ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 3. **Принципы, стратегии и модели информационной защиты**

Учебные вопросы

1. Общие понятия о принципах информационной защиты.
2. Стратегии и модели информационной защиты .

Введение

- Задача повышения безопасности информационных систем (ИС) и технологий в современных условиях характеризуется сложностью, неопределённостью, наличием большого количества взаимосвязанных внутренних и внешних факторов, влияющих на информационную безопасность (ИБ).
- Объектами информационной системы (ОИС) являются информационные ресурсы, средства и системы обработки, передачи и хранения информации, используемые в соответствии с заданными информационными технологиями. К ОИС относятся также средства их обеспечения: территории, здания, помещения, технические средства и т. п.

- Информационная безопасность – это все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, отказоустойчивости, подотчетности, аутентичности и достоверности информации или средств ее обработки. Решение задачи выявления факторов, воздействующих на безопасность ИС и технологий, является основой для планирования и применения эффективных мероприятий и технологий, направленных на повышение уровня ИБ.
- Информационные активы (information asset): Информационные ресурсы или средства обработки информации организации. Источник: ГОСТ Р ИСО/ТО 13569 2007:
- Обеспечение ИБ активов ИС требует выполнения защитных мероприятий: действий, процедур и механизмов, способных обеспечить безопасность при возникновении проблем и угроз, уменьшить уязвимость и ограничить воздействие на ИС, облегчить восстановление активов.
- Эффективность ИБ повышается при использовании комбинации различных защитных мероприятий. Конкретное мероприятие по обеспечению ИБ может выполнять много функций безопасности, однако может оказаться, что одна функция безопасности потребует нескольких защитных мер.
- Защитные мероприятия по ИБ могут выполнять одну или несколько следующих функций: предотвращение, сдерживание, обнаружение, ограничение угроз, исправление ошибок, восстановление активов системы, мониторинг состояния; уведомление о событиях в системе.

1. Общие понятия о принципах информационной защиты.

- В основу концепции безопасности необходимо положить контроль над информационными активами системы с целью нейтрализации воздействия негативных факторов.
- Прежде всего, нужно выполнить идентификацию активов и установить начальный уровень безопасности, которому отвечает ИС. В процессе идентификации следует рассмотреть основные характеристики активов: информационную ценность, чувствительность активов к угрозам, наличие защитных мер. При этом необходимо учесть, что в числе факторов, влияющих на безопасность, особое место занимают субъективные факторы, которые являются наименее прогнозируемыми.
- К активам ИС можно отнести: материальные ресурсы; информационные ресурсы (аналитическая, служебная, управляющая информация на всех этапах ее жизненного цикла: создание, обработка, хранение, передача, уничтожение); информационные технологические процессы жизненного цикла автоматизированных систем; предоставляемые информационные услуги.

- Создание и развитие эффективной системы обеспечения ИБ должно основываться на следующих основных принципах:
- **1. Принцип системности.**

Активы представляют собой совокупность консолидированных и взаимосвязанных элементов, служащих для обеспечения эффективного функционирования ИС. Такие системы выступают как единое и сложное целое. При их оптимальной консолидации наблюдается так называемый синергетический эффект: результат функционирования элементов в системе выше суммы результатов функционирования каждого элемента в отдельности.

- **2. Принцип рациональности.**

Принцип предполагает целесообразную деятельность, направленную на эффективное обеспечение безопасности, рациональный охват управленческими и организационными решениями информационных, ресурсных, технологических, экологических, финансово-экономических, нормативно-метрологических и социальных требований к активам ИС.

- **3. Принцип транспарентности и конфиденциальности.**
  Принцип, с одной стороны, предполагает полную доступность активов и процессов ИС для легальных пользователей, с другой – требует недоступности и закрытости информационных активов для неавторизованного пользователя.
- **4. Принцип непрерывности, обучаемости и накопления опыта.**
  Информационная система должна обеспечить непрерывность реализации безопасного функционирования всех своих элементов и объектов. Это, в свою очередь, предполагает необходимость накопления, обобщения и использования всего имеющегося в сфере ИБ опыта.
- **5. Принцип прогнозируемости и функциональной взаимосвязанности.**
  Безопасность неотделима от общих проблем функционирования активов ИС, в том числе в области информационно-технологических процессов, процессов потребления ресурсов, финансово-экономических, социальных, экологических и т. д. Принцип предполагает выявление причинно-следственных связей возникновения возможных проблем и угроз и построение на этой основе наиболее точного прогноза развития ситуации.

- **6. Принцип своевременности, оперативного реагирования и адекватности.**

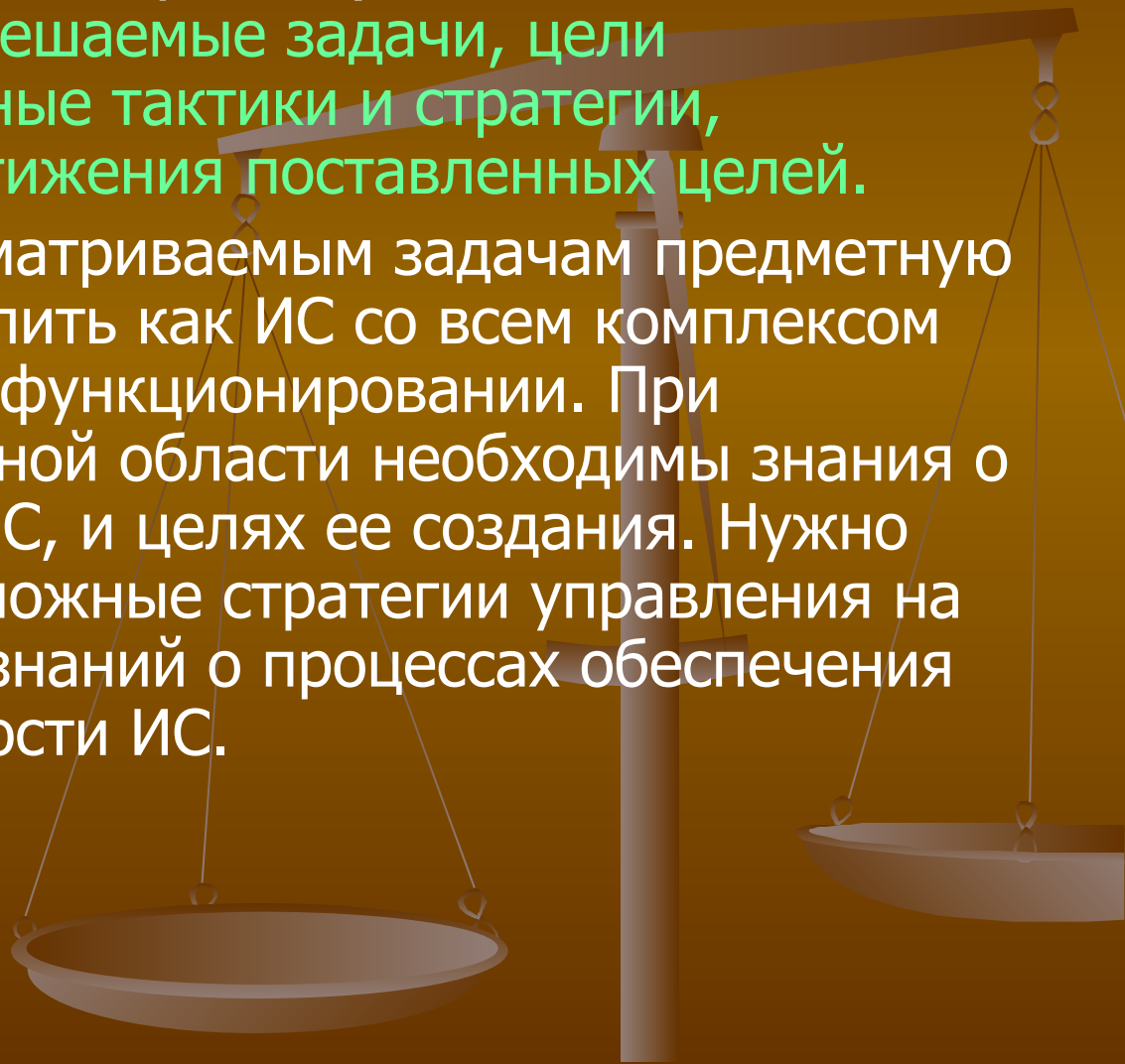
  Принцип предполагает своевременность выявления проблем и угроз, потенциально способных повлиять на безопасность активов системы и дальнейшее оперативное реагирование с целью их блокирования и устранения последствий. Выбор необходимых защитных мер обеспечения безопасности должен быть адекватен возникающим проблемам и угрозам, с учетом затрат на реализацию этих мер и объема возможных потерь от реализации угроз.
- **7. Принцип контролируемости.**

  Для обеспечения безопасности необходимо применять только те защитные меры и технологии, правильность работы которых может быть проверена. При этом необходимо регулярно оценивать адекватность защитных мер и эффективность применяемых технологий.

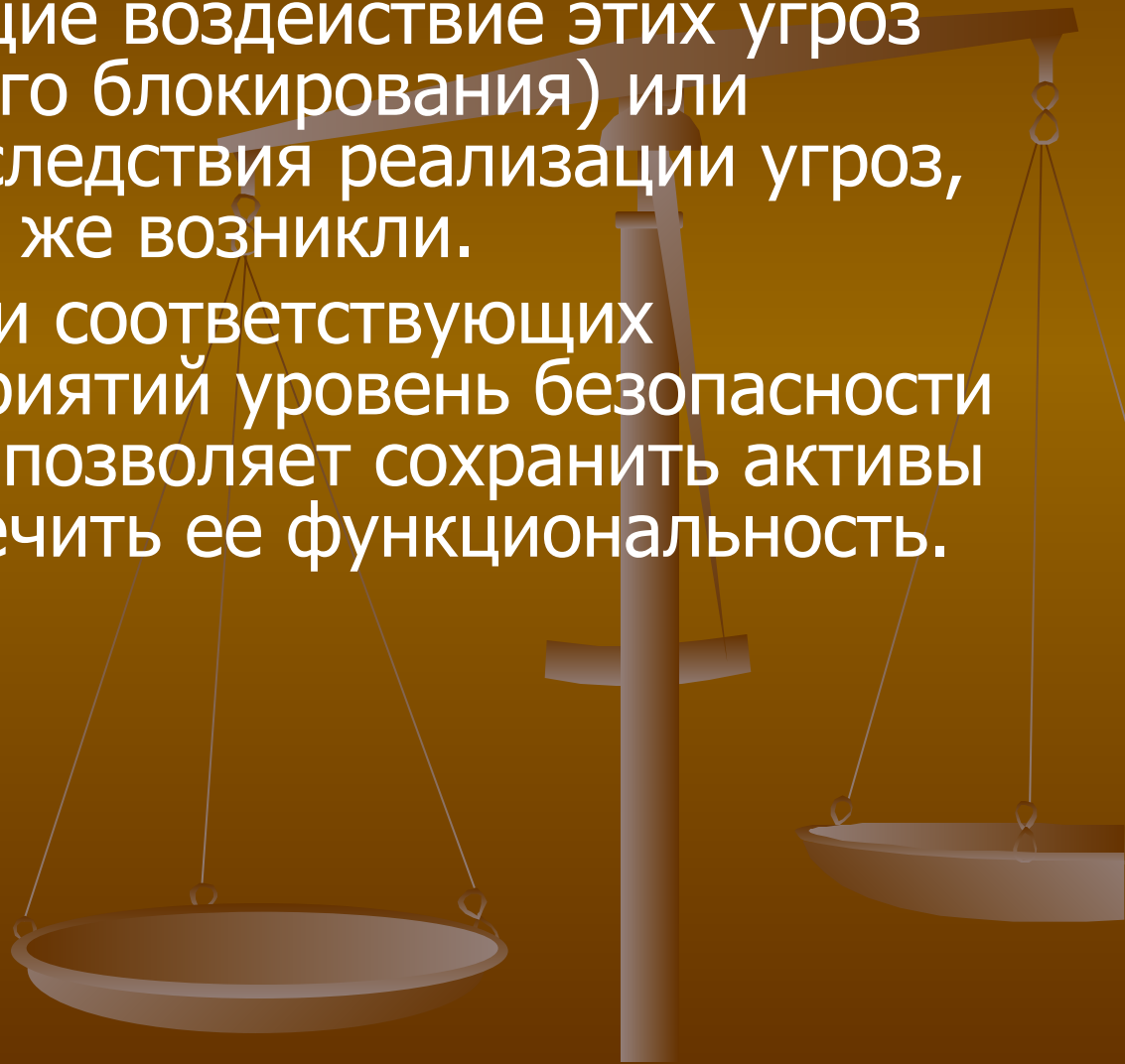
- Структурную схему решения задачи обеспечения комплексной безопасности ИС можно описать следующим образом:

- проблемная область задачи обеспечения комплексной безопасности ИС (понятия, определяющие суть ИБ и связи между ними);
- факторы, влияющие на безопасность ИС (внешние объективные факторы, внутренние объективные факторы, внешние субъективные факторы, внутренние субъективные факторы);
- мероприятия и технологии обеспечения комплексной безопасности ИС;
- методология обеспечения комплексной безопасности ИС (эвристические знания о состоянии безопасности ИС, стратегии обеспечения комплексной безопасности);
- решаемые задачи (идентификация активов ИС, определение критерия и показателей эффективности обеспечения безопасности; разработка процедур оценок этих критериев и показателей; разработка модели комплексного обеспечения ИБ и др.);
- принципы комплексного обеспечения безопасности ИС (системности, рациональности, транспарентности и конфиденциальности, непрерывности, обучаемости и накопления опыта, прогнозируемости и функциональной взаимосвязанности, своевременности, оперативного реагирования и адекватности, контролируемости);
- экономические, организационно-технологические, информационные решения.

- Таким образом, проблемная область решения задачи обеспечения комплексной информационной безопасности (совокупность основных понятий, определяющих суть исследования, и связи между ними) включает в себя: предметную область, решаемые задачи, цели исследования, возможные тактики и стратегии, используемые для достижения поставленных целей.
- Применительно к рассматриваемым задачам предметную область можно определить как ИС со всем комплексом понятий и знаний о ее функционировании. При исследовании проблемной области необходимы знания о задачах, решаемых в ИС, и целях ее создания. Нужно также определить возможные стратегии управления на основе эвристических знаний о процессах обеспечения комплексной безопасности ИС.



- В случае прогнозирования возникновения либо реального возникновения угроз безопасности для активов ИС применяются меры, ослабляющие воздействие этих угроз (вплоть до полного блокирования) или устраняющие последствия реализации угроз, если таковые все же возникли.
- После реализации соответствующих защитных мероприятий уровень безопасности повышается, что позволяет сохранить активы системы и обеспечить ее функциональность.



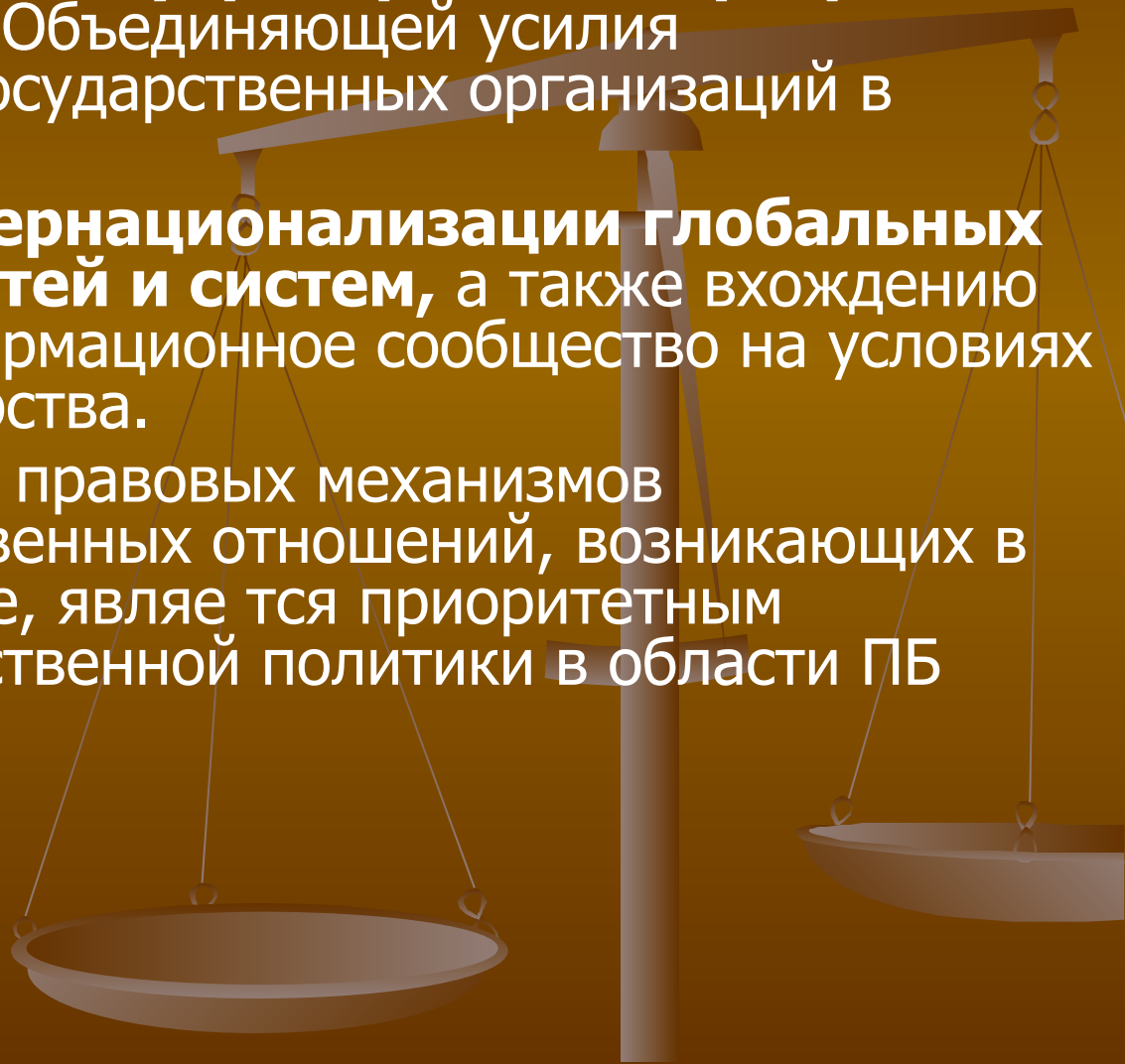
2. Стратегии и модели информационной безопасности.

ФУНКЦИИ ГОСУДАРСТВА ПО ОБЕСПЕЧЕНИЮ ИБ РФ

1 Проводит объективный и всесторонний анализ и прогнозирование угроз ИБ РФ, разрабатывает меры по ее обеспечению;

- **2 Организует работу законодательных (представительных) и исполнительных органов государственной власти РФ по реализации комплекса мер. направленных на предотвращение, отражение и нейтрализацию угроз ИБ РФ;**
- **3 Поддерживает деятельность общественных объединений, направленную на объективное информирование населения о социально значимых явлениях общественной жизни, защиту общества от искаженной и недостоверной информации;**
- **4 Осуществляет контроль за разработкой, созданием, развитием, использованием, экспортом и импортом средств защиты информации посредством их сертификации и лицензирования деятельности в области зашиты информации;**
- **5 Проводит необходимую протекционистскую политику в**

- **6 Способствует предоставлению физическим и юридическим лицам доступа** к мировым информационным ресурсам, **глобальным информационным сетям;**
- **7 Организует разработку федеральной программы обеспечения ИБ РФ.** Объединяющей усилия государственных и негосударственных организаций в данной области;
- **8 Способствует интернационализации глобальных информационных сетей и систем,** а также вхождению России в мировое информационное сообщество на условиях равноправного партнерства.
- **9** Совершенствование правовых механизмов регулирования общественных отношений, возникающих в информационной сфере, являе тся приоритетным направлением государственной политики в области ПБ РФ!!!



СИСТЕМА ОБЕСПЕЧЕНИЯ ИБ РФ (СОСТАВ)

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИБ РФ

Органы законодательной, исполнительной, судебной власти

1. Законы РФ и международные договоры. 2. Подзаконные акты: Президента РФ, Правительства РФ

МВК Совета Безопасности РФ в области ИБ

Координирует деятельность органов и сил по обеспечению ИБ

ОРГАНИЗАЦИОННАЯ ОСНОВА СОИБ РФ

Организационное обеспечение ИБ РФ

Президент РФ, Правительство РФ, Совет федерации, Госдума, Совет безопасности, МВК,
Органы исполнительной, судебной власти,
Общественные объединения, граждане,

СИСТЕМА ЗАЩИТЫ ГОСУДАРСТВЕННОЙ ТАЙНЫ (СЗИ ГТ)

Органы защиты ГТ: 1. МВК ЗГТ, 2.ФСБ РФ, 3. СВР РФ, 4. МО РФ, 5. Организации и их подразд-я по защите ГТ
(МВК по защите ГТ) – координирует деятельность

ГОСУДАРСТВЕННАЯ СИСТЕМА ПДТР и ТЗИ (противодействия техн-ким разведкам и технической защиты информации)

Организует ФСТЭК России

СИСТЕМА ПОДГОТОВКИ КАДРОВ В ОБЛАСТИ ИБ

Организует Минобрнауки

СИСТЕМА ЗАЩИТЫ ИНТЕЛ-ЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

ФОИВИС (Роспатент)

СИСТЕМЫ ЛИЦЕНЗИРОВАНИЯ (3 системы)

1. В области защиты гостайны
2. В области защиты конфид-й информации
3. В области криптографической зашиты информации

СИСТЕМЫ СЕРТИФИКАЦИИ СрЗИ (3 системы сертификации)

1. По требованиям безопасности информации
2. Криптографических средств защиты
3. Средств защиты ГТ (СЗИ-ГТ)

СИСТЕМА ЭКСПОРТНОГО КОНТРОЛЯ

ФСТЭК России

СИСТЕМА ЗАЩИТЫ информационных прав субъектов и противодействия преступлениям в информационной сфере

Органы судебной власти, Общественная палата
Уполномоченные по правам человека
Прокуратура, МВД России (Управление К)

ОСНОВНЫЕ ФУНКЦИИ СОИБ РФ:

1	**Разработка и совершенствование нормативной правовой базы в области обеспечения ИБ РФ;**
2	**Создание условий для реализации прав граждан и общественных объединений в информационной сфере,** определение и поддержание баланса между потребностью субъектов в свободном обмене информацией и необходимыми ограничениями на её распространение;
4	**Оценка состояния, источников угроз ИБ РФ, определение приоритетных направлений противодействия этим угрозам** (предотвращения, отражения и нейтрализации этих угроз);
4	**Координация и контроль деятельности органов, решающих задачи обеспечения ИБ РФ** (федеральных органов государственной власти и других государственных органов)
5	**Защита государственных ИР**, (прежде всего в федеральных органах государственной власти и органах государственной власти субъектов РФ, на предприятиях оборонного комплекса);
6	**Предупреждение, выявление и пресечение правонарушений, в информационной сфере, осуществление судопроизводства по делам о преступлениях в этой области;**
7	**Совершенствование системы подготовки кадров, используемых в области ИБ РФ**;
8	**Обеспечение контроля за созданием и использованием СрЗИ посредством обязательного лицензирования деятельности в данной сфере и сертификации СрЗИ;**
9	**Организация разработки федеральной и региональных программ,** фундаментальных и прикладных научных исследований, проведение единой технической политики **обеспечения ИБ и координация деятельности по их реализации**
10	**Осуществление международного сотрудничества в области обеспечения ИБ**, представление интересов РФ в соответствующих международных организациях.

Правовое обеспечение ИБ РФ

- **Правовое обеспечение информационной безопасности** является самостоятельным комплексным направлением правового регулирования отношений в области проявления угроз объектам информационной безопасности и противодействия эти угрозам на основе норм и институтов различных отраслей права (конституционного, гражданского. уголовного, и информационного).
- *Система правового обеспечения И Б РФ.* Включает отдельные нормативные правовые акты, специально предназначенные для регулирования отношений в области обеспечения информационной безопасности, и отдельные нормы в этой области, содержащиеся в нормативных правовых актах различных отраслей законодательства. К нормативным правовым актам относятся:
- - федеральные законы РФ и законы субъектов РФ. в том числе технические регламенты:
- - Указы Президента РФ:
- - Постановления Правительства РФ;
- - нормативные правовые акты федеральных органов исполнительной власти уполномоченных осуществлять правовое регулирование в области информационной безопасности и защиты информации.
- Правовое обеспечение создаёт правовую основу для функционирования всех других систем в области ИБ и управления ими со стороны Президента РФ и Правительства РФ.

Система защиты государственной тайны

- *Система зашиты государственной тайны - совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих целях.* Вся деятельность по защите государственной тайны в России осуществляется в соответствии с законом РФ ≪О государственной тайне≫.
- Коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны в интересах разработки и выполнения государственных программ, нормативных и методических документов, обеспечивающих реализацию законодательства Российской Федерации о государственной тайне, является Межведомственная комиссия по защите государственной тайны. Руководство деятельностью Межведомственной комиссии осуществляет Президент Российской Федерации.

Государственная система противодействия техническим разведкам (ПДТР) и технической защиты информации (ТЗИ).

- *Государственная система противодействия техническим разведкам (ПДТР) и технической защиты информации (ТЗИ).* Организация деятельности государственной системы противодействия техническим разведкам и технической зашиты информации на федеральном, межрегиональном, региональном, отраслевом и объектовом уровнях, а также руководство указанной государственной системой возложено законодательством РФ на Федеральную службу по техническому и экспортному контролю (до 2004 года именовалась Гостехкомиссия России).

Система подготовки кадров в области информационной безопасности.

- *Система подготовки кадров в области информационной безопасности* включает:
- - учреждения высшего и среднего профессионального образования, ведущие подготовку по направлению Информационная безопасность с уровнем подготовки: техник, бакалавр, специалист, магистр:
- - государственные образовательные стандарты высшего (ГОС ВО) и среднего специального образования в области информационной безопасности;
- - научную специальность 05.13.19 ≪Методы и системы защиты информации, информационная безопасность≫, для подготовки кадров высшей квалификации (кандидат наук, доктор наук), включающей физико-математические науки, технические науки, юридические науки;
- - учебно-методическое объединение (УМО) вузов по образованию в области информационной безопасности и учебно-методический совет (в структуре УМО в области истории и архивоведения).
- - курсы переподготовки и повышения квалификации в этой области, действующие на базе вузов и центров информационной безопасности.

Система защиты интеллектуальной собственности

- ***Система защиты интеллектуальной собственности.*** Образуется совокупностью:
- - законодательства РФ в области интеллектуальной собственности, основу которого составляет часть IV Гражданского кодекса РФ;
- - федерального органа исполнительной власти уполномоченного в области интеллектуальной собственности (Роспатент);
- - органами МВД, осуществляющими борьбу с нарушениями в области интеллектуальной собственности;
- - общественными организациями в области коллективного управления авторскими правами (Российское авторское общество и др.).

Система защиты информационных прав субъектов и противодействия преступлениям в информационной сфере.

- *Система защиты информационных прав субъектов* и противодействия преступлениям в информационной сфере. Эта система включает:
- - нормы Конституции РФ и нормы федеральных законов, содержащие информационные права:
- - суды различных инстанций, органы прокуратуры, осуществляющие защиту информационных прав граждан, общественных организаций:
- - общественные институты (общественная палата при Президенте РФ) и специальные институты по правам человека (уполномоченные по п р авам человека) и др.;
- - специальные органы в системе МВД России (Управление ≪К≫) по борьбе с преступлениями в сфере высоких технологий.

- ***Система экспортного контроля.***
  Руководство указанной государственной системой возложено законодательством РФ на Федеральную службу по техническому и экспортному контролю
- ***Система научно-исследовательских институтов (НИИ), научных и научно-****исследовательских центров в области ИБ предназначена для осуществления* фундаментальных и прикладных научных исследований в области обеспечения ИБ РФ. Она включает:
- - специализированные в области ИБ научно-исследовательские институты при Академии наук РФ, вузах, ведомствах и ведомственных вузах (ФСБ России, ФСТЭК России);
- - специализированные научные и научно - исследовательские центры в области ИБ, как при государственных учреждениях и органах государственной власти, так и негосударственных;
- - учебно-научные центры при ведущих вузах России.

Системы лицензирования по видам деятельности в области ИБ.

Для регламентации деятельности в области информационной безопасности в России функционируют три системы лицензирования:

- система лицензирования в области защиты государственной тайны (регламентируется законодательством ≪О государственной тайне≫):
- система лицензирования в области защиты конфиденциальной информации (регламентируется законом ≪О лицензировании отдельных видов деятельности≫ и нормативными актами Правительства РФ);
- система лицензирования в области криптографической зашиты информации (регламентируется законом ≪О лицензировании отдельных видов деятельности≫ и нормативными актами Правительства РФ).

Каждая из систем имеет сеть аккредитованных лицензионных центров в субъектах РФ. Виды деятельности и условия лицензирования по ним в рамках каждой системы определены нормативными актами Правительства РФ.

- ***Системы сертификации средств обеспечения ИБ***

  Сертификация средств защиты информации осуществляется в целях подтверждения их соответствия требованиям технических регламентов, стандартов, специальных нормативных документов в области ИБ. К сертификации относится также аттестация объектов информатизации по требованиям безопасности информации. Она проводится в соответствии с нормами Федерального закона ≪О техническом регулировании≫.
- **Системы сертификации:**
- 1.Система сертификации средств защиты информации по требованиям безопасности информации РОСС RU. 0001. 01БИ00:
- 2. Система сертификации средств криптографической защиты информации РОСС.R.U.0001.030001;
- 3. Система сертификации средств защиты информации по требованиям безопасности для сведений, составляющих государственную тайну (СЗП-ГТ).

ПОНЯТИЕ И КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИБ ОРГАНИЗАЦИИ

Теоретические основы информационной безопасности организации, призваны в форме научного знания, дать целостное представление об объектах информационной безопасности организации, угрозах этим объектам и интересам субъектов, политике и системе обеспечения информационной безопасности организации, их закономерностях и существенных связях между собой и окружающей средой.

В качестве такой формы научных знаний, основанных на практическом опыте следует считать международные стандарты в области информационной безопасности, принятые в России на уровне национальных. Их необходимо рассматривать как основные источники теории ИБ организации:

- **Стандарты одна из форм накопления знаний;**
- **В них зафиксированы апробированные, высококачественные решения и методологии, разработанные наиболее квалифицированными специалистами**

ГОСТ Р ИСО/МЭК 27001 -2006 Национальный стандарт РФ. Информационная технология. Методы и средства обеспечения безопасности. **Системы менеджмента ИБ**. Требования.

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

ГОСТ Р ИСО/МЭК 13335 Национальный стандарт РФ. Информационная технология. Методы и средства обеспечения безопасности. Части 1-5.(2006-2007)

ГОСТ Р ИСО/МЭК 15408-2008 Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. **Критерии оценки безопасности информационных технологий**. Части 1-3.

Стандарты предназначены для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями) и содержат концепции и модели по менеджменту ИБ, руководства по управлению безопасностью ИТ и ИТТ на которых основаны бизнес-процессы организации, методы управления рисками в этой области, меры организационного, технического характера по обеспечению безопасности ИТ (ИТТ), меры физической защиты и

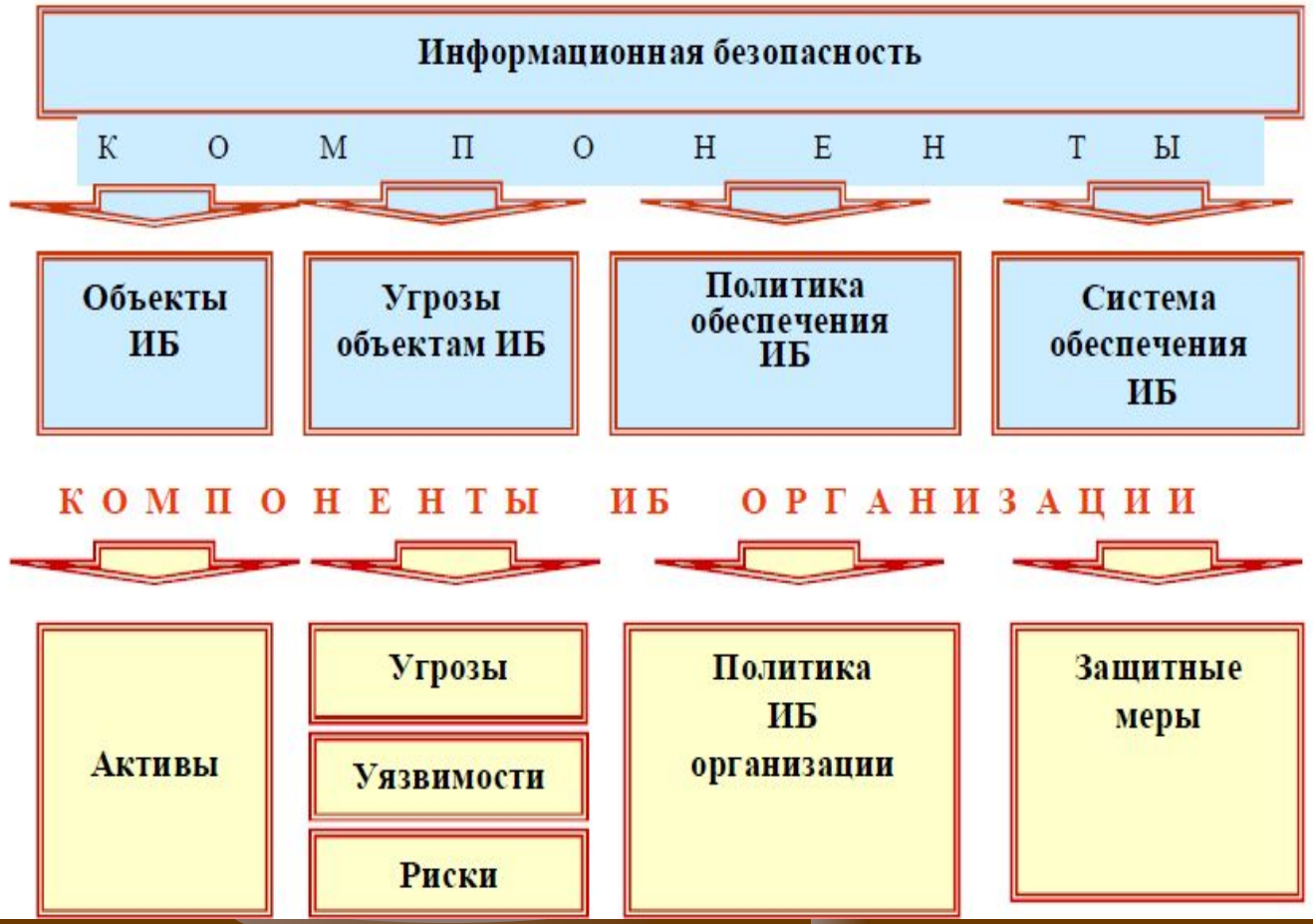
ПОНЯТИЕ И КОНЦЕПТУАЛЬНАЯ МОДЕЛЬ ИБ ОРГАНИЗАЦИИ

Информационная безопасность организации - это состояние защищённости объектов (активов) организации, при котором обеспечивается конфиденциальность, целостность, доступность информации.

Проблемы ИБ организации могут включать в себя потерю:

- **Конфиденциальности;**
- **целостности;**
- **доступности ;**
- **подотчетности;**
- **аутентичности;**
- **Достоверности информации или средств её обработки**

Концептуальная модель информационной безопасности организации



- Говоря о свойствах информационной сферы, необходимо детализировать состав информационных объектов, входящих в нее. Для этого рассмотрим фрагмент структуры информационной сферы организации, показанный на рис. 4, где приведены наиболее характерные для современных организаций составные части:
- — правовая среда бизнеса, находящаяся, как правило, за рамками конечных пользователей, предприятий и организаций;
- — учредительная и лицензионная база организации (предприятия);
- — специфичная информация бизнеса, которая, в свою очередь, может быть классифицирована на несколько видов, наиболее важные из них показаны в нижней части рис. 4.
- Входные информационные потоки (информация о состоянии, предполагаемые последствия деятельности в виде прогнозов) превращаются менеджментом в управляющую информацию: оперативную — планы, распоряжения; стратегическую — цели, концепции, политики. Отношения субъект / субъект и субъект / объект, включая управление, обозначены на рисунке 4 синими линиями.
- В нижней части рис. 4 приведен перечень видов информационных объектов. Совсем необязательно, чтобы любые объекты этих видов хранились в виде компьютерных баз данных или файлов. Это могут быть и бумажные документы, и даже просто договоренности между субъектами, например владельцами бизнеса, но все равно это остается информацией. Вопрос лишь в том, насколько эта информация приспособлена для автоматизированной обработки, какие следы остались на материальных носителях, имеет ли эта информация юридическую силу.

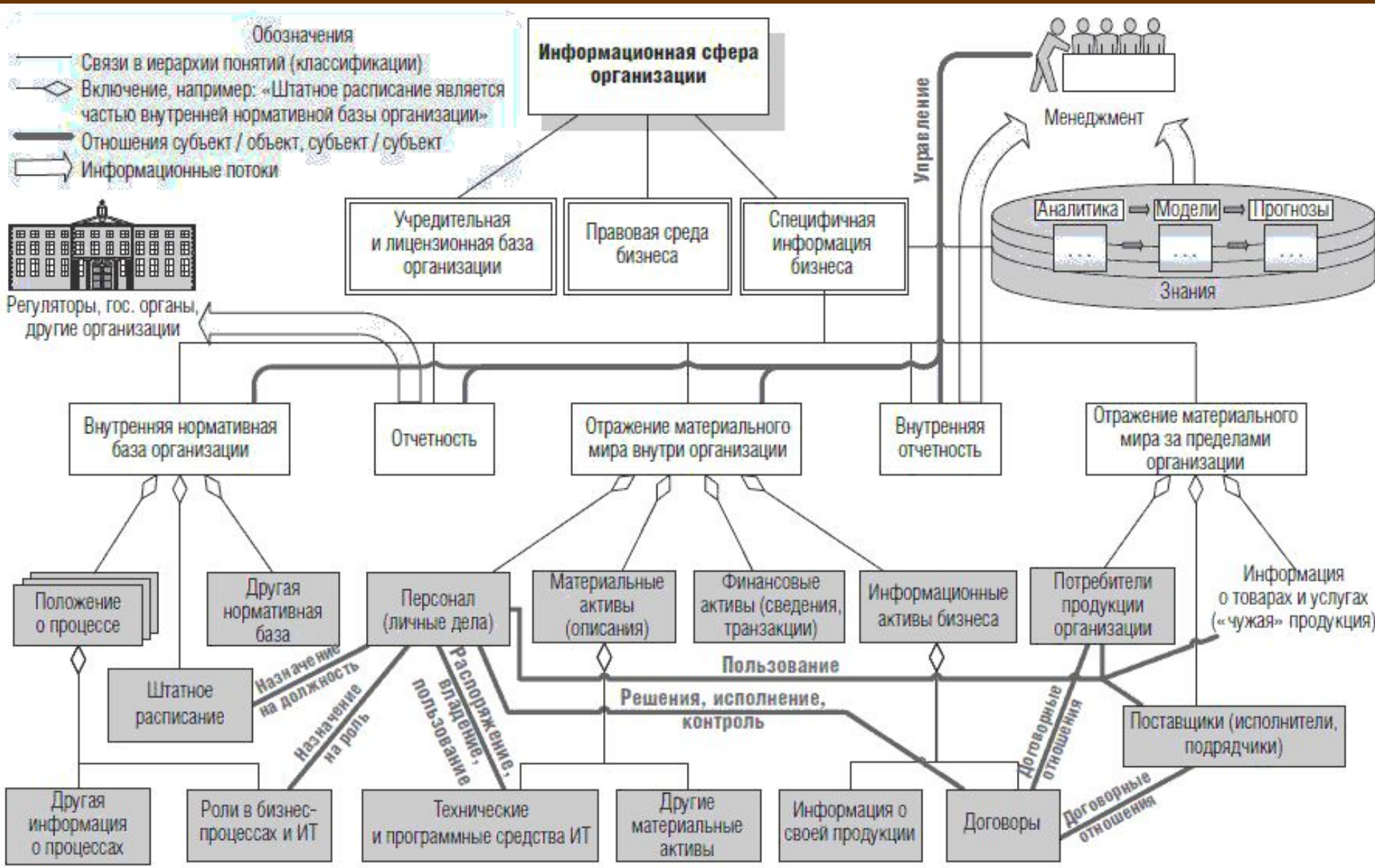


Рис. 4. Структура информационной сферы организации

Модель (цикл) Деминга – Шухарта.

Модель (цикл) Деминга – Шухарта легла в основу большинства современных управленческих стандартов для различных областей деятельности и «де-факто» становится базовой моделью.

“Цикл Деминга” известен еще и как “Цикл Шухарта”, цикл “PDCA” или цикл “PDSA”». Аббревиатура циклов «PDCA» и «PDSA» раскрывается как «планируй – сделай – проверь – действуй» для PDCA и «планируй – сделай – изучи – действуй» для PDSA. Аббревиатура PDCA является наиболее распространенной, хотя сам Деминг более предпочитает использовать PDSA».

В практической деятельности при работе над внедрением в различных организациях систем менеджмента информационной безопасности, систем менеджмента информационными активами организации, систем менеджмента рисками информационной безопасности и прочих систем менеджмента в области информационной безопасности нередко приходится слышать применительно к модели Деминга – Шухарта фразу «волшебный цикл». По большому счету это не преувеличение, а лишь отражение того, что теория системного и процессного подходов попала в цель и практика многократно подтвердила эту теорию.

Рис. 14 Эталонная модель Деминга-Шухарта (модель Деминга)

- Рис. 14 иллюстрирует эталонную модель Деминга – Шухарта (модель Деминга), как это представляется экспертами технических комитетов ИСО, использующих данную модель в основе международных управленческих стандартов [8]. Эта методология в равной степени применима к высокоуровневым стратегическим процессам и простой операционной деятельности.
- Основные фазы модели следующие:
- – «планирование»: установление целей и процессов, необходимых для выработки результатов в соответствии с требованиями клиентов и политиками организации;
- – «выполнение» («реализация»): реализация запланированных процессов и решений;
- – «проверка»: контроль и измерение процессов и производимых продуктов относительно политик, целей и требований к продукции и отчетность о результатах;
- – «действие» («совершенствование»): принятие корректирующих и превентивных мер для постоянного совершенствования функционирования процесса.

- В основе практики реализации модели Деминга лежит процессный подход. При этом само практическое наполнение понятия «процесс» не предполагает жесточайшей регламентации. В процессном подходе любая деятельность, которая выполняется или для управления которой используются ресурсы организации, считается процессом, преобразующим входы в выходы. Это методология (подход), идентифицирующая процессы в организации так, чтобы их взаимосвязи могли быть поняты, видимы и измеримы, а итоговая совокупность процессов понималась бы как единая система реализации целей деятельности организации (см. рис. 15).
- Процессный подход вводит горизонтальный менеджмент, пересекающий барьеры между различными функциональными единицами и консолидирующий их внимание на основных целях деятельности организации.

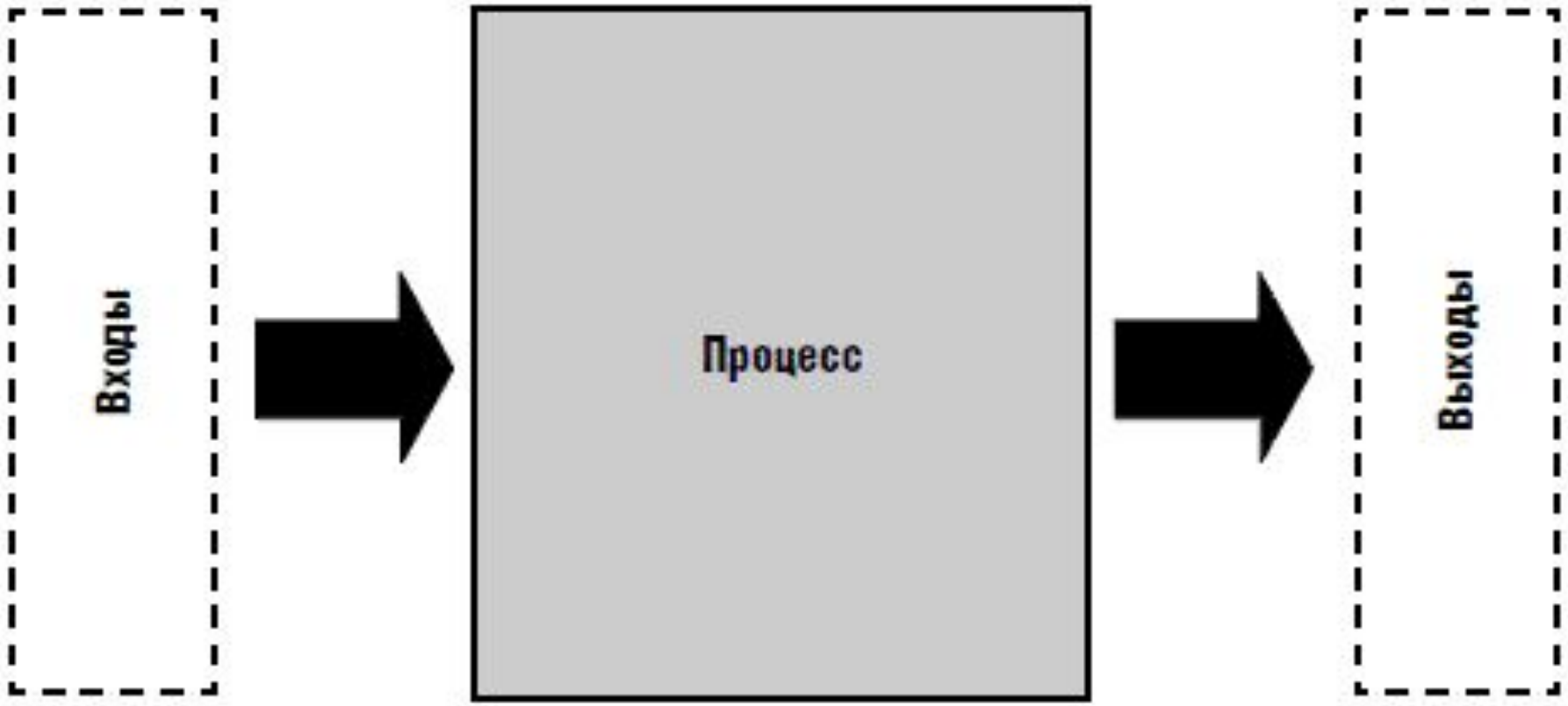


Рис. 15. Процессный подход

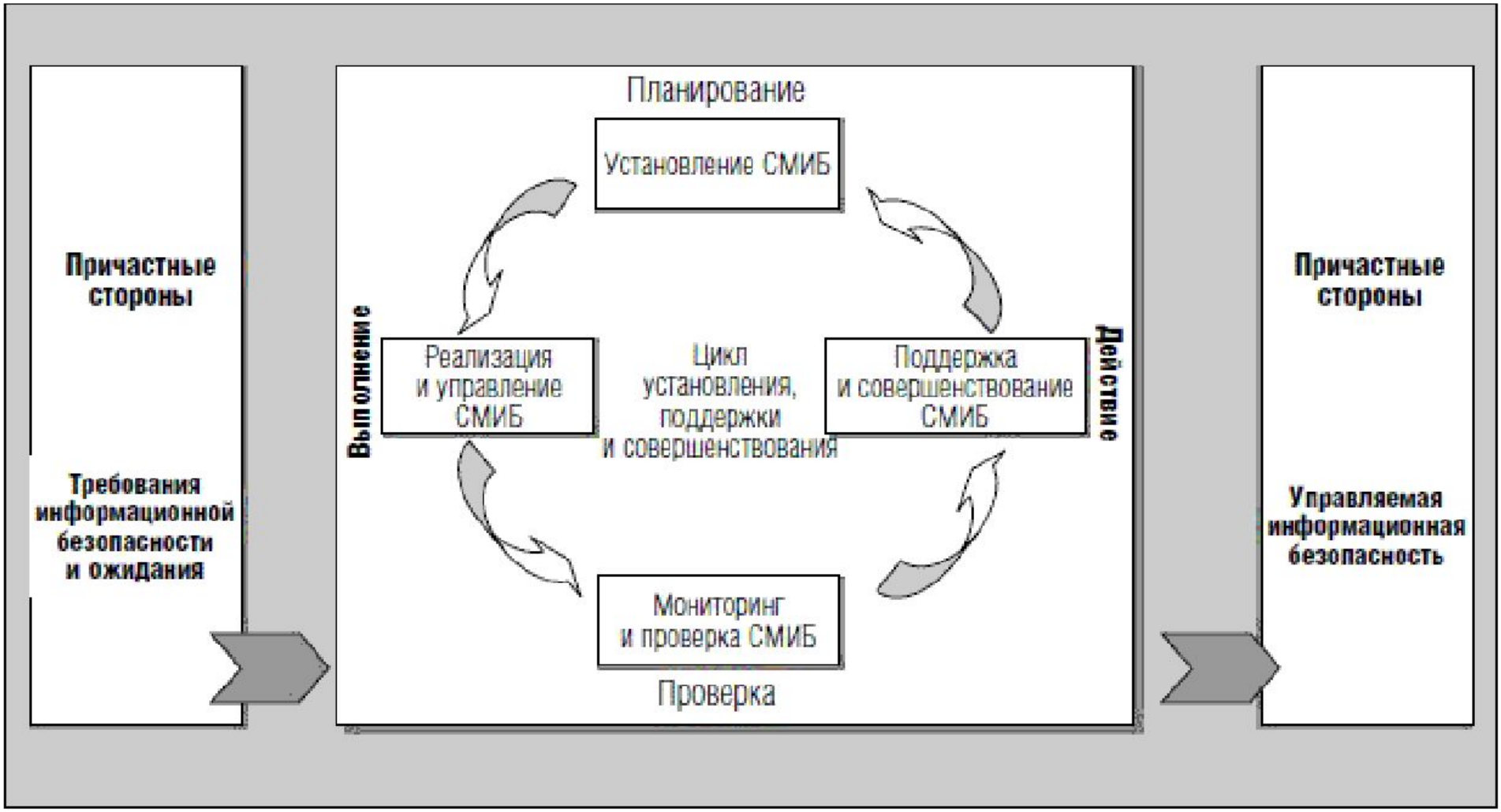


Рис. 20. Компоненты структуры системы менеджмента информационной безопасности организации в соответствии с ISO/IEC 27001