**РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ**
**Кафедра информационной безопасности**

# УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УСЛОВИЯ ЕЕ ПРАВОВОГО ОБЕСПЕЧЕНИЯ

***ЛЕКЦИЯ***
***23-30 сентября 2015 г.***

**ДЕРБИН Евгений Анатольевич,**
**профессор кафедры, доктор военных наук**
**8-926-754-13-75,**
**evg.derbin@yandex.ru**

## Учебные вопросы:

**1.** Угрозы информационной безопасности.

**2.** Обеспечение информационной безопасности как комплексная задача реализации правовых, организационных и технических мер.

**3.** Социально-правовые нормы в обеспечении информационной безопасности: моральные, правовые, политические, эстетические, корпоративные

**4.** Технико-правовые нормы в обеспечении информационной безопасности. Основы технического регулирования

## Литература:

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

**2.** Закон ФЗ №310 «О безопасности», 26 декабря 2010 г.

**3.** Стрельцов А.А. Информационная безопасность Российской Федерации. - М.: Высшая школа, 2003., С. 27-48

**4.** http//www.secuteck.ru/articles2/security-director/tonkostibezopasnosti

**5.** «Гражданский кодекс РФ» от 21.01.96 г., №14-ФЗ ч.2, ст. 857;

**6.** «Уголовный Кодекс РФ» от 13.06.96г. №63-ФЗ ст. 183, 272, 273, 274;

Литература:

**7.** «Трудовой Кодекс РФ» от 30.12.01, №197-ФЗ ст. 85,86,87,88,89,90;

**8.** «Кодекс Российской Федерации об административных правонарушениях» от 30.12.01, №195-ФЗ ст. 13.12, 13.13, 13.14;

**9.** ФЗ РФ «О банках и банковской деятельности» от 02.12.90г. №395-1, ст.26.

**10.** ФЗ РФ «Об информации, информационных технологиях и о защите информации» от 27.07.2006г. № 149-ФЗ.

**11.** ФЗ РФ «О лицензировании отдельных видов деятельности» от 08.08.2001 №128-ФЗ (в ред. от 21.03.2002 № 31-ФЗ).

**12.** Указ Президента РФ от 06.03.97г. № 188 «Об утверждении перечня сведений конфиденциального характера».

**13.** Постановление Правительства РФ от 15.08.06. №504 «О лицензировании деятельности по технической защите конфиденциальной информации».

**14.** Приказ ФАПСИ от 13.06.01г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»

# БАЗОВЫЕ ПОНЯТИЯ

**ИНФОРМАЦИЯ** – **ИНФОРМАЦИЯ – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.**

**ИНФОРМАЦИОННЫЙ ОБЪЕКТ** – **ИНФОРМАЦИОННЫЙ ОБЪЕКТ – информация или ее носитель.**

**ИНФОРМАЦИОННАЯ ОБСТАНОВКА** – **ИНФОРМАЦИОННАЯ ОБСТАНОВКА – совокупность условий и факторов, оказывающих влияние на состояние информационной сферы и функционирование информационных объектов.**

**УГРОЗА** – **УГРОЗА – высший уровень опасности, характеризуемый наличием намерения, возможности и готовности субъекта (фактора) угрозы к нанесению (реализации) ущерба объекту, влекущего:**

- **утрату элементов структуры объекта;**
- **нарушение связей, программ и функций объекта;**
- **потерю способности объекта к развитию;**
- **утрату самоидентичности объекта.**

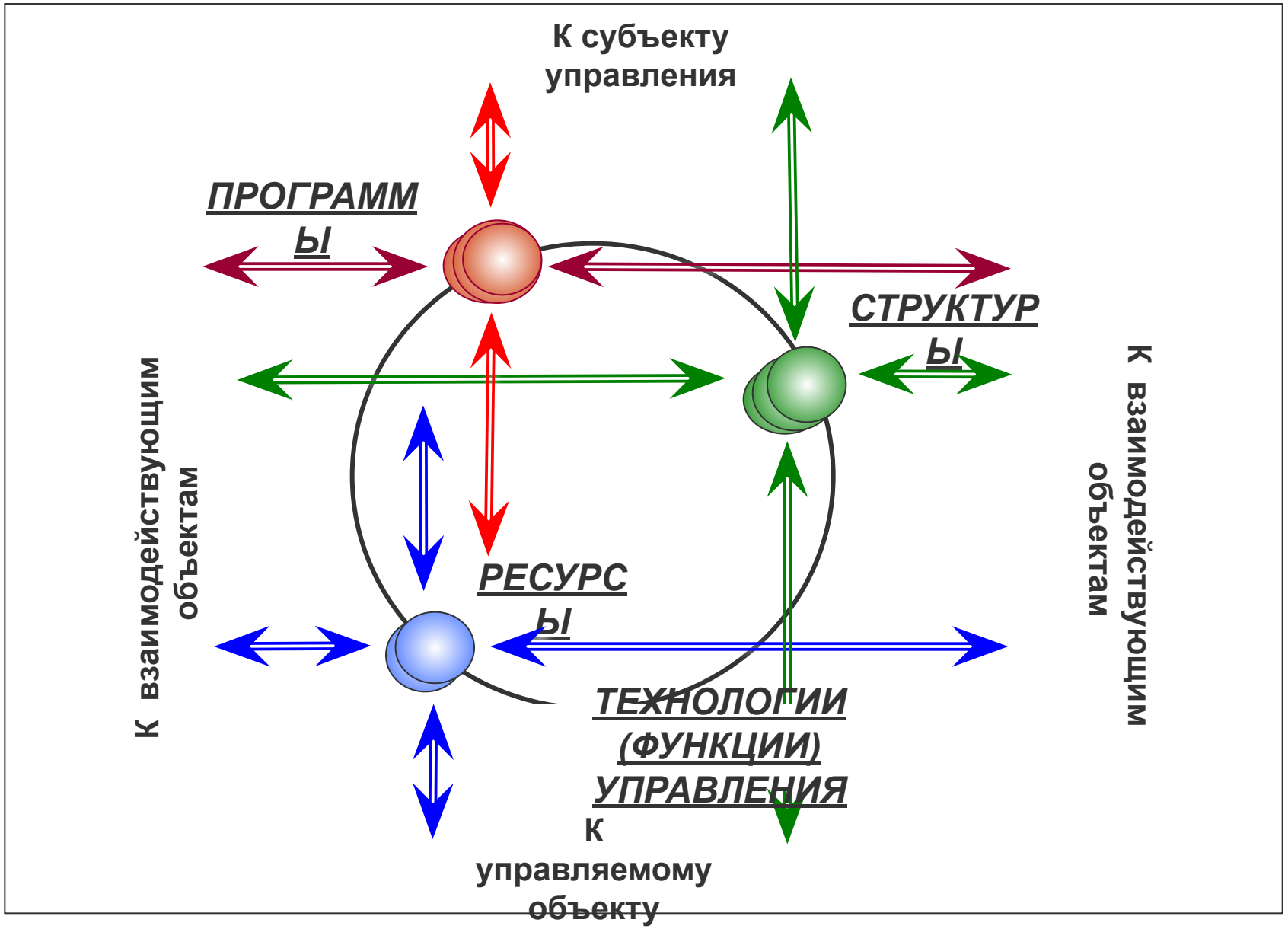
**ОПАСНОСТЬ** – **ИНФОРМАЦИОННАЯ ОПАСНОСТЬ – состояние информационной обстановки, характеризуемое обострением рисков объекта (вызовов, угроз объекту), реализация которых сделает его менее соответствующим своему предназначению**

**БЕЗОПАСНОСТЬ** – **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТА – состояние информационной обстановки, характеризуемое отсутствием опасности, готовностью субъекта управления защитить объект от ущерба воздействий (вызовов и угроз) и (или) способностью объекта самостоятельно их нейтрализовывать.**

# 1. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

# ИНФОРМАЦИЯ КАК ИНФОРМАЦИОННЫЙ ОБЪЕКТ

# ТОПОЛОГИЯ ИНФОРМАЦИОННОГО ОБЪЕКТА

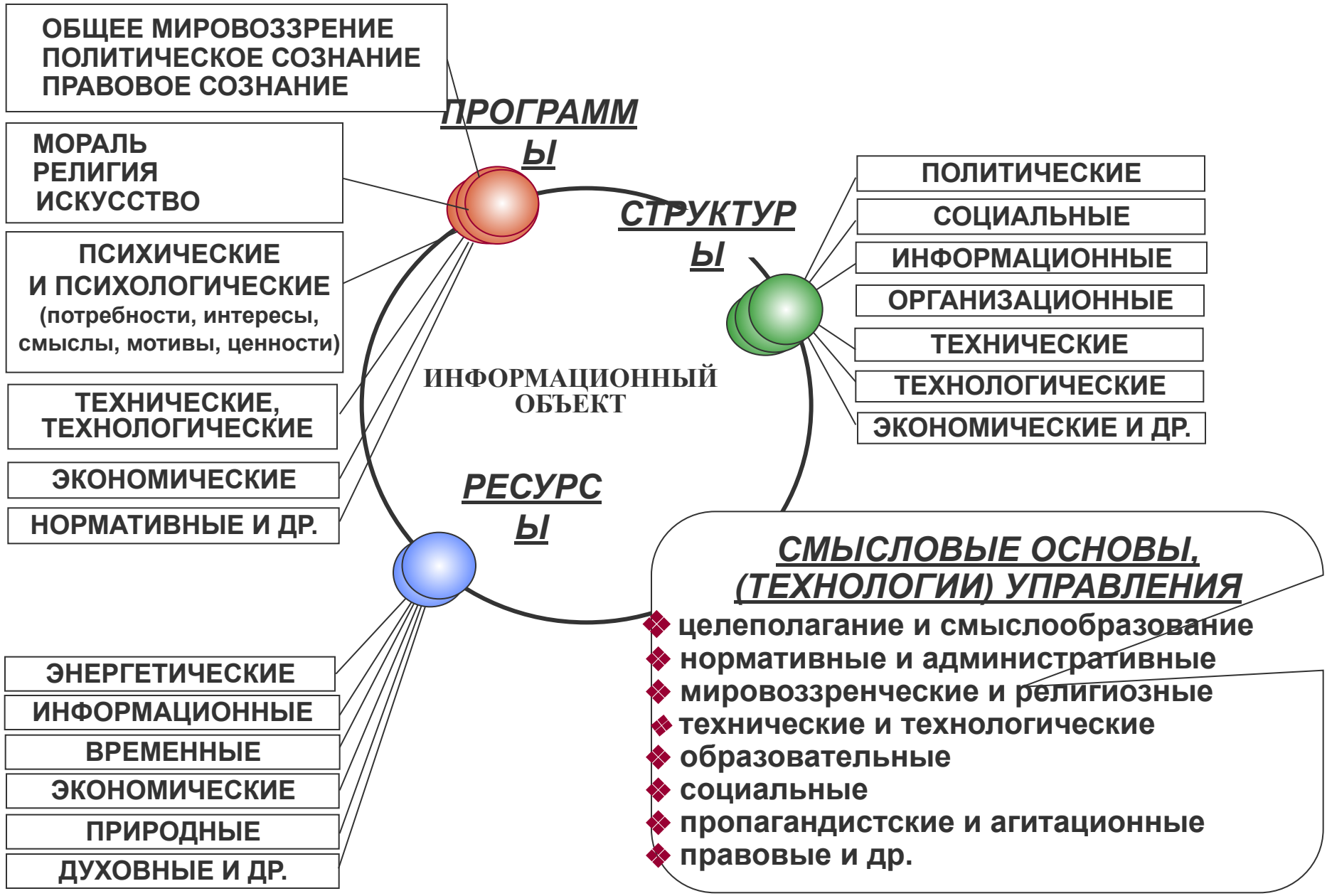


# УНИВЕРСАЛЬНЫЕ ПРИЗНАКИ ИНФОРМАЦИОННЫХ ХАРАКТЕРИСТИК ОБЪЕКТОВ С УЧЕТОМ СОДЕРЖАНИЯ ЭЛЕМЕНТОВ ИХ ТОПОЛОГИИ



| ЭЛЕМЕНТЫ ТОПОЛОГИИ | ОБЪЕКТЫ: | | |
|---|---|---|---|
| | ИНФОРМАЦИЯ | ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ | ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКИЕ |
| Структуры | Форма, логичность, последовательность), целостность, сохранность и др. | Конфигурация вычислительной сети, телекоммуникацион-ных систем и пр. | Для индивида: структура личности, психологическая и биологическая структуры. Для социальной группы: политическая, социальная, психологическая, организационная и др. структуры |
| Программы | Смыслообусловленность | Уровень программного обеспечения и алгоритмов защиты информации и др. | Доминирующие духовные и материаль-ные потребности; мировоззренческие, ценностно-смысловые аспекты, цели, задачи, планы, интересы, мотивы деятельности и др. |
| Ресурсы | Объем, качество (актуальность, новизна, важность, истинность) и др. | Объем ресурсов: информационного, энергетического и др., техническая надежность, защищенность и пр. | Для индивида: власть, социальный и профессиональный опыт, квалификация, компетентность, память, качество и объем знаний, состояние физического здоровья и психологической устойчивости; меры удовлетворения потребностей. Для социальной группы: экономичес-кие, психологические, моральные и др. |
| Системные основы (функции, требования) | Уровень обобщения; смысловой, когнитивный, аксиологический, мотивационной и др. аспекты, конфиденциальность, достоверность и др. | Принадлежность, роль и место в системе управления, зависимость от человеческого фактора и др. | Роль в обществе, важность, функций; моральные, нравственные и рационально-волевые качества, идеология. Слаженность коллектива и др. |
| Связи | Логические связи с другими объектами, принадлежность, направленность: причина-следствие; посылки-выводы; аргументы-факты и др. | Системные связи вычислительной сети | Субъектность в структуре, политические и социальные отношения, коммуникабельность, гибкость. Доминирующие отношения (противо-борство, конкуренция, сосуществование, сотрудничество, дружба и пр.) |

# АНАЛИЗ СОЦИОТЕХНИЧЕСКОГО ИНФОРМАЦИОННОГО ОБЪЕКТА

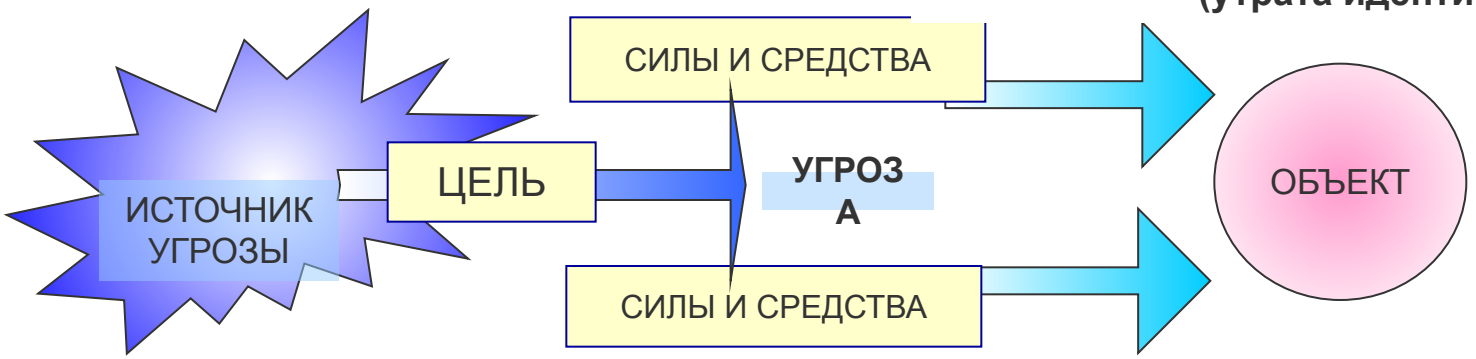


# СУЩНОСТЬ ПОНЯТИЙ «ОПАСНОСТЬ» И «БЕЗОПАСНОСТЬ»



**ИНФОРМАЦИОННАЯ ОПАСНОСТЬ – состояние информационной обстановки, характеризуемое обострением рисков объекта (вызовов, угроз объекту), реализация которых сделает его менее соответствующим своему предназначению**

**ВЫЗОВЫ (УГРОЗЫ):**
**утрата элементов структуры;**
**нарушение системных связей;**
**нарушение программ и функций;**
**потеря способности к развитию;**
**прекращение существования (утрата идентичности).**




**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 ИНФОРМАЦИИ**

***Конфиденциальность, целостность и доступность: «модель CIA (Confidentiality-Integrity-Availability)»***
***Стандарты ISO 27001, ISO 27002***

# ОПАСНОСТЬ И БЕЗОПАСНОСТЬ ОБЪЕКТА КАК ХАРАКТЕРИСТИКИ СОСТОЯНИЯ ОБСТАНОВКИ

**БЕЗОПАСНОСТЬ**

**ПОЛИТИКА**

Компетенция политики – применение технологий перевода угроз в вызовы и вызовов в риски

**ОПАСНОСТЬ**

| Степени | Компоненты | | Готовность к нанесению ущерба |
|---|---|---|---|
| | намерения | возможность | |
| **РИСК** | нет | нет | мнимая |
| **ВЫЗОВ** | нет | есть | гипотетическая (возможная) |
| | есть | нет | |
| **УГРОЗА** | есть | есть | реальная (явная) |

## СТЕПЕНИ (УРОВНИ) ОПАСНОСТИ

- степени готовности противника к конфликтным действиям;
- степени зарождения (насыщения, обострения) противоречий между сторонами;
- уровни предконфликтного состояния сторон;
- персонификация (наличие или отсутствие явных субъектов и объектов противоречий)

### *РИСК* → *ВЫЗОВ* → *УГРОЗА*

- наличие условий и факторов (интересов, ограниченных ресурсов, противоречий) для реализации;
- наличие возможности у объекта воздействия помешать достижению цели субъектом (US National Security Strategy)

- стремление сторон начать спорить (бороться, конфликтные отношения);
- проявление (усиление) факторов обострения обстановки (противоречий);
- возможность противодействия со стороны объекта в ответ на воздействие субъекта (US National Security Strategy)

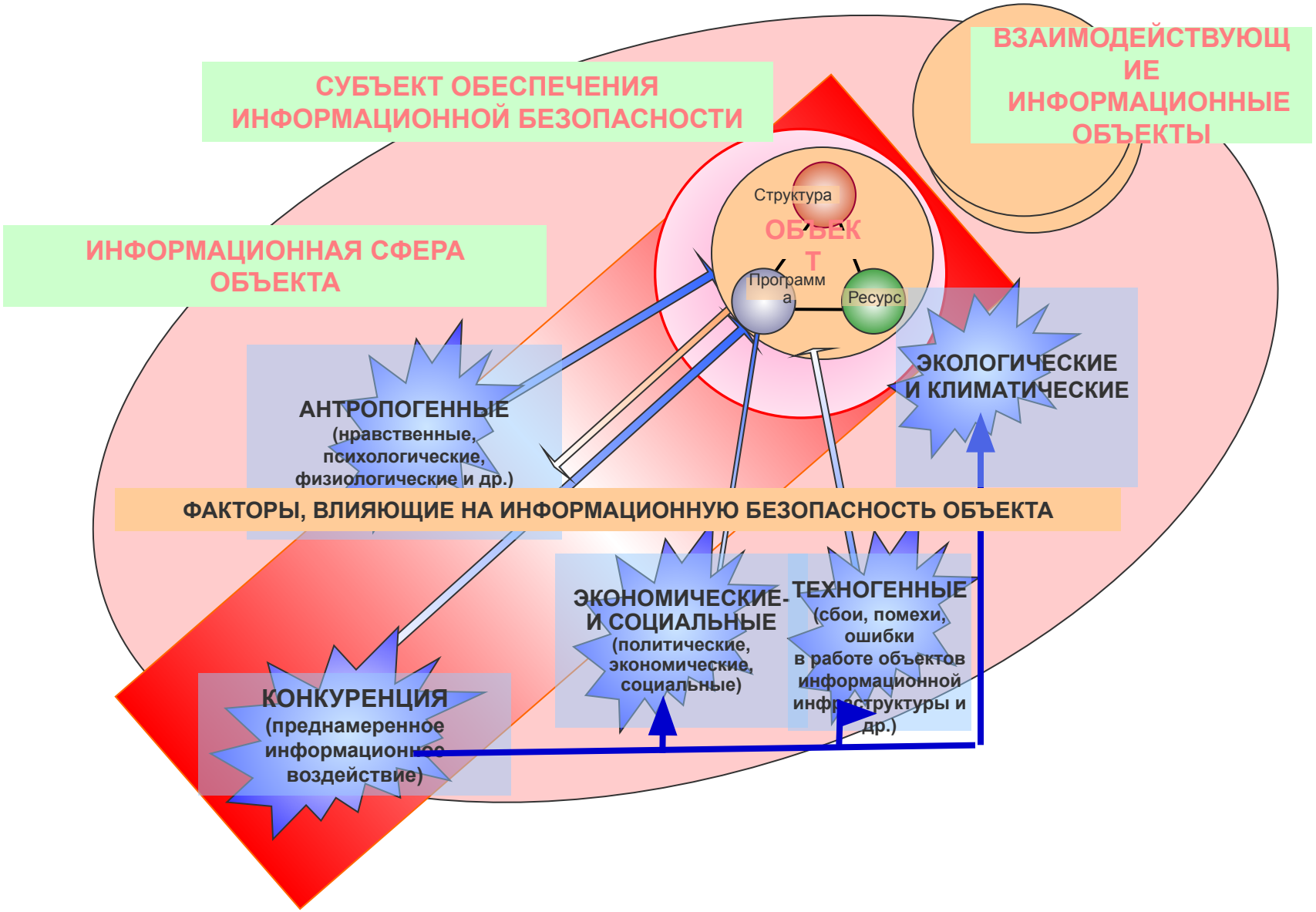
- обещание (намерение) сторон причинить вред, ущерб (потерю, убыток, урон);
- подготовительные (демонстративные) действия сторон, которые могут привести к конфликту

а) Субъективные намерения (замыслы, желания) противника

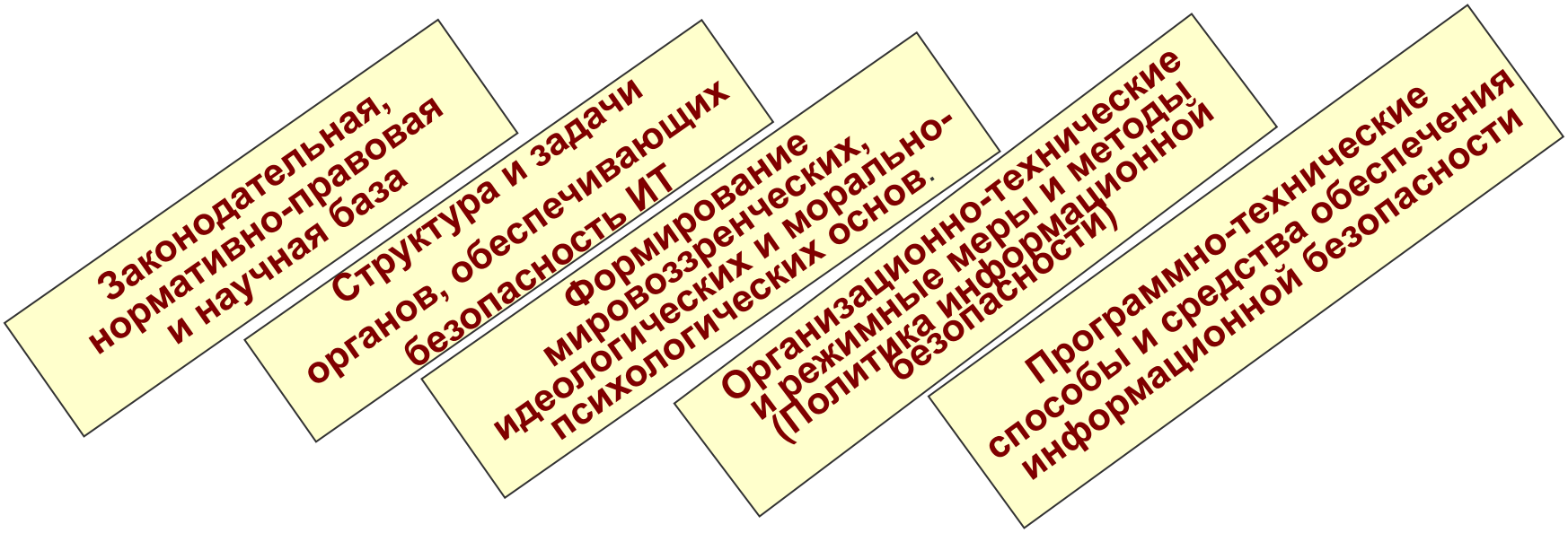
б) Объективные возможности у противника (наличие сил и средств) для реализации своих замыслов

# ФАКТОРЫ, ОКАЗЫВАЮЩИЕ ВЛИЯНИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ





# АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

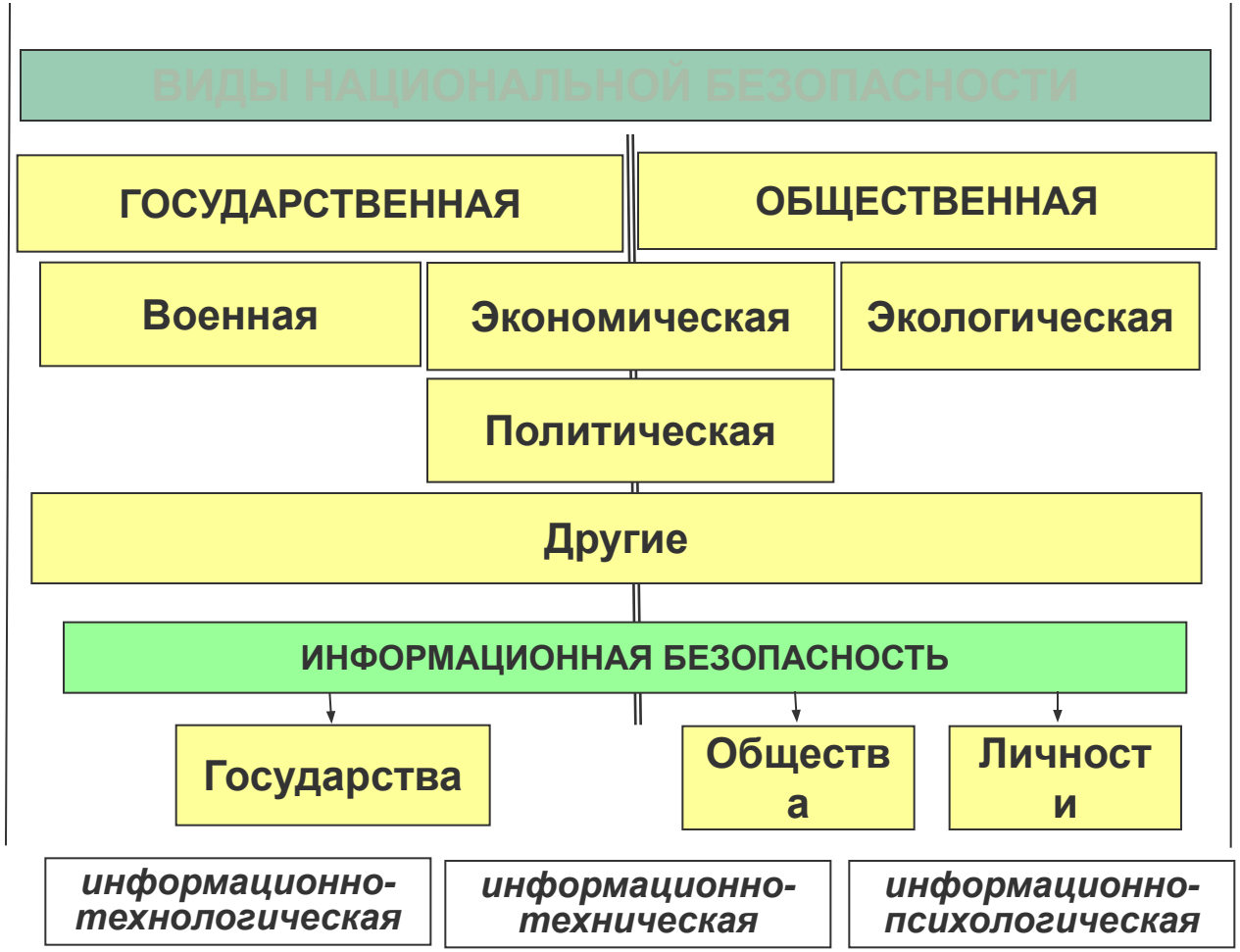



## ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НЕОБХОДИМО:

- 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

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

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СТРУКТУРЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ




**СОСТОЯНИЕ ЗАЩИЩЕННОСТИ НАЦИОНАЛЬНЫХ ИНТЕРЕСОВ В ИНФОРМАЦИОННОЙ СФЕРЕ, ОПРЕДЕЛЯЮЩИХСЯ СОВОКУПНОСТЬЮ СБАЛАНСИРОВАННЫХ ИНТЕРЕСОВ ЛИЧНОСТИ, ОБЩЕСТВА, ГОСУДАРСТВА**

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ, ст. 1, п.3

# ИНТЕРЕСЫ КОРПОРАТИВНОГО ВЕДОМСТВА В ИНФОРМАЦИОННОЙ СФЕРЕ

## Личности

- доступ к информации для удовлетворения потребностей;
- защита информации, обеспечивающей личную безопасность

## Общества (коллектива)

- обеспечение интересов акционеров в информационной сфере;
- укрепление правовых основ информационной деятельности;
- поддержание согласия;
- защита духовных ценностей

## Ведомства

- реализация интересов ведомства в информационной сфере;
- информационная поддержка деловой политики;
- регулирование и укрепление позиций на рынке;
- развитие информационной инфраструктуры

# МЕТОДИЧЕСКИЙ АППАРАТ ФОРМИРОВАНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Е Н И Я  И Н Ф О Р М А - Ц И О Н Н О Й  Б Е З О П А С Н О С Т И

## ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Формирование эффективной системы управления
- Формирование национального патриотического, корпоративного мировоззрения, ценностей, смыслов, целей
- Развитие современных технико-технологических основ управления
- Совершен-ствование образованности и профессио-нальной компетентности
- Обеспечение целостности, доступности и конфиден-циальности информации
- Нейтрали-зация угроз в информа-ционной сфере и их источников

СИСТЕМА

**МЕТОДЫ**: Организационные | Экономические | Технические | Специальные

ИНФОРМА

- ПОДДЕРЖАНИЕ УСЛОВИЙ ЭФФЕКТИВНОГО УПРАВЛЕНИЯ
- СОХРАНЕНИЕ ПОЗИТИВНЫХ ТЕНДЕНЦИЙ РАЗВИТИЯ
- СОХРАНЕНИЕ ОСНОВ КУЛЬТУРЫ, РАЗВИТИЕ БИЗНЕСА И ПОДДЕРЖАНИЕ СПЛОЧЕННОСТИ КОЛЛЕКТИВА

- Организационная структурно-функциональная подсистема
- Подсистема правового обеспечения
- Подсистема подготовки кадров и образования
- Подсистема морально-психологического обеспечения
- Подсистема лингвистического, семантико-логического обеспечения
- Подсистема научных исследований
- Подсистема мер обеспечения безопасности информации
- Подсистема технического обеспечения
- Подсистема анализа, прогнозирования и контроля
- Подсистема работы со СМИ и общественностью
- Подсистема взаимодействия с другими предприятиями и конкурентами

## ВИДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

- Методическое
- Правовое
- Психологическое
- Информационное
- Научно-технологическое
- Лингвистическое
- Математическое (алгоритмическое)
- Защиты информации и др.
- Программное
- Аппаратно-техническое

УГРОЗЫ ИНФОРМА ЦИОННОЙ БЕЗОПАС

# 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

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРЕДПРИЯТИЯ

**Определяется способностью руководства предприятия и его коллектива адекватно реагировать на угрозы в информационной сфере, обеспечивать устойчивость функционирования, эффективное управление и способность к совершенствованию (развитию) производства (деятельности)**

## ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Цель: создание условий для достижения эффективности управления предприятием и его позитивного развития**

**Задачи: достижение стабильности состояния, функций и тенденций к позитивному развитию производства, успешного выполнения задач, совершенствованию коллектива и личности**

**Содержание: деятельность органов управления, выделенных сил и средств по поддержанию состояния информационной безопасности предприятия, коллектива и личности**

# ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Реализация конституционных прав и свобод акционеров в сфере информационной деятельности по защите персональных данных, банковской тайны и других норм финансовых регуляторов в части информационной безопасности кредитных организаций и мер контроля защищенности, содействие в обеспечении защищенности акционеров и клиентов, контрагентов, поставщиков продуктов и услуг, информирование о факторах рисков информационной безопасности и возможным мерам противодействия

Формирование и реализация требований соблюдения государственной тайны и, в соответствии с потребностями и возможностями, по режиму коммерческой тайны

Выявление угроз в информационной сфере и защита информации от несанкционированного доступа, выбор мер противодействия угрозам в информационной сфере и использования средств контроля (защитных мер) в технологических процессах, планирование, реализация и контроль использования защитных мер информационной безопасности, прогнозирование развития событий на основе мониторинга и менеджмента инцидентов информационной безопасности

Совершенствование и защита информационной инфраструктуры предприятия, содействие в обеспечении защищенности реализуемых технологических процессов и предоставляемых продуктов и услуг

Своевременное информирование руководства и акционеров по состоянию информационной безопасности, согласование с руководством планов и стратегий развития и совершенствования обеспечения информационной безопасности

Координация всех видов деятельности в целях обеспечения информационной безопасности, в том числе и через инициирование/согласование/принятие внутренних документов информационной безопасности, реализацию программ по осведомленности и обучению персонала

Содействие минимизации ущерба и быстрейшему восстановлению деятельности пострадавших в результате кризисных ситуаций в информационной сфере, участие в расследовании причин возникновения таких ситуаций и принятие соответствующих мер по их предотвращению

# СЕМЕЙСТВО СТАНДАРТОВ СМИБ в РОССИЙСКОЙ ФЕДЕРАЦИИ

## (Information technology – Security techniques – Информационные технологии. Методы и средства обеспечения безопасности)

ISO/IEC 27000:2009, Information security management systems – Overview and vocabulary (Система менеджмента информационной безопасности. Общий обзор и терминология);

ISO/IEC 27001:2005, Information security management systems – Requirements (Система менеджмента информационной безопасности. Требования);

ISO/IEC 27002:2005, Code of practice for information security management (Свод правил по управлению защитой информации);

ISO/IEC 27003, Information security management system implementation guidance (Руководство по реализации системы менеджмента информационной безопасности

ISO/IEC 27004, Information security management – Measurement (Менеджмент информационной безопасности. Измерения);

ISO/IEC 27005:2008, Information security risk management (Управление рисками информационной безопасности);

ISO/IEC 27006:2007, Requirements for bodies providing audit and certification of information security management systems (Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности);

ISO/IEC 27007, Guidelines for information security management systems auditing (Руководство для аудитора СМИБ);

ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002).

Международные стандарты, не имеющие общего названия:

ISO 27799:2008, Health informatics – Information security management in health. Using ISO/IEC 27002 (Информатика в здравоохранении. Менеджмент ИБ по стандарту ISO/IEC 27002).

*«Методы защиты ИТ» Совместного технического комитета ISO/IEC JTC 1 «Информационные технологии». ГОСТ Р ИСО/МЭК 27000*

# СТАНДАРТЫ, ЗАДАЮЩИЕ ТРЕБОВАНИЯ

## ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Область применения: определяет требования для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения документированной СМИБ в контексте общих деловых рисков организации, для реализации средств управления защитой, приспособленных к потребностям отдельных организаций или их подразделений. Этот международный стандарт применим ко всем типам организаций (например, коммерческие, государственные, некоммерческие).

Назначение: содержит нормативные требования для развёртывания и функционирования СМИБ, включая набор средств управления для управления и уменьшения рисков, относящихся к информационным активам, которые организация стремится защитить. Организации, использующие СМИБ, могут проводить её аудиторскую проверку и сертификацию соответствия.

## ГОСТ Р ИСО/МЭК 27006-2008 Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности

Область применения: задаёт требования и является руководством для органов, проводящих аудит и сертификацию СМИБ на соответствие ISO/IEC 27001, в дополнение к требованиям, содержащимся в ISO/IEC 17021. Предназначен, главным образом, для проведения аккредитации органов, проводящих сертификацию СМИБ на соответствие ISO/IEC 27001.

Назначение: дополняет стандарт ISO/IEC 17021 в части требований для аккредитации органов сертификации.

**К организационным основам обеспечения информационной безопасности следует отнести ЦЕЛИ, ЗАДАЧИ, МЕТОДЫ (СПОСОБЫ) И ПРИНЦИПЫ ОРГАНИЗАЦИИ:**

- **режима и охраны** с целью исключения возможности тайного проникновения на территорию и в помещения посторонних лиц;
- **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, воспитание и др.);
- **работы с документами** и документированной информацией (разработка документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение);
- **использования технических средств** сбора, обработки, накопления и хранения информации;
- **анализа** внутренних и внешних угроз информационной безопасности и выработке и руководства мерами по их нейтрализации;
- **систематического контроля** за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

# ОРГАНЫ, ОБЕСПЕЧИВАЮЩИЕ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

Комитет Государственной думы по безопасности

Совет Безопасности России

Федеральная служба по техническому и экспортному контролю (ФСТЭК России)

Федеральная служба безопасности Российской Федерации (ФСБ России)

Служба внешней разведки Российской Федерации (СВР России);

Министерство обороны Российской Федерации (Минобороны России)

Министерство внутренних дел Российской Федерации (МВД России)

Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)

# 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

# РОЛЬ СЛУЖБЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



Регламентирование оборота информации на предприятии безотносительно технологий, с учетом требований регуляторов в области той информации, которая защищается законом

Отслеживание юридического фона бизнеса, оценка информационных рисков и внесение изменения в регламенты использования доступа к информации на уровне регулирующих документов - «Положения о коммерческой тайне», трудовых соглашений, должностных инструкций и т.д.

Разработка ИТ-регламентов – политики доступа к приложениям, контентных маршрутов, жизненных циклов электронных документов и т.д. на основе утвержденных регламентов работы с информацией

Поддержание работоспособности информационной инфраструктуры компании – защита приложений и каналов движения информации, противодействие зловредному программному коду и др.

Обеспечение бизнеса современными и безопасными инструментами службы ИТ , функция которых заключается не только в обеспечении невозможности нарушить его работоспособность или получить несанкционированный доступ к данным, но и в готовности обеспечить быструю адаптацию к требованиям законодательства

Создание и контроль соблюдения политики безопасности предприятия, контроль информационных рисков: как традиционных ИТ (недоступности ресурсов, потери или утечки информации), так и регуляторных, и юридических рисков, связанных с функционированием информационной системы предприятия

# 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, включая установку 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 фактов нарушения безопасности;

изучение, 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

# НАПРАВЛЕНИЯ НЕЙТРАЛИЗАЦИИ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

| НА СТРУКТУРЫ | НА ПРОГРАММЫ | НА РЕСУРСЫ | НА СИСТЕМ. ОСНОВЫ |
|---|---|---|---|
| Формирование руководства и коллектива, жизнеспособных во всех сферах деятельности и упреждение угроз безопасности | | | |
| Активизация общественного контроля за действиями руководства | | | |
| Строгое научное обоснование принимаемых решений, меняющих основы политики предприятия | | | |
| Установление приоритета интересов в предприятия | | | |
| Мониторинг и прогнозирование угроз безопасности | | | |
| Неотвратимость наказания за нарушения должностных обязанностей | Оценка критичности угроз безопасности, принятие решений, мобилизация усилий и ресурсов | | Организационная, физическая, инженерно-техническая и др. виды защиты объектов |
| | Активизация научных исследований | Создание запасов ресурсов, развитие информационной инфраструктуры | |
| | Установление приоритетов национальных ценностей, культуры | | |
| Установление приоритета духовного над материальным как основы государственной политики | | Усиление всех форм контроля над ресурсами | Установление общественного контроля |
| Создание обстановки взаимопонимания и взаимной поддержки в коллективе | | | |
| Противодействие деструктивным проявлениям | | | |
| Строгая персональная ответственность | | | |

# СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ



## НОРМАТИВНО-ПРАВОВЫЕ СРЕДСТВА (ДОКУМЕНТЫ)

- УК РФ
- КоАП РФ
- ГК РФ
- Внутренние нормативные документы административной ответственности
- Внутренние нормативные документы материальной ответственности

## ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ СРЕДСТВА

- Средства видеонаблюдения
- Средства сигнализации и пожарной охраны
- Средства контроля и ограничения физического доступа
- Средства идентификации личности
- Средства обнаружения аппаратных средств
- Средства маскировки информационной деятельности

## СРЕДСТВА КАДРОВО-ВОСПИТАТЕЛЬНОЙ РАБОТЫ С ПЕРСОНАЛОМ И ЗАЩИТЫ ОТ ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

- Средства массовой информации
- Средства воспитания, мотивации и морального стимулирования
- Средства материального стимулирования
- Санкции дисциплинарной ответственности
- Средства кадровой работы
- Средства психологической регуляции и релаксации

## СРЕДСТВА ЗАЩИТЫ ОТ ПРОГРАММНО-АППАРАТНОГО ВОЗДЕЙСТВИЯ

- Средства предупреждения и обнаружения компьютерных атак
- Средства сокрытия и создания ложных элементов в сетях АСУ
- Средства разграничения доступа к информации
- Средства защиты информации в каналах передачи данных
- Антивирус-ные средства
- Криптографические средства защиты

# СОДЕРЖАНИЕ И СРЕДСТВА НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ

## *УДАЛЕННЫЙ ДОСТУП К ИНФОРМАЦИОННЫМСИСТЕМАМ*

- через каналы связи
- через аппаратные и программные средства абонентов
- через технические и программные средства других сетей

## *НЕПОСРЕДСТВЕННОЕ ПРОНИКНОВЕНИЕ В АППАРАТНО-ПРОГРАММНЫЕ СРЕДСТВА*

- АРМ должностных лиц
- средства контроля и управления
- технологические средства регламентных и ремонтных работ

## СРЕДСТВА

### Средства компьютерной разведки и дешифрования

- Средства исследования параметров
- Средства подключения
- Средства преодоления систем защиты ИТКС
- Средства добывания информации
- Средства подбора паролей, ключей и вскрытия алгоритмов
- Средства сбора, передачи, обработки и хранения

### Средства нарушения конфиденциальности и целостности информации

- Средства реализации компьютерных атак
- Средства применения компьютерных вирусов
- Закладки, вызывающие ошибки в общем и специальном программном обеспечении
- Средства реализации несанкционированного доступа к информации

### Средства нарушения доступности информации

- Программно-аппаратные закладные устройства
- Спам-программы
- Закладки, вызывающие повышенный износ оборудования
- Закладки, вызывающие имитацию сбоев и нарушения в технических средствах
- Средства подавления информационного обмена в телекоммуникационных сетях

# ТРЕБОВАНИЯ АДМИНИСТРАТИВНО-ПРАВОВОВЫХ СРЕДСТВ К НАРУШЕНИЯМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ (гл. 13 КоАП РФ)



- самовольное проектирование, строительство, изготовление, приобретение, установку или эксплуатацию радиоэлектронных средств и (или) высокочастотных устройств (ст. 13.3),
- нарушение правил проектирования, строительства, установки, регистрации или эксплуатации радиоэлектронных средств и (или) высокочастотных устройств (ст. 13.4),
- нарушение правил охраны линий или сооружений связи (ст. 13.5),
- использование н/с средств связи либо предоставление несертифицированных услуг связи (ст. 13.6),
- несоблюдение установленных правил и норм, регулирующих порядок проектирования, строительства и эксплуатации сетей и сооружений связи (ст. 13.7),
- изготовление, реализацию или эксплуатацию технических средств, не соответствующих стандартам или нормам, регулирующим допустимые уровни индустриальных радиопомех (ст. 13.8),
- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных) (ст. 13.11),
- нарушение правил защиты информации (ст. 13.12),
- незаконную деятельность в области защиты информации (ст. 13.13),
- разглашение информации с ограниченным доступом (ст. 13.14), з
- злоупотребление свободой массовой информации (ст. 13.15),
- воспрепятствование распространению продукции средства массовой информации (ст. 13.16),
- нарушение правил распространения обязательных сообщений (ст. 13.17),
- воспрепятствование уверенному приему радио- и телепрограмм (ст. 13.18),
- нарушение порядка представления статистической информации (ст. 13.19),
- нарушение правил хранения, комплектования, учета или использования архивных документов (13.20),
- нарушение порядка изготовления или распространения продукции СМИ (ст. 13.21),
- нарушение порядка объявления выходных данных (ст. 13.22),
- нарушение порядка представления обязательного экземпляра документов, письменных уведомлений, уставов и договоров (ст. 13.23),
- использование служебной информации на рынке ценных бумаг (ст. 15.21),
- разглашение сведений о мерах безопасности (ст. 17.13),
- непредставление сведений (информации) (ст. 19.7),
- незаконное использование специальных ТС, предназначенных для негласного получения информации (ст. 20.24) и др.

# 3. СОЦИАЛЬНО-ПРАВОВЫЕ НОРМЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: МОРАЛЬНЫЕ, ПРАВОВЫЕ, ПОЛИТИЧЕСКИЕ, ЭСТЕТИЧЕСКИЕ, КОРПОРАТИВНЫЕ

# СОЦИАЛЬНЫЕ НОРМАТИВНЫЕ СИСТЕМЫ

**ПРАВО** | **МОРАЛЬ** | **РЕЛИГИЯ** | **ОБЫЧАИ**

- **естественное**
- **либертарное**
- **формальное**

**легистское, позитивное**

Система социальных норм и ценностей, охраняемых государством:

- **законодательное**
- **прецедентное**

- **Гражданское право** – закрепляет отношения собственности
- **Трудовое право** – регулирует распределение труда
- **Конституционное право, административное право** – регламентирует организацию и деятельность государственного аппарата
- **Уголовное право** – определяет меры борьбы с посягательствами на общественные отношения
- **Процессуальное право** – регламентирует рассмотрение ответственности за противоправные действия
- **Семейное право** – воздействует на формы межличностных отношений
- **Международное право** – регламентирует межгосударственные отношения

# КЛАССИФИКАЦИЯ НОРМ

1. **По функции реализации правовых норм**: регулятивные, охранительные.

2. **По отношению к отрасли права**: конституционные, гражданские, уголовные, административные, трудовые и т.д.

3. **По методу правового регулирования**: императивные - носят властный характер и содержат предписания, обязательные для исполнения; диспозитивные - нормы, которые имеют автономный характер и предоставляют свободу в выборе модели поведения; рекомендательные – предусматривающие желательную модель поведения; поощрительные - предусматривающие меры поощрения за определенную социально полезную модель поведения.

4. **По характеру предписаний**: обязывающие - устанавливают обязанность совершать определенные положительные действия; запрещающие - запрещают совершать определенные, действия; управомочивающие - предоставляют участникам общественных отношений право совершать положительные действия в цепях удовлетворения своих интересов.

5. **По форме воздействия на общественные отношения**: материальные - непосредственно воздействуют на общественные отношения путем прямого закрепления определенного правила поведения в законодательстве (конституционные, уголовные, гражданские и т.д.); процессуальные - регулируют организационно-процедурный порядок реализации материальных норм права, относящиеся к сфере уголовно-процессуального, гражданского процессуального и арбитражного процессуального права.

6. **По субъекту правотворчества**: федеральные; региональные; местные; локальные.

7. **По степени определенности содержащихся в них предписаний:**

абсолютно определенные - с абсолютной точностью определяют условия их действия, права и обязанности участников отношений или меры юридической ответственности за их нарушение. Конкретизация предписания, предусмотренного нормой права, не допускается;

относительно определенные - не содержат достаточно полных сведений об условиях их действия, правах и обязанностях участников общественных отношений или мерах юридической ответственности и предоставляют правоприменительным органам возможность решать дело с учетом конкретных обстоятельств;

альтернативные - предусматривают несколько вариантов, условий их действия, поведения сторон или мер, санкций за их нарушение.

# КЛАССИФИКАЦИЯ НОРМ

8. **По способу изложения в статье нормативно-правового акта:**

прямые - нормы, структурные элементы которых излагаются в одной статье нормативно-правового акта;

отсылочные - нормы, структурные элементы которых излагаются в нескольких статьях одного и того же нормативно-правового акта;

бланкетные – нормы, структурные элементы которых излагаются в статьях различных нормативно-правовых актов.

9. **По специальному назначению**:

декларативные (нормы-принципы) – нормы, в которых сформулированы общие или отраслевые правовые принципы и задачи данной совокупности юридических норм (принципы уголовного процесса, задачи гражданского законодательства и т. п.);

дефинитивные (нормы-определения) – нормы, в которых содержатся научно сформулированные определения юридических понятий и категорий (например понятие преступления, гражданской правоспособности и дееспособности, сделки, должностного лица);

общие – нормы, содержащиеся в общей части отрасли права и распространяющие свое действие на всю особенную часть этой отрасли, либо содержащие общие положения для всех отраслей права;

специальные – нормы, регулирующие определенный вид общественных отношений, конкретизируя общие положения);

коллизионные – нормы, направленные на устранение противоречий между другими правовыми нормами.

10. **По кругу лиц:**

общие - распространяются на всех лиц, проживающих на данной территории; специальные нормы действуют только в отношении определенной категории лиц (учителей, врачей, военнослужащих, пенсионеров).

11. **По времени действия** – временные, постоянные.

12. **По юридической силе** и т.д.

# ПРИЗНАКИ ПРАВА



- **НОРМАТИВНОСТЬ** – устанавливаются правила поведения общего характера
- **ОБЩЕОБЯЗАТЕЛЬНОСТЬ** – действие права распространяется на всех, либо на большой круг субъектов
- **ГАРАНТИРОВАННОСТЬ** государством – нормы права подкреплены мерами государственного принуждения
- **ИНТЕЛЛЕКТУАЛЬНО-ВОЛЕВОЙ ХАРАКТЕР** – право выражает волю и сознание людей
- **ФОРМАЛЬНАЯ ОПРЕДЕЛЁННОСТЬ** - нормы права выражены в официальной форме
- **СИСТЕМНОСТЬ** – право как внутренне согласованный, упорядоченный организм

# СТРУКТУРА ПРАВОВОЙ НОРМЫ

**Структура правовой нормы – это способ организации содержания правила поведения, находящегося в этой норме.**

**Юридическая структура** – строение нормы права, которое состоит из трех взаимосвязанных элементов – гипотезы, диспозиции, санкции.

**Гипотеза** отвечает, когда, при каких обстоятельствах действует правило поведения

**Диспозиция** дает ответ, что, собственно, требует норма права, что надо делать или, наоборот, нельзя делать.

**Санкция** отвечает, что может произойти с адресатом нормы, если он станет нарушать предписание нормы.

Только в наличии и единстве все эти три элемента составляют норму права. Отсутствие какого-либо из элементов - это признак несовершенства нормы права.

**Логическая структура** – охватывает в логических понятиях и их связках юридическую структуру формулой «если - то - иначе»:

**«если»** -- условие действия нормы права,

**«то»** - само правило поведения,

**«иначе»** - неблагоприятные последствия, которые возникают у правонарушителя.

Иная структура строится на выделении **модулей:**

адресату разрешено, запрещено,

адресат правомочен,

адресат обязан,

безразлично.

**Социологическая структура –**

определяется в социологических понятиях:

**смысл,**

**цель,**

**назначение нормы.**

Социологическая структура раскрывается при толковании нормы права и в процессе ее реализации.

**ИНФОРМАЦИОННО-ПРАВОВЫЕ НОРМЫ** регулируют обособленные группы общественных отношений применительно к особенностям информационной сферы и содержат права и обязанности субъектов – участников правоотношений, исполнение которых обеспечивается принудительной силой государства, которые устанавливаются государством в определенном порядке и форме, вводятся в действие в установленный законодателем срок.

**Отличие информационно-правовых норм от норм других отраслей права:**

регулируют отношения, возникающие в информационной сфере в связи с реализацией информационных прав и свобод и осуществлением информационных процессов при обращении информации.

**Содержание информационно-правовой нормы**: гипотезы, диспозиции и санкции.

Гипотеза определяет условия, обстоятельства, при которых могут возникать информационные правоотношения, и указывает на круг субъектов – участников этих правоотношений.

Основу информационно-правовой нормы составляет диспозиция, которая содержит предписание о том, как должны поступать субъекты правоотношений, устанавливаются их права и обязанности.

Защита прав и обеспечение исполнения установленных правил производятся с помощью санкций.

http://www.modernlib.ru/books/yakubenko_nina/shpargalka_po_informacionnomu_pravu/read/

# КЛАССИФИКАЦИЯ ИНФОРМАЦИОННО-ПРАВОВЫХ НОРМ

1. **В зависимости от вида и формы представления информации, субъектов** – императивные и диспозитивные.
2. **В зависимости от их содержания** – материальные и процессуальные.

   Материальные – устанавливают структуру элементов и частей информационной сферы, правовой статус субъектов в информационной сфере в части их обязанностей и ответственности за организацию и обеспечение процессов обращения информации, в том числе за формирование информационных ресурсов и предоставление пользования ими в соответствии с действующим законодательством.

   Процессуальные – регламентируют процедуру (порядок, правила) реализации обязанностей и прав, установленных информационными нормами в рамках регулируемых информационных отношений.
3. **В зависимости от способов их воздействия на субъектов правоотношений** – диспозитивные и императивные.
4. **По сфере применения (по масштабу действия):**
   - нормы федерального уровня и действия;
   - нормы субъектов РФ;
   - нормы органов местного самоуправления.
5. **По объему регулирования:**
   - общего действия, распространяющие действие на все сферы и отрасли правового регулирования, регламентирующие важнейшие стороны информационной деятельности;
   - межотраслевые, регулирующие информационные отношения между группами государственных органов по обеспечению информационных процессов;
   - отраслевые, действующие в пределах сферы ведения конкретного органа государственной власти;
   - на уровне органа местного самоуправления, действующие в пределах территорий.

# МОРАЛЬ И МОРАЛЬНЫЕ НОРМЫ В ОБЕСПЕЧЕНИИ СОЦИАЛЬНЫХ ПРАВООТНОШЕНИЙ

**МОРА́ЛЬ** (лат. moralis, касающийся нравов) – принятая в обществе система норм, идеалов, принципов и ее выражение в реальной жизни людей, один из основных способов нормативной регуляции их действий в обществе, форма общественного сознания и вид общественных отношений.

## Особенности проявлений моральных норм:

- охватывает нравственные взгляды и чувства, жизненные ориентации и принципы, цели и мотивы поступков и отношений, проводя границу между добром и злом, справедливостью и несправедливостью, милосердием и жестокостью;
- проявляется в обществе как совокупность моральной деятельности, нравственных отношений и морального сознания:
- по содержанию часто совпадает с правовыми нормами или конфликтует с ними;
- является проявлением коллективной воли, которая через систему требований и оценок пытается согласовать интересы индивидов друг другом и с интересами общества в целом;
- в отличие от других проявлений духовной жизни общества (наука, искусство, религия) не является сферой организованной деятельности;
- большинство моральных требований апеллирует не к внешней целесообразности, а к моральному долгу, т. е. имеет форму императива – прямого и безусловного повеления (строгое выполнение моральных правил не всегда приводит к жизненному успеху).
- формализованная мораль может становиться правом: религиозные нормы – одновременно моральный и правовой закон многих культур. Нравственная оправданность норм права для создания правового государства настолько же важна как и их единство.
- в праве отражено понятие «морального вреда», однако мораль остается делом совести и служит критерием для исторических правовых реформ;

# ФУНКЦИИ МОРАЛИ

## РЕГУЛЯТИВНАЯ

Мораль выступает как способ регулирования и саморегулирования поведения;

не нуждается в организационном подкреплении;

осуществляется через усвоение соответствующих норм и принципов поведения;

действенность моральных требований определяется внутренним убеждением отдельного человека,

общественная мораль оказывает влияние на нравственность человека и становится неотъемлемой частью его духовного мира, механизмом мотивации его поведения

## ОЦЕНОЧНАЯ

Мораль рассматривает явления и процессы с точки зрения их гуманистического потенциала – в какой мере они способствуют объединению людей и их развитию;

классифицирует все как положительное или отрицательное, добро или зло («справедливость» и «несправедливость», «честь» и «бесчестье»);

выражает форму нравственной оценки (похвалу, согласие, порицание, критику), ставит человека в активное, деятельное отношение к ней

## ВОСПИТАТЕЛЬНАЯ

Мораль выполняет задачу формирования личности;

концентрирует нравственный опыт человечества и делает его достоянием каждого нового поколения;

придает всем видам воспитания правильную социальную ориентацию через нравственные идеалы и цели, обеспечивает гармоничное сочетание личных и общественных интересов;

рассматривает общественные связи как связи людей, каждый их которых имеет самоценное значение;

ориентирует на такие действия, которые, выражая волю данной личности, не попирают в то же время воли других людей

## КОНТРОЛИРУЮЩАЯ

Мораль служит контролю над выполнением норм путем общественного осуждения и/или совести самого человека

## ИНТЕГРИРУЮЩАЯ

Мораль включена во все сферы жизни, обеспечивает поддержание единства человечества и целостности духовного мира человека

# ОТЛИЧИЕ НОРМ МОРАЛИ ОТ ПРАВА И ОБЫЧАЕВ

**Обычаи – исторически сложившийся стереотип массового поведения в конкретной ситуации.**

Обычаи отличаются от моральных норм:

следование обычаю предполагает беспрекословное и буквальное подчинение его требованиям, моральные нормы предполагают осмысленный и свободный выбор человека;

обычаи различны для разных народов, эпох, социальных групп, тогда как мораль универсальна - она задает общие нормы для всего человечества;

исполнение обычаев нередко основано на привычке и страхе перед неодобрением окружающих, а мораль основывается на чувстве долга и поддерживается чувством стыда и угрызениями совести

**Нормы права** :

право санкционируется государством, а мораль основана на личном убеждении и общественном мнении;

правовые нормы имеют обязательный характер, тогда как моральные нормы не обязательны, а только желательны для исполнения;

правовые нормы документально зафиксированы в законах, конституции и т.д., а моральные нормы могут быть неписаными и устно передаваться из поколения в поколение;

за невыполнение правовых норм следует административная или уголовная ответственность, а моральные санкции выражаются в общественном неодобрении и муках совести.

- право вырабатывается государством, мораль – обществом;
- мораль может вступать в противоречие с правом;
- право закреплено в государственных актах, мораль – нет;
- за нарушение нормы права предполагаются санкции государства, за нарушение нормы морали – общественное осуждение и в некоторых случаях санкции государства

# ПОЛИТИЧЕСКИЕ НОРМЫ



**НОРМА ПОЛИТИЧЕСКАЯ** (от лат. norma) –

выработанная в процессе политической жизни и закрепленная в законах, важнейших политических и иных общественно значимых документах, мера регуляции и реализации тех или иных политических действий;

установленное или санкционированное политическими институтами и общественными организациями правило, регулирующее политические процессы, поведение и деятельность субъектов политики;

сложившийся в политической жизни порядок реализации политических программных установок, принципов и целей государства, партий, общественно-политических движений, социальных и этнических общностей и групп, отдельных лиц.

**Политическая норма:**

воплощает или отражает важную политическую традицию, ее смысл;

содержит в себе правило, модель должного поведения, деятельности субъекта политики;

органично включена в соответствующую политическую систему или организацию конкретного общества, вне которых, если нет согласования с другими системами и организациями, она может и не действовать;

выражает правила деятельности и функционирования как самих субъектов политики, так и отношений между ними;

вырабатываются, гарантируются и используется не только государством, но и всей политической системой общества, всеми заинтересованными политическими институтами, социальными общностями и группами.

Политические нормы часто выступают в виде общеполитических деклараций и заявлений, могут предшествовать принятию соответствующих законов и влиять на процесс законотворчества

# ЭСТЕТИЧЕСКИЕ НОРМЫ

**ЭСТЕТИЧЕСКИЕ НОРМЫ – выражают правила (критерии, оценки) красоты и прекрасного в их противопоставлении безобразному**.

**В этических явлениях присутствуют:**

1) личностный момент (автономия индивида и самосознательная мотивация им правил морального поведения и моральных оценок) – относится к характеристике нравственности;

2) объективный, внеличностный момент (сложившиеся в данной культуре, социальной группе, общности нравственные воззрения, ценности, нравы, формы и нормы человеческих отношений) относится к характеристике морали

Нравственные нормы выступают в качестве внешних регуляторов поведения индивида: там, где индивид принял, усвоил и превратил в свою внутреннюю установку коллективные нравственные представления, ценности, нормы и руководствуется ими в своем поведении, имеет место сочетание и согласованное действие обоих регуляторов – морального и нравственного.

# КОРПОРАТИВНЫЕ НОРМЫ

**КОРПОРАТИВНЫЕ НОРМЫ – групповые нормы внутриорганизационного характера о порядке формирования и полномочиях руководящих органов, внесения изменений и дополнений в устав, о правах и обязанностях членов и участников, принимаемые общественными объединениями и корпорациями и регулирующие отношения между их членами или участниками, которые закреплены в уставе и иных документах общественного объединения (политической партии, профсоюза, органа общественной самодеятельности и др.)**

Корпоративные нормы не имеют всеобщности и общезначимости права и общеобязательности закона, это лишь форма и способ использования и реализации конституционных прав граждан на объединение в соответствии со всеобщими требованиями права и правовой формы общественных отношений (соблюдение принципа правового равенства, добровольности, взаимосвязи прав и обязанностей и т.д.).

«…Члены и участники общественных объединений — физические и юридические лица — имеют равные права и несут равные обязанности. Нарушение общественным объединением этих и целого ряда иных требований закона может повлечь за собой (по решению суда) приостановление его деятельности и даже его ликвидацию».

*Федеральный закон РФ «Об общественных объединениях»*
*(принят Государственной Думой 14 апреля 1995 г.).*

# 4. ТЕХНИКО-ПРАВОВЫЕ НОРМЫ В ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ОСНОВЫ ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ

# ТЕХНИКО-ПРАВОВЫЕ НОРМЫ

**ТЕХНИКО-ПРАВОВЫЕ НОРМЫ – технические нормы, получившие закрепление в правовых актах и таким образом приобретшие юридическую силу в материально-производственной и управленческой сфере**.

*Большой юридический словарь. Академик.ру. 2010.*

**Особенности понятия**:

- Юридические нормы с техническим содержанием в юридической науке получили название «технико-юридические» (А.Ф. Черданцев), в отдельных источниках - «юридико-технические» (А.Б. Венгеров).
- Технико-юридические нормы появляются тогда, когда техническая деятельность и ее результаты перестают быть исключительно интересом частных лиц.
- Структура технико-юридических норм характеризуется особенными системными связями элементов. Если их гипотеза и диспозиция всегда содержатся в одном источнике, то санкция, как правило, расположена в ином, распространяется на большое число норм и имеет отсылочный характер.
- Содержание диспозиции технико-юридической нормы выражается в нормативно-правовом акте с помощью технического предписания. В отличие от иных правовых предписаний, выраженных предложением, для выражения технических предписаний могут использоваться математические знаки, формулы, таблицы, графические изображения. Применение тех или иных характерных для науки и техники способов изложения знания (рисунки, чертежи, схемы, таблицы) не является обязательным признаком технического предписания.

# ЗНАЧЕНИЕ, ФУНКЦИИ И КЛАССИФИКАЦИЯ ТЕХНИКО-ПРАВОВЫХ НОРМ

**Инструментальное значение технико-правовых норм** применяется по отношению к потребностям в обеспечении безопасности жизни или здоровья граждан, имущества, окружающей среды, жизни или здоровья животных и растений и др. законных интересов лиц, не являющихся субъектами такой деятельности при осуществлении технической деятельности.

**Собственная ценность технико-правовых норм** – благодаря приданию общеобязательного либо рекомендательного характера техническим действиям, направленным на удовлетворение признаваемых и защищаемых государством потребностей субъектов, способствуют максимальному удовлетворению этих потребностей.

**Функции технико-юридических норм**: общеправовые (регулятивная и охранительная); соответствующие сферам общественной жизни (экономическая, научно-техническая, социальная и экологическая); общенормативные (информационная, государственной ориентации субъектов общественных отношений, государственной оценки разнообразных вариантов поведения субъектов права, мотивационная); специальные (конкретизационная, определительно-ограничительная и восполнительная).

**Классификация технико-юридических норм:** 1) от цели (на защиту человека и результатов его труда, а также окружающей природной среды от воздействия различных факторов, либо на удовлетворение экономических интересов); 2) по функциональной роли в механизме правового регулирования (общие или специальные); 3) от метода правового регулирования, нормативную основу которого они составляют (императивные, диспозитивные и рекомендательные); 4) по форме выражения предписания (обязывающие, запрещающие и управомочивающие); 5) от способа изложения предписания (грамматические, графические, нормы-таблицы и нормы-формулы); 6) по юридической силе (нормы международных договоров; нормы федеральных законов; нормы указов Президента; нормы нормативно-правовых актов Правительства РФ; нормы подзаконных нормативно-правовых актов ФОИВ; нормы нормативно-правовых актов органов исполнительной власти субъектов федерации; нормы нормативно-правовых актов органов местного самоуправления; нормы локальных источников); 7) по сфере действия (общего действия и ограниченного действия).

# СУЩНОСТЬ ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ

**ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ – правовое регулирование отношений в области установления, применения и исполнения обязательных требований к продукции или к связанным с ними процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, а также в области установления и применения на добровольной основе этих требований, выполнению работ или оказанию услуг и правовое регулирование отношений в области оценки соответствия.**

Совершенствование системы технического регулирования в целях повышения качества и конкурентоспособности предприятий осуществлялось и продолжается в настоящее время на основе:

ФЗ «О техническом регулировании» №184-ФЗ от 15 декабря 2002 г., вступившего в силу с 1 июля 2003 г.;

«Программы разработки технических регламентов», утвержденной расп. Правительства РФ от 6 ноября 2004 г. №1421-р;

«Концепции развития национальной системы стандартизации» от 28 февраля 2006 г. № 266-р;

«Программы разработки национальных стандартов».

Деятельность по стандартизации носит рыночный характер, т.е. подчиняется основным рыночным законам и выходит на рынок со своим товаром – национальным стандартом.

Государство при этом является одним из участников рынка, который может при передаче функций по организации национальной системы стандартизации национальному органу оговорить свои интересы через соответствующее соглашение с ним.

# ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ

**ТЕХНИЧЕСКИЙ РЕГЛАМЕНТ – документ, принятый международным договором, ратифицированным в РФ, или заключенным межправительственным соглашением или федеральным законом, или указом Президента РФ, или постановлением Правительства РФ, устанавливает обязательные для применения и исполнения требования к объектам технического регулирования (продукции, в том числе зданиям, строениям и сооружениям или к связанным с требованиями к продукции процессам проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации).**

ФОИВ вправе издавать в сфере технического регулирования акты только рекомендательного характера, за исключением случаев, установленных для оборонных отраслей промышленности, где подобные акты носят обязательный характер.

**Технические регламенты принимаются в целях:**

защиты жизни или здоровья граждан, имущества;

охраны окружающей среды, жизни или здоровья животных и растений;

предупреждения действий, вводящих в заблуждение приобретателей;

обеспечения энергетической эффективности.

Правительством РФ до дня вступления в силу технического регламента утверждается перечень национальных стандартов, содержащих правила и методы исследований (испытаний) и измерений.

Экспертиза проектов технических регламентов осуществляется экспертными комиссиями по техническому регулированию, в состав которых на паритетных началах включаются представители ФОИВ, научных организаций, саморегулируемых организаций, общественных объединений предпринимателей и потребителей.

# ЦЕЛИ И ПРИНЦИПЫ СТАНДАРТИЗАЦИИ

**Стандартизация осуществляется в целях:**

повышения уровня безопасности жизни и здоровья граждан, имущества имущества, объектов с учетом риска возникновения чрезвычайных ситуаций природного и техноген-ного характера, повышения уровня экологической безопасности, безопасности жизни и здоровья животных и растений;

обеспечения конкурентоспособности и качества продукции (работ, услуг), единства измерений, рационального использования ресурсов, взаимозаменяемости технических средств, технической и информационной совместимости, сопоставимости результатов исследований (испытаний), технических и экономико-статистических данных, проведения анализа характеристик продукции, исполнения государственных заказов, добровольного подтверждения соответствия продукции (работ, услуг);

содействия соблюдению требований технических регламентов;

создания систем классификации и кодирования технико-экономической и социальной информации, систем каталогизации  и обеспечения качества продукции (работ, услуг), систем поиска и передачи данных, содействия проведению работ по унификации.

**Стандартизация осуществляется в соответствии со следующими принципами:**

добровольного применения стандартов;

максимального учета законных интересов заинтересованных лиц;

применения международного стандарта как основы разработки национального стандарта, за исключением случаев, если такое применение признано невозможным вследствие несоответствия требований международных стандартов климатическим и географическим особенностям РФ, техническим и (или) технологическим особенностям,

недопустимости создания препятствий производству и обращению продукции, выполнению работ и оказанию услуг в большей степени, чем это минимально необходимо для выполнения целей, определенных в настоящем Федеральном законе;

недопустимости установления таких стандартов, которые противоречат техническим регламентам;

обеспечения условий для единообразного применения стандартов.

# ЗАДАЧИ НАЦИОНАЛЬНОГО ОРГАНА ПО СТАНДАРТИЗАЦИИ



## Национальный орган Российской Федерации по стандартизации:

утверждает национальные стандарты;

принимает программу разработки национальных стандартов;

организует экспертизу проектов национальных стандартов;

обеспечивает соответствие системы стандартизации интересам национальной экономики, состоянию материально-технической базы и научно-техническому прогрессу;

осуществляет учет национальных стандартов, правил стандартизации, норм и рекомендаций в этой области и обеспечивает их доступность заинтересованным лицам;

создает технические комитеты по стандартизации, утверждает положение о них и координирует их деятельность;

организует официальное опубликование и распространение национальных стандартов, общероссийских классификаторов технико-экономической и социальной информации, правил стандартизации, норм и рекомендаций в области стандартизации в печатном издании и в информационной системе общего пользования;

участвует в соответствии с уставами международных организаций в разработке международных стандартов и обеспечивает учет интересов РФ при их принятии;

утверждает изображение знака соответствия национальным стандартам;

представляет РФ в международных организациях, осуществляющих деятельность в области стандартизации;

обеспечивает в информационной системе общего пользования доступ на безвозмездной основе к национальным стандартам и к другим документам;

предоставляет информацию и документы в области стандартизации в соответствии с обязательствами РФ, вытекающими из международных договоров.

# ОГРАНИЧЕНИЯ СФЕРЫ ТЕХНИЧЕСКОГО РЕГУЛИРОВАНИЯ

**Стандарты коммерческих, общественных, научных организаций, саморегулируемых организаций, объединений юридических лиц** могут разрабатываться и утверждаться ими самостоятельно исходя из необходимости применения этих стандартов для целей, определенных данным законом, для совершенствования производства и обеспечения качества продукции, выполнения работ, оказания услуг, а также для распространения и использования полученных в различных областях знаний результатов исследований (испытаний), измерений и разработок.

**Ограничения сферы технического регулирования (в рамках системы технических регламентов):**

техническими регламентами регулируются не любые виды безопасности, а лишь связанные с возможностью непосредственного причинения вреда либо самой продукцией, либо в процессе ее производства;

техническими регламентами регулируются лишь те виды деятельности, к субъектам которых государством не могут быть предъявлены обязательные требования иначе, чем посредством технического законодательства;

техническими регламентами регулируется исключительно сфера технической безопасности, но не безопасности вообще;

техническими регламентами покрывается преимущественно сфера регулирования государством разного рода видов деятельности (ограничения прав граждан); но не сфера выполнения государственными органами функций по обеспечению безопасности граждан, национальной безопасности и т.п.