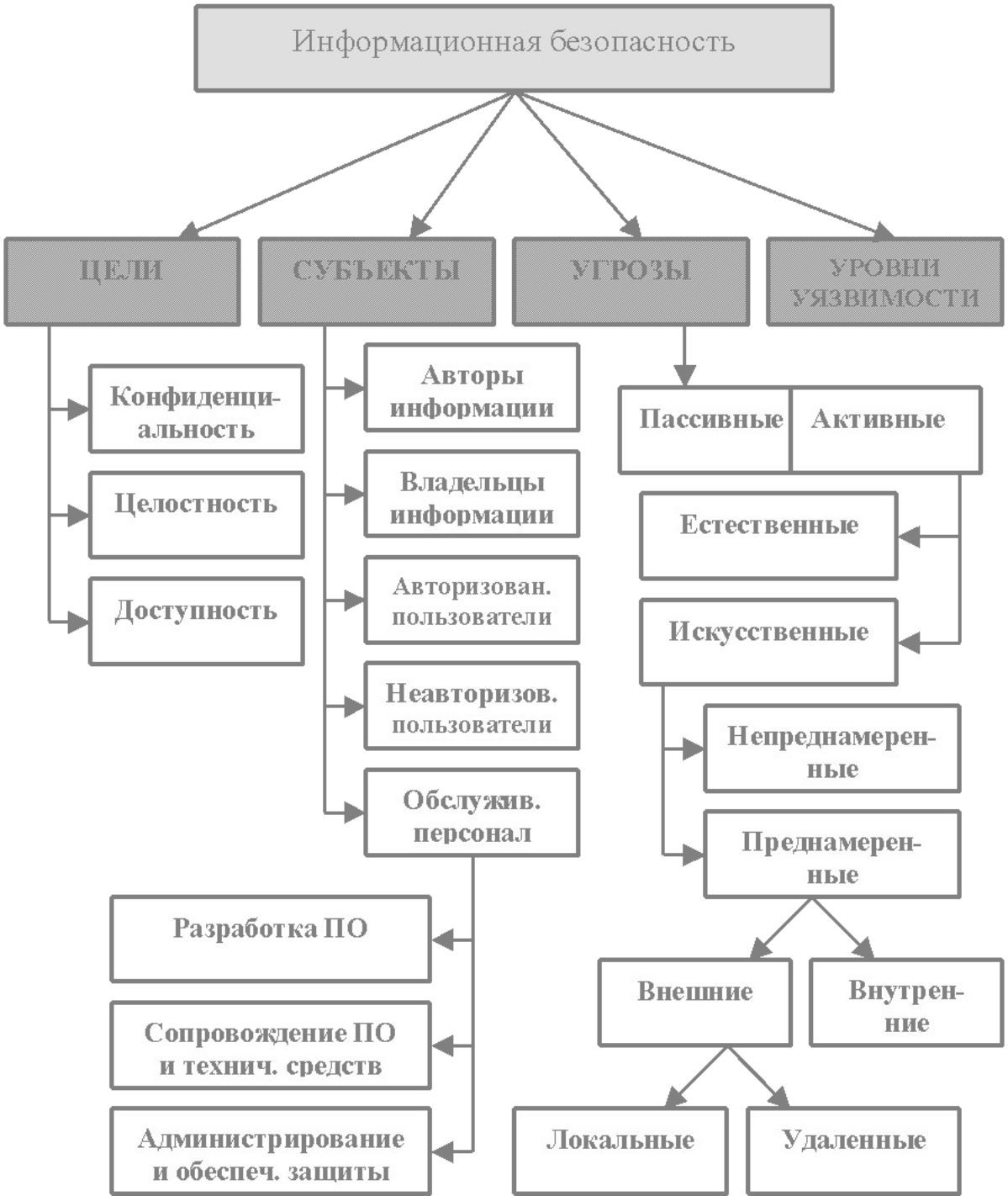
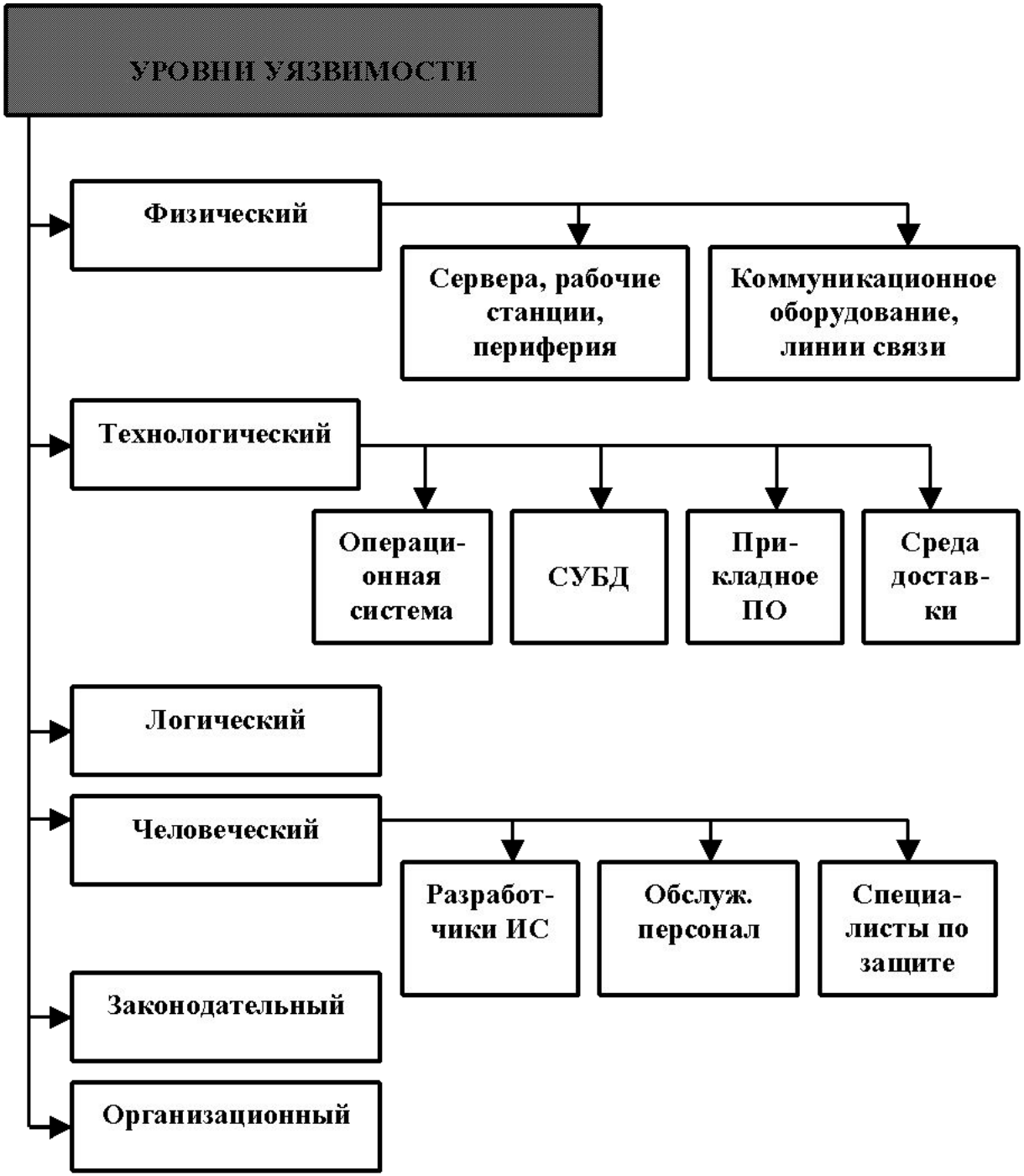
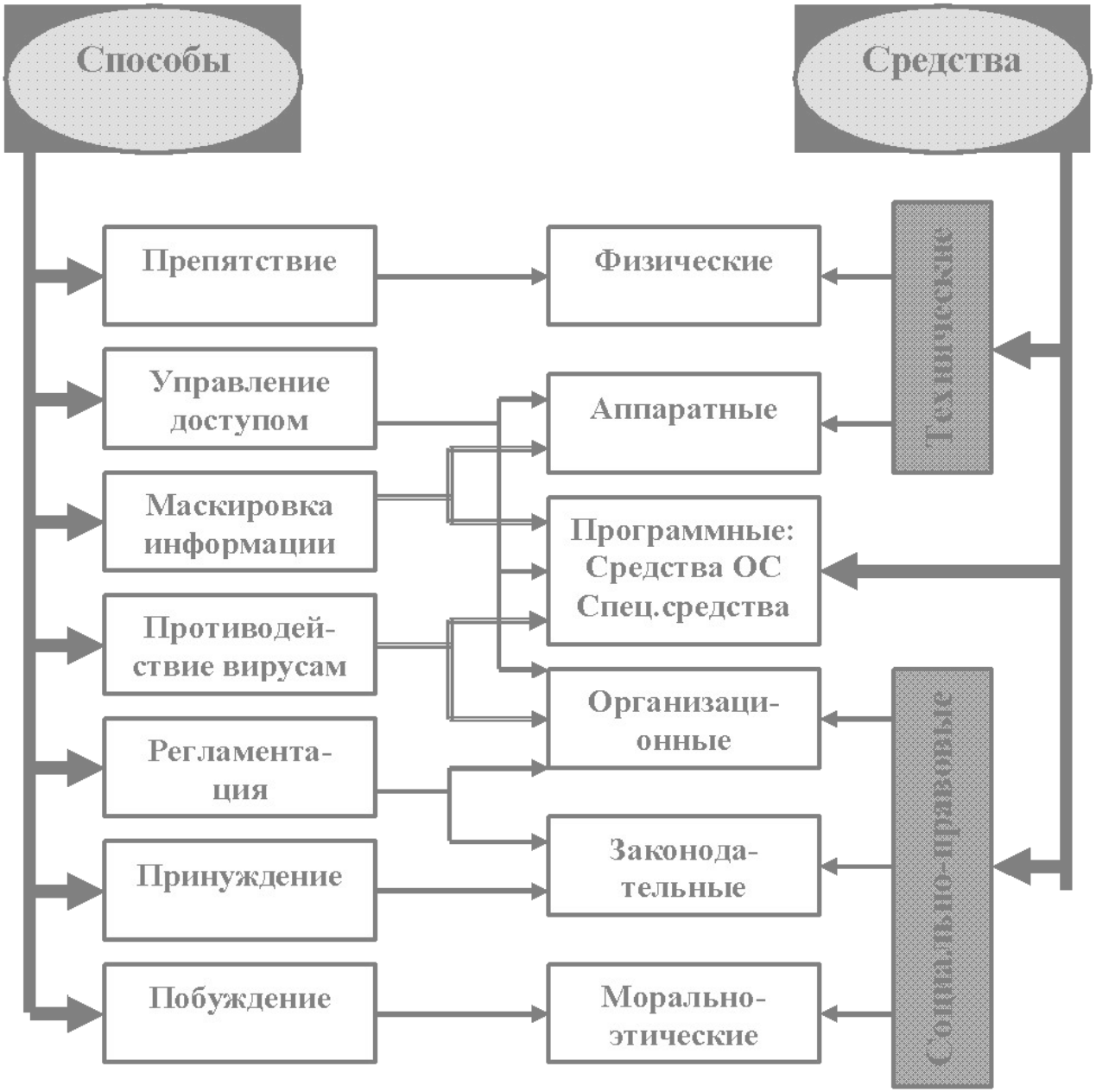
Модель информационной безопасности



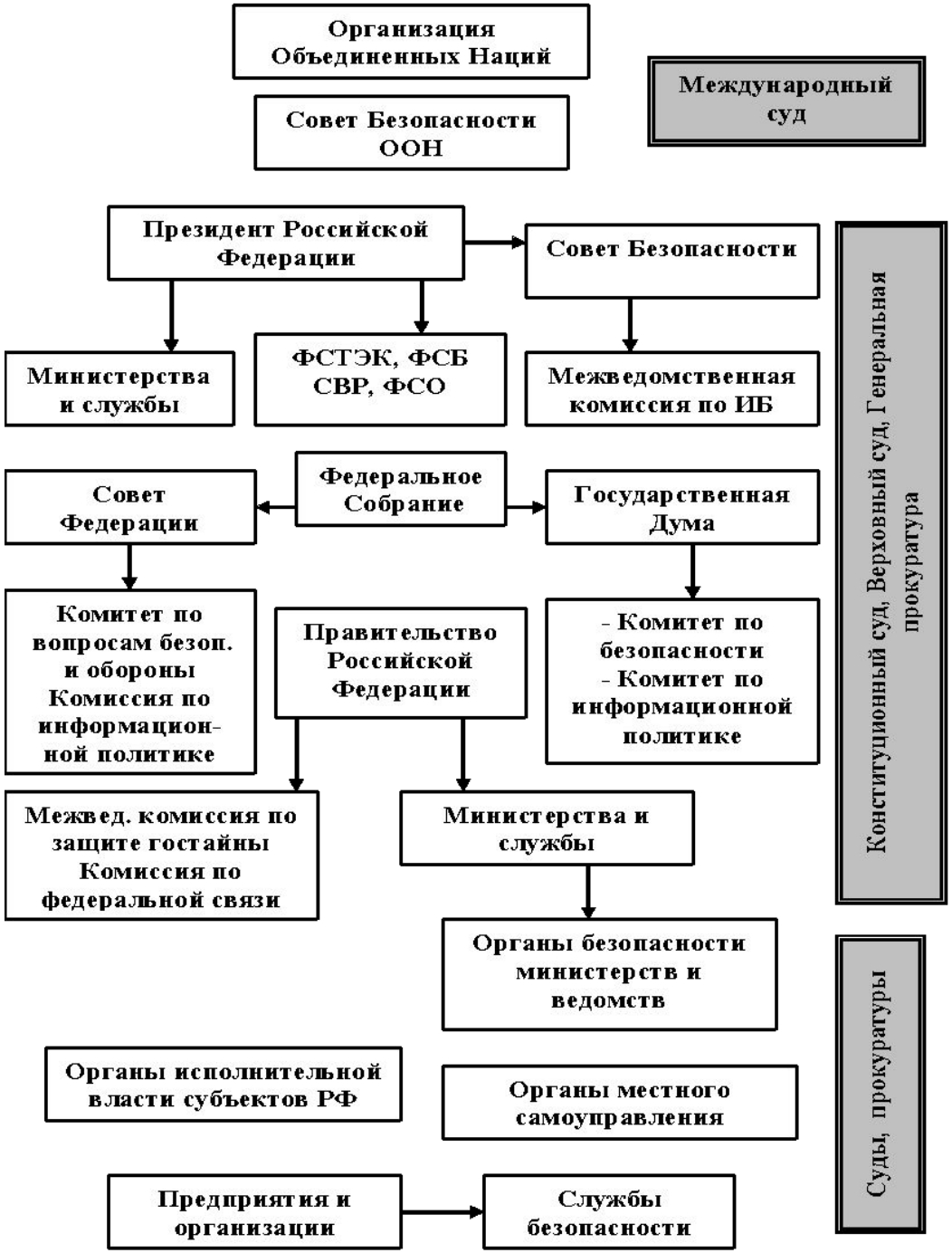
Модель информационной безопасности



Способы и средства защиты информации



Органы обеспечения ИБ



Сайт органов государственной власти РФ: **http://www.gov.ru**

Основные элементы государственной системы защиты информации

п. 11 «Положения о государственной системе защиты информации в Российской Федерации от ИТР и от ее утечки по техническим каналам», утвержденное Постановлением Совета министров – Правительства Российской Федерации от 15 сентября 1993 г. № 912- 51 («Положение - 93»)

ГОСУДАРСТВЕННУЮ СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ ОБРАЗУЮТ:

- Федеральная служба по техническому и экспортному контролю России
- Федеральная служба безопасности России и подразделения по защите информации
- Министерство внутренних дел России и подразделения по защите информации
- Министерство обороны России и подразделения по защите информации
- Служба внешней разведки России и подразделения по защите информации
- Федеральная служба охраны и подразделения по защите информации
- Структурные и межотраслевые подразделения органов государственной власти
- Головные НИИ, предприятия ОПК, ВУЗы и институты повышения квалификации
- Предприятия, специализирующиеся на проведении работ в области защиты информации

Президент РФ (www.kremlin.ru):
в пределах своих полномочий создает, реорганизует и руководит органами по обеспечению информационной безопасности (ИБ), определяет приоритетные направления государственной политики в данной области.

Совет Безопасности РФ (www.scrf.gov.ru):
проводит работу по выявлению и оценке угроз ИБ РФ;

разрабатывает важнейшие концептуальные документы в области национальной безопасности;

координирует деятельность органов по обеспечению ИБ;

контролирует реализацию органами исполнительной власти решений Президента в этой области.

Указом Президента от 28.10.2005 № 1244 утверждена **Межведомственная комиссия Совета Безопасности по ИБ.**
Указом Президента 8.11.1995 № 1108 создана **Межведомственная комиссия по защите государственной тайны**.
(Указ от 6.10.2004 № 1286 переопределены функции)

Указ Президента Российской Федерации № 9 от 05.01.1992 г.
"О создании **Государственной технической комиссии** при Президенте Российской Федерации" - государственный орган, курирующий вопросы защиты информации.

Руководящие документы Гостехкомиссии:

1. «Концепция защиты средств вычислительной техники от несанкционированного доступа к информации», 1992 г.;

2. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», 1992 г.;

3. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992 г.
4. Критерии оценки безопасности информационных технологий. Введен в действие Приказом Гостехкомиссии от 19.06.02 г. № 187 (Часть 1, 2, 3). Соответствует ГОСТ Р ИСО/МЭК 15408-2002.

- ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования";
- ГОСТ Р 50922-96 Защита информации. Основные термины и определения.
- ГОСТ Р 51275-99 Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения.
- ГОСТ Р 51583-2000 Защита информации. Порядок создания систем в защищенном исполнении.

Государственный стандарт ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» («Общие критерии») – призваны заменить прежние руководящие документы путем интеграции с мировым сообществом.

Указом Президента РФ № 1085 от 16.08.2004 создана **Федеральная служба по техническому и экспортному контролю (ФСТЭК) -** преемник Государственной технической комиссии.

ФСТЭК выполняет специальные и контрольные функции в области государственной безопасности по вопросам:

1). Обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры;
2). Обеспечения защиты (не криптографическими методами) информации, содержащей сведения, составляющие государственную тайну;
3). Противодействия иностранным техническим разведкам

Полномочия ФСТЭК:

1. Разрабатывает стратегию по обеспечению безопасности информации.
2. Проводит лицензирование деятельности по оказанию услуг в области технической защиты государственной тайны, по созданию средств защиты информации.
3. Организует проведение сертификации средств технической защиты информации, обеспечения безопасности информационных технологий.
4. Организует разработку программ стандартизации, технических регламентов и национальных стандартов в области обеспечения безопасности информации.

Основные функции Федеральной службы по техническому и экспортному контролю

Федеральная служба по техническому и экспортному контролю

Противодействие иностранным техническим разведкам

Организационно-техническое обеспечение деятельности Межведомственной комиссии по защите государственной тайны
Координация работ и методическое руководство деятельностью органов государственной власти по подготовке развернутых перечней сведений, подлежащих засекречиванию.

Техническая защита информации

Координация размещения и использования иностранных технических средств наблюдения и контроля в ходе реализации международных договоров Российской Федерации и иных программ и проектов

Защита информации при разработке, производстве, эксплуатации и утилизации неинформационных излучающих комплексов, систем и устройств

Обеспечение безопасности информации в системах информационной и телекоммуникационной инфраструктуры, оказывающих существенное влияние на национальную безопасность Российской Федерации в информационной сфере

Реализация государственной политики и организация межведомственного взаимодействия в области экспортного контроля в Российской Федерации.
Организационно-техническое обеспечение деятельности Комиссии по экспортному контролю Российской Федерации

Федеральная служба безопасности (ФСБ) www.fsb.ru

1. Обеспечение защиты сведений, составляющих государственную тайну.
2. Формирование и реализация государственной и научно-технической политики в области обеспечения ИБ.
3. Организация обеспечения криптографической безопасности информационно-телекоммуникационных систем.
4. Разработка и утверждение нормативных и методических документов по вопросам обеспечения ИБ информационно-телекоммуникационных систем и сетей критически важных объектов.
5. Осуществляет и организует сертификацию средств защиты информации
6. Лицензирование деятельности по:
   - разработке, производству, техническому обслуживанию шифровальных (криптографических) средств;
   - предоставлению услуг в области шифрования информации.

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам создана Постановлением Правительства РФ от 7.04.2004 № 178 в ведении Министерства образования и науки Российской Федерации. (www.fips.ru)

Министерство информационных технологий и связи (www.minsvyaz.ru).

Федеральное агентство по информационным технологиям (Указ Президента от 20.05.2004 № 649).

Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Указ Президента РФ от 12.03.2007 № 320) образована слиянием Россвязьнадзора и Росохранкультуры.

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам создана Постановлением Правительства РФ от 7.04.2004 № 178 в ведении Министерства образования и науки Российской Федерации. (www.fips.ru)

Министерство информационных технологий и связи (www.minsvyaz.ru).

Федеральное агентство по информационным технологиям (Указ Президента от 20.05.2004 № 649).

Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Указ Президента РФ от 12.03.2007 № 320) образована слиянием Россвязьнадзора и Росохранкультуры.

Очередная реформа:

Указ Президента РФ от 12.05.2008 № 724:

Министерство связи и массовых коммуникаций

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам создана Постановлением Правительства РФ от 7.04.2004 № 178 в ведении Министерства образования и науки Российской Федерации. (www.fips.ru)

Министерство информационных технологий и связи (www.minsvyaz.ru).

Федеральное агентство по информационным технологиям (Указ Президента от 20.05.2004 № 649).

Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Указ Президента РФ от 12.03.2007 № 320) образована слиянием Россвязьнадзора и Росохранкультуры.

Очередная реформа:

Указ Президента РФ от 12.05.2008 № 724:

Министерство связи и массовых коммуникаций

Федеральная служба по надзору в сфере связи и массовых коммуникаций.

Федеральная служба по интеллектуальной собственности, патентам и товарным знакам создана Постановлением Правительства РФ от 7.04.2004 № 178 в ведении Министерства образования и науки Российской Федерации. (www.fips.ru)

Министерство информационных технологий и связи (www.minsvyaz.ru).

Федеральное агентство по информационным технологиям (Указ Президента от 20.05.2004 № 649).

Федеральная служба по надзору в сфере массовых коммуникаций, связи и охраны культурного наследия (Указ Президента РФ от 12.03.2007 № 320) образована слиянием Россвязьнадзора и Росохранкультуры.

Очередная реформа:

Указ Президента РФ от 12.05.2008 № 724:

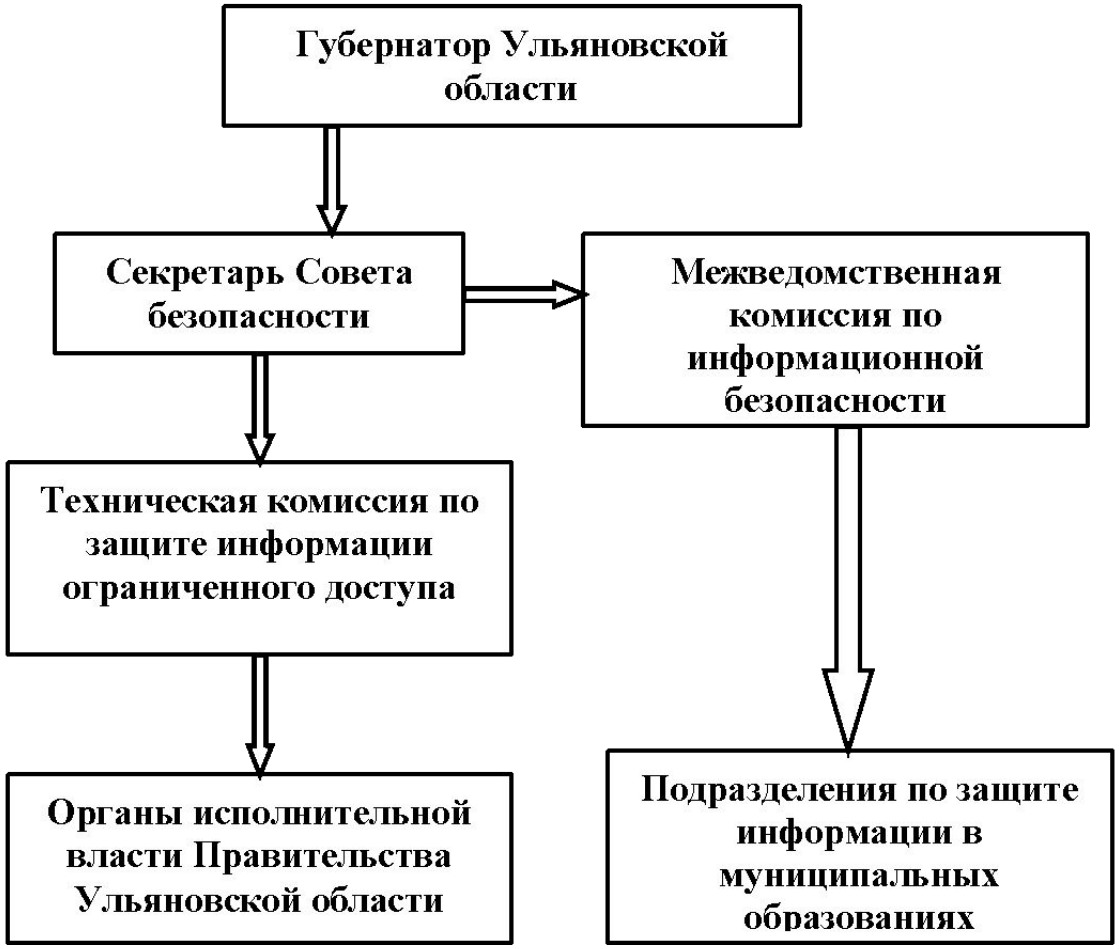
Министерство связи и массовых коммуникаций

Федеральная служба по надзору в сфере связи и массовых коммуникаций.

Упразднено Указом Президента РФ № 1060 от 25.08.2010

Обеспечение ИБ на региональном уровне

(Ульяновская обл. http://ulgov.ru/power/gov/informatization)



В составе Правительства Ульяновской области имеется департамент инноваций и информационных технологий.

Обеспечение ИБ на региональном уровне

(Ульяновская обл. http://ulgov.ru/power/gov/informatization)

Законодательные акты Ульяновской области:

- концепция информатизации «Электронный Ульяновск» на 2004-2010 годы;
- Закон № 087-ЗО от 04.10.05 «Об информационных ресурсах и информатизации Ульяновской области»;
- Постановление Губернатора от 9.03.2006 «О реестре информационных ресурсов и систем Ульяновской области и порядке организации информационного взаимодействия органов государственной власти Ульяновской области»;
- Распоряжение Правительства Ульяновской области № 178-пр от 13.12.05 «Об уполномоченном органе по информатизации Ульяновской области»;
- Распоряжение Губернатора № 497-р от 3.08.2006 «О координационном Совете по информатизации Ульяновской области»;
- Распоряжение Губернатора от 22.02.2006 №105-р об утверждении «Инструкции о порядке пользования вычислительной техникой, программным обеспечением и работе в информационной вычислительной сети Администрации Губернатора и аппарата Правительства Ульяновской области».

Классификация корпоративной информации

Коммерческая тайна – *№98-ФЗ «О коммерческой тайне»*

Налоговая тайна – *«Налоговый кодекс РФ»*

Банковская тайна – *№395-1 «О банках и банковской деятельности»*

Врачебная тайна – *2011 №323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации"*

Адвокатская тайна – *№63-ФЗ "Об адвокатской деятельности и адвокатуре в РФ"*

Тайна связи – *№ 126-ФЗ "О связи"*

Тайна следствия – *УПК*

Тайна усыновления – *Семейный кодекс*

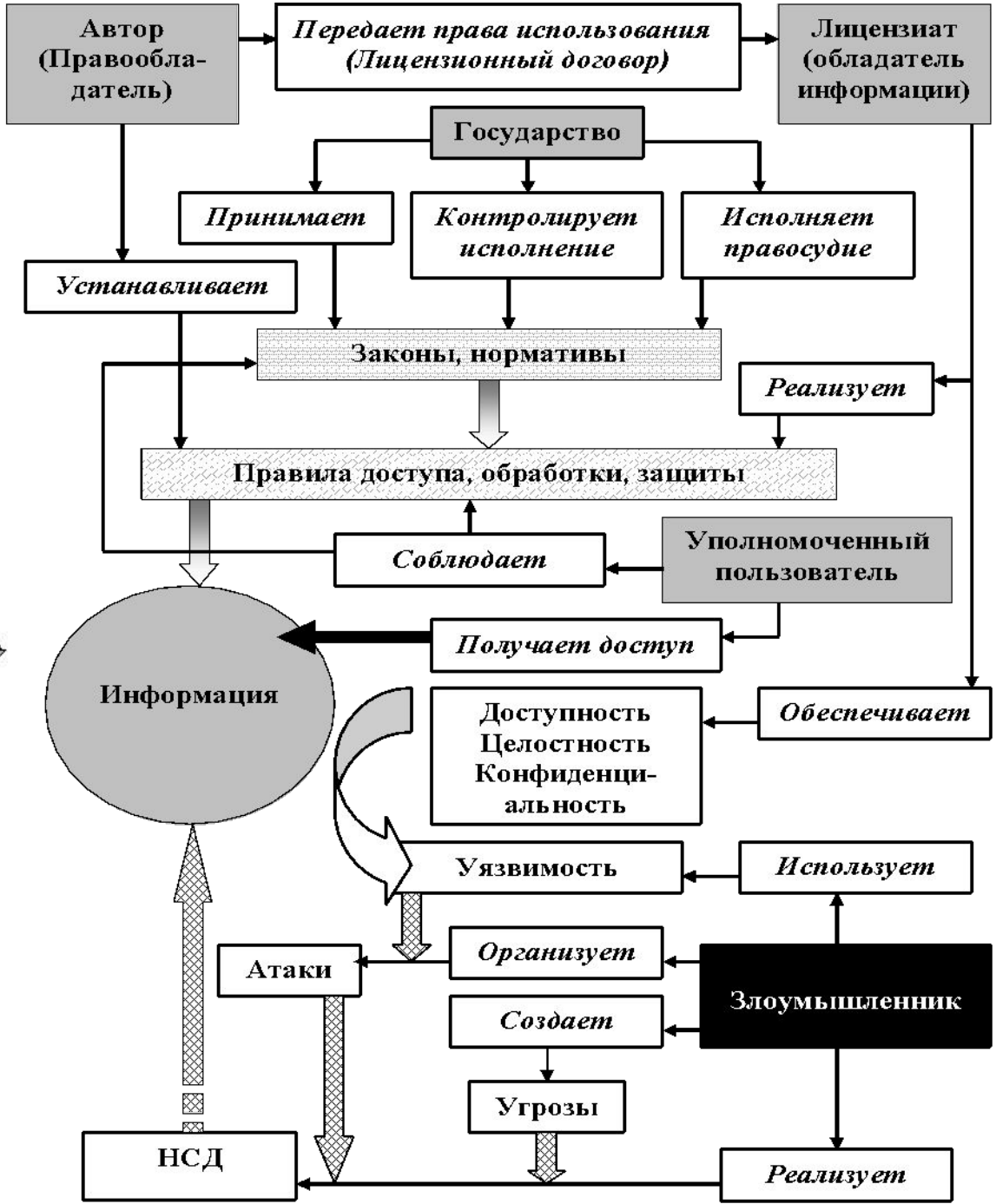
Аудиторская тайна – *№307-ФЗ «Об аудиторской деятельности»*

Основные причины уязвимости IP-сетей

1. Сеть Internet разрабатывалась как открытая и децентрализованная сеть с изначальным отсутствием политики безопасности.
2. Большая протяженность линий связи и уязвимость основных служб.
3. Модель «клиент — сервер», на которой основана работа в Internet, не лишена слабостей и лазеек в продуктах отдельных производителей.
4. Информация о существующих и используемых средствах защиты доступна пользователям.
5. Существует возможность наблюдения за каналами передачи данных.
6. Средства управления доступом сложно конфигурировать, настраивать и контролировать.
7. Использование большого числа сервисов, информационных служб и сетевых протоколов, освоение которых одному человеку в лице администратора сети практически недоступно.
8. Недостаток в специалистах по защите информации в Internet.
9. Существует потенциальная возможность обойти средства обнаружения отправителя информации либо посетителя Web-узла с помощью использования виртуальных IP-адресов.

В 1993 году создана рабочая группа IP Security Working Group, разработан набор протоколов IPSec, основанных на современных технологиях шифрования и электронной цифровой подписи данных.

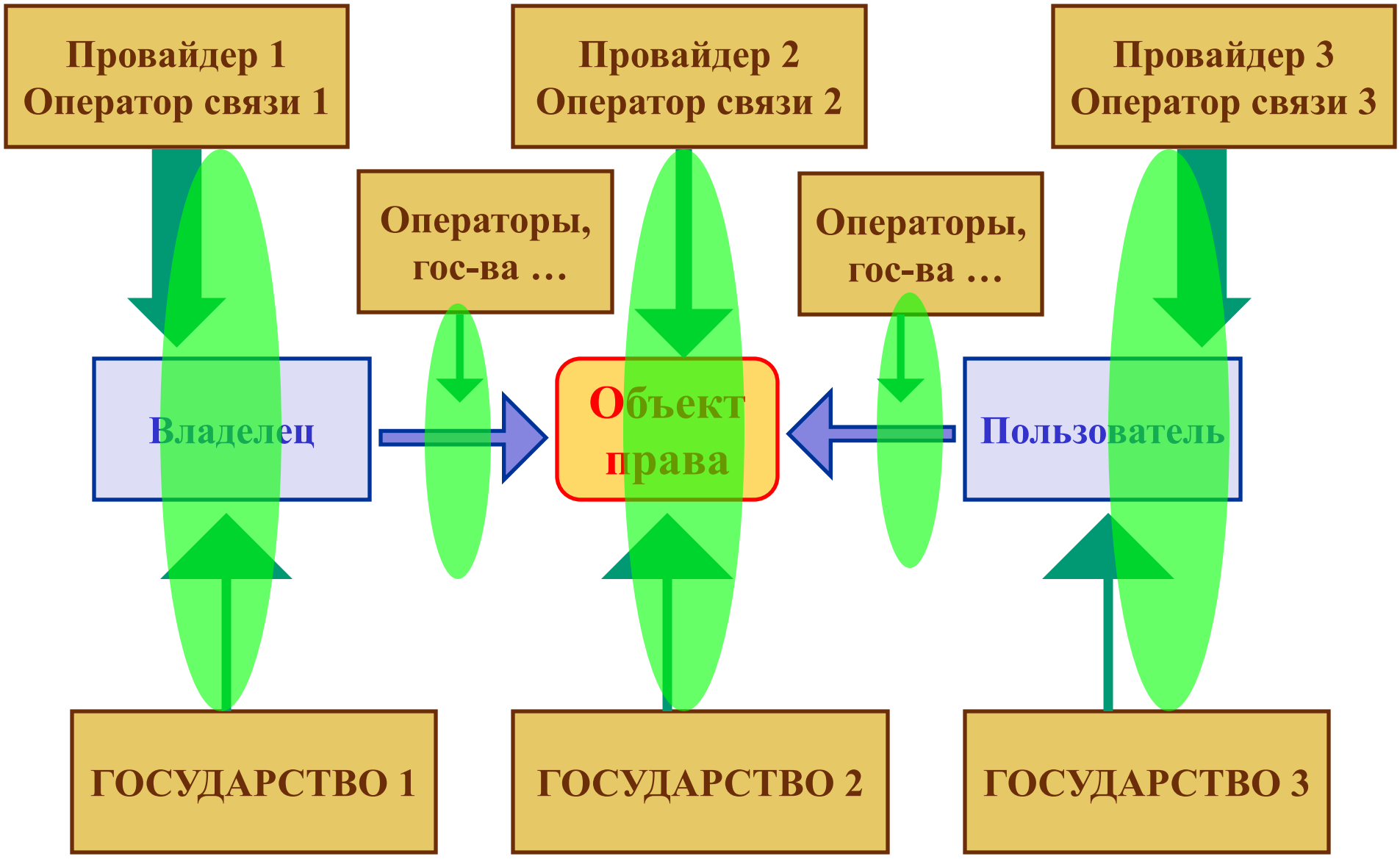
Модель отношений субъектов информационных отношений



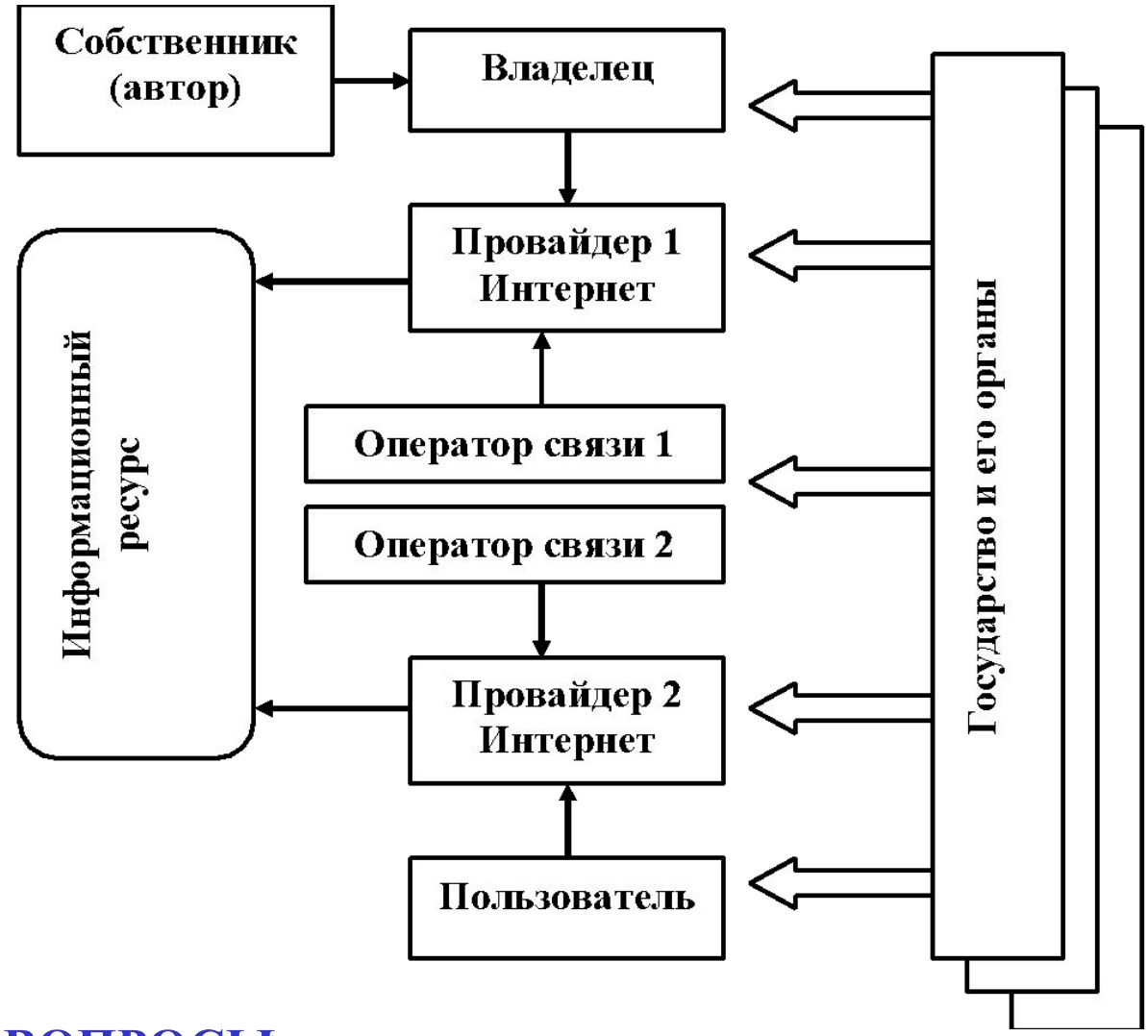
Упрощенная модель

А КАК В ИНТЕРНЕТЕ?

Новые субъекты с разной юрисдикцией



Модель отношений субъектов информационных отношений в сети Интернет



ПРОБЛЕМА:

Все субъекты могут находиться в юрисдикции разных государств

ВОПРОСЫ:

1. **Какой суд или госорган имеет полномочия**
2. **Какие законы применять**
3. **Как исполнять решения суда**

Основные причины уязвимости IP-сетей

1. Сеть Internet разрабатывалась как открытая и децентрализованная сеть с изначальным отсутствием политики безопасности.
2. Большая протяженность линий связи и уязвимость основных служб.
3. Модель «клиент — сервер», на которой основана работа в Internet, не лишена слабостей и лазеек в продуктах отдельных производителей.
4. Информация о существующих и используемых средствах защиты доступна пользователям.
5. Существует возможность наблюдения за каналами передачи данных.
6. Средства управления доступом сложно конфигурировать, настраивать и контролировать.
7. Использование большого числа сервисов, информационных служб и сетевых протоколов, освоение которых одному человеку в лице администратора сети практически недоступно.
8. Недостаток в специалистах по защите информации в Internet.
9. Существует потенциальная возможность обойти средства обнаружения отправителя информации либо посетителя Web-узла с помощью использования виртуальных IP-адресов.

В 1993 году создана рабочая группа IP Security Working Group, разработан набор протоколов IPSec, основанных на современных технологиях шифрования и электронной цифровой подписи данных.

Управление Интернетом

Характерные черты современного Интернета:

1. Рост числа пользователей
2. Важное влияние на общество
3. Киберпреступность
4. Незаконное использование технологии (вирусы, спам)

Необходимость регулирования Интернета:

1. Минимизировать риск распада Интернета на части
2. Сохранить техническую совместимость всех компонентов
3. Защитить права и определить ответственность субъектов
4. Оградить пользователей от незаконного использования технологий
5. Способствовать дальнейшему развитию Интернет

Управление Интернетом

Что значит регулирование Интернета:

1. **Специалисты по телекоммуникациям** – техническая инфраструктура
2. **Программисты** – разработка языков, стандартов
3. **Юристы** – вопросы юрисдикции
4. **Политики** – Интернет как средство массовой информации
5. **Дипломаты** – защита национальных интересов
6. **И т.д.**

Всемирная встреча на высшем уровне (2003, 2005):

«Управление Интернетом представляет собой разработку и применение правительствами, частным сектором и гражданским обществом, при выполнении ими своей роли, общих принципов, норм, правил, процедур принятия решений и программ, регулирующих эволюцию и применение Интернета.»

Управление Интернетом

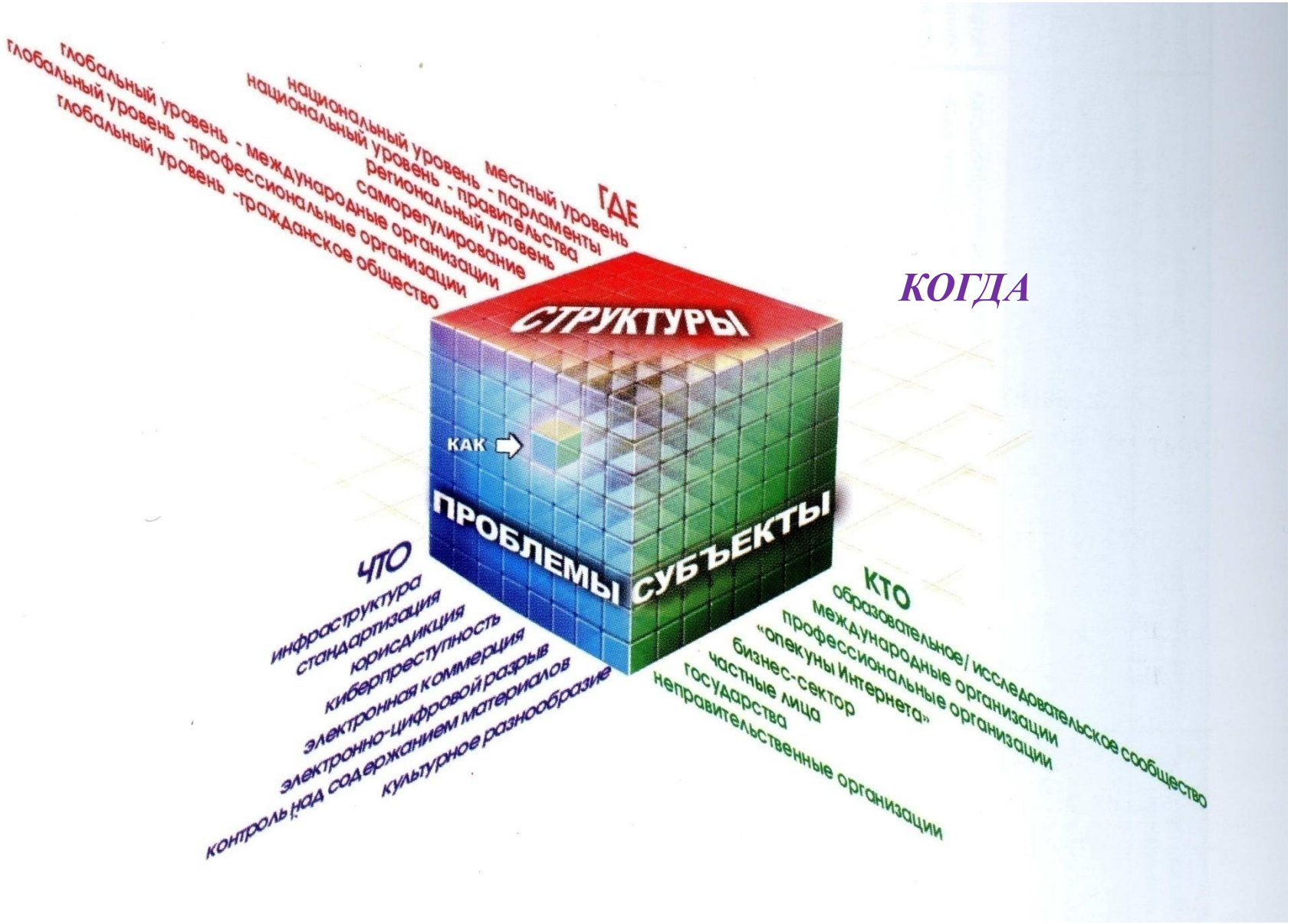
Эволюция управления Интернетом:

1. 60-е годы – Минобороны США (сеть ARPANet)
2. 1986 г. – рабочая группа по проектированию Интернета (IETF)
3. 1998 г. – корпорация по присвоению доменных имен и номеров сетей в Интернете (ICANN)
4. 2006 г. – Форум по вопросам управления использованием Интернета

Основные аспекты управления Интернетом:

1. Инфраструктура и стандартизация (13 корневых серверов управления Интернетом, 10 из них в США)
1. Правовые аспекты
2. Экономические аспекты
3. Аспекты, связанные с развитием
4. Социокультурные аспекты

Куб управления Интернетом



Правовое регулирование Интернет

Указ Президента РФ от 12.05.2004 № 611 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» (с изм. от 22.03.2005 № 329, от 03.03.2006 № 175).

Постановление Правительства РФ от 3.06.1998 № 564 «Об утверждении Положения о лицензировании деятельности по международному информационному обмену» (в ред. от 03.10.2002 № 731)

27.08.2005 г. № 538 «Об утверждении правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность»;

23.01.2006 г. № 32 «Об утверждении правил оказания услуг связи по передаче данных»

10.09.2007 № 575 «Об утверждении Правил оказания телематических услуг связи». Правила вводятся с 1 января 2008 года.

На сайте www.russianlaw.net/law/acts/z47.htm 10.05.2005 опубликован проект Федерального закона “О правовом регулировании оказания Интернет-услуг».

Правовое регулирование Интернет

25.07.2007 Совет Безопасности Российской Федерации принял концептуальный документ:

«Стратегия развития информационного общества в России».

В Стратегии отмечена необходимость обеспечения безопасности функционирования российских информационных и коммуникационных систем в составе глобальной информационной инфраструктуры, выработке международных норм и механизмов, регулирующих отношения в области использования глобальной информационной инфраструктуры, включая вопросы управления использованием Интернета.

Приказ Минкомсвязи РФ №66 от 19.05.2009
"О создании Совета по вопросам использования и развития информационно-телекоммуникационной сети «Интернет» в Российской Федерации"

Совет осуществляет следующие функции:

- формирует совместные инициативы по вопросам использования и развития сети «Интернет» в Российской Федерации;
- разрабатывает программы и проекты по вопросам использования и развития сети «Интернет» в Российской Федерации и проводит их согласование;
- подготавливает согласованные планы реализации программ и проектов, предусматривающих использование и развитие сети «Интернет» ;
- осуществляет выработку согласованной политики по вопросам использования и развития сети «Интернет» в Российской Федерации, в том числе определение приоритетных направлений;
- готовит предложения по совершенствованию нормативной правовой и нормативной методической базы в области использования и развития сети «Интернет» в Российской Федерации;
- рассматривает иные вопросы в области использования и развития сети «Интернет» в Российской Федерации.

Постановление Правительства от 26.10.2012 № 1101
"О единой автоматизированной информационной системе "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено".

Единый реестр создается в целях ограничения доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в РФ запрещено.

Ведение единого реестра осуществляется Роскомнадзором в электронной форме в ежедневном круглосуточном режиме.

Реестр обновляется ежедневно в 9.00 часов и 21.00 час по московскому времени. В течение суток с момента такого обновления оператор связи обязан ограничить доступ к таким сайтам в сети "Интернет".

Правовое регулирование Интернет

Указ Президента РФ от 17.03.2008 г. № 351
«О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

Указ Президента РФ № 31С от 15.01.2013 г.
«О СОЗДАНИИ ГОСУДАРСТВЕННОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ, ПРЕДУПРЕЖДЕНИЯ И ЛИКВИДАЦИИ ПОСЛЕДСТВИЙ КОМПЬЮТЕРНЫХ АТАК НА ИНФОРМАЦИОННЫЕ РЕСУРСЫ РОССИЙСКОЙ ФЕДЕРАЦИИ»
(ФСБ)

Указ Президента РФ № 146 от 8.02.2012 г.
«О ФЕДЕРАЛЬНЫХ ОРГАНАХ ИСПОЛНИТЕЛЬНОЙ ВЛАСТИ, УПОЛНОМОЧЕННЫХ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ, СОЗДАННЫХ С ИСПОЛЬЗОВАНИЕМ СУПЕРКОМПЬЮТЕРНЫХ И ГРИД-ТЕХНОЛОГИЙ»
(ФСБ, ФСТЭК)

Распоряжение Правительства РФ от 15.04.2013 N 611-р
«Об утверждении перечня нарушений целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации»

Правовое регулирование Интернет

Постановление Правительства от 18.05.2009 г. № 424
«Об особенностях подключения федеральных государственных информационных систем к информационно-телекоммуникационным сетям».

Приказ Минкомсвязи РФ от 25.08.2009 № 104
"Об утверждении Требований по обеспечению целостности, устойчивости функционирования и безопасности информационных систем общего пользования".

Приказ Минкомсвязи России от 27.06.2013 № 149
"Об утверждении Требований к технологическим, программным и лингвистическим средствам, необходимым для размещения информации государственными органами и органами местного самоуправления в сети "Интернет" в форме открытых данных, а также для обеспечения ее использования".

Приказ ФСБ и ФСТЭК № 416/489 от 31.08.2010
«Об утверждении требований о защите информации, содержащейся в информационных системах общего пользования»

Правовое регулирование Интернет

Приказ ФСТЭК России от 11.02.2013 № 17
"Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах".

"Методический документ. Меры защиты информации в государственных информационных системах"
(утв. **ФСТЭК России 11.02.2014**)

Приказ ФСО РФ от 07.08.2009 № 487
"Об утверждении Положения о сегменте информационно-телекоммуникационной сети "Интернет" для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации".

Правовое регулирование Интернет

Постановления Правительства РФ:

№ 743 от 31.07.2014 **№ 744 от 31.07.2014**

№ 745 от 31.07.2014 **№ 746 от 31.07.2014**

№ 758 от 31.07.2014 **№ 759 от 31.07.2014**

1. Устанавливается порядок взаимодействия организаторов распространения информации в сети "Интернет" с МВД, ФСБ, Роскомнадзором.

2. Оказание услуг доступа к сети Интернет с использованием пунктов коллективного доступа осуществляется оператором после проведения идентификации пользователей. Идентификация пользователя осуществляется путем установления фамилии, имени, отчества пользователя, подтверждаемых документом, удостоверяющим личность.

3. Определен состав информации о пользователях, подлежащей хранению организатором распространения информации в сети "Интернет" при обеспечении функционирования коммуникационного интернет-сервиса.

Правовое регулирование Интернет

Вводится **понятие блогера**, которым считается владелец Интернет-сайта или страницы Интернет-сайта, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более 3 тыс. пользователей.

С 1 августа 2014 г. вводится **ответственность блогеров** за размещение информации:

- соблюдать требования законодательства РФ, регулирующие порядок распространения массовой информации;
- проверять достоверность размещаемой информации до ее размещения и незамедлительно удалять размещенную недостоверную информацию;
- не допускать использование сайта в целях совершения уголовно наказуемых деяний и распространения материалов, запрещенных в соответствии с законодательством;
- не допускать распространение информации о частной жизни гражданина с нарушением гражданского законодательства, а также соблюдать честь, достоинство и деловую репутацию граждан и организаций.

Блогеров также обязали размещать свою фамилию и инициалы, а также электронный адрес для направления юридически значимых сообщений.

Правовое регулирование Интернет

Федеральные законы № 97-ФЗ от 5.05.2014, № 274-ФЗ от 21.07.2014, № 179-ФЗ от 28.06.2014

Устанавливается административная ответственность за:

- воспрепятствование работе сайтов в сети "Интернет";
- неисполнение обязанностей организатором распространения информации в сети "Интернет";
- непредставление сведений или представление заведомо недостоверных сведений в орган, осуществляющий функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций.

Ужесточается уголовная ответственность за публичные призывы в сети Интернет к осуществлению экстремистской деятельности и действий, направленных на нарушение территориальной целостности РФ (ст. 280, 280.1 УК РФ).

Управление Интернетом

12.09.2011 г. на 66-й сессии Ген. Ассамблеи ООН РФ, Китай, Таджикистан и Узбекистан предложили совместный проект **«Правила поведения в области обеспечения международной информационной безопасности».**

В январе 2015 г. государствами-членами ШОС (Шанхайская организация сотрудничества) внесены в качестве официального документа ООН обновленные **«Правила».**

22.09.2011 г. на закрытой встрече глав спецслужб и силовых ведомств 52 стран в Екатеринбурге Россия ознакомила участников с разработанным Совбезом и МИД проектом **«Конвенция об обеспечении международной информационной безопасности (концепция)» (МИБ).**

Конвенция запрещает использование интернета в военных целях и для свержения режимов в других странах, но при этом оставляет властям полную свободу действий внутри национальных сегментов сети.

Проект подвергается резкой критике, прежде всего со стороны США – страны, открыто стремящейся к «глобальному контролю над киберпространством».

Российские инициативы о принятии конвенции по МИБ и правил поведения в международном информационном пространстве сталкиваются в ООН с противодействием США.

«Конвенция об обеспечении международной ИБ»

Некоторые определения:

«информационная война» - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

«информационное оружие» - информационные технологии, средства и методы, предназначенные для ведения информационной войны.

«международная информационная безопасность» - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

«Конвенция об обеспечении международной ИБ»

Некоторые определения:

«критически важный объект информационной инфраструктуры» - часть (элемент) информационной инфраструктуры, воздействие на которую может иметь последствия, непосредственно затрагивающие национальную безопасность, включая безопасность личности, общества и государства.

«правонарушение в информационном пространстве» - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях.

«терроризм в информационном пространстве» - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях.

«угроза в информационном пространстве (угроза информационной безопасности)» - факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.