекта | Потен-циал | Реали-зация | Итог |
|---|---|---|---|
| Источник | $x^1_1$ | $x^2_1$ | $x^1_1 x^2_1$ |
| Важность (конфиденциаль-ность) | $x^1_2$ | $x^2_2$ | $x^1_2 x^2_2$ |
| Смысл | $x^1_3$ | $x^2_3$ | $x^1_3 x^2_3$ |
| Актуальность | $x^1_4$ | $x^2_4$ | $x^1_4 x^2_4$ |
| Объем | $x^1_5$ | $x^2_5$ | $x^1_5 x^2_5$ |
| Достоверность | $x^1_6$ | $x^2_6$ | $x^1_6 x^2_6$ |
| Информационная характеристика | $\sum_1^n x^1_n x^2_n / n$ | | |

Сравнение значений показателей

**Факторы угроз воздействия на информацию**

| | Искажение | | | Подмена (уничтожение) | | | Дискредитация (вскрытие) | | | Дезинформация | | | Интеллект. воздействие | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Потенциал | Интенсивность | Актуальность | Потенциал | Интенсивность | Актуальность | Потенциал | Интенсивность | Актуальность | Потенциал | Интенсивность | Актуальность | Потенциал | Интенсивность | Актуальность |
| | … | … | … | … | … | … | $y^1_1$ | $y^2_1$ | $y^3_1$ | … | … | … | $y^{12}_1$ | $y^{22}_1$ | $y^{32}_1$ |
| | … | … | … | … | … | … | $y^1_2$ | $y^2_2$ | $y^3_2$ | $y^{12}_2$ | $y^{22}_2$ | $y^{32}_2$ | … | … | … |
| | $y^1_3$ | $y^2_3$ | $y^3_3$ | … | … | … | $y^{12}_3$ | $y^{22}_3$ | $y^{32}_3$ | … | … | … | $y^{13}_3$ | $y^{23}_3$ | $y^{33}_3$ |
| | $y^1_4$ | $y^2_4$ | $y^3_4$ | … | … | … | … | … | … | … | … | … | … | … | … |
| | … | … | … | $y^1_5$ | $y^2_5$ | $y^3_5$ | … | … | … | … | … | … | … | … | … |
| | … | … | … | … | … | … | … | … | … | $y^1_6$ | $y^2_6$ | $y^3_6$ | … | … | … |
| $\sum_1^m \sum_1^n Y^1_n y^2_n y^3_n \dots y^m_n / n/m$ | | | | | | | | | | | | | | | |

# 9.4.4. ПОСЛЕДОВАТЕЛЬНОСТЬ АНАЛИЗА СИТУАЦИЙ В ПРОЦЕССЕ ЗАЩИТЫ ИНФОРМАЦИИ



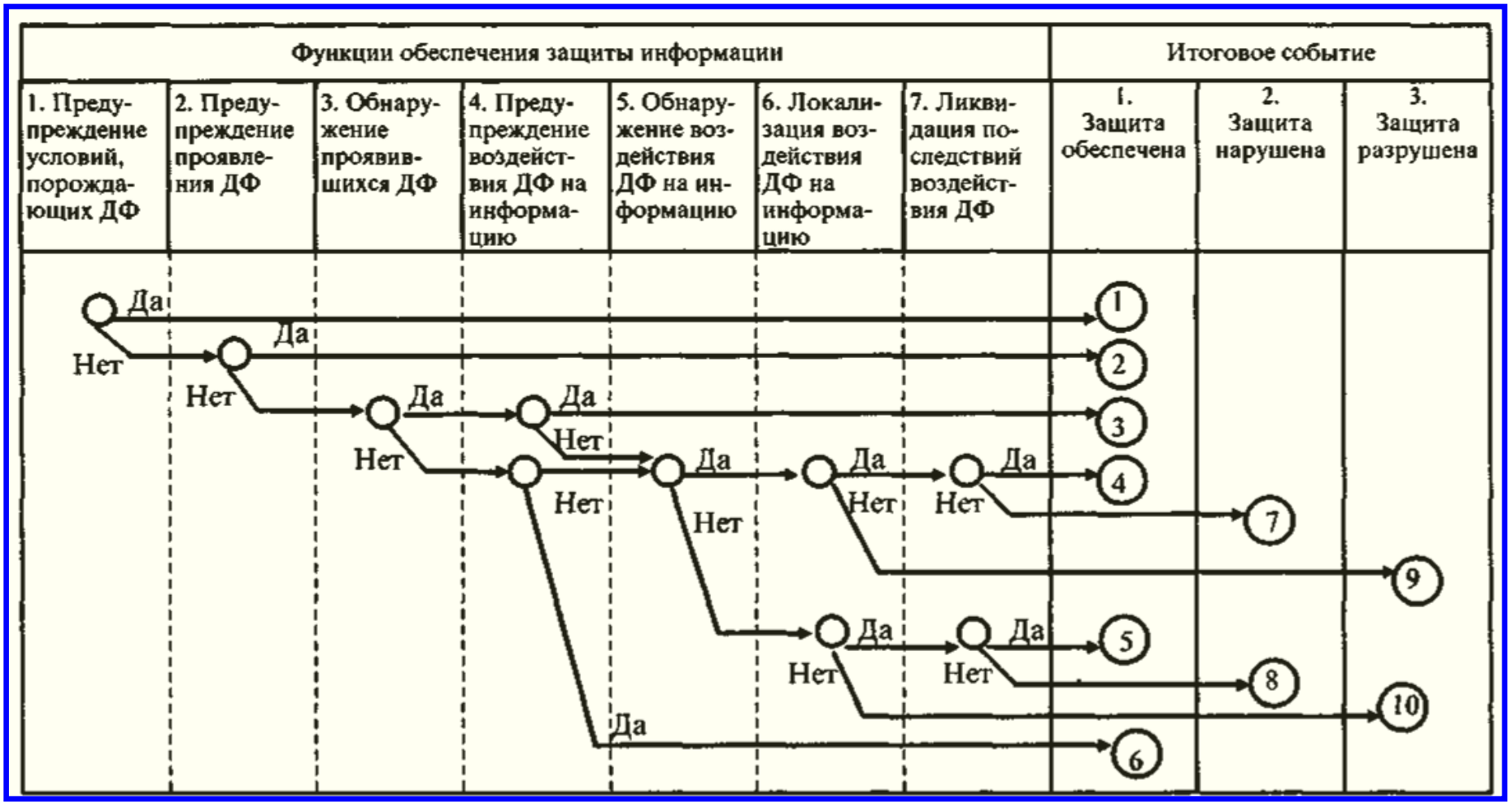

**ДФ – дестабилизирующий фактор**

*Событие №1* – защита информации обеспечена, поскольку даже при условии проявления дестабилизирующих факторов предотвращено их воздействие на защищаемую информацию или ликвидированы последствия такого воздействия

*Событие №2* - защита информации нарушена, поскольку не удалось предотвратить воздействие дестабилизирующих факторов на информацию, однако это воздействие локализовано

*Событие №3* - защита информации разрушена, поскольку воздействие дестабилизирующих факторов на информацию не только не предотвращено, но даже не локализовано

## 9.4.5. АНАЛИТИЧЕСКАЯ МОДЕЛЬ ИСХОДОВ ПРИ ОСУЩЕСТВЛЕНИИ ФУНКЦИЙ ЗАЩИТЫ ИНФОРМАЦИИ




ДФ – дестабилизирующий фактор

## 9.4.6. ФОРМА ИЗЛОЖЕНИЯ ДАННЫХ АНАЛИТИЧЕСКОГО ОТЧЕТА

1. **Заключение.**
   Ответы на вопросы, какова степень важности полученной информации, ее значение для принятия конкретных решений, идет ли речь о каких-либо угрозах, подозрениях, выявленных негативных факторах и т.п., какое отношение имеет предмет отчета к другим областям аналитической работы. Факты и сведения, на основе которых получены результаты анализа, не должны смешиваться с самими результатами.
2. **Рекомендации.**
   Конкретные направления дальнейших действий службы безопасности и других структурных подразделений предприятия для улучшения системы безопасности, предотвращения утраты информации, принятия наиболее эффективных решений и т.п.
3. **Обобщение информации.**
   Изложение самой существенной информации без излишней детализации.
4. **Источники и надежность информации.**
   Предполагаемые оценки надежности данных и источника на момент написания отчета.
5. **Основные и альтернативные гипотезы.**
   Наиболее вероятные гипотезы для принятия адекватных решений, а также дополнительной оценки правильности выбранной гипотезы.
6. **Недостающая информация.**
   Четко указывается, какая именно дополнительная информация необходима для подтверждения окончательной гипотезы и принятия решения.

# Глава 10.
# ОЦЕНКА РИСКОВ ДЛЯ ПРИНЯТИЯ ОРГАНИЗАЦИОННЫХ МЕР В ИНТЕРЕСАХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**10.1.** Содержание понятия «риски» и технологии их анализа в интересах защиты информации.

**10.2.** Понятие качественной и количественной оценки рисков, шкалы и критерии измерения.

**10.3.** Комплексная оценка рисков безопасности и ее основные этапы.

**10.4.** Критерии оценки уровня информационной безопасности предприятия.

**10.5.** Оценка текущего состояния информационной безопасности компании.

## Литература:


**1.** Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность/Петренко С. А., Симонов С. В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.

**2.** ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Ч.1. Концепция и модели менеджмента безопасности ИТК технологий.

**3.** ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч.1. Введение и общая модель

# 10.1. СОДЕРЖАНИЕ ПОНЯТИЯ «РИСКИ» И ТЕХНОЛОГИИ ИХ АНАЛИЗА В ИНТЕРЕСАХ ЗАЩИТЫ ИНФОРМАЦИИ

## 10.1.1. ИНФОРМАЦИОННЫЕ РИСКИ И ЦЕЛЬ ИХ АНАЛИЗА

**ПРОБЛЕМА:** ФИНАНСИРОВАНИЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПО ОСТАТОЧНОМУ ПРИНЦИПУ

Непонимание руководством необходимости должного уровня инвестиций

Неумение специалистов по безопасности убеждать руководство вкладывать в информационную безопасность соответствующие средства

НАПРАВЛЕННОСТЬ УБЕЖДЕНИЯ РУКОВОДСТВА

Анализ информационных рисков и его представление для доклада

Убеждение о необходимости соответствовать тому или иному нормативному акту

Оценка того, какие угрозы и через какие уязвимости могут быть реализованы

Способ обоснования инвестиций (затрат)

Обоснование содержания проекта системы обеспечения информационной безопасности

**Риск – это вероятный ущерб, который понесет компания при раскрытии, модификации, утрате или недоступности своей информации**

**ИНФОРМАЦИОННЫЙ РИСК ЗАВИСИТ**

**от стоимости информации**

**от защищенности информационной системы**

## 10.1.2. БАЗОВЫЕ ПОНЯТИЯ

**Риск** - комбинация вероятности события и его последствий, опасность возникновения убытков или ущерба в результате применения информационных технологий, связанных с созданием, передачей, хранением и использованием информации с помощью информационных ресурсов.

**Оценка риска** - общий процесс анализа риска (систематические использование информации для идентификации источников и для оценки риска) и оценки риска (процесс сравнения оцененного риска с данными критериями риска для определения значимости риска).

**Управление риском** - координированные действия для направления и контроля организации в отношении риска (оценка риска, обработка риска, приемлемость риска и сообщение риска);

процессы, связанные с идентификацией, анализом рисков и принятием решений, которые включают максимизацию положительных и минимизацию отрицательных последствий наступления рисковых событий.

**Обработка риска** - процесс выбора и осуществления контролей для изменения риска.

**Заявление и применимости** - документ, описывающий задачи контроля и контроли, которые релевантны и применимы для ISMS организации, на основе результатов и выводов оценки риска и процесса обработки риска.

***РУКОВОДСТВО BS 7799***

**Угроза** - это возможность реализации нарушения правил политики ИБ.

**Объект оценки** – это подлежащая оценке информационная система.

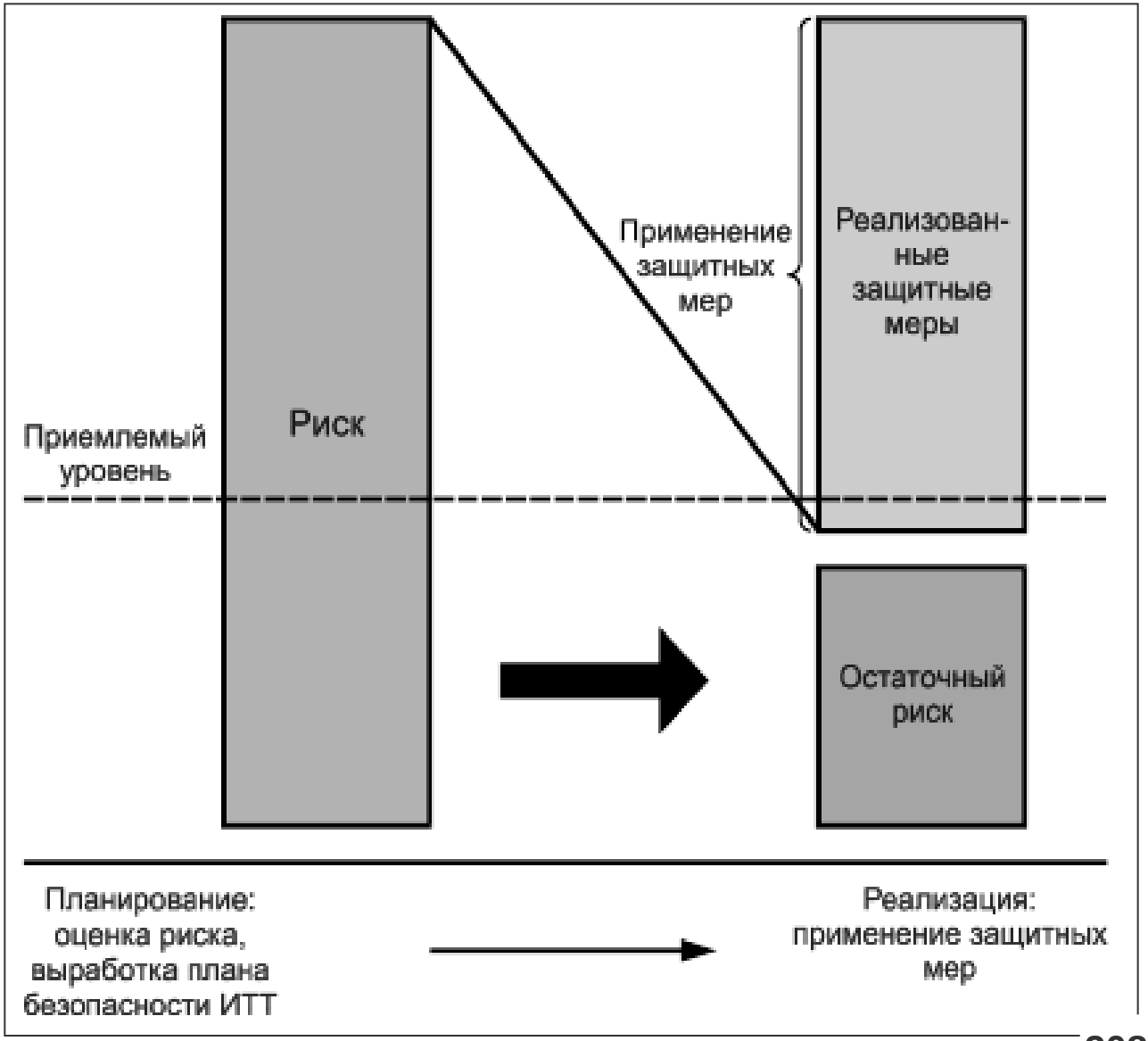
**Информационный актив** – это набор информации, который используется в работе и состоящий из информации и её физического носителя

## 10.1.3. ВЗАИМОСВЯЗЬ ЗАЩИТНЫХ МЕР И РИСКА

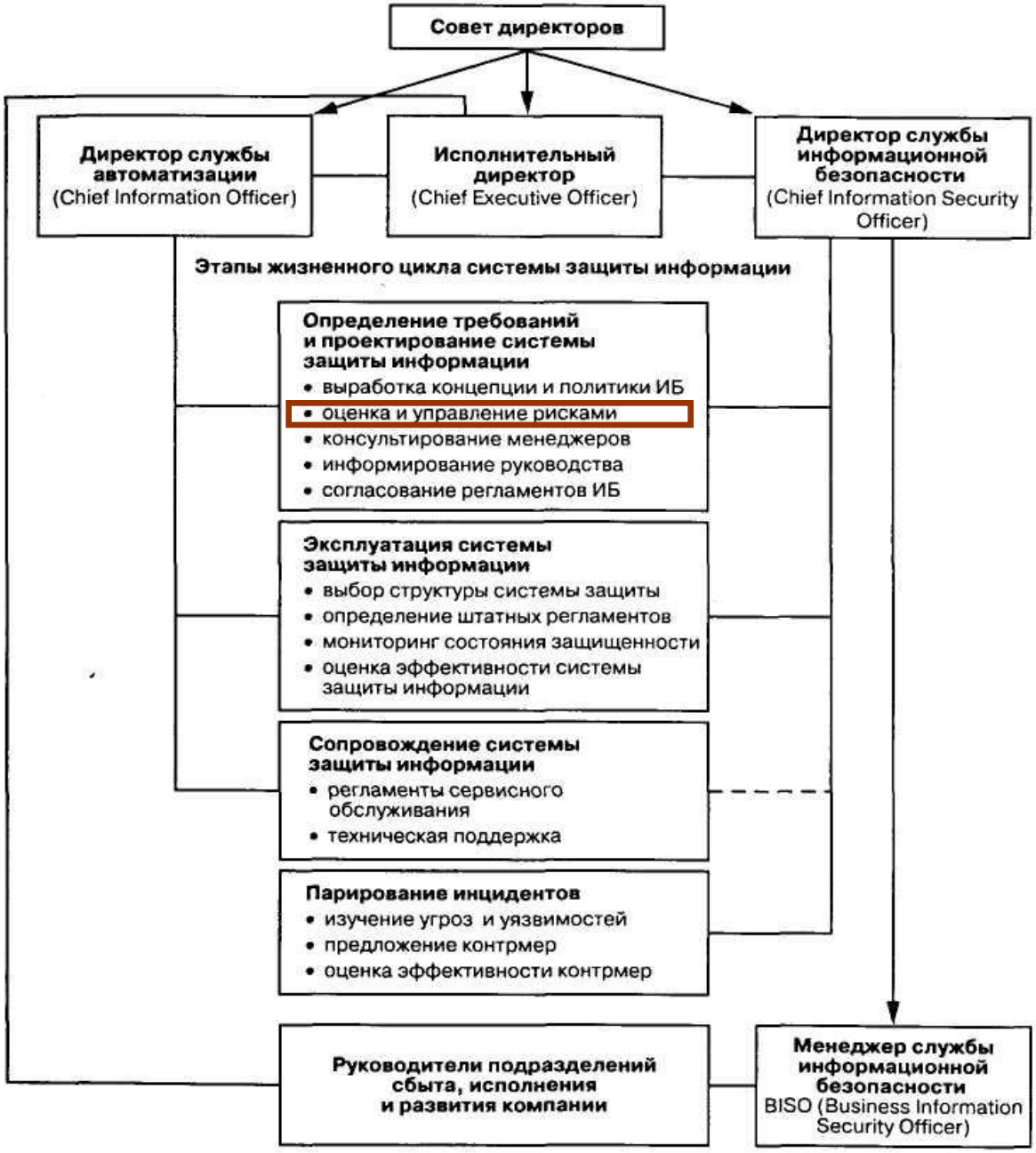
**Возможности снижения уровня риска применением защитных мер:**

- ❖ избегать риска;
- ❖ уступить риск (путем страховки и пр.);
- ❖ снизить уровень угроз;
- ❖ снизить степень уязвимости системы ИТ;
- ❖ снизить возможность воздействия нежелательных событий;
- ❖ отслеживать появление нежелательных событий, реагировать на их появление и устранять их последствия

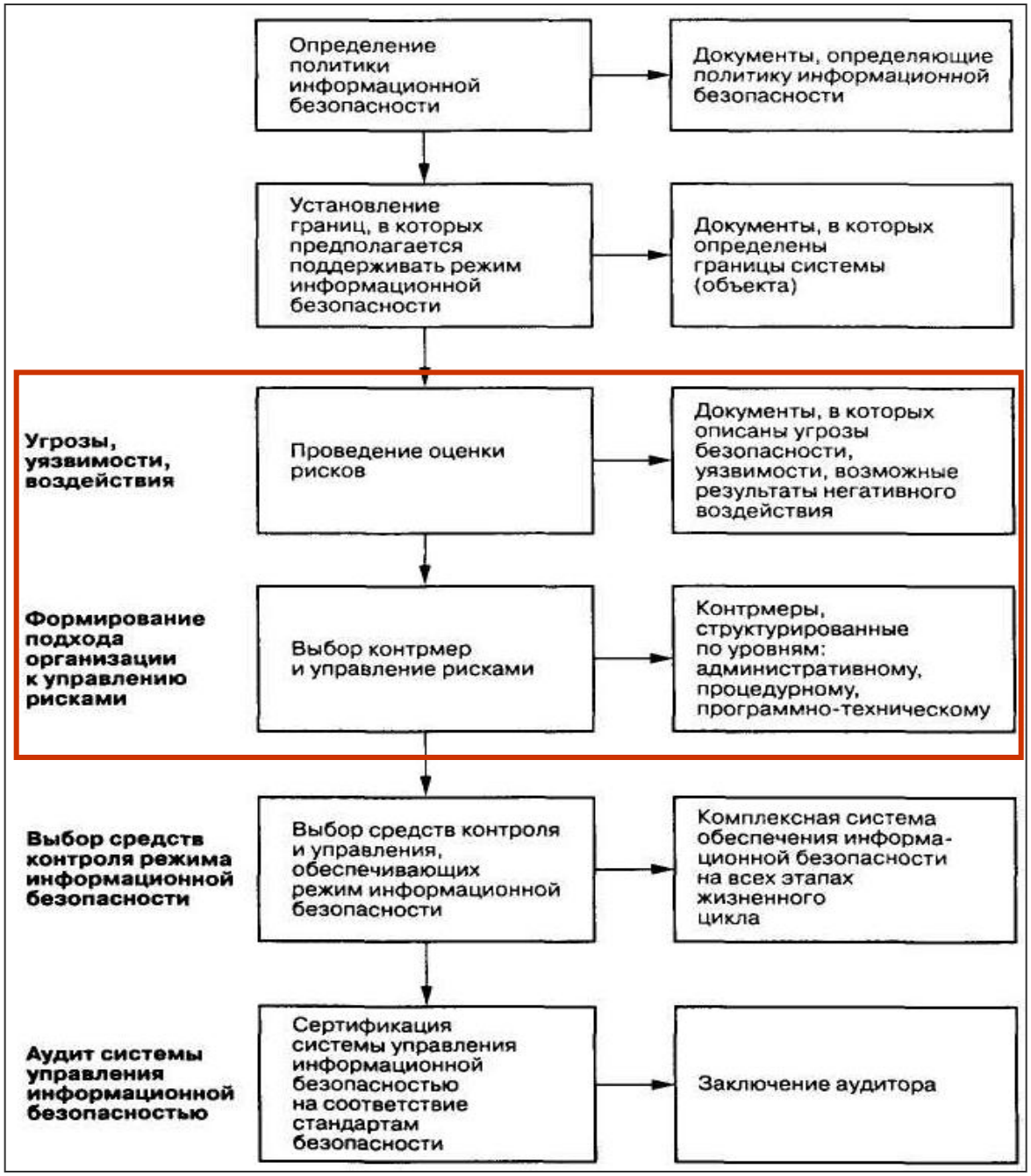
*ГОСТ Р ИСО/МЭК 13335-1-2006*



# 10.1.4. ОРГАНИЗАЦИОННАЯ СТРУКТУРА РУКОВОДСТВА КОМПАНИИ, ОТВЕТСТВЕННОГО ЗА ОИБ



# 10.1.5. ЭТАПЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



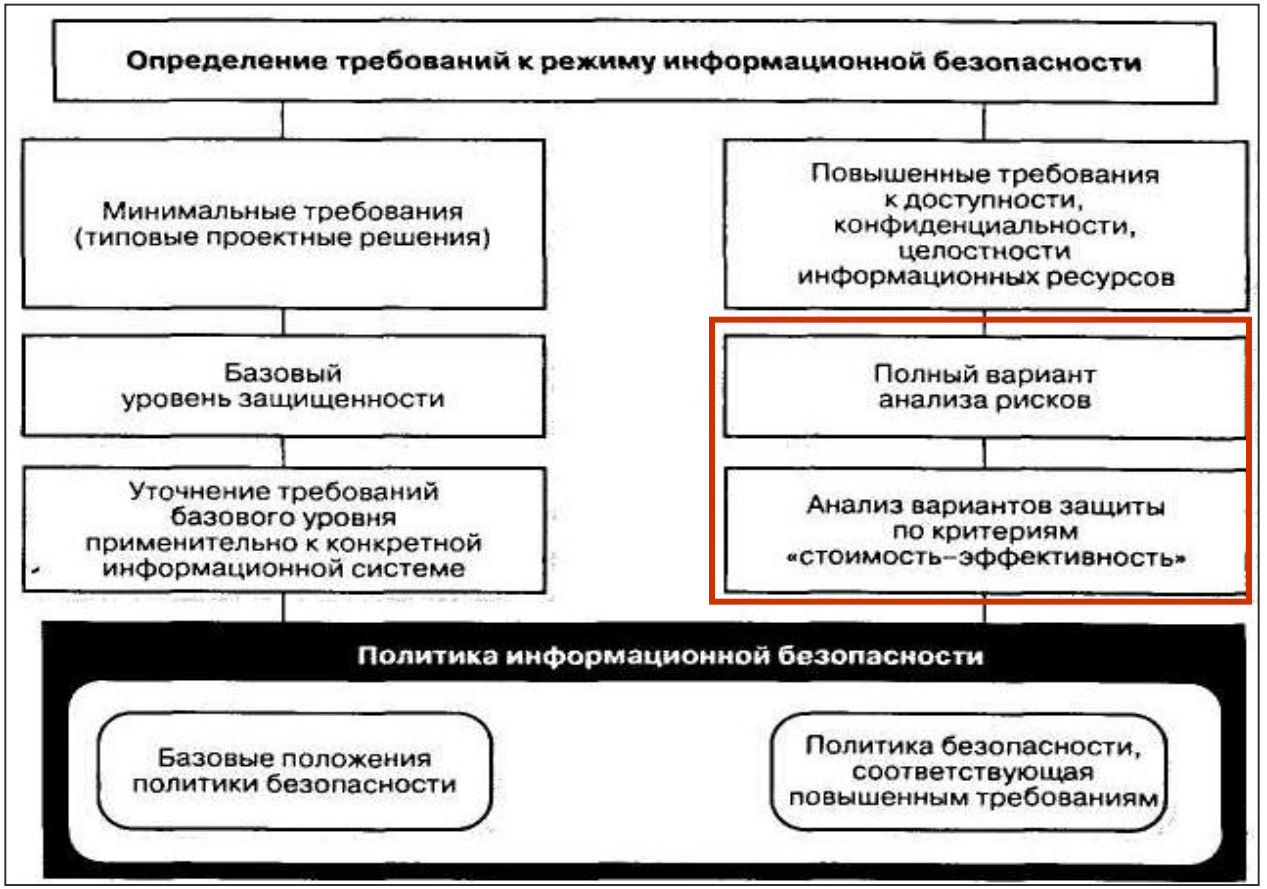
# 10.1.6. ПОДХОДЫ К УПРАВЛЕНИЮ ИНФОРМАЦИОННЫМИ РИСКАМИ

***1. Уменьшение рисков.*** Многие риски удается значительно уменьшить за счет простых контрмер управление паролями снижает риск НСД

***2. Уклонение от риска.*** От некоторых классов рисков можно уклониться. Так, вынесение Web-сервера организации за пределы ЛВС позволяет избежать риска НСД со стороны Web-клиентов

***3. Изменение характера риска.*** Если не удается уклониться или эффективно уменьшить риск, следует принять меры страховки: от пожара; заключить договор с поставщиками СВТ о их сопровождении и компенсации ущерба

***4. Принятие риска.*** Риски нельзя довести до пренебрежимо малой величины, хотя после принятия контрмер некоторые риски уменьшаются до остаточной величины




***5. Выбор контрмер,*** обеспечивающих режим ИБ для защиты информации, структурированных по нормативно-правовому, организационно-управленческому, технологическому и аппаратно-программному уровням ОИБ

***6. Аудит системы управления ИБ.*** Проверяется соответствие выбранных контрмер по ЗИ целям и задачам бизнеса, декларированным в политике безопасности, выполняется оценка остаточных рисков и их оптимизация

# 10.1.7. ИДЕНТИФИКАЦИЯ РИСКОВ
## Каталоги угроз в Германском стандарте IT Baseline Protection Manual

**Группы угроз:**
T1. Угрозы в связи с форс-мажорными обстоятельствами.
T2. Угрозы на организационном уровне.
T3. Угрозы, связанные с ошибками людей.
T4. Угрозы, связанные с техникой.
T5. Угрозы, возникающие на предпроектном этапе.
http://www.bsi.bund.de/gshb/english/t/t1000.htm.

### *T 1. Угрозы в связи с форс-мажорными обстоятельствами*
T1.1. Потеря персонала.
T1.2. Отказ информационной системы.
T1.3. Молния.
T1.4. Пожар.
T1.5. Затопление.
T1.6. Возгорание кабеля.
T1.7. Недопустимая температура и влажность.
T1.8. Пыль, загрязнение.
T1.9. Потеря данных из-за воздействия интенсивных магнитных полей.
T1.10. Отказ сети на большой территории.
T1.11. Катастрофы в окружающей среде.
T1.12. Проблемы, вызванные неординарными общественными событиями.
T1.13. Шторм

### *T2. Угрозы на организационном уровне*
T2.1. Отсутствие или недостатки регламентирующих документов.
T2.2. Недостаточное знание требований регламентирующих документов.
T2.3. Недостаточно совместимые или неподходящие ресурсы.
T2.4. Недостатки контроля и измерения уровня безопасности в информационной технологии.
T2.5. Недостатки в обслуживании.
T2.6. Несоответствие помещений требованиям в области безопасности.
T2.7. Превышение полномочий.
T2.8. Нерегламентированное использование ресурсов.
T2.9. Недостатки в процедурах отслеживания изменений в информационной технологии.
T2.10. Несоответствие среды передачи данных предъявляемым требованиям.
T2.11. Недостаточный горизонт планирования.
T2.12. Недостатки в документировании коммуникаций.
T2.13. Недостаточная защищенность от действий дистрибьюторов.
T2.14. Ухудшение использования информационных технологий из-за плохих условий на рабочих местах.
T2.15. Возможность несанкционированного доступа к конфиденциальным данным в ОС UNIX.
T2.16. Несанкционированное (недокументированное) изменение пользователей портативной ЭВМ.
T2.17. Неправильная маркировка носителей данных.
T2.18. Неверная доставка носителей данных.
T2.19. Некорректная система управления криптографическими ключами.
T2.20. Неподходящее обеспечение расходными материалами факсов

# 10.1.8. АЛГОРИТМ АНАЛИЗА ИНФОРМАЦИОННЫХ РИСКОВ

## ИСХОДНЫЕ ДАННЫЕ ДЛЯ АНАЛИЗА РИСКОВ

- перечень ценной информации с указанием ее уровня критичности
- сведения об уязвимостях информационной системы
- сведения об угрозах, которые действуют на информационную систему

## АЛГОРИТМ АНАЛИЗА РИСКОВ

1. Инвентаризация информационных ресурсов
2. Оценка стоимости информационных ресурсов
3. Определение защищенности информационной системы
4. Оценка информационных рисков
5. Категоризация информационных ресурсов по уровню риска
6. Управление рисками (определение мер по снижению рисков)
7. Определение уровня приемлемого риска

## 10.1.9. МЕРЫ КОНТРОЛЯ УЯЗВИМОСТИ КАНАЛОВ ОБЪЕКТИВНОГО РАСПРОСТРАНЕНИЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ

- выявление и классификация реального максимального состава каналов объективного распространения конфиденциальной информации в фирме;
- изучение составных элементов каждого канала с целью нахождения опасных участков, способствующих возникновению канала несанкционированного доступа к информации;
- исследование и обобщение способов и сферы распространения информации в каждом канале;
- изучение и учет состава конфиденциальной информации, циркулирующей в каждом канале;
- изучение и учет состава конфиденциальной информации**,** циркулирующей между источниками;
- изучение сферы распространения информации при коммуникативных связях фирмы (по конкурентам, СМИ, выставкам, рекламным изданиям и т.п.);
- контроль и перекрытие каналов несанкционированного ознакомления с информацией ограниченного доступа для третьих лиц и посторонних людей;
- исследование состава и эффективности методов защиты, предпринятых по каждому каналу, и дополнительных мер противодействия злоумышленнику при активных угрозах и в экстремальных ситуациях.

# 10.2. ПОНЯТИЕ КАЧЕСТВЕННОЙ И КОЛИЧЕСТВЕННОЙ ОЦЕНКИ РИСКОВ, ШКАЛЫ И КРИТЕРИИ ИЗМЕРЕНИЯ

## 10.2.1. ВЫБОР ШКАЛЫ ДЛЯ ОЦЕНКИ ПАРАМЕТРОВ РИСКОВ

**Под оценкой параметров рисков понимается определение вероятности реализации потенциальной уязвимости, которая приведет к инциденту**

Риски могут быть оценены с помощью **количественных шкал**. Это даст возможность упростить анализ по критерию «стоимость-эффективность» предлагаемых контрмер. Однако в этом случае предъявляются более высокие требования к шкалам измерения исходных данных и проверке адекватности принятой модели.

Наиболее распространенной шкалой является **качественная (балльная) шкала** с несколькими градациями, например: низкий средний и высокий уровень. Оценка производится экспертом с учетом ряда объективных факторов. Уровни рисков:

| Уровень риска | Определение |
|---|---|
| **ВЫСОКИЙ** | **Источник угрозы (нарушитель) имеет очень высокий уровень мотивации, существующие методы уменьшения уязвимости малоэффективны** |
| **СРЕДНИЙ** | **Источник угрозы (нарушитель) имеет высокий уровень мотивации, однако используются эффективные методы уменьшения уязвимости** |
| **НИЗКИЙ** | **Источник угрозы (нарушитель) имеет низкий уровень мотивации, либо существуют чрезвычайно эффективные методы уменьшения уязвимости** |

# 10.2.2. ОЦЕНКА ТЯЖЕСТИ ПОСЛЕДСТВИЙ НАРУШЕНИЯ РЕЖИМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

| Уровень тяжести | Определение |
|---|---|
| **Высокий** | **Происшествие оказывает сильное (катастрофичное) воздействие на деятельность организации:**<br>- большая сумма (конкретизируется) прямых финансовых потерь;<br>- существенный ущерб здоровью персонала (гибель, инвалидность или необходимость длительного лечения сотрудника);<br>- потеря репутации, приведшая к существенному снижению деловой активности организации;<br>- дезорганизация деятельности на длительный (конкретизируется) период времени |
| **Средний** | **Происшествие приводит к заметным негативным результатам:**<br>- заметная сумма (конкретизируется) прямых финансовых потерь;<br>- потеря репутации, которая может вызвать уменьшение потока заказов и негативную реакцию деловых партнеров;<br>- неприятности со стороны государственных органов, в результате чего снизилась деловая активность компании |
| **Низкий** | **Происшествие сопровождается небольшими негативными последствиями:**<br>- небольшая сумма (конкретизируется) прямых финансовых потерь;<br>- задержки в работе некоторых служб либо дезорганизация деятельности на непродолжительный период времени;<br>- необходимость восстановления информационных ресурсов |

# 10.2.3. ОЦЕНИВАНИЕ РИСКОВ

## Шкалы и критерии

**Шкалы:** прямые (естественные), косвенные (производные).

**Примеры производной шкалы:**
а) субъективное свойство типа «ценность информационного ресурса» может измеряться в единицах, таких как стоимость или время восстанов-ления ресурса и др.
б) шкала для получения экспертной оценки: пример - ресурс: малоценный, средней ценности, ценный.

Риски оцениваются только по произ-водной шкале и **по критериям: объек-тивным (вероятность выхода из строя оборудования за определен-ный промежуток времени) либо субъективным (методики анализа рисков).**

В последнем случае разрабатывает-ся качественная шкала с несколькими градациями, например: низкий, средний, высокий уровень - в качественных единицах, поскольку оценка должна отражать субъективную точку зрения владельца информацион-ных ресурсов и учитывать не только технические, но организационные, психологические и др. аспекты

## Оценка вероятностей событий

Субъективная вероятность - мера уверенности человека или группы людей в том, что данное событие в действитель-ности будет иметь место: вероятностным распределением или бинарным отношением на множестве событий, не полностью заданным вероятностным распределением или бинарным отношением и другими способами. Субъективная вероятность увязывается с системой предпочтений

***Первый этап.*** Во время этого этапа формируется объект исследования - множество событий, а также выпол-няется предварительный анализ свойств этого множества (устанавливается зависимость или независимость событий, дискретность или непрерывность случайной величины, порождающей данное множество событий). На основе такого анализа выбирается один из подходящих методов определе-ния субъективной вероятности. На этом же этапе произво-дится подготовка эксперта или группы экспертов, ознакомле-ние их с методом и проверка понимания ими поставленной задачи.

***Второй этап.*** Состоит в применении метода, выбранного на первом этапе. Результатом этого этапа является набор чисел, который отражает субъективный взгляд эксперта или группы экспертов на вероятность того или иного события, однако далеко не всегда может считаться окончательным распределением, поскольку нередко оказывается противоречивым.

***Третий этап.*** На этом этапе исследуются результаты опроса. Если вероятности, представленные экспертами, не согласуются с аксиомами вероятности, то на это обращается внимание экспертов и ответы уточняются с целью приведе-ния их в соответствие с выбранной системой аксиом

# 10.3. КОМПЛЕКСНАЯ ОЦЕНКА РИСКОВ БЕЗОПАСНОСТИ И ЕЕ ОСНОВНЫЕ ЭТАПЫ.
## 10.3.1. ОЦЕНКА РИСКОВ ПО ДВУМ ФАКТОРАМ

**Факторы:** вероятность происшествия и тяжесть возможных последствий.

Риск тем больше, чем больше вероятность происшествия и тяжесть последствий:

«РИСК = Рпроисшествия × ЦЕНА ПОТЕРИ».

Если переменные являются количественными величинами, то риск - это оценка математического ожидания потерь.

**1. Определение шкал при использовании качественных величин**

**а) субъективная шкала вероятностей событий:**

A - событие практически никогда не происходит; B - событие случается редко;
C - вероятность события за рассматриваемый промежуток времени - около 0,5;
D - скорее всего, событие произойдет; E - событие почти обязательно произойдет.

**б) субъективная шкала серьезности происшествий**

N (Negligible) - воздействием можно пренебречь;

Mi (Minor) - незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий (ЛП) невелики, воздействие на ИТ незначительно;

Mo (Moderate) - происшествие с умеренными результатами: ЛП не связана с крупными затрата-ми, воздействие на ИТ небольшое и не затрагивает критически важные задачи;

S (Serious) - происшествие с серьезными последствиями: ЛП связана со значительными затра-тами, воздействие на ИТ ощутимо, влияет на выполнение критически важных задач;

C (Critical) - происшествие приводит к невозможности решения критически важных задач.

**в) шкала для оценки рисков:** низкий риск; средний риск; высокий риск.

| Шкала | Negligible | Minor | Moderate | Serious | Critical |
|---|---|---|---|---|---|
| A | Низкий риск | Низкий риск | Низкий риск | Средний | Средний |
| B | Низкий риск | Низкий риск | Средний | Средний | Высокий |
| C | Низкий риск | Средний | Средний | Средний | Высокий |
| D | Средний | Средний | Средний | Средний | Высокий |
| E | Средний | Высокий | Высокий | Высокий | Высокий |

## 10.3.2. ОЦЕНКА ВОЗМОЖНОГО УЩЕРБА (ПОТЕРЬ)

**Оценивая тяжесть ущерба, необходимо иметь в виду:**

- непосредственные расходы на замену оборудования, исследование причин преодоления защиты, восстановление информации и функционирования АС по ее обработке;
- косвенные потери, связанные со снижением банковского доверия, потерей клиентуры, подрывом репутации, ослаблением позиций на рынке.

**Для оценки потерь необходимо построить сценарий действий:**

- нарушителя по использованию добытой информации;
- службы ОИБ по предотвращению последствий и восстановлению нормального функционирования системы;
- третьей стороны.

**Оценивая последствия потери ресурса нужно учитывать:**

- цену ресурса - затраты на производство;
- стоимость восстановления или создания (покупку) нового ресурса;
- стоимость восстановления работоспособности организации;
- стоимость вынужденного простоя;
- стоимость упущенной выгоды (потерянный контракт);
- стоимость выплаты неустоек, штрафов (за невыполнение обязательств контракта);
- стоимость затрат на реабилитацию репутации, престижа, имени фирмы;
- стоимость затрат на поиск новых клиентов, взамен не доверяющих фирме;
- стоимость затрат на поиск (или восстановление) новых каналов связи, информационных источников.

**Мотивы нарушений**

- неопытность;
- корыстный интерес;
- безответственность (самоутверждение).

# 10.3.3. ОЦЕНКА РИСКОВ ПО ТРЕМ ФАКТОРАМ

**Факторы:** угроза, уязвимость, цена потери.

Вероятность происшествия, которая может быть объективной либо субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

«$P_{происшествия} = P_{угрозы} \times P_{уязвимости}$»

«РИСК = $P_{угрозы}$ x $P_{уязвимости}$ × ЦЕНА ПОТЕРИ»

Если хотя бы одна из шкал – качественная, применяются табличные методы для расчета риска.

**Например, показатель риска измеряется по 8-балльной шкале:**

**1** - риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик;

**2** - риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики;

…

**8** - риск очень велик. Событие, скорее всего, наступит, и последствия будут чрезвычайно тяжелыми

**Уровни уязвимости Н, С, В означают, соответственно, низкий, средний и высокий.**

| Степень серьезности происшествия (цена потери) | Уровень угрозы | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | низкий | | | средний | | | высокий | | |
| | Уровни уязвимостей | | | | | | | | |
| | Н | С | В | Н | С | В | Н | С | В |
| Negligible | 0 | 1 | 2 | 1 | 2 | 3 | 2 | 3 | 4 |
| Minor | 1 | 2 | 3 | 2 | 3 | 4 | 3 | 4 | 5 |
| Moderate | 2 | 3 | 4 | 3 | 4 | 5 | 4 | 5 | 6 |
| Serious | 3 | 4 | 5 | 4 | 5 | 6 | 5 | 6 | 7 |
| Critical | 4 | 5 | 6 | 5 | 6 | 7 | 6 | 7 | 8 |

## 10.3.4. ОЦЕНКА ФАКТОРОВ РИСКА

**Для оценки *угроз* выбраны следующие косвенные факторы:**

статистика по зарегистрированным инцидентам;
тенденции в статистке по подобным нарушениям;
наличие в системе информации, представляющей интерес для потенциальных внутренних или внешних нарушителей;
моральные качества персонала;
возможность извлечь выгоду из изменения обрабатываемой в системе информации;
наличие альтернативных способов доступа к информации;
статистика по подобным нарушениям в других информационных системах организации.

**Оценка *уязвимостей* выполняется на основе следующих косвенных факторов:**

количество рабочих мест (пользователей) в системе;
размер рабочих групп;
осведомленность руководства о действиях сотрудников (разные аспекты);
характер установленного на рабочих местах оборудования и ПО;
полномочия пользователей.

**По косвенным факторам предлагаются вопросы и несколько фиксированных вариантов ответов, которые «стоят» определенное количество баллов.**

**Итоговая оценка определяется путем суммирования баллов:**

**а) угрозы**

| | |
|---|---|
| До 9 | Очень низкая |
| От 10 до 19 | Низкая |
| От 20 до 29 | Средняя |
| От 30 до 39 | Высокая |
| 40 и более | Очень высокая |

**б) уязвимости**

| | |
|---|---|
| До 9 | Низкая |
| От 10 до 19 | Средняя |
| 20 и более | Высокая |

## 10.3.5. ОЦЕНКА УГРОЗЫ

**1**. Сколько раз за последние три года сотрудники организации пытались получить НСД к хранящейся в информационной системе информации с использованием прав других пользователей?

| | | |
|---|---|---|
| a | Ни разу | 0 |
| b | Один или два раза | 10 |
| c | В среднем раз в год | 20 |
| d | Чаще одного раза в год | 30 |
| e | Неизвестно | 10 |

**2.** Какова тенденция в статистике такого рода попыток несанкционированного проникновения в информационную систему?

| | | |
|---|---|---|
| a | К возрастанию | 10 |
| b | Оставаться постоянной | 0 |
| c | К снижению | -10 |

**3.** Хранится ли в информационной системе информация (напр., личные дела), которая может представлять интерес для сотрудников организации и побуждать к НСД к ней?

| | | |
|---|---|---|
| a | Да | 5 |
| b | Нет | 0 |

**4**. Известны ли случаи нападения, угроз, шантажа, давления на сотрудников со стороны посторонних лиц?

| | | |
|---|---|---|
| a | Да | 10 |
| Ь | Нет | 0 |

## 10.3.6. ОЦЕНКА УГРОЗЫ

**5**. Есть ли среди персонала группы лиц или отдельные лица с недостаточно высокими моральными качествами?

| | | |
|---|---|---|
| a | Нет, все сотрудники отличаются высокой честностью и порядочностью | 0 |
| b | Существуют группы лиц и отдельные личности с недостаточно высокими моральными качествами, но это вряд ли может спровоцировать их на несанкционированное использование системы | 5 |
| c | Существуют группы лиц и отдельные личности с настолько низкими моральными качествами, что это повышает вероятность несанкционированного использования системы сотрудниками | 10 |

**6**. Хранится ли в системе информация, несанкционированное изменение которой может принести прямую выгоду сотрудникам?

| | | |
|---|---|---|
| a | Да | 5 |
| b | Нет | 0 |

**7**. Предусмотрена ли в информационной системе поддержка пользователей, обладающих техническими возможностями совершить подобные действия?

| | | |
|---|---|---|
| a | Нет | 0 |
| b | Да | 5 |

**8**. Существуют ли другие способы просмотра информации, позволяющие злоумышленнику добраться до нее более простыми методами, чем с использованием «маскарада»?

| | | |
|---|---|---|
| a | Да | -10 |
| Ь | Нет | 0 |

**9**. Имеются ли другие способы несанкци-онированного изменения информации, позволяющие злоумышленнику достичь желаемого результата более простыми методами?

| | | |
|---|---|---|
| a | Да | -10 |
| Ь | Нет | 0 |

**10**. Сколько раз за последние три года сотрудники пытались получить НСД к информации, хранящейся в других подобных системах вашей организации?

| | | |
|---|---|---|
| a | Ни разу | 0 |
| b | Один или два раза | 5 |
| c | В среднем раз в год | 10 |
| d | В среднем чаще одного раза в год | 15 |
| e | Неизвестно | 10 |

# 10.3.7. ОЦЕНКА УЯЗВИМОСТИ

**1.** Сколько людей имеют право пользоваться информационной системой?

| | | |
|---|---|---|
| a | От 1 до 10 | 0 |
| b | От 11 до 50 | 4 |
| c | От 51 до 200 | 10 |
| d | От 200 до 1000 | 14 |
| e | Свыше 1000 | 20 |

**2.** Будет ли руководство осведомлено о том, что сотрудники, работающие под его началом, ведут себя необычным образом?

| | | |
|---|---|---|
| a | Да | 0 |
| b | Нет | 10 |

**3.** Какие устройства и программы доступны пользователям?

| | | |
|---|---|---|
| a | Только терминалы или сетевые контроллеры, ответственные за предоставление и маршрутизацию информации, но не за ПД | -5 |
| b | Только стандартные офисные устройства и программы, а также управляемые с помощью меню подчиненные программы | 0 |
| c | Пользователи могут получить доступ к ОС, но не к компиляторам | 5 |
| d | Пользователи могут получить доступ к компиляторам | 10 |

**4.** Возможно ли, что сотрудникам, предупрежденным о предстоящем увольнении, разрешается логический доступ к ИС?

| | | |
|---|---|---|
| a | Да | 10 |
| Ь | Нет | 0 |

**5.** Каковы в среднем размеры рабочих групп сотрудников пользовательских подразделений, имеющих доступ к информационной системе?

| | | |
|---|---|---|
| a | Менее 10 человек | 0 |
| b | От 11 до 20 человек | 5 |
| c | Свыше 20 человек | 10 |

**6.** Станет ли факт изменения хранящихся в информационной системе данных очевидным сразу для нескольких человек?

| | | |
|---|---|---|
| a | Да | 0 |
| b | Нет | 10 |

**7.** Насколько велики официально предоставленные пользователям возможности по просмотру всех хранящихся данных?

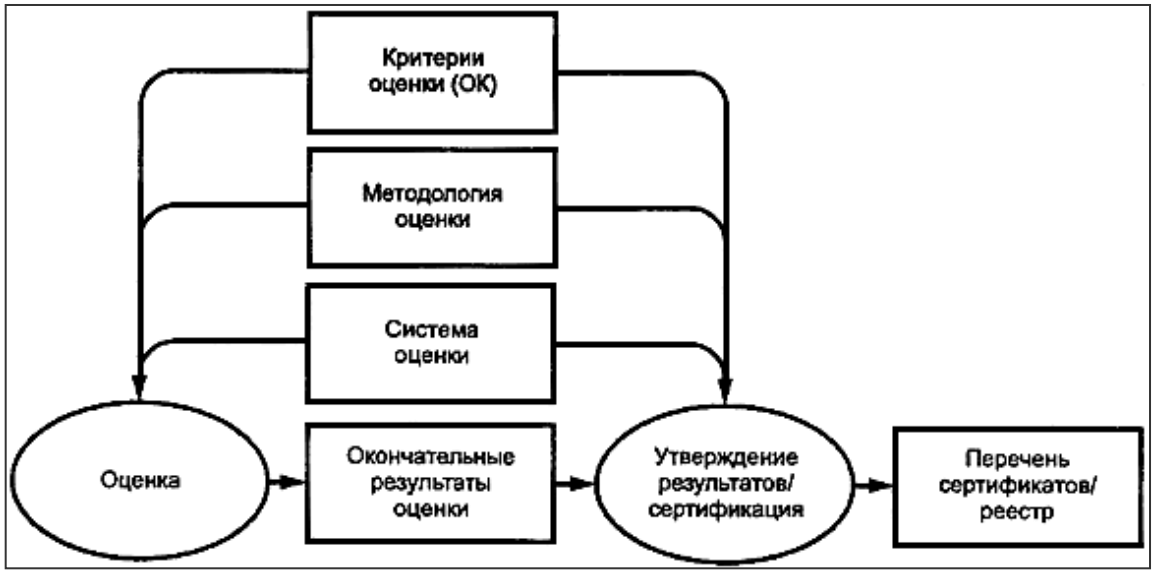
| | | |
|---|---|---|
| a | Официальное право предоставлено всем пользователям | --2 |
| b | Официальное право предоставлено только некоторым пользователям | 0 |

**8.** Насколько необходимо пользователям знать всю информацию, хранящуюся в системе?

| | | |
|---|---|---|
| a | Всем всю информацию | -4 |
| b | Только в части касающейся | 0 |

# 10. 4. КРИТЕРИИ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ.
## 10.4.1. ФОРМИРОВАНИЕ КОНТЕКСТА ОЦЕНКИ

**Для достижения большей сравнимости результатов оценок их следует проводить в рамках полномочной системы оценки, которая устанавливает стандарты, контролирует качество оценок и определяет нормы, которыми необходимо руководствоваться организациям, проводящим оценку, и самим оценщикам**




**Для повышения согласованности выводов, полученных при оценке, ее конечные результаты могут быть представлены на сертификацию. Процедура сертификации представляет собой независимую инспекцию результатов оценки, которая завершается их утверждением или выдачей сертификата**

*ISO 15408 и ISO 17799 (BS 7799)*

## 10.4.2. КРИТЕРИИ ОЦЕНКИ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

| Критерии оценки | Эффективность, % |
|---|---|
| Корпоративные стандарты контроля собственной разработки | 43 |
| Замечания аудиторов | 40 |
| Стандарты лучшей мировой практики | 29 |
| Число инцидентов в области безопасности | 22 |
| Финансовые потери в результате инцидентов | 22 |
| Расходы на ИБ | 16 |
| Эффективность в достижении поставленных целей | 14 |

**Оценка эффективности вложенных средств**

ROSI (Return of Security Investment) – коэффициент окупаемости инвестиций в ИБ, ко-торый определяет эффективность каждой единицы денежных средств, вложенных в информационную безопасность.

В общем случае ROI (Return of Investment) определяется как отношение прибыли к вложенным средствам. В сфере ИБ прибыль – величина, на которую снизился информационный риск после внедрения контрмер. Таким образом

**ROSI = (R1-R2):C,** где:

R1 – риск до внедрения контрмер
R2 – риск после внедрения контрмер
C – затраты на внедрение контрмер

## 10.4.3. МЕТОД OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET AND VULNERABILITY EVALUATION)

**Метод OCTAVE - метод оперативной оценки критических угроз, активов, уязвимостей и рисков информационной безопасности группой анализа из сотрудников бизнес-подразделений, эксплуатирующих систему, и сотрудников отдела информационных технологий.**

**На первой стадии** осуществляется оценка организационных аспектов и определяются:

- критерии (показатели) оценки ущерба (неблагоприятных последствий), которые будут использоваться при оценке рисков;
- наиболее важные организационные ресурсы и оценка текущего состояния практики обеспечения безопасности в организации;
- требования безопасности и строится профиль угроз для каждого критического ресурса.

**На второй стадии** проводится высокоуровневый анализ ИТ-инфраструктуры организа-ции, при этом обращается внимание на степень, с которой вопросы безопасности решаются и поддерживаются подразделениями и сотрудниками, отвечающими за эксплуатацию инфраструктуры.

**На третьей стадии** проводится разработка стратегии обеспечения безопасности и плана защиты информации:

- определение и анализ рисков и разработки стратегии ОИБ и плана сокращения рисков
- оценивается ущерб от реализации угроз, устанавливаются вероятностные критерии оценки угроз, оценивается вероятность реализации угроз.
- описывают текущую стратегию безопасности,
- выбирают подходы сокращения рисков,
- разрабатывают план сокращения рисков,
- определяют изменения в стратегии обеспечения безопасности,
- определяют перспективные направления обеспечения безопасности.

# Глава 11.
# ОРГАНИЗАЦИЯ И ПРОВЕДЕНИЕ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

**11.1.** Сущность и содержание аудита, направленного на оценку системы управления информационной безопасностью.

**11.2.** Требования COBIT в реализации аудита информационной безопасности

**11.3.** Инструментальные средства анализа информационной безопасности.

## Литература:


1. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность/Петренко С. А., Симонов С. В. - М.: Компания АйТи; ДМК Пресс, 2004. - 384 с.
2. ГОСТ Р ИСО/МЭК 15408-2. Методы и средства ОИБ. Критерии ИБ информационных технологий. Прил. С.


Оглавление

# 11.1. СУЩНОСТЬ И СОДЕРЖАНИЕ АУДИТА, НАПРАВЛЕННОГО НА ОЦЕНКУ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

## 11.1.1. СУЩНОСТЬ И ЦЕЛЬ АУДИТА

**ПРОВЕРКА И ОЦЕНКА ИБ ОРГАНИЗАЦИИ**

- **Аудит ИБ**
- **Самооценка ИБ**
- **Мониторинг ИБ**

**АУДИТ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (комплексное обследование защищенности) – системный процесс получения и оценки объективных данных о текущем состоянии обеспечения информационной безопасности объектов информатизации, действиях и событиях, происходящих в информационной системе, определяющих уровень их соответствия определенному критерию;**

**независимая оценка текущего состояния системы ИБ, устанавливающая уровень ее соответствия определенным критериям, и предоставление результатов в виде рекомендаций для принятия обоснованных управленческих решений по обеспечению необходимой защищенности информационных активов**

**ЦЕЛЬ АУДИТА БЕЗОПАСНОСТИ:**

проверка и оценка соответствия ИБ требованиям стандарта, а также **выявление текущего уровня ИБ организации; уровня зрелости процессов менеджмента ИБ организации; уровень осознания ИБ организации.**

методологическое обследование процессов, методов и средств ОИБ при выполнении ИС своего главного предназначения - информационного обеспечения бизнеса;

получение объективных данных о текущем состоянии ОИБ на объектах ИС, позволяющих провести минимизацию вероятности причинения ущерба собственнику информационных активов в результате нарушения конфиденциальности, целостности или доступности информации, за счет получения НСД к ней, а также выработка комплекса мер, направленных на повышение степени защищенности информации

## 11.1.2. ЗАДАЧИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Повышение уровня защиты информации до приемлемого;
2. Оптимизация и планирование затрат на обеспечение информационной безопасности;
3. Обоснование инвестиций в системы защиты;
4. Получение максимальной отдачи от инвестиций, вкладываемых в системы защиты информации;
5. Подтверждение того, что используемые внутренние средства контроля соответствуют задачам организации и позволяют обеспечить эффективность и непрерывность бизнеса.

### ОСНОВНЫЕ ВИДЫ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:

- **экспертный аудит** безопасности, в ходе которого выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в процедуре обследования;
- **оценка соответствия рекомендациям международного стандарта ISO 17799**, а также требованиям руководящих документов ФСТЭК;
- **инструментальный анализ защищенности ИС**, направленный на выявление и устранение уязвимостей программно-аппаратного обеспечения системы;
- **комплексный аудит**, включающий в себя все вышеперечисленные формы проведения обследования

## 11.1.3. МОДЕЛЬ ЗРЕЛОСТИ ПРОЦЕССОВ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (на примере ОИБ БС РФ)

Универсальная **модель зрелости процессов, определенная стандартом COBIT**, определяет шесть уровней зрелости организации.

**Нулевой уровень** характеризует полное отсутствие каких-либо процессов менеджмента ИБ. Организация не осознает существования проблем ИБ.

**Первый уровень** (“начальный”) характеризует наличие документально зафиксированных свидетельств осознания организацией существования проблем обеспечения ИБ, используемые процессы менеджмента ИБ нестандартизованы, применяются эпизодически и бессистемно. Общий подход к менеджменту ИБ не выработан.

**Второй уровень** (“повторяемый”) характеризует проработанность процессов менеджмента ИБ до уровня, когда их выполнение обеспечивается различными людьми, решающими одну и ту же задачу. Однако отсутствуют регулярное обучение и тренировки по стандартным процедурам, а ответственность возложена на исполнителя. Руководство организации в значительной степени полагается на знания исполнителей, что влечет за собой высокую вероятность возможных ошибок.

**Третий уровень** (“определенный”) характеризует то, что процессы стандартизованы, документированы и доведены до персонала посредством обучения, но порядок использования данных процессов оставлен на усмотрение самого персонала. Это определяет вероятность отклонений от стандартных процедур, которые могут быть не выявлены. Применяемые процедуры не оптимальны и недостаточно современны.

**Четвертый уровень** (“управляемый”) характеризует то, что обеспечиваются мониторинг и оценка соответствия используемых в организации процессов. При выявлении низкой эффективности реализуемых процессов менеджмента ИБ обеспечивается их оптимизация. Процессы менеджмента ИБ находятся в стадии непрерывного совершенствования и основываются на хорошей практике. Средства автоматизации менеджмента ИБ используются частично и в ограниченном объеме.

**Пятый уровень** (“оптимизированный”) характеризует проработанность процессов до уровня лучшей практики, непрерывное совершенствование и сравнение уровня зрелости относительно других организаций. Защитные меры в организации используются комплексно, обеспечивая основу совершенствования процессов менеджмента ИБ. Организация способна к быстрой адаптации при изменениях

# 11.1.4. ПАРАМЕТРЫ ДОСТИЖЕНИЯ ЧЕТВЕРТОГО УРОВНЯ ЗРЕЛОСТИ ПРОЦЕССОВ МЕНЕДЖМЕНТА ИБ

- разработана и совершенствуется нормативная и распорядительная документация по ИБ (политика ИБ, регламенты и положения ИБ, должностные инструкции персонала и т.п.);
- создана организационная структура управления ИБ и четко определена ответственность персонала за деятельность, связанную с обеспечением ИБ;
- финансирование ИБ осуществляется по отдельной статье бюджета;
- есть назначенный куратор службы ИБ;
- осуществляется приобретение необходимых средств обеспечения ИБ;
- защитные меры (технические, технологические, организационные) встроены в банковские технологические процессы, непрерывно совершенствуются и основываются на хорошей практике. В процессе внедрения защитных мер используется анализ затрат и результатов, обеспечивается их оптимизация;
- последовательно выполняется анализ ИБ организации и рисков нарушения ИБ, а также возможных негативных воздействий;
- краткие занятия с работниками организации по вопросам обеспечения ИБ носят обязательный характер;
- введена аттестация персонала по вопросам обеспечения безопасности;
- проверки на возможность вторжения в ЛС являются стандартизованным и формализованным процессом;
- осуществляется оценка соответствия организации требованиям ИБ;
- стандартизованы идентификация, аутентификация и авторизация пользователей, защитные меры совершенствуются с учетом накопленного опыта;
- уровень стандартизации и документирования процессов управления ИБ позволяет проводить аудит ИБ в достаточном объеме;
- процессы обеспечения ИБ координируются со службой безопасности всей организации;
- деятельность по обеспечению ИБ увязана с целями бизнеса;
- руководство организации понимает проблемы ИБ и участвует в их решении через куратора службы ИБ из состава высшего руководства организации

# 11.1.5. ПЕРЕЧЕНЬ ИСХОДНЫХ ДАННЫХ ДЛЯ АУДИТА БЕЗОПАСНОСТИ

| Тип информации | Состав исходных данных |
|---|---|
| **Организационно-распорядительная документация по вопросам ИБ** | • политика информационной безопасности ИС;<br>• руководящие документы (приказы, распоряжения, инструкции) по вопросам хранения, доступа и передачи информации;<br>• регламенты работы пользователей с информационными ресурсами ИС |
| **Информация об аппаратном обеспечении хостов** | • перечень серверов, рабочих станций и коммуникационного оборудования, установленного в ИС;<br>• аппаратные конфигурации серверов и рабочих станций;<br>• сведения о периферийном оборудовании |
| **Информация об общесистемном ПО** | • сведения об ОС, установленных на рабочих станциях и серверах;<br>• сведения о СУБД, установленных в ИС |
| **Информация о прикладном ПО** | •перечень прикладного ПО общего и специального назначения, установленного в ИС;<br>•описание функциональных задач, решаемых с помощью прикладного ПО |
| **Информация о средствах защиты, установленных в ИС** | •производитель средства защиты;<br>•конфигурационные настройки средства защиты;<br>•схема установки средства защиты |
| **Информация о топологии ИС** | •карта ЛВС, включая схему распределения серверов и рабочих станций по сегментам сети;<br>•типы каналов связи, используемых в ИС;<br>•используемые в ИС сетевые протоколы;<br>•схема информационных потоков ИС |

# 11.1.6а. СБОР И АНАЛИЗ ИНФОРМАЦИИ ДЛЯ ПРОВЕДЕНИЯ АУДИТА

**А) Организационные характеристики:**

- наличие, полнота и актуальность организационно-регламентных и нормативно-технических документов;
- разделение зон ответственности ролей персонала по ОИБ и его корректность;
- наличие документированных списков, описывающих полномочия по доступу к сетевым устройствам и серверам;
- наличие планов по поддержке квалификации персонала, ответственного за ОИБ;
- осведомленность пользователей и персонала о требованиях ОИБ;
- корректность процедур управления изменениями и установления обновлений;
- порядок предоставления доступа к внутренним ресурсам информационных систем;
- наличие механизмов разграничения доступа к документации.

**Б) Организационно-технические характеристики:**

- возможности использования найденных уязвимых мест в сетевых устройствах и серверах для реализации атак;
- наличие оперативного анализа журналов аудита и реагирования на события, связанные с попытками НСД, оценка полноты анализируемых событий, оценка адекватности защиты журналов аудита;
- наличие процедур по обнаружению и фиксации инцидентов ИБ и механизмов расследования таких инцидентов;
- наличие процедуры и документирование любых действий, связанных с модификацией прав доступа и изменениями параметров аудита;
- периодичность контроля защищенности сетевых устройств и серверов;
- наличие процедуры отслеживания новых уязвимостей в СПО и его обновления;
- ограничение доступа в серверные помещения;
- адекватность времени восстановления в случае сбоев;
- наличие зоны опытной эксплуатации новых решений, процедуры тестирования и ввода в промышленную эксплуатацию

# 11.1.6б. СБОР И АНАЛИЗ ИНФОРМАЦИИ ДЛЯ ПРОВЕДЕНИЯ АУДИТА

## В) Технические характеристики, связанные с архитектурой ИС:

- топология и логическая организация сетевой инфраструктуры, адекватность контроля логических путей доступа, адекватность сегментирования;
- топология и логическая организация системы защиты периметра, адекватность контроля доступа из внешних сетей;
- топология, логическая организация и адекватность контроля доступа между сегментами;
- наличие узлов, сбои на которых приведут к невозможности функционирования значительной части ИС;
- наличие точек удаленного доступа к информационным ресурсам ИС и адекватность защиты такого доступа

## Г) Технические характеристики, связанные с конфигурацией сетевых устройств и серверов ИС:

- права доступа персонала к сетевым устройствам и серверам, оценка минимально необходимых прав, которые требуются для выполнения производственных задач;
- соответствие списков контроля доступа на критичных сетевых устройствах документированным требованиям;
- соответствие конфигурации ОС и использованию штатных механизмов ИБ рекомендациям производителя и лучшей практике;
- наличие неиспользованных сервисов или сервисов, содержащих известные уязвимости;
- соответствие механизма и стойкости процедуры аутентификации - критичности ресурсов, оценка адекватности парольной политики и протоколирования деятельности операторов.

## Д) Технические характеристики, связанные с использованием встроенных механизмов ИБ:

- оценка соответствия конфигурации встроенных средств защиты документированным требованиям и оценка адекватности существующей конфигурации;
- оценка адекватности использования криптографической защиты информации и процедуры распределения ключевой информации;
- наличие антивирусной проверки трафика, а также антивирусного контроля на рабочих станциях пользователей;
- наличие резервных копий файлов конфигурации и образов дисков для критичных сетевых устройств и серверов;
- наличие источников бесперебойного питания для критичных сетевых устройств и серверов и их адекватность требованиям по времени бесперебойной работы.

## 11.1.7. ОСНОВНЫЕ НАПРАВЛЕНИЯ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

| ТЕХНОЛОГИЧЕСКИЙ АУДИТ | АУДИТ СИСТЕМЫ УПРАВЛЕНИЯ ИБ | АНАЛИЗ ИНФОРМАЦИОННЫХ РИСКОВ |
|---|---|---|
| **Применяемые методики**:<br>- NSA Infosec,<br>- NIST,<br>- OSSTM.<br>**Модель нарушителя:**<br>субъект, имеющий физический доступ к корпоративной ИС и не обладающий правами доступа к информационным ресурсам.<br>**Объекты аудита:**<br>сетевая инфраструктура,<br>серверы,<br>рабочие станции | **Организационные ОИБ**<br>Классификация и управление ресурсами.<br>Безопасность персонала<br>Физическая безопасность<br>Управление коммуникациями и процессами.<br>Контроль доступа.<br>Разработка и техническая поддержка ВС.<br>Управление непрерывностью бизнеса.<br>Соответствие системы основным требованиям | **Цель** - разработка экономически эффективной и обоснованной СОИБ.<br>**Задачи**:<br>комплексная оценка защищенности ИС<br>оценка стоимости информации (потенциального ущерба);<br>оценка риска (вероятного ущерба);<br>разработка комплексной СОИБ в соответствии с оценками информационных рисков.<br>**Для чего необходим анализ информационных рисков**?<br>определение вероятного ущерба (риска) по существующим видам ценной информации,<br>сравнение риска с затратами на ОИБ,<br>оценка эффективности затрат на ОИБ |

*ISO 17799*

# 11.1.8. СТАДИИ И МЕТОДЫ ОБСЛЕДОВАНИЯ В ХОДЕ АУДИТА

**Сбор и предварительный анализ исходных данных** (стадия планирования)

**Оценка соответствия** состояния защищенности ИС предъявляемым требованиям и стандартам (стадии моделирования, тестирования и анализа): документы ФСТЭК России, ФСБ, ГОСТ ИСО/МЭК 15408, IS0 17799 (BS 7799), HIPPA

**Формулирование рекомендаций** по повышению безопасности в обследуемой ИС (стадии разработки предложений и документирования результатов)

## ОСНОВНЫМИ ГРУППАМИ МЕТОДОВ ПРИ ОБСЛЕДОВАНИИ ЯВЛЯЮТСЯ:

**Экспертно-аналитические методы** - предусматривают проверку соответствия обследуемого объекта установленным требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации оборудования предъявляемым требованиям по размещению, монтажу и эксплуатации технических и программных средств

**Экспертно-инструментальные методы** - предполагают проведение проверки функций или комплекса функций защиты информации с помощью специального инструментария (тестирующих средств) и средств мониторинга, а также путем пробного запуска средств защиты информации и наблюдения реакции за их выполнением

**Моделирование действий злоумышленника** - («дружественный взлом» СЗИ) – применяются после анализа результатов, полученных в ходе использования первых двух групп методов, - они необходимы как для контроля данных результатов, а также для подтверждения реальных возможностей потенциальных злоумышленников.

# 11.1.9. МЕТОДИКИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## Good Practice

1.Стандарт **Good Practice** создан ассоциацией Information Security Forum (более 11 лет, 240 организаций).

2. Стандарт ориентирован на анализ безопасности ИТ системы с точки зрения функционирования и поддержания бизнес-процессов.

3. **Совокупность бизнес-требований к системе**:

Security Management (управление безопасностью);
Critical Business Applications (критичные бизнес-приложения);
Information Processing (обработка информации);
Communications networks (вычислительные сети);
Systems Development (разработка систем)

## GAO FISCAM

**GAO** (General Accounting Office) и National State Auditors Association (NSAA) разработали «Management Planning Guide for Information Systems Security Auditing» - «Руководство планирования и управления для аудита СИБ»

**FISCAM** - Federal Information Systems Control Audit Manual –методология аудита безопасности ИТ систем GAO:

- Introduction and Methodology (введение и методология)
- Planning the Audit (планирование аудита)
- Evaluation and Testing General Controls (общий контроль: расчет и тестирование)
- Evaluation and Testing Application Controls (контроль приложений: расчет и тестирование)
- Appendixes (приложения).

## NIST

**NIST** - Национальный институт стандартов и технологий (National Institute of Standard and Technologies) разработал серию документов по аудиту ИБ:

- Draft Guideline on Network Security Testing (методы инструментальной проверки сетевой безопасности )
- Security Self Assessment Guide for Information Technology Systems (типовые вопросы аудитора)
- Risk management Guide for Information Technology Systems (методология анализа и управления рисками)

**Этапы анализа рисков :**

- Характеристики системы;
- Идентификация угрозы;
- Идентификация уязвимостей;
- Анализ существующих методов и требований по управлению ИБ;
- Вероятность проявления;
- Анализ воздействия;
- Определение риска;
- Рекомендации по управлению рисками и ИТ-защита;
- Итоговая документация.

# 11.1.10. МЕТОДИКА АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Методика NSA INFOSEC Assessment Methodology АНБ США (National Security Agency) - разработана во второй половине 90-х годов XX в.**

**1. Предварительная оценка**

Ранжирование и определение ценности информации.
Определение систем и границ.
Сбор документации по информационной системе и системе ИБ.
Приготовление плана обследования

**2. Непосредственный анализ**

1. Документация ИБ.
2. Роли и ответственности.
3. Идентификация и аутентификация.
4. Управление доступом.
5. Контроль сессий.
6. Внешние связи.
7. Телекоммуникации.
8. Аудит.
9. Вирусная защита.
10. План непрерывности.
11. Поддержка.
12. Управление конфигурациями.
13. Резервирование.
14. Категорирование.
15. Уничтожение материалов.
16. Физическая защита.
17. Персонал.
18. Обучение и информирование

**Уровень 1:**
- Проверка документации.
- Интервью персонала.
- Цели; анализ критичности.

**Уровень 1+:**
- Сканирование без проникновения.
- Краткие выводы: достоинства/ слабости.

**Уровень 2:**
- Техническое обследование и тестирование.
- Специфичные технич. экспертизы.
- Инструменты по проникновению.
- Диагностические инструменты.

**Уровень 3 (Красная группа):**
- Внешнее обследование.
- Внешние тесты на проникновение.
- Симуляция действий потенциального злоумышленника

**3. Выводы**

**Анализ и формирование отчета** выполняется в течение 45-60 дней после фазы 2.

# 11.1.11. СОСТАВ РАБОТ ПО ПРОВЕДЕНИЮ АУДИТА

**1. Планирование проведения обследования:**

- определение границ проведения обследования;
- выбор критериев оценки (требования, стандарты), по которым проводится обследование;
- определение порядка взаимодействия в ходе обследования;
- разработку программы обследования;
- определение условий обращения с конфиденциальной информацией.

**2. Проведение комплексного обследования:**

- сбор исходных данных для обследования;
- классификация информационных ресурсов компании;
- моделирование процессов нарушения безопасности информации и анализ угроз;
- определение требуемого уровня гарантий безопасности в соответствии с выбранными критериями;
- анализ организационно-распорядительных документов о функционировании ИС и ЗИ;
- анализ структуры состава и принципов функционирования корпоративной ИС и существующей СЗИ;
- анализ деятельности персонала компании по обеспечению безопасности информации.

**3. Оценка эффективности существующей СЗИ с применением инструментариев:**

а) определение и фиксирование на момент проверки реальной конфигурации СЗИ

б) проведение испытаний программных и программно-аппаратных средств защиты, а также встроенных механизмов защиты общесистемного программного обеспечения, используемых в СЗИ;

- тестовые испытания программных средств защиты;
- тестовые испытания защиты ИС от утечки за счет наводок и ПЭМИН;
- тестовые испытания ЗИ от утечки по акустическому и виброакустическому каналу;
- подготовка предложений по повышению защищенности сети от НСД.

в) проведение испытаний функций СЗИ методом моделирования действий злоумышленника:

- определение места и порядка подключения тестирующих средств;
- анализ сетевой топологии и установленных сервисов;
- проведение сетевого сканирования и определение установленных сервисов;
- проведение анализа трафика и сбор критичной информации с применением программ пассивного анализа (программ-снифферов и программ обнаружения вторжений);
- обнаружение имеющихся уязвимостей по имеющимся сигнатурам;
- оценка защищенности коммутируемого доступа и анализ полученных результатов

## 11.1.12. СТРУКТУРА АУДИТОРСКОГО ОТЧЕТА

**Оценка текущего уровня защищенности информационной системы:**

описание и оценка текущего уровня защищенности информационной системы;

анализ конфигурации конфигурационной информации, найденные уязвимости;

анализ рисков, связанных с возможностью осуществления внутренних и внешних угроз в отношении ресурсов ИС.

**Рекомендации по технической составляющей ИБ:**

по изменению конфигурации существующих сетевых устройств и серверов;

по изменению конфигурации существующих средств защиты;

по активации дополнительных штатных механизмов безопасности на уровне СПО;

по использованию дополнительных средств защиты.

**Рекомендации по организационной составляющей ИБ:**

по разработке политики информационной безопасности;

по организации службы ИБ;

по разработке организационно-распорядительных и нормативно-технических документов;

по пересмотру ролевых функций персонала и зон ответственности;

по разработке программы осведомленности сотрудников в части ИБ;

по поддержке и повышению квалификации персонала.

# 11.2. ТРЕБОВАНИЯ COBIT ПО РЕАЛИЗАЦИИ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
## 11.2.1. ИСТОЧНИК COBIT

**Ассоциация Контроля и Аудита Систем (The Information Systems Audit and Control Association & Foundation (ISACA)** основана в 1969 г., объединяет около 30 000 членов из более чем 100 стран и координирует деятельность более чем 26000 аудиторов информационных систем (**CISA** - Certified Information System Auditor и **CISM** - Certified Information Security Manager), имеет свою систему стандартов в этой области, ведет исследовательские работы, занимается подготовкой кадров и проводит конференции.

Основная декларируемая **цель ISACA** - это исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем.

В помощь профессиональным аудиторам, руководителям IT- подразделений, администраторам и заинтересованным пользователям ассоциацией ISACA и привлеченными специалистами из ведущих мировых консалтинговых компаний был разработан стандарт **CoBiT (Control Objectives for Information and Related Technology).**

## 11.2.2. НАЗНАЧЕНИЕ COBIT И РОЛЬ ДЛЯ АУДИТА ИБ

**CobiT (Control Objectives for Information and Related Technology** («Задачи информаци-онных и смежных технологий») – пакет открытых (около 40) международных и националь-ных стандартов и руководств в области управления IT, аудита и IT-безопасности с анали-зом и оценкой лучших из международных технических стандартов, стандартов управления качеством, аудиторской деятельности и практических требований.

**Задачи CobiT:**

ликвидация разрыва между руководством компании с их видением бизнес-целей и IT-департаментом;

организация конструктивного диалога между топ-менеджерами; руководителями среднего звена (IT-директором, начальниками отделов); непосредственными исполнителями (инженерами, программистами и т. д.) и аудиторами.

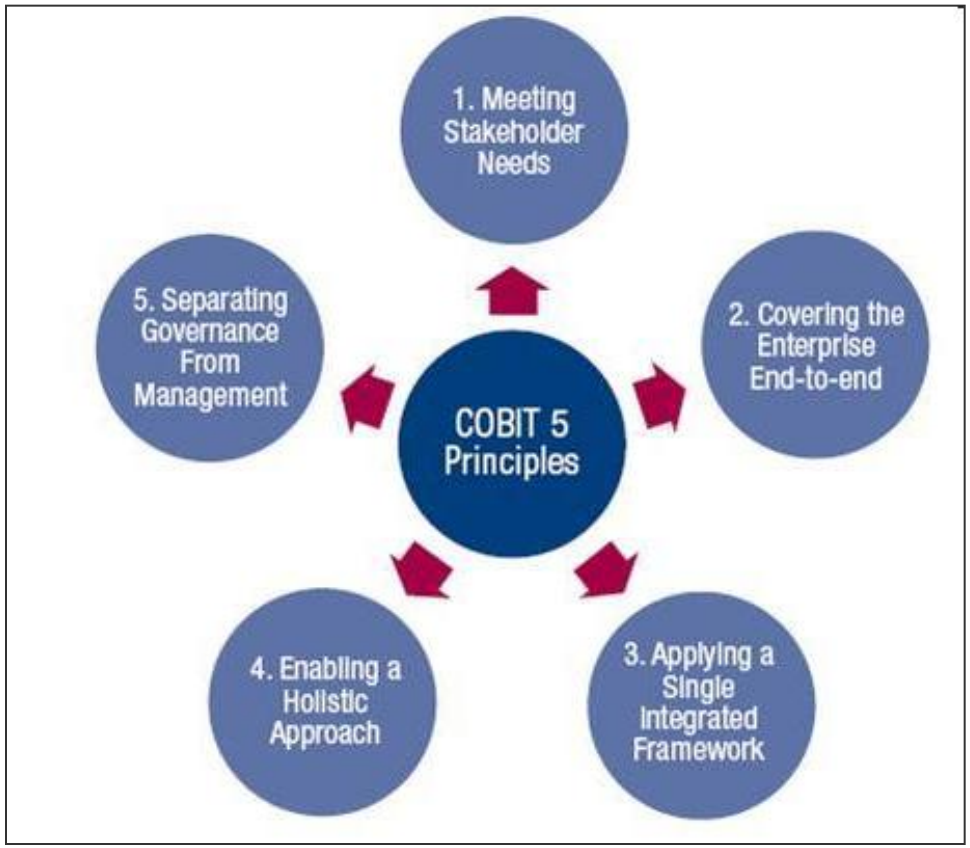
**CobiT содержит:**

описание целей и принципов управления, объектов управления, всех IT-процессов (задач), требований к ним, инструментария для их реализации и практических рекомендаций по управлению IT-безопасностью;

показатели (метрики) для оценки эффективности реализации системы управления IT, которые используются аудиторами IT-систем: показатели качества и стоимости обработки информации, характеристики её доставки получателю, показатели, относящиеся к субъективным аспектам обработки информации (стиль, удобство интерфейсов);

показатели, описывающие соответствие IT-системы принятым стандартам и требованиям, достоверность информации, её действенность, конфиденциальность, целостность и доступность

## 11.2.3. ОСНОВНЫЕ ПРИНЦИПЫ COBIT 5




Рекомендации по внедрению COBIT.
Модель зрелости процессов.
Взаимодействие между целями (заинтересованных сторон, ИТ) и процессами.
Краткое пояснение про взаимодействие и соответствие другим стандартам и практикам (ISO 38500, ITIL\ISO 20000, ISO 27001, TOGAF, CMMI, PMBOK и PRINCE2)

# 11.2.4. ОПИСАНИЕ ПРОЦЕССОВ COBIT 5 (Enabling Processes)

COBIT 5 Process Reference Model

Processes for Governance of Enterprise IT

**Все процессы разбиты на группы (домены):**

- **Evaluate, Direct and Monitor (EDM)**
- **Align, Plan and Organise (APO)**
- **Build, Acquire and Implement (BAI)**
- **Deliver, Service and Support (DSS)**
- **Monitor, Evaluate and Assess (MEA)**

**Каждый процесс представлен в табличном виде и описан по следующей схеме:**

- **Process identification** (идентификаторы процесса: префикс и номер, название, область (governance или management), домен)
- **Process description** (краткое описание)
- **Process purpose statement** (назначение процесса)
- **Goals cascade information** (связь с целями ИТ)
- **Process goals and metrics** (цели и метрики процесса)
- **RACI chart** (матрица распределения ответственности)
- **Detailed description of the process practices** (подробное описание процесса, включая входы и выходы)
- **Related guidance** (связанные стандарты)

Source: COBIT 5, figure 16

# 11.3. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
## 11.3.1. ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА ИБ

- **Microsoft в программе IT Advisor for Risk Management**
- **CRAMM согласно методике BIS Applied Systems Limited**
- **RiskWatch**

- **Microsoft security assessment tool (MSAT)** разработан для определения и устранения угроз безопасности в ИТ-среде и предоставляет следующие возможности:
  понятную, исчерпывающую и постоянную осведомленность об уровне безопасности;
  инфраструктуру эшелонированной защиты, соответствующую отраслевым стандартам;
  подробные, постоянные отчеты, сравнивающие базовые показатели с достигнутыми успехами;
  проверенные рекомендации и действия для улучшения безопасности;
  структурированные рекомендации от Microsoft и отрасли.

MSAT состоит из более чем 200 вопросов, охватывающих инфраструктуру, приложения, операции и персонал. Вопросы, связанные с ними ответы и рекомендации выводятся из общепринятых практических рекомендаций, стандартов ISO 17799 и NIST-800.x, а также рекомендаций и предписаний от группы надежных вычислений Microsoft.

Эта оценка разработана для организаций среднего размера, содержащих от 50 до 1500 настольных систем и предназначена для широкого охвата областей потенциального риска в среде, а не для предоставления глубокого анализа конкретных технологий или процессов.

Как следствие, средство не может оценивать эффективность примененных мер безопасности и его следует использовать как предварительное руководство, помогающее в разработке базовых показателей для конкретных областей, требующих более пристального внимания.

## 11.3.2a. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ MSAT

| ИНФРАСТРУКТУРА | ВАЖНОСТЬ ДЛЯ БЕЗОПАСНОСТИ |
|---|---|
| Защита периметра | Защита периметра касается безопасности на границах сети, где внутренняя сеть соединяется с внешним миром. Она составляет первую линию обороны против нарушителей. |
| Проверка подлинности | Строгие процедуры проверки подлинности для пользователей, администраторов и удаленных пользователей предотвращают получение доступа к сети чужаками путем использования локальных и удаленных атак. |
| Управление и наблюдение | Управление, наблюдение и правильное ведение журнала имеют ключевое значение для поддержки и анализа ИТ-сред. Эти средства еще более важны после того, как атака произошла и требуется анализ инцидента. |
| Рабочие станции | Защита отдельных рабочих станций является ключевым фактором в защите любой среды, особенно когда разрешен удаленный доступ. Рабочие станции должны обладать мерами безопаасности для защиты от распространенных атак. |

| ПРИЛОЖЕНИЯ | ВАЖНОСТЬ ДЛЯ БЕЗОПАСНОСТИ |
|---|---|
| Развертывание и использование | Когда ключевые для бизнеса приложения развертываются в производственной среде, необходимо защитить безопасность и доступность этих приложений и серверов. Постоянное обслуживание важно для надежного исправления ошибок безопасности и избежания внесения в среду новых ошибок. |
| Проектирование приложений | Проектирование, которое не в должной мере решает вопросы с такими механизмами безопасности, как проверка подлинности, авторизация и проверка данных, может позволить взломщикам воспользоваться уязвимостями безопас-ности и получить доступ к важной информации.<br>Безопасные методологии разработки приложений являются ключом к обеспечению того, что приложения решают проблемы с моделью угроз, способной создать уязвимости в защите организации.<br>Целостность и конфиденциальность данных является одними из важнейших требований для бизнеса. Потеря или хищение данных может отрицательно сказаться на прибыли организации и на ее репутации. Важно понимать, как приложения обрабатывают ключевые данные и как эти данные защищены |

# 11.3.2б. ТРЕБОВАНИЯ БЕЗОПАСНОСТИ MSAT

| ЭКСПЛУАТАЦИЯ | ВАЖНОСТЬ ДЛЯ БЕЗОПАСНОСТИ |
|---|---|
| Среда | Безопасность компании зависит от рабочих процедур, процессов и рекомендаций, примененных к среде. Точное документирование среды и наличие руководств имеют ключевое значения для способности рабочей группы управлять, поддерживать и обслуживать безопасность среды. |
| Политика безопасности | Корпоративной политикой безопасности именуется совокупность отдельных политик и рекомендаций для управления безопасным использованием технологии и процессов внутри организации. Эта область охватывает политики, касающиеся всех типов безопасности - пользователя, системы и данных. |
| Резервное копирование и восстановление | Резервное копирование и восстановление имеют ключевое значение для поддержания бесперебойности бизнес-операций в случае сбоя оборудования или программного обеспечения. Отсутствие должных процедур резервного копирования и восстановления может привести к значительным потерям данных и продуктивности. |
| Управление исправлениями и обновлениями | Надежное управление исправлениями и обновлениями важно в обеспечении безопасности ИТ-среды организации. Своевременное применение обновлений и исправлений необходимо, чтобы помочь в защите от известных и потенциальных уязвимостей |

| ПЕРСОНАЛ | ВАЖНОСТЬ ДЛЯ БЕЗОПАСНОСТИ |
|---|---|
| Требования и оценки | Требования безопасности должны быть понятны всем, кто принимает решения, чтобы их технические и бизнес-решения улучшали безопасность. Регулярные оценки сторонними консультантами могут помочь компании в обозрении, оценке и определении мер для улучшений |
| Политики и процедуры | Четкие процедуры по управлению отношениями с поставщиками и партнерами могут помочь в предотвращении угроз. Контроль приема и увольнения может помочь защитить компанию от беспринципных или обозленных сотрудников |
| Подготовка и осведомленность | Сотрудники должны быть осведомлены о политиках безопасности и о том, как безопасность касается их обязанностей |

# 11.3.3. СИСТЕМА COBRA – ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ ПРОВЕРКИ РИСКОВ БАЗОВОГО УРОВНЯ ТРЕБОВАНИЙ СТАНДАРТА ISO 17799

**Разработана в компании C & A Systems Security Ltd. и обеспечивает анализ соответствия информационной системы компании положениям стандарта, а также автоматизацию анализа рисков.**

**Оценка соответствия производится путем проверки ответов на вопросы из следующих групп:**

1. Классификация активов (материальных и информационных ценностей), их учет, классификация и управление ими.
2. Планирование непрерывности ведения бизнеса (разработка планов, их тестирования и распределения ответственности).
3. Управление компьютерами и операциями - процессами и сервисами безопасности.
4. Соответствие информационной инфраструктуры требованиям, инструкциям и рекомендациям.
5. Безопасность персонала - распределение ответственности по реализации положений ПБ между сотрудниками, а также порядок приема сотрудников.
6. Физическая безопасность и безопасность среды, организация физической защиты на территории, охраны, контроля физического доступа, энергетической и противопожарной безопасности.
7. Организация безопасности (организация службы ИБ, создание форумов по безопасности, порядок взаимодействия со сторонними экспертами по безопасности и распределение ролей в ходе реализации мероприятий по защите информации между сотрудниками.
8. Политика безопасности - определить положение ПБ в системе мер по обеспечению ИБ организации, а также оценить структуру этого документа и его применяемость на практике.
9. Управление доступом к системе - вопросы контроля и разграничения доступа, а также категорирования защищаемой информации.
10. Разработка и поддержка системы на протяжении всего жизненного цикла, оценка применяемых технологий анализа рисков.

**На основании сведений, полученных в ходе выполнения всех вопросников или некоторой их части, COBRA автоматически генерирует отчет со структурой:**

1. Введение. Содержит общую информацию о сгенерированном отчете.
2. Обзор проверки соответствия. В разделе детализируется информация об использованном вопроснике, выделяются использованные модули и категории вопросов.
3. Анализ несоответствий с указанием ссылок на соответствующие разделы стандарта ISO 17799.
4. Требования по улучшению и рекомендации по устранению обнаруженных несоответствий.
5. Перечень вопросов, которые были использованы при построении отчета, и соответствующих ответов

*http://www.npo-echelon.ru/about/articles/politics_development.php*

# 11.3.4. СИСТЕМА КОНДОР – ПРОГРАММНЫЙ ПРОДУКТ ДЛЯ ПРОВЕРКИ РИСКОВ БАЗОВОГО УРОВНЯ ИБ СТАНДАРТА ISO 17799

**Система КОНДОР** (разработчик- компания Digital Security) - русскоязычный аналог системы COBRA . Концепции аналогичны: на основании ответов на вопросы генерируется отчет. Вопросы структурированы в следующие разделы:

- политика безопасности;
- организационные меры;
- управление ресурсами;
- безопасность персонала;
- физическая безопасность;
- управление процессами;
- контроль доступа;
- непрерывность бизнеса;
- соответствие системы;
- разработка систем.

По числу вопросов КОНДОР проще, чем COBRA.

Возможности по анализу рисков у текущей версии системы отсутствуют.

Наименее проработанным компонентом системы КОНДОР является генератор отчетов. Отчет представляет собой перечень разделов стандарта с указанием тех из них, с которыми выявлено соответствие. При построении диаграммы в отчете полученные данные анализируются исключительно с количественной точки зрения. Просмотр отчета достаточно неудобен и требует навигации в четырех направлениях, то же самое можно сказать о справочной системе. К некоторым из положений стандарта доступны краткие комментарии, имеется возможность построения диаграмм, показывающих степень соответствия системы требованиям стандарта. Рекомендации или выводы частично отсутствуют

*http://www.npo-echelon.ru/about/articles/politics_development.php*

# Глава 12.
# РАБОТА РУКОВОДСТВА ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

**12.1.** Содержание политики информационной безопасности.

**12.2.** Организационные меры по обеспечению информационной безопасности автоматизированных систем управления

**Литература:**


1. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
2. ГОСТ Р ИСО/МЭК 13335-1-2006 «Методы и средства обеспечения безопасности. Ч. 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
3. ОСТ 45.127-99 «Система обеспечения информационной безопасности взаимоувязанной сети связи РФ. Термины и определения».
4. http://asher.ru/security/book/its/09


Оглавление

# 12.1. СОДЕРЖАНИЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.
## 12.1.1. БАЗОВЫЕ ПРИНЦИПЫ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

| | |
|---|---|
| Принципы построения политики | «Все, что явно не запрещено, то разрешено»: при организации доступа системный администратор вообще не ставит никаких ограничений или ставит те ограничения, которые заранее уже известны, и в дальнейшей работе при возникновении необходимости, закрывает те или иные ресурсы для доступа. Это резко ускоряет работу, но и увеличивает на первом этапе опасность утечки информации |
| | «Все, что явно не разрешено, то запрещено»: при организации доступа систем-ный администратор первоначально закрывает все, что только возможно и предоста-вляет пользователю минимум возможностей, и в дальнейшей работе при возник-новении необходимости открывает те или иные ресурсы для доступа. Это на началь-ном этапе резко замедлит работу, но является наиболее безопасным |
| Принципы реакции на инциденты | «Защититься и продолжить»: устранить последствия, закрыть «дыру» и продол-жить нормальную работу, сведя вынужденный простой и возможные убытки к минимуму. Нахождение виновного, применение к нему санкций – второй вопрос, и, если защита восстановлена, то служба безопасности выполнила основную задачу |
| | «Выявить и осудить»: главное – это найти виновного и применить к нему санк-ции даже в ущерб безопасности. Служба безопасности при инциденте специально не закрывает уязвимость – лишь бы найти злоумышленника |
| Принципы контроля ИБ | «Условно-постоянный»: предполагает контроль работы пользователей и состоя-ние системы практически в режиме реального времени |
| | «Дискретный»: предполагает проверки стандартных событий (*попытки входа в систему (успешные или неудачные); выход из системы; ошибки доступа к файлам или системным объектам; попытки удаленного доступа (успешные или неудачные); действия привилегированных пользователей (администраторов), успешные или неудачные; системные события (выключение и перезагрузка)*) с какой-то периодичностью, а внеочередные – в случае инцидентов |
| Принцип аудита | Периодическое проведение внешних или внутренних аудитов, а в промежутке между ними – проверка систем на соответствие политике безопасности в автома-тическом режиме или вручную. *Процедура проверки политики должна определять, насколько часто должна проводиться эта проверка, кто получает результаты, и каким образом разрешаются вопросы, возникающие при обнаружении несоответствий* |

## 12.1.2. ИСХОДНЫЕ ДАННЫЕ ДЛЯ ФОРМИРОВАНИЯ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- общая характеристика и специализация организации (наименование, специализация, род деятельности, решаемые задачи, характер и объем работ), сведения о распределении обязанностей и инструкциях по обработке и защите информации;
- описание административной структуры и категорий зарегистрированных пользователей, технологии обработки информации, субъектов и объектов доступа;
- общее описание рабочего процесса, технологическая схема операций при выполнении рабочего процесса, интенсивность с которой выполняется рабочий процесс, технологические ограничения, средства контроля и критерии качества результатов рабочего процесса, перечень проблемных вопросов подразделений по обеспечению защиты информации;
- информация которая подлежит защите, сведения конфиденциального характера, органи-зация и структура информационных потоков и их взаимодействие;
- организация хранения данных;
- угрозы информационной безопасности, модель нарушителя и уязвимости;
- анализ рисков;
- общая характеристика автоматизированных систем организации, топология и расположение ЛВС, схема коммуникационных связей, структура и состав потоков данных (перечень входных и выходных информационных объектов, их источники и получатели, перечень внутренних информационных объектов);
- технические и программные средства ЛВС и доступа к ней из сетей общего доступа (физическая среда передачи, используемые протоколы, операционные системы, серверы баз данных, места хранения конфиденциальных данных, средства защиты информации);
- принадлежность и типы каналов связи;
- общее и специальное ПО (наименование и назначение, фирма разработчик, аппаратные требования, размещение);
- применяемые меры защиты (организационные меры, средства защиты ОС, средства защиты, встроенные в ПО, специализированные средства защиты)

# 12.1.3. СОДЕРЖАНИЕ ДОКУМЕНТА «ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

**Определение информационной безопасности**, ее составляющих и понятий.

**Цели и принципы** обеспечения информационной безопасности.

**Разъяснение политики** безопасности, принципов, стандартов и требований к ее соблюдению (основные направления, способы и требования по обеспечению безопасности информации, выполнение правовых и договорных требований, требования к обучению персонала правилам безопасности, обеспечения бесперебойной работы организации).

**Определение общих и конкретных обязанностей** должностных лиц по обеспечению информационной безопасности, включая уведомления о случаях нарушения защиты

**Перечень документов, выпускаемых в поддержку политики безопасности:**

- Правила, инструкции и требования для обеспечения ИТ-безопасности:
- Правила парольной защиты
- Правила защиты от вирусов и злонамеренного программного обеспечения
- Правила использования системных утилит
- Правила удаленной работы мобильных пользователей
- Правила осуществления локального и удаленного доступа
- Правила контроля вносимых изменений
- Инструкция по безопасному уничтожению информации или оборудования
- Инструкция по безопасности рабочего места (документов на рабочем столе и на экране монитора)
- Требования по контролю за физическим доступом
- Требования по физической защите оборудования
- Требования резервного сохранения информации
- Требования мониторинга
- Требования при обращении с носителями данных
- Требования по проверке прав пользователей
- Распределение ответственности при обеспечении безопасности
- Инструкция по приему на работу и допуску новых сотрудников к работе в АС и наделения их необходимыми полномочиями по доступу к ресурсам системы,
- Инструкция по увольнению работников и лишения их прав доступа в систему
- Инструкция по действиям различных категорий персонала по ликвидации последствий кризисных ситуаций, в случае их возникновения

# 12.1.4. УРОВЕНЬ ДЕТАЛИЗАЦИИ ПОЛИТИКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

**Политика безопасности ИТТ должна распространяться на:**

- предмет и задачи безопасности;
- цели безопасности с учетом правовых и регулирующих обязательств, а также с учетом бизнес целей;
- требования безопасности ИТТ к обеспечению конфиденциальности, целостности, доступности, безотказности, подотчетности и аутентичности информации и средств ее обработки;
- ссылки на стандарты, лежащие в основе данной политики;
- администрирование информационной безопасности, охватывающее организационные и индивидуальные ответственности и полномочия;
- подход к управлению риском, принятый в организации;
- метод определения приоритетов реализации защитных мер;
- уровень безопасности и остаточный риск, определяемый руководством организации;
- общие правила контроля доступа (логический контроль доступа, а также контроль физического доступа в здания, помещения, к системам и информации);
- подходы к осведомленности о безопасности и повышение квалификации в области безопасности в рамках организации;
- процедуры проверки и поддержания безопасности;
- общие вопросы защиты персонала;
- способы, которыми политика безопасности будет доведена до сведения всех заинтересованных лиц;
- условия анализа или аудита политики безопасности;
- метод контроля изменений в политике безопасности

*ГОСТ Р ИСО/МЭК 13335-1 - 2006*

# 12.1.5. ЦЕЛИ И СТРАТЕГИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

- общий уровень риска, приемлемый для данной организации;
- допустимый общий уровень безопасности определяемый целями, которые ставит перед собой организация при создании системы обеспечения безопасности ИТ;
- имеющиеся активы и их ценность для данной организации:
- какие важные (очень важные) элементы деловой практики предприятия не могут осуществляться без привлечения ИТ;
- какие вопросы могут решаться исключительно с помощью использования ИТ;
- принятие каких важных решений зависит от достоверности, целостности или доступности информации, обрабатываемой с использованием ИТ, или от ее своевременного получения;
- какие виды конфиденциальной информации, обрабатываемой с использованием информационных технологий, подлежат защите;
- какие последствия могут наступить для организации после появления нежелательного инцидента нарушения системы обеспечения безопасности;
- степень важности целей деловых операций, а также их связь с вопросами безопасности;
- стратегия достижения целей, которая должна соответствовать ценности активов;
- общие положения о том, как организация собирается обеспечить достижение своих целей (**специфического характера**, когда первичной целью системы обеспечения безопасности ИТ является, исходя из деловых соображений, необходимость обеспечения высокого уровня доступности. В этом случае одно из направлений стратегии должно заключаться в сведении к минимуму опасности заражения системы ИТ вирусами путем повсеместного размещения антивирусных программных средств (или выделения отдельных сайтов, через которые должна проходить вся получаемая информация для ее проверки на наличие вирусов); **общего характера**, когда основная работа заключа-ется в оказании информационных услуг, в связи с чем возможные потребители должны быть уверены в защищенности ее систем ИТ. В этом случае основным положением стратегии может быть проведение аттестации систем ИТ на безопасность с привлечением третьей стороны, обладающей соответствующим опытом);
- стратегия и методы анализа риска, используемые в масштабе всей организации;
- оценка необходимости разработки политики безопасности ИТ для каждой системы;
- оценка необходимости создания рабочих процедур безопасности для каждой системы;
- разработка схемы классификации систем по уровню чувствительности информации в масштабах всей организации;
- оценка необходимости учета и проверка условий безопасности соединений до места подключения к ним других организаций;
- разработка схем обработки инцидентов, связанных с нарушением системы безопасности для универсального использования

*ГОСТ Р ИСО/МЭК 13335-3 - 2006*

# 12.2. ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СИСТЕМ УПРАВЛЕНИЯ

## 12.2.1.ПОДХОДЫ К УПРАВЛЕНИЮ

**ПРОЦЕССНЫЙ**

**СИСТЕМНЫЙ**

рассматривает организацию как совокупность взаимосвязанных элементов, ориентированных на достижение разных целей на фоне меняющихся внешних условий

**Рассматриваемый объект представляется совокупностью взаимосвязанных элементов, имеет входы, выходы и связи с другими объектами, на состояние системы влияют внешние, внутренние и случайные составляющие**

**Принципы:**

**Целостность.** Возможность рассматривать систему как единое целое.

**Иерархичность строения**. Наличие внутри системы элементов вышестоящего и нижестоящего уровня, находящихся в отношениях подчиненности.

**Структуризация**. Функционирование системы определяется её структурой, то есть её элементами и взаимосвязями, подлежащими для изучения.

**Множественность.** Возможность использования различных моделей и инструментов для описания системы и её элементов.

**Использование постулатов системного подхода приводит к пониманию того, что** недостаточно решать возникшие проблемы - это не изменит систему в целом, необходимо пересматривать саму систему, её элементы или взаимосвязи; устойчивое состояние системы препятствует эволюции – необходим постоянный пересмотр и совершенствование.

**СИТУАЦИОННЫЙ**

применение тех или иных методов управления определяется ситуацией

# 12.2.2. ТЕХНОЛОГИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ

**Под технологией обеспечения информационной безопасности в АС понимается определенное распределение функций и регламентация порядка их исполнения, а также взаимодействия подразделений и сотрудников по обеспечению комплексной защиты ресурсов АС в процессе ее эксплуатации.**

**Требования к технологии :**

- соответствие современному уровню развития информационных технологий;
- учет особенностей построения и функционирования различных подсистем АС;
- точная и своевременная реализация политики безопасности организации;
- минимизация затрат на реализацию самой технологии обеспечения безопасности.

**Для реализации технологии обеспечения безопасности в АС необходимо**:

- наличие полной и непротиворечивой правовой базы (системы взаимоувязанных нормативно-методических и организационно-распорядительных документов) по вопросам ОИБ;
- распределение функций и определение порядка взаимодействия подразделений и должностных лиц организации по вопросам ОИБ на всех этапах жизненного цикла подсистем АС, обеспечивающее четкое разделение их полномочий и ответственности;
- наличие специального органа (подразделения обеспечения информационной безопасности), наделенного необходимыми полномочиями и непосредственно отвечающего за формирование и реализацию единой политики информационной безопасности организации и осуществляющего контроль и координацию действий всех подразделений и сотрудников организации по вопросам ОИБ.

# 12.2.3. РЕАЛИЗАЦИЯ ТЕХНОЛОГИЙ, ОБЕСПЕЧИВАЮЩИХ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

• **назначение и подготовка должностных лиц**, ответственных за организацию, реализацию функций и осуществление мероприятий обеспечения информационной безопасности;

• **инвентаризация, классификация и учет** всех подлежащих защите ресурсов (информации, носителей, серверов, автоматизированных рабочих мест, процессов обработки) и определение требований к организационно-техническим мерам и средствам защиты;

• **разработка** реально выполнимых и непротиворечивых **организационно-распорядительных документов** по вопросам обеспечения информационной безопасности;

• **реализация технологических процессов обработки информации** с учетом требований информационной безопасности;

• **принятие эффективных мер сохранности и обеспечения физической целостности** технических средств и поддержку необходимого уровня защищенности компонентов АС;

• **применение программно-аппаратных средств защиты** ресурсов системы и непрерывную административную поддержку их использования;

• **регламентация всех процессов обработки информации** и действий сотрудников подразделений на основе утвержденных организационно-распорядительных документов по вопросам обеспечения информационной безопасности;

• обеспечение **четкого знания и строгого соблюдения всеми сотрудниками**, использующими и обслуживающими аппаратные и программные средства, требований организационно-распорядительных документов;

• организация процесса **обучения обслуживающего персонала и пользователей** правилам эксплуатации и технического обслуживания средств защиты информации;

• **персональная ответственность** сотрудников, участвующих в процессах автоматизированной обработки информации и имеющего доступ к ресурсам АС, контроль за ними;

• организация процесса **расследования инцидентов и нарушений** установленных регламентов и инструкций по обеспечению информационной безопасности;

• **организация сертификации средств защиты** информации, контроль за использованием лицензионного программного обеспечения

• **контроль эффективности** и достаточности принимаемых мер защиты в связи с постоянным развитием средств информатизации и изменяющимися источниками угроз;

• **проведение постоянного анализа** эффективности и достаточности принятых мер и применяемых средств защиты информации, предложений по совершенствованию системы

# 12.2.4. РОЛЬ ОРГАНОВ УПРАВЛЕНИЯ ПРЕДПРИЯТИЕМ В ОБЕСПЕЧЕНИИ ЕГО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Оценивают риски, влияющие на достижение поставленных целей, и принимают меры, обеспечивающие реагирование на меняющиеся обстоятельства и условия в целях обеспечения эффективности оценки рисков в информационной сфере

Обеспечивают участие во внутреннем контроле информационной безопасности персонала в соответствии с их должностными обязанностями

Устанавливают порядок, при котором служащие доводят до сведения органов управления и руководителей структурных подразделений информацию обо всех нарушениях законодательства, учредительных и внутренних документов, случаях злоупотреблений, несоблюдения норм профессиональной этики в обращении с корпоративной и личной информацией

Утверждают документы по вопросам взаимодействия службы информационной безопасности с другими подразделениями и персоналом и контролируют их соблюдение

Исключают принятие правил или осуществление практики, которые могут стимулировать совершение действий, противоречащих законодательству и целям внутреннего контроля.

Осуществляют ежедневное повышение сознательного выполнения обязанностей и осведомленности сотрудников, обучение в сочетании с регулярной аттестацией, участие в корпоративных программах повышения лояльности в интересах повышения ответственности к обеспечению информационной безопасности

# 12.2.5. СУЩНОСТЬ ПРОЦЕССНОГО ПОДХОДА

**CPI (Continuous Process Improvement) - методология управления, в основе которой лежит идея непрерывного усовершенствования процесса:**

- **CPI** дает предприятию существенное конкурентное преимущество и способствует достижению стратегических целей за счет повышения эффективности ее бизнес-процессов и их непрерывной адаптации к изменяющимся внешним условиям;
- **CPI** направлена на достижение результата в области повышения качества продукции через обеспечение качества процессов;
- отличительной особенностью модели **CPI** от реинжиниринга является идея необходимости поддержки всего жизненного цикла процесса: нововведения в бизнес-процессах рекомендуется проводить поэтапно, сначала – в отдельных структурных подразделениях, а при положительном результате – и во всей организации в целом с обучением сотрудников и передачей новой технологии;
- корпоративная философия **CPI** формирует у сотрудников чувство ответственности за результат командной работы, поощряет инициативу и мотивирует к поддержанию эффекта;
- определяющие **принципы CPI** – постоянство и постепенность улучшений, обеспечивающие длительный и стабильный эффект при минимальных затратах;
- **CPI** включает в себя не только описание бизнеса как сети взаимосвязанных процессов, но и постоянный контроль, управление и совершенствование, что подхода требует **описания, оптимизации и автоматизации бизнес-процессов**

**ЭТАПЫ ВНЕДРЕНИЯ:**

- **выявляется сеть бизнес-процессов,**
- **ранжирование по значимости, документирование и моделирование процессов «как есть» (модель AS-IS).**
- **анализ построенных моделей и выявление «узких мест» процессов**
- **построение модели «как надо» (модельTO-BE) на основании полученных результатов**

## 12.2.6. МОДЕЛИ ПРОЦЕССНОГО ПОДХОДА

| «AS-IS» - МОДЕЛЬ | «TO-BE» - МОДЕЛЬ |
|---|---|
| **AS IS - модель «как есть», модель существующего состояния организации.**<br>Позволяет систематизировать протекающие в данный момент процессы, а также используемые информационные объекты.<br>На основе этого выявляются узкие места в организации и взаимодействии бизнес-процессов, определяется необходимость тех или иных изменения в существующей структуре.<br>Такую модель часто называют функциональной и выполняют с использованием различных графических нотаций.<br>На этапе построения модели AS-IS важным считается строить максимально приближенную к действительности модель, основанную на реальных потоках процессов.<br>Проектирование информационных систем и управление процессами подразумевает построение модели AS IS и дальнейший переход к модели TO-BE | **TO BE (SHOULD-BE, AS-TO-BE) - модель «как должно быть».**<br>Создается на основе модели AS IS, с устранением недостатков в существующей организации бизнес-процессов, а так же с их совершенствованием и оптимизацией за счет устранения выявленных узких мест.<br>В традиционном реинжиниринге на основе модели TO BE рекомендуется производить автоматизацию бизнес-процессов и проектировать КИС.<br>В настоящее время, в связи с возрастающей популярностью **CPI,** снижается необходимость в долгой и трудоемкой подготовке данной модели TO BE |

# 12.2.7. ПРИНЦИПЫ ПРОЦЕССНОГО ПОДХОДА

| Восприятие бизнеса как системы | Восприятие деятельности как процесса | Стандартизация и прозрачность ответственности |
|---|---|---|
| ❖ любое предприятие рассматривается как система, а его развитие - как происходящее по законам сложных систем;<br>❖ будучи в устойчивом состоянии, никакая система не может эволюционировать;<br>❖ решение локальных проблем не может изменить систему. Ее изменение возможно лишь в целом | ❖ любую деятельность можно улучшить;<br>❖ деятельность любого предприятия можно рассматривать как сеть связанных между собой процессов, поскольку все виды деятельности предприятия и процессы, соответствующие им, взаимосвязаны;<br>❖ в любой деятельности может иметь место разделение как по времени, так по материальным ресурсам и персоналу;<br>❖ любая целенаправленная, спланированная и при этом использующая ресурсы деятельность преобразует входную продукцию в выходную;<br>❖ каждый процесс имеет внешнего или внутреннего поставщика входных ресурсов и внешнего или внутреннего потребителя | ❖ высшее руководство полностью отвечает за создание системы качества на предприятии и управление качеством;<br>❖ каждый процесс должен иметь владельца, то есть персонифицирован, и ответственность должна распределяться по всем видам деятельности;<br>❖ все процессные составляющие должны быть максимально стандартизированными и прозрачными;<br>❖ стандартизацию следует проводить на основе взаимосвязанных стандартов, которые реализуются в виде нормативной документации и корпоративных стандартов |

# 12.2.8a. ISO/IEC 27001: МЕЖДУНАРОДНЫЙ СТАНДАРТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Разработан международной организацией по стандартизации (ISO) и международной электротехнической комиссией (IEC)** и содержит требования в области информационной безопасности для создания, развития и поддержания системы информационной безопасности

## АЛГОРИТМ ВНЕДРЕНИЯ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Первый этап. Управленческий**
Осознать цели и выгоды внедрения
Получить поддержку руководства на внедрение и ввод в эксплуатацию
Распределить ответственность

**Второй этап. Организационный**
Создать и обучить группу по внедрению и поддержке СМИБ
Определить область действия

**Третий этап. Первоначальный анализ СМИБ**
Провести анализ существующей
Определить перечень работ по доработке существующей СМИБ

**Четвертый этап. Определение политики и целей СМИБ**
Определить политику СМИБ
Определить цели СМИБ по каждому процессу СМИБ

**Пятый этап. Сравнение текущей ситуации со стандартом**
Провести обучение ответственных требованиям стандарта
Проработать требования стандарта
Сравнить требования стандарта с существующим положением дел

**Шестой этап. Планирование внедрения СМИБ**
Определить перечень мероприятий для достижения требований стандарта
Разработать руководство по информационной безопасности

**Седьмой этап. Внедрение системы управления рисками**
Разработать процедуру по идентификации рисков
Идентифицировать и ранжировать активы
Каталог «Модули»
Определить ответственных за активы
Оценить активы
Идентифицировать угрозы и уязвимости
Каталог «Угрозы»
Рассчитать и ранжировать риски
Разработать план по снижению рисков
Каталог «Меры защиты»
Определить неприменимые направления безопасности
Разработать положение о применимости контролей

# 12.2.8б. ISO/IEC 27001: МЕЖДУНАРОДНЫЙ СТАНДАРТ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

## АЛГОРИТМ ВНЕДРЕНИЯ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Восьмой этап. Разработка документации СМИБ**

Определить перечень документов (процедур, записей, инструкций) для разработки.

**Разработка процедур и других документов:**

- управленческие процедуры (стандарт на разработку документов, управление документацией, записями; корректирующие и предупреждающие мероприятия; внутренний аудит; управление персоналом);
- технические процедуры (приобретение, развитие и поддержка информационных систем; управление доступом; регистрация и анализ инцидентов; резервное копирование; управление съемными носителями);
- записи управленческие (отчеты о внутренних аудитах; анализ СМИБ со стороны высшего руководства; отчет об анализе рисков; отчет о работе комитета по информационной безопасности; отчет о состоянии корректирующих и предупреждающих действий; договора; личные дела сотрудников и др.)
- записи технические (реестр активов; план предприятия; план физического размещения активов; план компьютерной сети; журнал регистрации резервного копирования; журнал регистрации факта технического контроля после изменений в операционной системе; логи информационных систем; логи системного администратора; журнал регистрации инцидентов; журнал регистрации тестов по непрерывности бизнеса и др.);
- инструкции, положения (правила работы с ПК и с информационной системой, правила обращения с паролями, инструкция по восстановлению данных из резервных копий, политика удаленного доступа, правила работы с переносным оборудованием и др.).

**Разработка и введение в действие документов**

**Девятый этап.**
**Обучение персонала**

Обучение руководителей подразделений требованиям ИБ

Обучение всего персонала требованиям ИБ

**Десятый этап.**
**Разработка и принятие мер по обеспечению работы СМИБ**

Внедрение средств защиты: административных, учебных, технических

**Одиннадцатый этап.**
**Внутренний аудит СМИБ**

Подбор команды внутреннего аудита

Планирование внутреннего аудита СМИБ

Проведение внутреннего аудита СМИБ

**Двенадцатый этап.**
**Анализ СМИБ со стороны высшего руководства**

**Тринадцатый этап.**
**Официальный запуск СМИБ**

Приказ о введении в действие СМИБ

**Четырнадцатый этап.**
**Оповещение заинтересованных сторон**

Информирование клиентов, партнеров, СМИ о запуске СМИБ

# ЛИТЕРАТУРА

## НОРМАТИВНО-ПРАВОВЫЕ АКТЫ


1. Окинавская хартия глобального информационного общества. 22 июля 2000 г.
2. Доктрина информационной безопасности Российской Федерации, 2000 г. Поручение Президента РФ 2000 г. № Пр-1895
3. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895)
4. Федеральный закон № 5485-1 «О государственной тайне», 21 июля 1993 г. (с изм. от 11.12.2011 г.), 5. Федеральный закон № 98-ФЗ «О коммерческой тайне», 29 июля 2004 г.
6. Федеральный закон № 152-ФЗ «О персональных данных», 27 июля 2006 г.
7. Федеральный закон № 69-ФЗ «О пожарной безопасности».
8. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.
9. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.
10. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.


## ОСНОВНАЯ ЛИТЕРАТУРА


1. Рассолов И.М. Информационное право. Учебник. – М.: Норма: ИНФРА-М, 2010.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Фонд «Мир», 2009.


## ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА


1. 1. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность/Петренко С. А., Симонов С. В. - М.: Компания АйТи; ДМК Пресс, 2011.
2. Садердинов А.А. Информационная безопасность предприятия. – М.: Дашков и Ко, 2004.
3. Ярочкин В.И. Система безопасности фирмы. – М.: Ось-89, 2010.
4. Курносов Ю.В., Конотопов П.Ю. Аналитика: методология, технология и организация информационно-аналитической работы. – М.: Издательство «Русаки», 2004.
5. Викентьев И.Л. Приемы рекламы и Public Relations. – СПб, 2008.


Оглавление