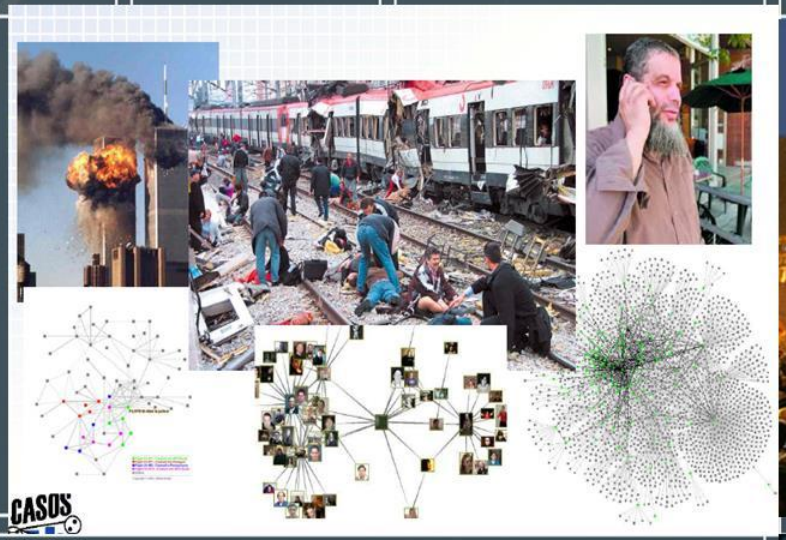
# НАЦИОНАЛЬНАЯ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(вводная лекция)

Российский технологический университет -МИРЭА
(Институт комплексной безопасности и специального приборостроения)





Григорьев В.Р. (РТУ - ИКБиСП)
зав. кафедрой «Информационное противоборство», зам. директора ИКБСП
к.т.н., доцент, член-корр. РАЕН

# ЭПИГРАФЫ

*“...Тот, кто умеет вести войну, покоряет чужую армию, не сражаясь, берет чужие крепости, не осаждая; сокрушает чужое государство, не держа свое войско долго”* **(гл. III, п. 3).**
*“Поэтому сто раз сразиться и сто раз победить — это не лучшее из лучшего; лучшее из лучшего — покорить чужую армию не сражаясь”* **(гл. III, п. 1).**

**Сунь Цзы** (孫子) — китайский стратег и мыслитель, предположительно, живший в VI или, по другим источникам, в IV веке до н. э. Автор знаменитого трактата о военной стратегии «Искусство войны»

*"...всему есть мать безконфузство, ибо сие едино войско возвышает и низвергает"*

**ПЕТР I ВЕЛИКИЙ (1672-1725), российский царь с 1682 (правил с 1689), первый российский император (с 1721),**

*"Слухи преувеличивают действие",-* **писала Екатерина II Потемкину, советуя тревожить турок пугающими слухами в дополнение к боевым действиям.**

# ЭПИГРАФЫ

- *«Мятежевойна - это война всех против всех, причем врагом бывает и соплеменник, а союзником - и иноплеменный. У каждого человека должен быть колчан с психологическими стрелами и психологический щит».*
- *«В мятежевойне психология мятежных масс отодвигает на второй план оружие войска и его психологию и становится решающим фактором победы или поражения..»*
- *«В прежних войнах важным почиталось завоевание территории. Впредь важнейшим будет почитаться завоевание душ во враждующем государстве.»*
- *«Война на нервах в эпоху, когда народы неврастеничны, требует от стратегов весьма продуманного обращения с главным фактором войны - с психикой воюющего народа...»*
- *"Народная масса мало восприимчива к логике ума, но легко поддается логике чувств".*

**Генерального штаба полковник профессор Евгений Эдуардович Месснер (1891-1974), один из крупнейших представителей военной мысли Русского Зарубежья.**
**Автор работ "Мятеж - имя третьей всемирной", "Современные офицеры", "Всемирная мятежевойна", изданных в 1960-1971 гг. в Буэнос-Айресе и Нью-Йорке.**

*«Идет борьба за умы и души - лишь затем за жизни и территории».*

*«Бои - лишь эпизоды, похожие на взрыв ракеты. Умелая организация мобилизует универсальные духовные силы».*

*генерал А.Е.Снесарёв (1.12.1865 — 4.12.1937)*

*Русский военачальник и учёный-востоковед. Герой Труда (1928). В Советской Армии с 1918. Окончил матем. фак. Моск. ун-та (1888), пех. уч-ще (1890) и Академию Генштаба (1899); владел 14 языками. С 1888 на воен. службе в Туркестане, занимался изучением и военно-геогр. описанием Ср. Востока. Совершил поездки по Индии, Афганистану, Тибету и Кашгарии. С 1904 в Генштабе, одновременно преподавал воен. географию в воен. училищах. С 1910 нач-к штаба казачьей дивизии. В 1-ю мировую войну командовал полком, бригадой и дивизией, ген.-лейтенант (1917). Георгиевский кавалер.*

# ЭПИГРАФЫ

- "Холодная война на самом деле была Третьей мировой войной, а сейчас США ввязались в Четвертую мировую войну, которая продлится много лет", - признал бывший директор ЦРУ США Джеймс Вулси, выступая в Калифорнийском университете 3 апреля 2003 года.

- "С целью управления всем миром, Соединенные Штаты вступили в войну, до конца которой мы не доживем", - вторил ему вице-президент США Ричард Чейни.

# Медаль «За победу в холодной войне»

# 2. Информационная безопасность и ее место в системе национальной безопасности РФ

# Конституция Российской Федерации

**Конституция РФ является основным источником права в области обеспечения информационной безопасности в России.**

Согласно Конституции РФ:

- каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (статья 23);
- сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются (статья 24);
- каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом (статья 29);
- каждый имеет право на достоверную информацию о состоянии окружающей среды (статья 42).

- **Информационная безопасность Российской Федерации** - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.
- **Информация** - сведения (сообщения, данные) независимо от формы их представления.

Основным *содержанием* обеспечения ИБ должна являться работа по реализации комплекса мер, направленных на предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации:

- **прогнозирование** (выявление) угроз ИБ;
- **защита** информационных объектов;
- комплексное **противодействие** угрозам ИБ;
- целенаправленное **воздействие** на объекты, представляющие угрозу ИБ.

# Роль и место информационной безопасности в обеспечении национальной безопасности России



# Место ИБ в системе национальной безопасности РФ

**ИБ – составляющая национальной безопасности РФ**

Состояние защищенности жизненно важных интересов граждан в сфере ИБ

**Стратегия национальной безопасности до 2020 года (Указ ПР. 31 декабря 2015 года № 683)**

Военная доктрина Российской Федерации (25 декабря 2014 г.)

**Национальные интересы России в информационной сфере**

- Соблюдение конституционных прав и свобод граждан в информационной деятельности
- Безопасность информационных ресурсов РФ
- Развитие современных информационных и телекоммуникационных технологий и средств

**Цели и задачи ИБ**

- Совершенствование информационной структуры, ускорение развития новых информационных технологий и их распространение
- Установление баланса между потребностью информации и существующими ограничениями ее распространения
- Унификация средств сбора, обработки и анализа информации с учетом вхождения РФ в глобальную информационную инфраструктуру
- Защита государственных информационных ресурсов от утечки важной политической, экономической, технической и военной информации
- Расширение международного сотрудничества в области развития информационных ресурсов
- Развитие отечественной индустрии информационных и телекоммуникационных средств
- Разработка нормативной правовой базы, координация сил и органов обеспечения ИБ

**Доктрина информационной безопасности РФ (Указ Пр РФ от 5 декабря 2016 № Пр-646)**

Основные направления государственной политики в области обеспечения безопасности автоматизированных систем производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации (3 февраля 2012 № 803)

Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (12 декабря 2014и№ К 1274)

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (24 июля 2013 г., № Пр-1753)

Конвенция об обеспечении международной информационной безопасности (концепция)

# «Доктрина информационной безопасности Российской Федерации»

## (Указ Президента Российской Федерации № 646 от 05.12.2016 г. )

1. Настоящая Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.
2. В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.
3. Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.
4. Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

# Составляющие информационной безопасности, согласно Доктрине информационной безопасности (Указ Президента Российской Федерации № 646 от 05.12.2016 г. )



Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности. При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

# В Ы В О Д

## «Доктрина информационной безопасности Российской Федерации» (Указ Президента Российской Федерации № 646 от 05.12.2016 г. )

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательных решений таких з а д а ч, как:

1. Разработка основных направлений в области обеспечения информационной безопасности, а также мероприятий и механизмов, связанных с реализацией этой политики

2. Развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области

3. Разработка федеральных целевых программ обеспечения информационной безопасности

4. Разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации

5. Совершенствование нормативной базы обеспечения информационной безопасности

6. Установление ответственности должностных лиц органов государственной власти субъектов РФ, органов местного самоуправления, юридических лиц за соблюдением требований информационной безопасности

7. Развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны

# Выписка из Доктрины информационной безопасности Российской Федерации

## утвержденной Указом Президента РФ № 646 от 5 декабря 2016 года

•12. Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

•13. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

• 21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

•23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

# УКАЗ ПРЕЗИДЕНТА УКРАИНЫ № 47/2017
## О решении Совета национальной безопасности и обороны Украины от 29 декабря 2016 года «О Доктрине информационной безопасности Украины»

- **2. Цель и принципы Доктрины**
  - Целью Доктрины является уточнение принципов формирования и реализации государственной информационной политики, прежде всего по противодействию разрушительному информационному воздействию Российской Федерации в условиях развязанной ею гибридной войны.
- **3. Национальные интересы Украины в информационной сфере**
  - 2) жизненно важные интересы общества и государства:
  - защита украинского общества от агрессивного воздействия деструктивной пропаганды, прежде всего со стороны Российской Федерации;
  - защита украинского общества от агрессивного информационного воздействия Российской Федерации, направленного на пропаганду войны, разжигание национальной и религиозной вражды, изменение конституционного строя насильственным путем или нарушение суверенитета и территориальной целостности Украины;
- **5. Приоритеты государственной политики в информационной сфере**
  - выявление и привлечение к ответственности в соответствии с законодательством субъектов украинского информационного пространства, которые созданы и/или используются государством-агрессором для ведения информационной войны против Украины, и пресечения их подрывной деятельности;
  - невозможность свободного оборота информационной продукции (печатной и электронной), прежде всего происхождением с территории государства-агрессора, содержащей пропаганду войны, национальной и религиозной вражды, изменения конституционного строя насильственным путем или нарушение суверенитета и территориальной целостности Украины, провоцирует массовые беспорядки;
- **6. Механизм реализации Доктрины**
  - Министерство культуры Украины, Государственное агентство Украины по вопросам кино, Национальный совет Украины по вопросам телевидения и радиовещания, Государственный комитет телевидения и радиовещания Украины согласно компетенции должны участвовать в обеспечении защиты украинского информационного пространства от пропагандистской аудиовизуальной и печатной продукции государства-агрессора; разрабатывать приоритеты и стимулы развития украинского кино, телевизионного контента, книгопечатания, в частности освещение героического сопротивления Украинского народа российской агрессии.

# Организационная структура системы обеспечения информационной безопасности Российской Федерации

# Нормативно-правовая база обеспечения информационной безопасности в РФ

# Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ

Предметом регулирования данного Закона являются общественные отношения, возникающие в трех взаимосвязанных направлениях:

- формирование и использование информационных ресурсов;
- создание и использование информационных технологий и средств их обеспечения;
- защита информации, прав субъектов, участвующих в информационных процессах и информатизации.

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

В Законе также отражены вопросы, связанные с порядком обращения с персональными данными, сертификацией информационных систем, технологий, средств их обеспечения и лицензированием деятельности по формированию и использованию информационных ресурсов.

# Федеральный закон "О безопасности" от 28.12.2010 № 390-ФЗ

ФЗ-390 регулирует принципы обеспечения безопасности:

- личной;
- общественной;
- государственной;
- экологической;
- национальной.

Федеральным законом №390 устанавливаются полномочия и функции государственных органов в сфере сохранности.

# Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ

**Основными принципами обеспечения безопасности** являются:

1. соблюдение и защита прав и свобод человека и гражданина;
2. законность;
3. системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;
4. приоритет предупредительных мер в целях обеспечения безопасности;
5. взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

# Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»

**Государственная тайна** – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

**Средства защиты информации** – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Устанавливаются три степени секретности сведений, составляющих государственную тайну, и соответствующие этим степеням грифы секретности для носителей указанных сведений: "**особой важности**", "**совершенно секретно**" и "**секретно**".

Должностные лица и граждане, виновные в нарушении законодательства Российской Федерации о государственной тайне, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством.

# Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) «О государственной тайне»

**Государственную тайну** составляют:

1. сведения в военной области;
2. сведения в области экономики, науки и техники;
3. сведения в области внешней политики и экономики;
4. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

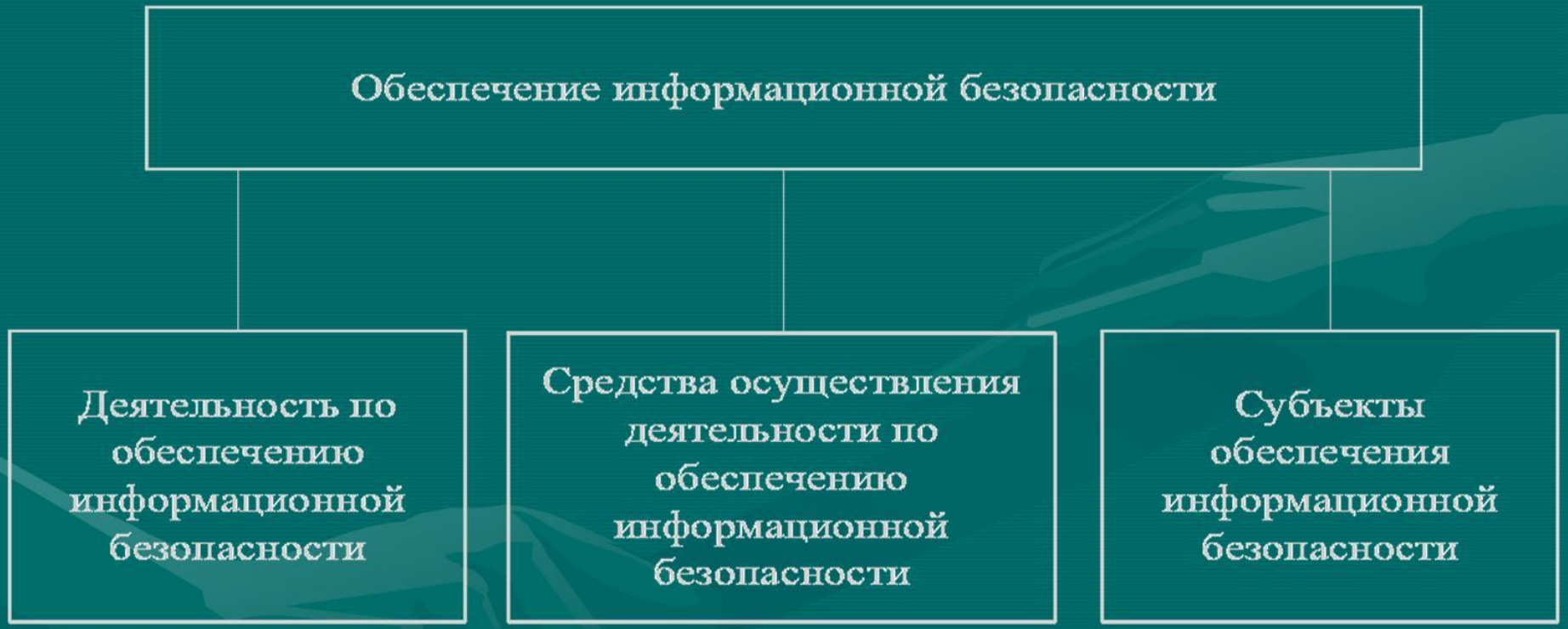
**Не подлежат отнесению к государственной тайне сведения:**

1. **о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;**
2. **о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;**
3. **о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;**
4. **о фактах нарушения прав и свобод человека и гражданина;**
5. **о размерах золотого запаса и государственных валютных резервах Российской Федерации;**
6. **о состоянии здоровья высших должностных лиц Российской Федерации;**
7. **о фактах нарушения законности органами государственной власти и их должностными лицами.**

# Технологии обеспечения информационной безопасности

# Общая схема обеспечения информационной безопасности

# Структура понятия «обеспечение информационной безопасности»



- Таким образом, **обеспечение информационной безопасности** есть совокупность деятельности по недопущению вреда свойствам объекта безопасности, обусловливаемым информацией и информационной инфраструктурой, а также средств и субъектов этой деятельности.
- ***Деятельность по обеспечению информационной безопасности*** - комплекс планируемых и проводимых в целях защиты информационных ресурсов мероприятий, направленных на ликвидацию угроз информационной безопасности и минимизацию возможного ущерба, который может быть нанесен объекту безопасности вследствие их реализации.
- Под **субъектами обеспечения информационной безопасности** понимаются государственные органы, предприятия, должностные лица, структурные подразделения, принимающие непосредственное участие в организации и проведении мероприятий по обеспечению информационной безопасности.
- ***Средства, с помощью которых достигаются цели деятельности по обеспечению информационной безопасности***, - это системы, объекты, способы, методы и иные механизмы непосредственного решения задач обеспечения ин-формационной безопасности. Прежде всего, они представляют собой совокупность правовых и организационных средств обеспечения информационной без-опасности.

# Основные виды организационных средств обеспечения информационной безопасности

# Основные направления защиты информации

# Основные направления организационной защиты информации

# Основные принципы организационной защиты информации



- Принцип комплексного подхода заключается в использовании сил, средств, способов и методов защиты информации для решения поставленных задач в зависимости от конкретной складывающейся ситуации и наличия факто-ров, ослабляющих или усиливающих угрозу возможной утечки конфиденциальной информации.
- Принцип оперативности принятия управленческих решений существенно влияет на эффективность функционирования и гибкость системы защиты ин-формации и отражает целеустремленность должностных лиц на решение задач защиты информации.
- Принцип персональной ответственности заключается в наиболее эффективном и полном распределении сил структурных подразделений предприятия, участвующих в процессе защиты информации.

# Структура системы защиты информации

Система защиты информации должна отвечать совокупности следующих основных требований, то есть быть:

- ***централизованной*** - соответствующей эффективному процессу управления системой со стороны руководителя и ответственных должностных лиц по направлениям деятельности предприятия;
- ***плановой*** - объединяющей усилия различных должностных лиц и структурных подразделений при их участии в организации и обеспечении выполнения задач, стоящих перед предприятием;
- ***конкретной и целенаправленной*** - защите должны подлежать абсолютно конкретные информационные ресурсы, представляющие интерес для конкурирующих организаций;
- ***активной*** - обеспечивать защиту информации с достаточной степенью настойчивости и возможностью концентрации усилий на наиболее важных направлениях деятельности предприятия;
- ***надежной и универсальной*** - охватывать весь комплекс деятельности предприятия, связанной с созданием и обменом информацией.

# Структура перечня сведений, составляющих государственную тайну

Вместе с тем, в соответствии со статьей 7 Закона РФ "О государственной тайне", не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

- о привилегиях, компенсациях и льготах, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

- о фактах нарушения прав и свобод человека и гражданина;

- о размерах золотого запаса и государственных валютных резервах Российской Федерации;

- о состоянии здоровья высших должностных лиц Российской Федерации;

- о фактах нарушения законности органами государственной власти и их должностными лицами.

- Благодарю за внимание!