Виды атак в IP-сетях

Подслушивание (sniffing) – подключение к линиям связи
Парольные атаки
Изменение данных
«Угаданный ключ»
Подмена доверенного субъекта – хакер выдает себя за санкционированного пользователя (подмена IP-адреса)
Перехват сеанса – хакер переключает установленное соединение на новый хост
Посредничество в обмене незашифрованными ключами
«Отказ в обслуживании»
Атаки на уровне приложений – использование слабостей системного ПО (HTTP, FTP)
Злоупотребление доверием
Вирусы и приложения типа «троянский конь»
Сетевая разведка – сбор информации о сети

Причины уязвимости IP-сетей

1. Аутентификация отправителя осуществляется исключительно по его IP-адресу.
2. Процедура аутентификации выполняется только на стадии установления соединения — в дальнейшем подлинность принимаемых пакетов не проверяется.
3. Важнейшие данные, имеющие отношение к системе, передаются по сети в незашифрованном виде.

«Врожденные слабости» служб Интернет:

- простой протокол передачи электронной почты SMTP;
- программа электронной почты Sendmail;
- служба сетевых имен DNS;
- служба эмуляции удаленного терминала Telnet;
- всемирная паутина WWW;
- протокол передачи файлов FTP.

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.

Проблемы информационной безопасности существенно зависят от типа информационных систем и сферы их применения.

Особенности информационных систем распределенного типа:

1. Территориальная разнесенность компонентов системы и как следствие наличие обмена информацией между ними.

2. Широкий спектр способов представления, хранения и передачи информации.

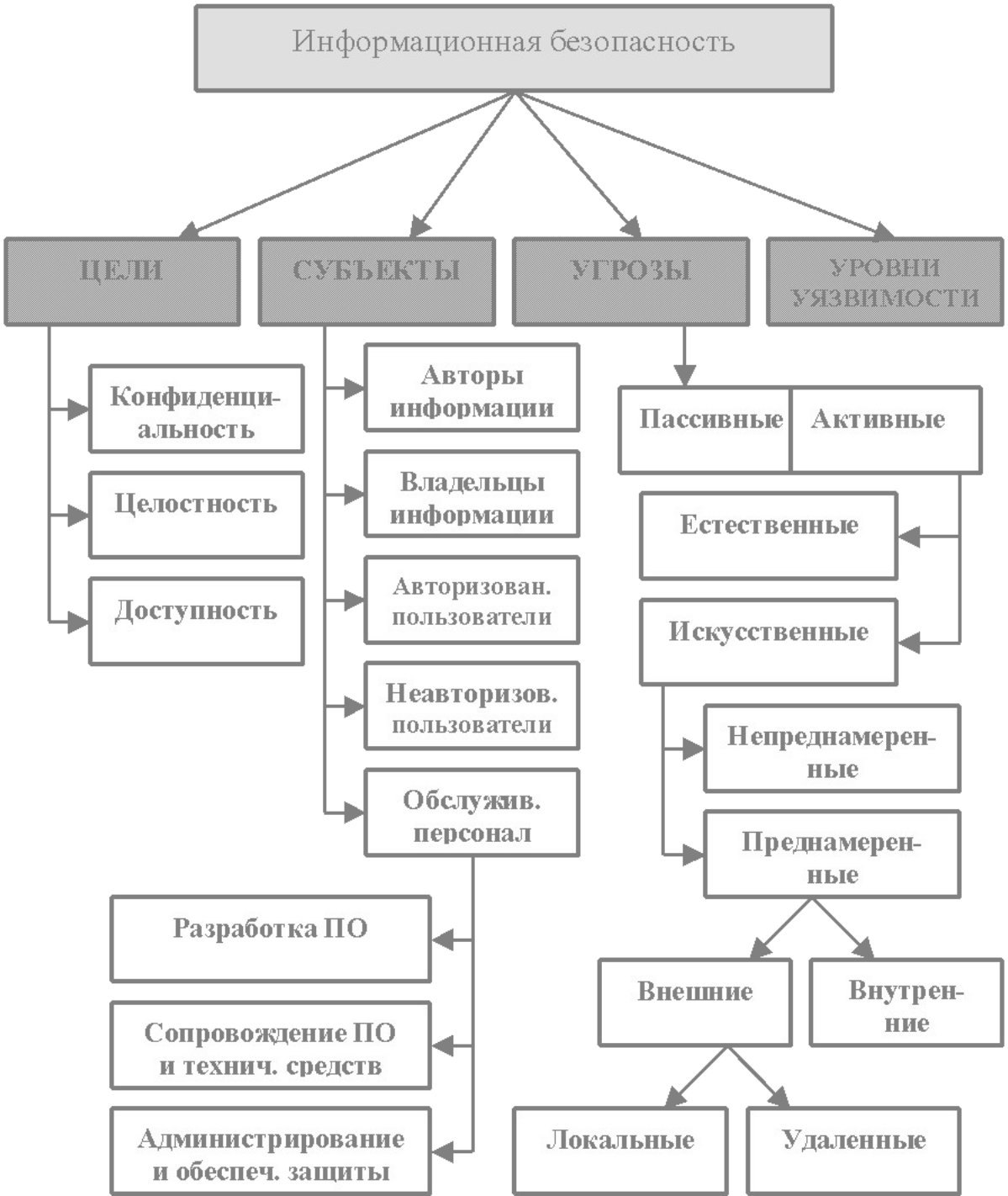
3. Интеграция данных различного назначения в единых базах данных и наоборот, размещение данных в различных узлах сети.

4. Использование режимов распределенной обработки данных.

5. Одновременное участие в процессах обработки информации большого количества пользователей с разными правами доступа.

6. Использование разнородных программно-технических средств обработки и систем телекоммуникаций.

Модель информационной безопасности



Специфические виды угроз для компьютерных сетей

- несанкционированный обмен информацией между пользователями;

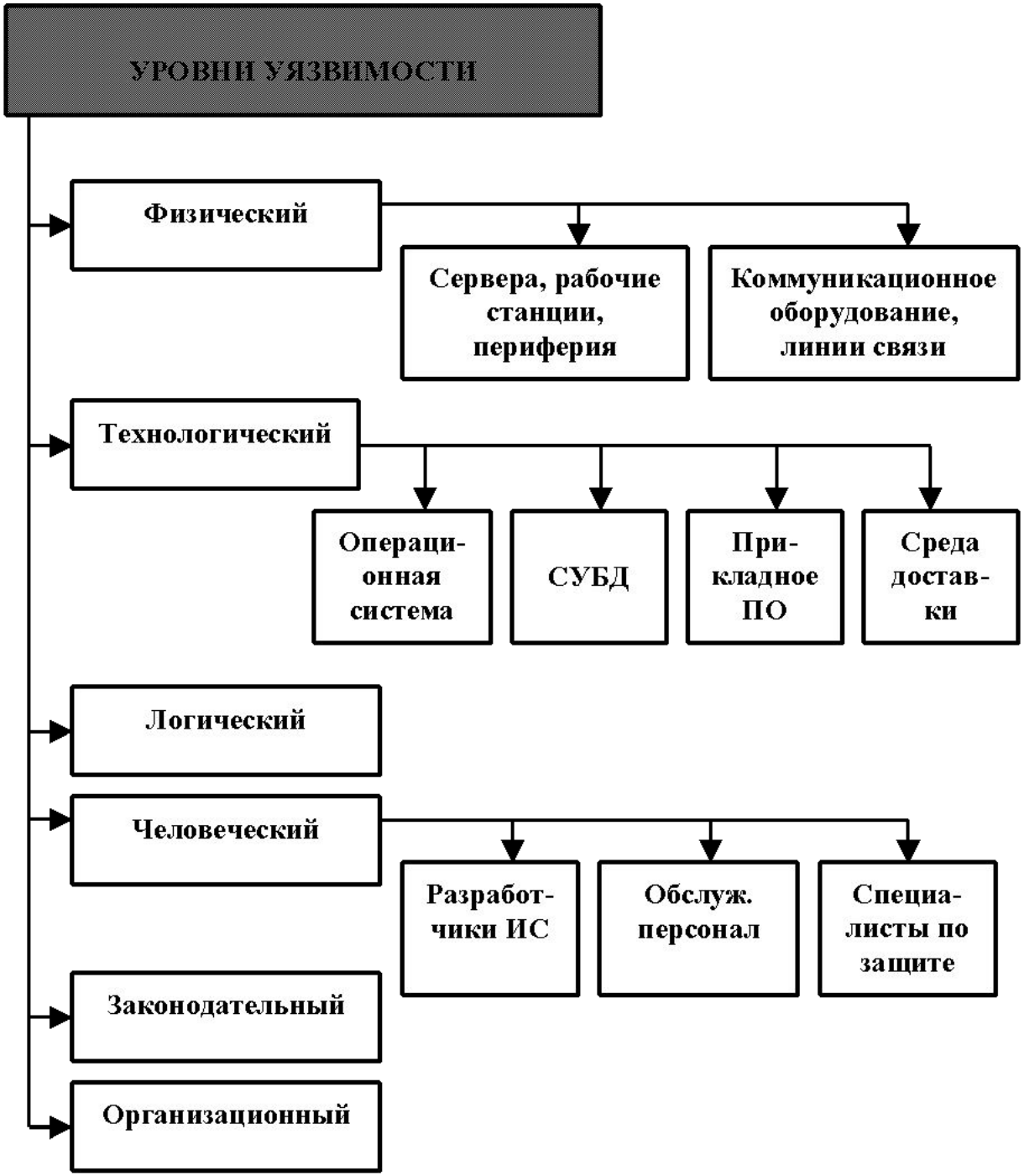
- несанкционированный межсетевой доступ к информационным и техническим ресурсам сети;

- отказ от информации, т.е. непризнание получателем (отправителем) этой информации факта ее получения (отправления);

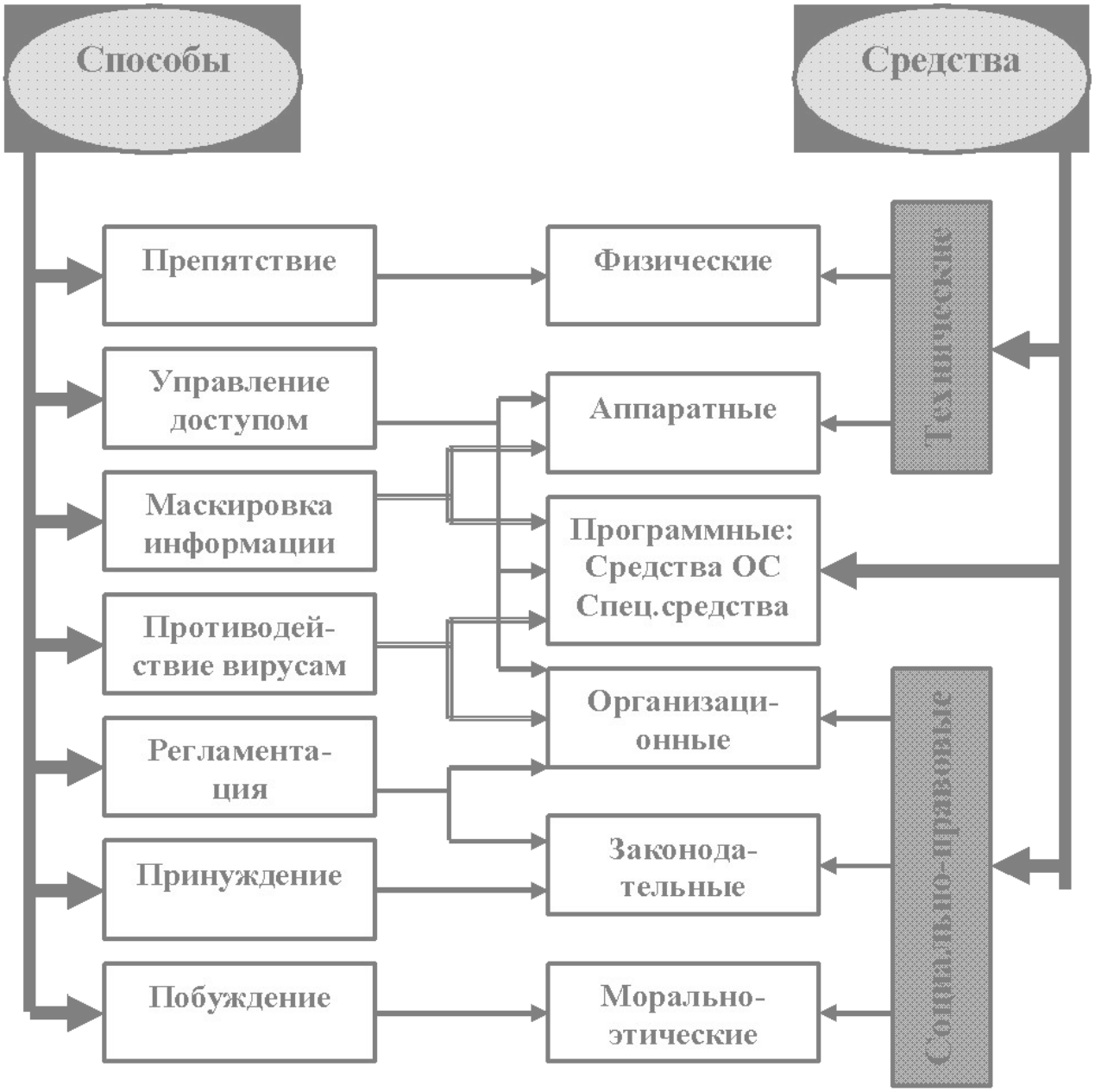
- отказ в обслуживании, который может сопровождаться тяжелыми последствиями для пользователя, обратившегося с запросом на предоставление сетевых услуг;

- распространение сетевых вирусов.

Модель информационной безопасности



Способы и средства защиты информации в сетях



Защита от компьютерных вирусов

Компьютерный вирус - это специально написанная программа, которая может "приписывать" себя к другим программам и выполнять различные нежелательные для пользователя действия на компьютере.

Черви – это независимые программы, размножающиеся путем копирования самих себя через компьютерную сеть.

Троянские кони (троян) – это программы, которые запускаются на компьютере не зависимо от согласия пользователя.

Смешанные коды – это сравнительно новый класс вредоносных программ, сочетающий в себе свойства вирусов, червей и троянов.

Жизненный цикл вируса:

1. Внедрение
2. Инкубационный период
3. Репродуцирование (саморазмножение)
4. Деструкция (искажение и/или уничтожение информации).

Классификация компьютерных вирусов

Симптомы заражения вирусами:

1. Подозрительная активность диска.
2. Беспричинное замедление работы компьютера.
3. Подозрительно высокий трафик в сети.
4. Изменение размеров и имен файлов.

Классические антивирусные средства основаны на анализе сигнатур вирусов.

Перспективным считается принцип отслеживания отклонений поведения программ и процессов от эталонного (например система Cisco Security Agent, разработанная компанией Cisco System).

В России наиболее распространенными средствами антивирусной защиты являются продукты и технологии компаний:
«Доктор WEB» (www.doctorweb.com)
«Лаборатория Касперского» (www.kaspersky.ru).

Методы защиты сетей

Парольная защита

Требования к паролю:

- в качестве пароля не может использоваться слово из какого бы то ни было языка;
- длина пароля не может быть менее 8 символов;
- один и тот же пароль не может быть использован для доступа к разным ресурсам;
- старый пароль не должен использоваться повторно;
- пароль должен меняться как можно чаще.

Идентификация - процедура распознавания пользователя (процесса) по его имени.

Аутентификация - процедура проверки подлинности пользователя, аппаратуры или программы для получения доступа к определенной информации или ресурсу.

Криптографические методы защиты

Привязка программ и данных к конкретному компьютеру (сети или ключу)

Методы защиты сетей

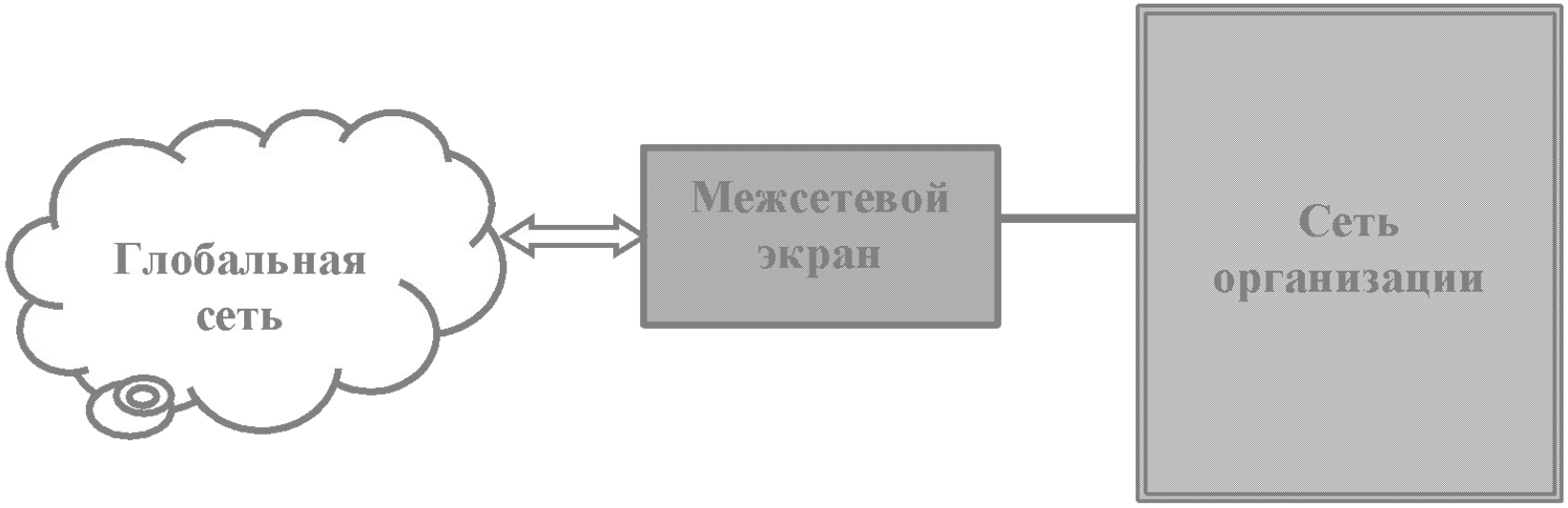
Разграничение прав доступа пользователей к ресурсам сети

Использование заложенных в ОС возможностей защиты

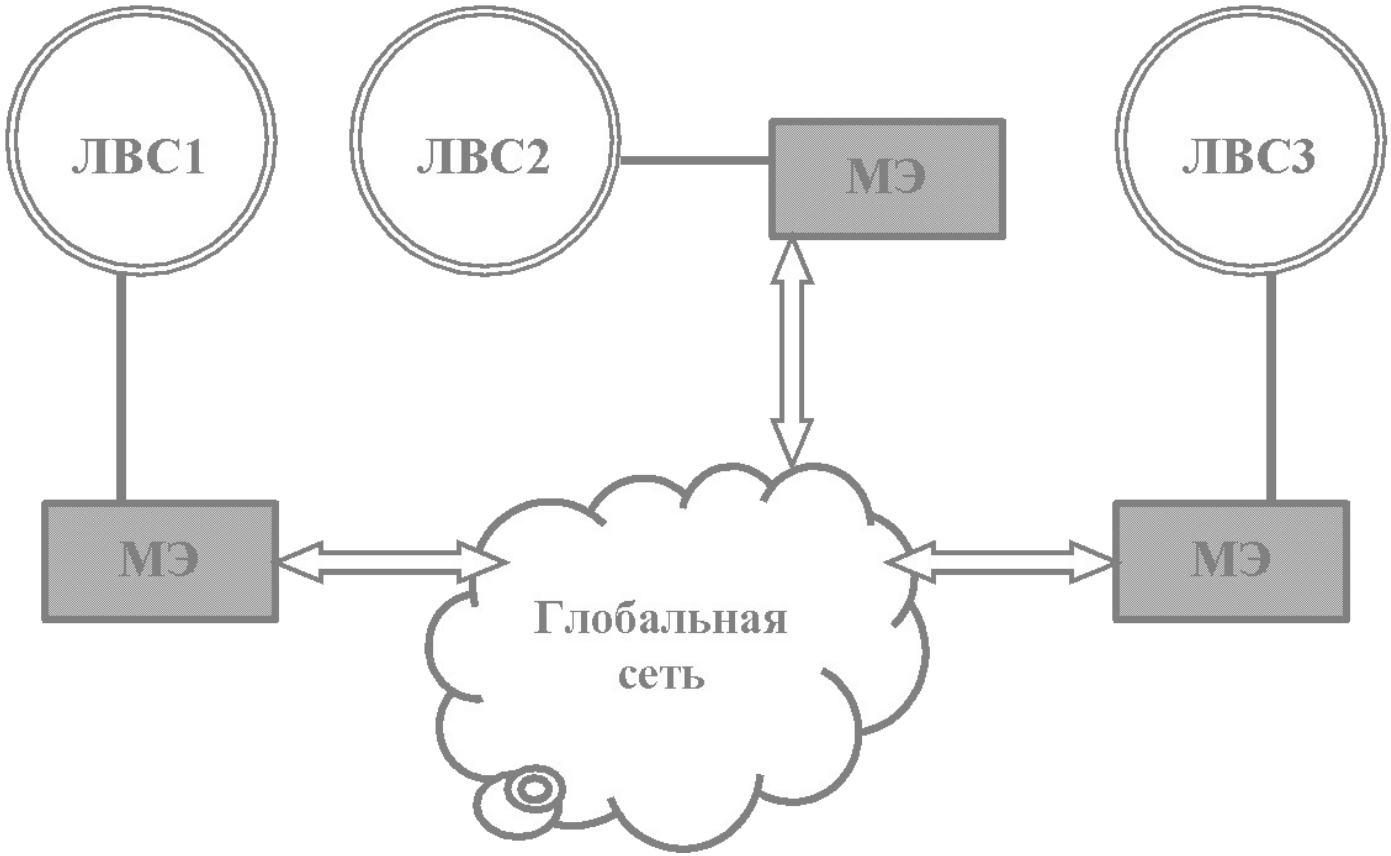
Архитектурные методы защиты

- физическая изоляция закрытого сегмента внутренней сети, содержащего конфиденциальную информацию, от внешней сети;
- функциональное разделение внутренней сети на подсети, при котором в каждой подсети работают пользователи, объединенные по профессиональным интересам;
- сеансовое (кратковременное) подключение внутренней сети к сегменту сети, подключенному к Internet, с помощью коммутатора или моста

Межсетевой экран (брандмауэр, firewall) - это программная или программно-аппаратная система межсетевой защиты, позволяющая разделить две (или более) взаимодействующие сети и реализовать набор правил, определяющих условия прохождения пакетов из одной сети в другую.

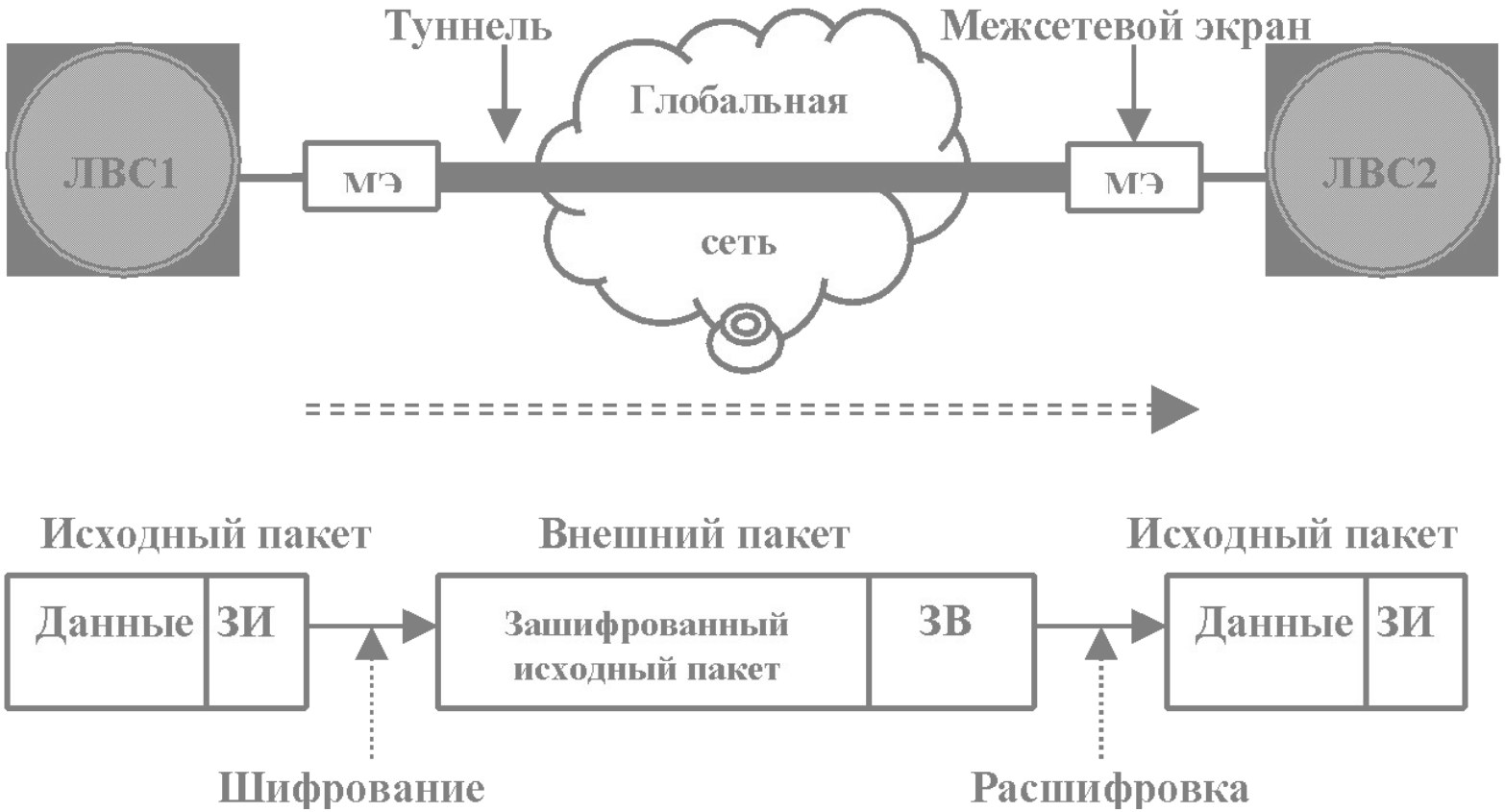


Методы защиты сетей



Построение защищенных виртуальных частных сетей VPN (Virtual Private Networks).

Защищенной виртуальной сетью VPN называют соединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность данных.



Виды рисков:

1. **Хищение услуг.** Злоумышленник может получить доступ к Интернету.
2. **Отказ в услугах.** Хакер может стать источником большого количества запросов на подключение к сети, в результате чего затруднить подключение законных пользователей.
3. **Хищение или разрушение данных.** Злоумышленник, подключившись к сети, может получить доступ к файлам и папкам, а следовательно получить возможность копирования, модификации и удаления.
4. **Перехват контроля над сетью.** Злоумышленник, используя слабые места в системе безопасности, может внедрить троянского коня или назначить такие права доступа, которые могут привести к незащищенности компьютера от атак из сети Интернет.

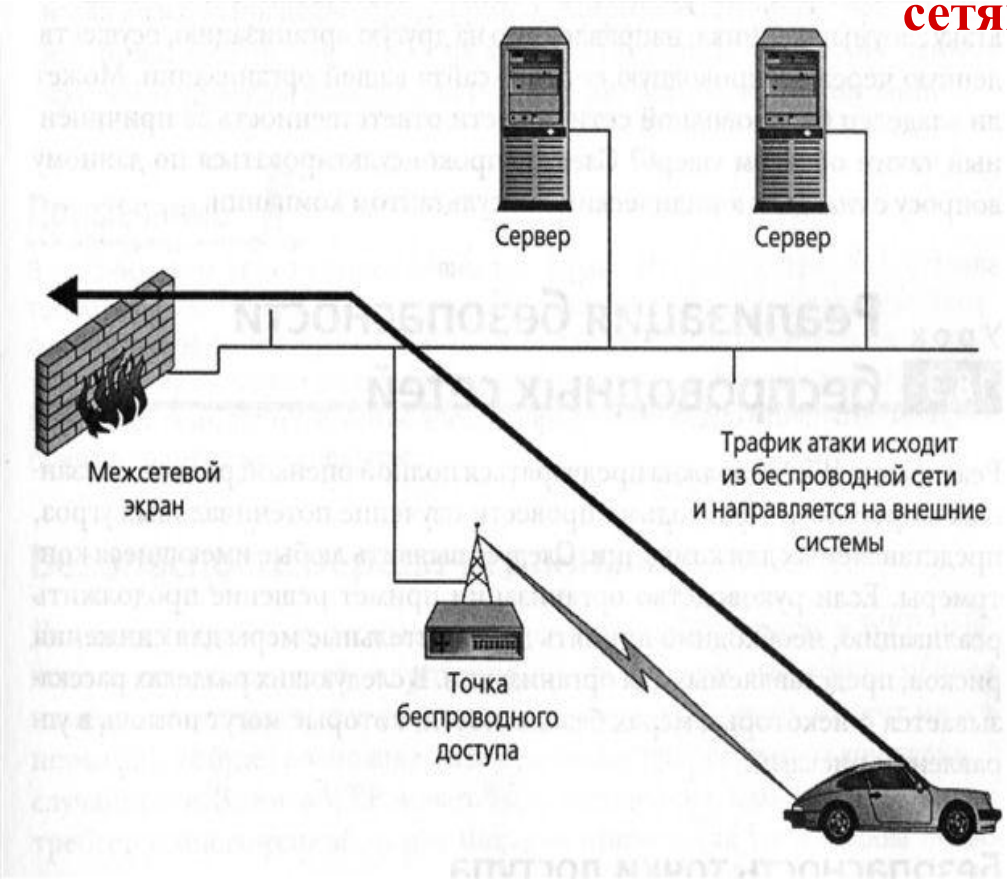
Спецификации беспроводных сетей: группа 802.11x института IEEE.
Web-сайты группы:
www.ieee802.org/11 **www.wi-fi.ogr**

Протокол безопасности уровня передачи данных WEP
(Wired Equivalent Privacy — секретность, эквивалентная проводным сетям)

Беспроводные сети. Проблемы с защитой информации

«На сегодняшний день не предложено ни одного действенного метода защиты для обеспечения полного управления рисками, связанными с беспроводными сетями»

Э. Мэйволд, «Безопасность сетей»



Угрозы безопасности

1. **Несанкционированный доступ к ресурсам корпоративной сети**
2. **Внедрение вредоносных программ**
3. **Использование сети для атак на другие сети**
   (2 уголовных дела в СамГУ)

Дополнительные меры безопасности:

1. Избегать соединения беспроводной сети с проводной ЛВС. Беспроводная точка доступа подключается к маршрутизатору или к интерфейсу брандмауэра.

2. Для реализации беспроводных соединений использовать виртуальные частные сети (VPN).

3. Использовать инструментальные средства сканирования для проверки сети на предмет наличия уязвимых мест в системе безопасности.

4. Регулярно проверять журнал регистрации подключений для контроля всех сетевых подключений.

Нормативная база

Информационная сфера - одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающихся в адекватном правовом регулировании.

Принятые во второй половине 90-х годов законодательные акты уже не отвечают современному состоянию общественных отношений и реалиям использования информационных технологий и информационно-телекоммуникационных сетей, по отдельным вопросам вступают в противоречие с более поздними актами, тормозят развитие информационного общества.

Нормативная база

Статья 15 Конституции РФ:
«Общепризнанные принципы и нормы международного права и международные договоры РФ являются составной частью ее правовой системы.
Если международным договором РФ установлены иные правила, чем предусмотренные законом, то применяются правила международного договора».

Международный уровень

1. **«Конвенция, учреждающая Всемирную организацию интеллектуальной собственности»** (Стокгольм, 1967. Вступила в силу для СССР 26.04.1970).
2. **«Всемирная конвенция об авторском праве»** (Женева, 1952. Пересмотрена в Париже 1971. Вступила в силу для СССР 27.05.1973).
3. **«Бернская конвенция об охране литературных и художественных произведений в редакции 1971 года».** РФ присоединилась 13.03.1995.
4. **«Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных».** Страсбург, 1998. Ратифицирована Законом РФ от 19.12.2005 № 160-ФЗ.
5. **«Окинавская Хартия глобального информационного общества»** Окинава. 22 июля 2000 года.
6. **Декларация принципов. «Построение информационного общества – глобальная задача в новом тысячелетии»**. Всемирная встреча на высшем уровне по вопросам информационного общества. Женева. 10.12.2003.
7. **«Международная конвенция об охране прав исполнителей, изготовителей фонограмм и вещательных организаций»** (Рим, 1961. Вступила в силу для Российской Федерации 26.05.2003).
8. **«Конвенция об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм»** (Женева, 1971. Вступила в силу для Российской Федерации 13.03.1995).

Нормативная база

Конвенция Совета Европы о компьютерных преступлениях. СДСЕ № 185. (Будапешт. Открыта для подписания 23.11.2001, вступила в силу 1.07.2004. Не подписана Российской Федерацией).

ЗАРУБЕЖНЫЕ НОРМАТИВЫ:

“Оранжевая книга" – гос. стандарт США "Критерии оценивания безопасности надежных вычислительных систем" (1984г.);

“Европейские критерии безопасности информационных технологий”;

“Федеральные критерии безопасности информационных технологий США”;

“Канадские критерии безопасности компьютерных систем”;

“Единые критерии оценивания безопасности информационных технологий”.

Единый международный стандарт оценивания безопасности информационных технологий (ISO 15408: 1999)

Нормативная база

Концептуальные документы РФ

1. **«Конституция Российской Федерации»** от 12.12.1993.
2. **«Доктрина информационной безопасности Российской Федерации»**. Утверждена Указом Президента РФ от 9.09.2000 № Пр-1895.
3. **«Концепция национальной безопасности Российской Федерации»** Утверждена Указом Президента РФ от 10.01.2000 № 24.
4. **«Концепция использования информационных технологий в деятельности федеральных органов государственной власти до 2010 года»**. Распоряжение Правительства РФ от 27.09.2004 № 1244-р.
5. **«Концепции создания системы персонального учета населения Российской Федерации».** Утверждена Распоряжением Правительства РФ от 9.06.2005 № 748-р.
6. **«Концепция региональной информатизации до 2010 года».** Одобрена распоряжением Правительства РФ от 17.07.2006 № 1024-р.
7. **«Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».** Утвержден решением Гостехкомиссии от 30.03.1992.
8. **Стратегия развития информационного общества в России.** Утверждена Советом Безопасности Российской Федерации 25.07.2007 г.

Нормативная база

Федеральные Законы

1. **«О средствах массовой информации» от 27.12.1991 № 2124-1**
   (с последними изменениями от 16.10.2006).
2. **«Об оперативно-розыскной деятельности» от 12.08.1995**
   (с последними изменениями от 02.12.2005).
3. **«Уголовный кодекс Российской Федерации» от 13.06.1996**
   (с последними изменениями и дополнениями от 09.04.2007)
4. **«О лицензировании отдельных видов деятельности» от 8.08.2001**
   (с последними изменениями и дополнениями от 05.02.2007).
5. **«Кодекс РФ об административных правонарушениях»** от 30.12.2001
   (с последними изменениями от 20.04.2007).
6. **«Трудовой Кодекс Российской Федерации»** от 30.12.2001
   (с последними изменениями от 30.12.2006).
7. **«Об электронной цифровой подписи»** от 10.01.2002.
8. **«О техническом регулировании»** от 27.12.2002 (с изм. от 9.05.2005).
9. **«О персональных данных»** от 27.07.2006 № 152-ФЗ.
10. **«О рекламе»** от 13.03.2006 (с изменениями от 09.02.2007).

Нормативная база

Федеральные Законы

11. «Гражданский кодекс Российской Федерации» от 30.11.1994
(ч. 4 вступила в силу с 1 января 2008 года)

Утратили силу законы:

от 23.09.1992 № 3520-1 "О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров"

от 23.09.1992 № 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных"

от 23.09.1992 № 3526-1 "О правовой охране топологий интегральных микросхем"

от 9.07.1993 № 5351-1 “Об авторском праве и смежных правах”

от 23.09.1992 № 3517-1 «Патентный закон»

12. «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Утратили силу законы:

«Об информации, информатизации и защите информации» от 20.02.1995

«Об участии в международном информационном обмене» от 4.06.1996

Составляющие авторского права

Права

Личные

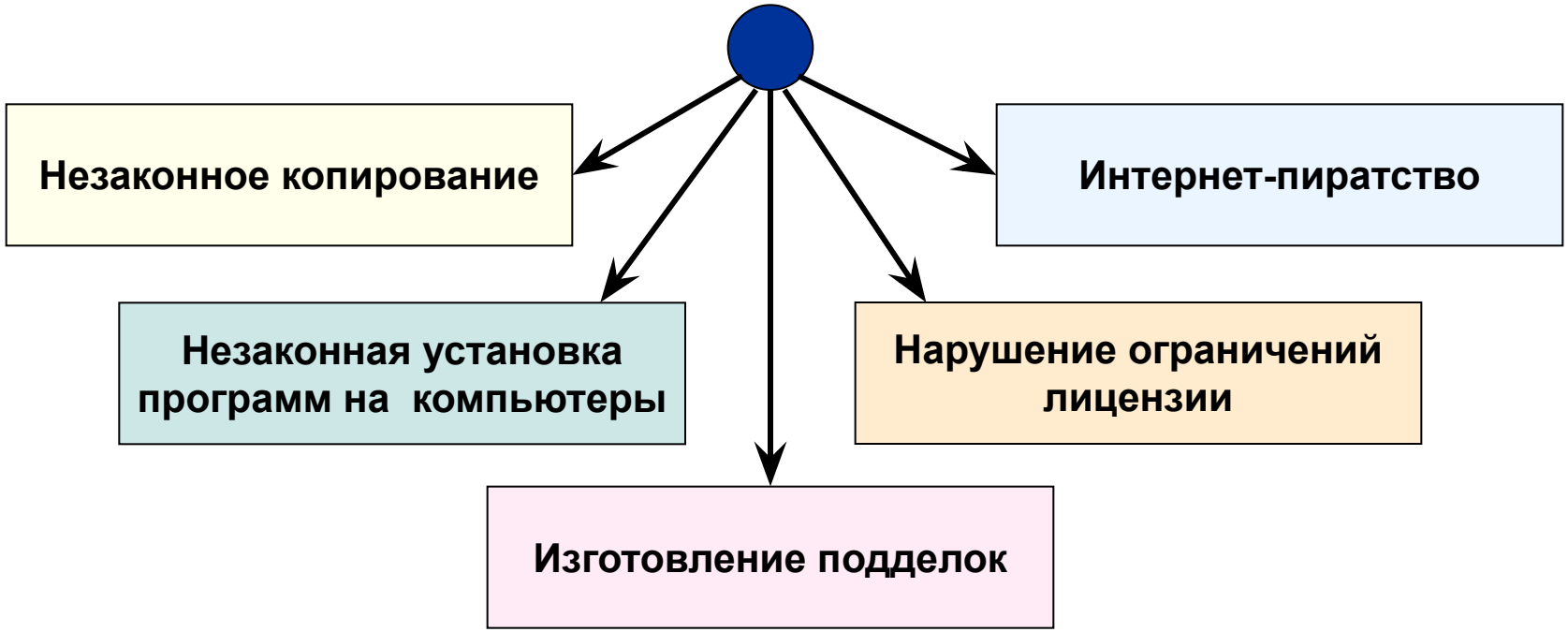
- Право авторства.
- Право на имя.
- Право на целостность.

Имущественные

- Выпуск в свет.
- Воспроизведение.
- Распространение.
- Иное использование.

Все действия без согласия правообладателя незаконны!

Компьютерное пиратство



Экземпляры программ для ЭВМ или базы данных, изготовленные (введенные в хозяйственный оборот) с нарушением авторских прав, называются **контрафактными**.

Ответственность, предусмотренная законом

Уголовная ответственность	1. непосредственный нарушитель 2. должностное лицо (руководитель) **Уголовный Кодекс РФ**
Административная ответственность	1. непосредственный нарушитель 2. должностное лицо (руководитель) 3. юридическое лицо **Кодекс РФ об административных правонарушениях**
Гражданско-правовая ответственность	1. непосредственный нарушитель (суд общей юрисдикции) 2. юридическое лицо (арбитражный суд) **Гражданский Кодекс РФ**

Нормативная база

«Окинавская Хартия глобального информационного общества» 22.07.2000 г.

Информационно-коммуникационные технологии являются одним из наиболее важных факторов, влияющих на формирование общества двадцать первого века.

Основные принципы:

защита прав интеллектуальной собственности на ИТ;

обязательство правительств использовать только лицензированное программное обеспечение;

защиты частной жизни при обработке личных данных.

Усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства.

Содействовать использованию бесплатного, общедоступного информационного наполнения и открытых для всех пользователей программных средств, соблюдая при этом права на интеллектуальную собственность.

Содействие подготовке специалистов в сфере ИТ, а также в нормативной сфере.

http://www.russianlaw.net/law/acts/z8.htm

Нормативная база

«Всемирная конвенция об авторском праве»
Постановление Правительства РФ от 3 ноября 1994 г. N 1224
«О присоединении Российской Федерации к Бернской конвенции об охране литературных и художественных произведений от 9 сентября 1886 г., пересмотренной в Париже 24 июля 1971 г. и измененной 2 октября 1979 г., Всемирной конвенции об авторском праве, пересмотренной в г. Париже 24 июля 1971 г., и дополнительным Протоколам 1 и 2, Конвенции от 29 октября 1971 г. об охране интересов производителей фонограмм от незаконного воспроизводства их фонограмм».

Каждое Договаривающееся Государство обязуется принять все меры по обеспечению соответствующей и эффективной охраны прав авторов и других лиц, обладающих авторским правом, на литературные, научные и художественные произведения.

Срок охраны произведений, предоставляемой в соответствии с Конвенцией, не может быть короче периода, охватывающего время жизни автора и двадцать пять лет после его смерти.

Нормативная база

Конституция Российской Федерации определяет базовые принципы общественных отношений в информационной сфере.

Статья 15. Любые нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина, не могут применяться, если они не опубликованы официально для всеобщего сведения.

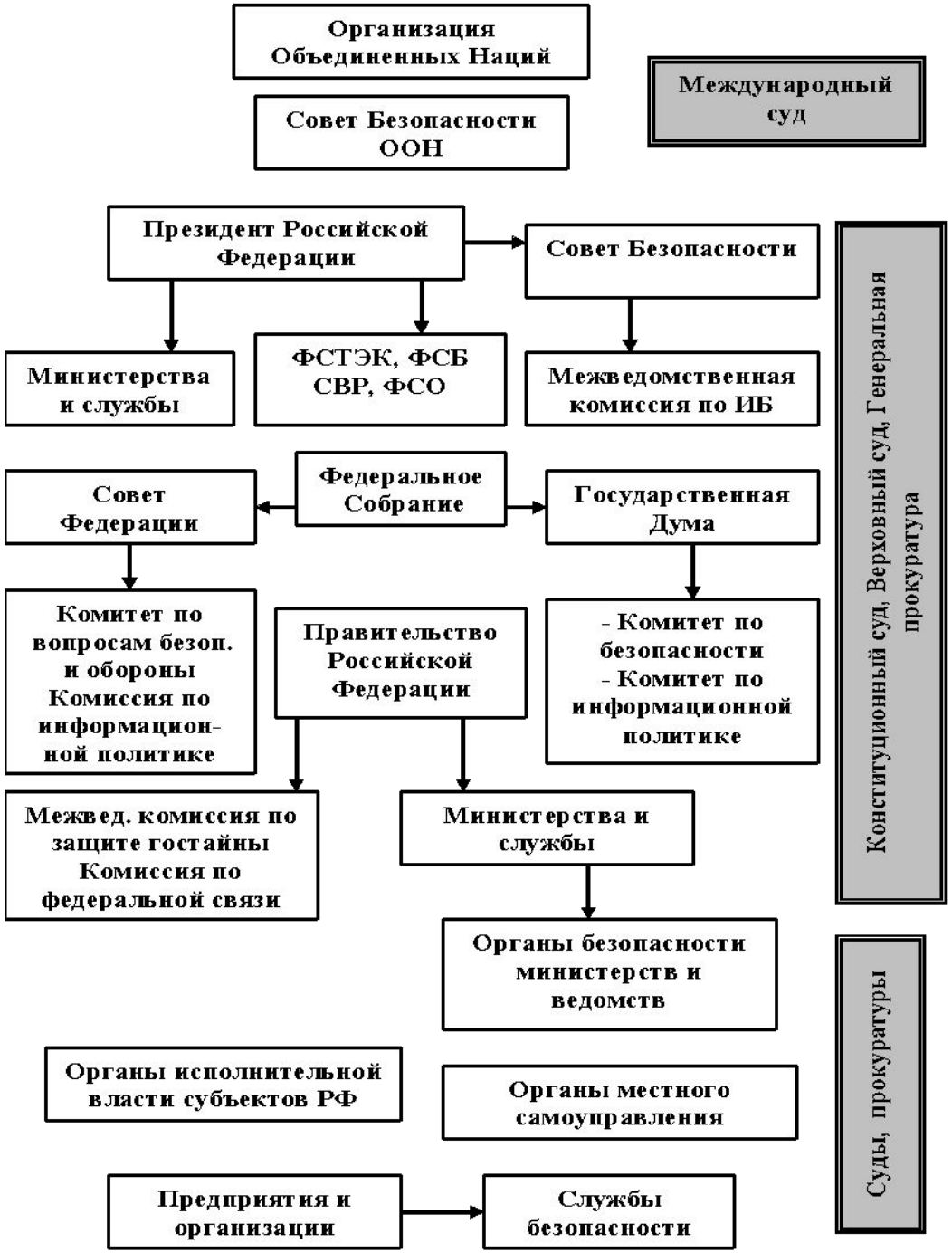
Статья 23. Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени.

Статья 24. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются.

Статья 29. Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом. Гарантируется свобода массовой информации. Цензура запрещается.

Статья 44. Интеллектуальная собственность охраняется законом.

Органы обеспечения ИБ



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

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)

Нормативная база

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.

Нормативная база

- 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.

ЗАРУБЕЖНЫЕ НОРМАТИВЫ:

“Оранжевая книга" – гос. стандарт США "Критерии оценивания безопасности надежных вычислительных систем" (1984г.);

“Европейские критерии безопасности информационных технологий”;

“Федеральные критерии безопасности информационных технологий США”;

“Канадские критерии безопасности компьютерных систем”;

“Единые критерии оценивания безопасности информационных технологий”.

Единый международный стандарт оценивания безопасности информационных технологий (ISO 15408: 1999)

Нормативная база

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 г. создана **Федеральная служба по техническому и экспортному Контролю (ФСТЭК)**, которая является преемником Государственной технической комиссии.

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.

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

Виды информации

5351-1 – Об авторском праве и смежных правах

3517-1 – Патентный закон

152-ФЗ – О персональных данных

5487-1 – Об основах законодательства РФ об охране здоровья граждан

395-1 – О банках и банковской деятельности

Новый базовый Закон

«Об информатизации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006.

Утратили силу:

«Об информации, информатизации и защите информации» № 24-ФЗ от 20.02.1995
«Об участии в международном информационном обмене» № 85-ФЗ от 4.06.1996.

Определяет принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации возникающие при:

1) **осуществлении права на поиск, получение, передачу, производство и распространение информации;**
2) **применении информационных технологий;**
3) **обеспечении защиты информации.**

Не распространяется на отношения, возникающие при правовой охране результатов интеллектуальной деятельности.

№ 149-ФЗ

Основные понятия:

Информация - сведения (сообщения, данные) независимо от формы их представления;

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

Информационная система - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

Обладатель информации - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

Доступ к информации - возможность получения информации и ее использования;

Конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

№ 149-ФЗ

Основные понятия:

Предоставление информации - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

Распространение информации - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

Электронное сообщение - информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

Документированная информация - зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

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

Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

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

Обладатель информации, оператор ИС обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

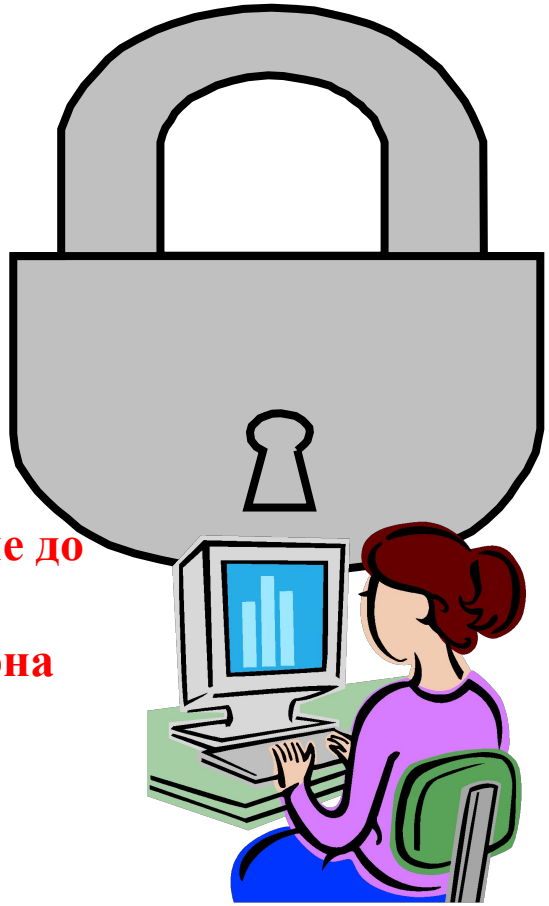
5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Федеральный закон от 19 декабря 2005 года N 160-ФЗ «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных»

Федеральный Закон от 27 июля 2006 года N 152-ФЗ «О персональных данных»

Целью закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.



Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных

Информационные системы персональных данных, созданные до дня вступления в силу закона, должны быть приведены в соответствие с требованиями настоящего Федерального закона не позднее 1 января 2010 года.

N 152-ФЗ Основные понятия:

Персональные данные (ПД) - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПД, а также определяющие цели и содержание обработки ПД;

Обработка ПД - действия (операции) с ПД, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных;

Распространение ПД - действия, направленные на передачу ПД определенному кругу лиц (передача ПД) или на ознакомление с ПД неограниченного круга лиц, в том числе обнародование ПД в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом;

Использование ПД - действия (операции) с ПД, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ПД или других лиц либо иным образом затрагивающих права и свободы субъекта ПД или других лиц;

N 152-ФЗ Основные понятия:

Блокирование ПД - временное прекращение сбора, систематизации, накопления, использования, распространения ПД, в том числе их передачи;

Уничтожение ПД - действия, в результате которых невозможно восстановить содержание ПД в информационной системе ПД или в результате которых уничтожаются материальные носители персональных данных;

Обезличивание ПД - действия, в результате которых невозможно определить принадлежность ПД конкретному субъекту персональных данных;

Информационная система ПД-информационная система, представляющая собой совокупность ПД, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПД с использованием средств автоматизации или без использования таких средств;

Конфиденциальность ПД - обязательное для соблюдения оператором или иным получившим доступ к ПД лицом требование не допускать их распространения без согласия субъекта ПД или наличия иного законного основания;

Трансграничная передача ПД - передача ПД оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства;

Общедоступные ПД - ПД, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта ПД или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Постановление Правительства от 17 ноября 2007 г. N 781
«ОБ УТВЕРЖДЕНИИ ПОЛОЖЕНИЯ ОБ ОБЕСПЕЧЕНИИ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ»

Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

Методы и способы защиты информации в информационных системах устанавливаются ФСТЭК и ФСБ.

ФСБ и ФСТЭК утвердить в 3-месячный срок нормативные правовые акты и методические документы, необходимые для выполнения требований, предусмотренных Положением.

Приказ ФСТЭК, ФСБ, Мининформсвязи от 13.02.2008 № 55/86/20
«ПОРЯДОК ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ»

ФСТЭК февраль 2008 г. документы «ДСП»:

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.

Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ

Пост. Правительства РФ от 15.09.2008 № 687 **«Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»**

Пост. Правительства РФ от 6.07.2008 № 512 **«Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»**

«Об утверждении образца формы уведомления об обработке персональных данных» (Россвязькомнадзор от 17.07.2008 № 8, от 18.02.2009 № 42)

Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использования средств автоматизации (ФСБ России, 21.02.2008 № 149/54-144)

Типовые требования по организации и обеспечению функционирования шифровальных средств, предназначенных для защиты информации, не содержащей сведений, составляющих гос. тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ФСБ России от 21.02.2008 № 149/6/6-622)

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПД

ИСХОДНЫЕ ДАННЫЕ ДЛЯ КЛАССИФИКАЦИИ:

категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни;

категория 2 - персональные данные, позволяющие идентифицировать субъекта и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;

категория 3 - персональные данные, позволяющие идентифицировать субъекта;

категория 4 - обезличенные и (или) общедоступные персональные данные.

Объем персональных данных (О):

1 - более чем 100 000 субъектов или персональные данные субъектов в пределах субъекта Российской Федерации или Российской Федерации в целом;

2 - от 1000 до 100 000 субъектов или субъектов, работающих в отрасли экономики РФ, в органе гос. власти, проживающих в пределах муниципального образования;

3 - менее чем 1000 субъектов или субъектов в пределах конкретной организации.

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПД

ИСХОДНЫЕ ДАННЫЕ ДЛЯ КЛАССИФИКАЦИИ:

заданные оператором характеристики безопасности персональных данных;
(**типовые**-только конфиденциальность, **специальные-**защищенность от несанкционированных действий)

структура информационной системы;
(автономные, объединенные в единую информационную систему)

наличие подключений информационной системы к сетям связи общего пользования и (или) сетям международного информационного обмена;

режим обработки персональных данных;
(однопользовательские, многопользовательские)

режим разграничения прав доступа пользователей информационной системы;
(с разграничением, без разграничения прав доступа)

местонахождение технических средств информационной системы.
(в пределах Российской Федерации, полностью или частично за пределами)

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПД

Информационные системы, для которых нарушение заданной характеристики безопасности персональных данных:

класс 1 (К1) - может привести к значительным негативным последствиям для субъектов ПД;
класс 2 (К2) - может привести к негативным последствиям для субъектов ПД;
класс 3 (К3) – может привести к незначительным негативным последствиям;
класс 4 (К4) - не приводит к негативным последствиям для субъектов ПД.

Кат \ О	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Результаты классификации информационных систем оформляются соответствующим актом оператора.

КЛАССИФИКАЦИЯ ИНФОРМАЦИОННЫХ СИСТЕМ ПД

Класс информационной системы может быть пересмотрен:

- по решению оператора на основе проведенных им анализа и оценки угроз безопасности с учетом особенностей и (или) изменений ИСПДн;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных.

Порядок оценки соответствия степени защищенности информационных систем требованиям безопасности:

-для информационных систем 1 и 2 класса соответствие степени защищенности устанавливается путем обязательной сертификации (аттестации);

-для информационных систем 3 класса соответствие требованиям безопасности подтверждается путем сертификации (аттестации) или (по выбору оператора) декларированием соответствия, проводимым оператором персональных данных;

-для информационных систем 4 класса оценка соответствия не регламентируется и осуществляется по решению оператора персональных данных.

«Положение о методах и способах защиты информации в информационных системах персональных данных»
Приказ ФСТЭК России от 5.02.2010 № 58

Федеральный закон «О связи» № 126-ФЗ от 7.07.2003
С поправкой от 09.02.2007 № 14-ФЗ

Он заменил собой ранее действовавший Закон «О связи» от 16.02.1995 N 15-ФЗ.

Одной из целей закона является создание условий для развития российской инфраструктуры связи, обеспечение ее интеграции с международными сетями связи

Гражданский Кодекс. Часть 4.
Принята федеральным законом № 230-ФЗ от 18.12.2006

В соответствии с законом № 231-ФЗ от 18.12.2006
Часть 4 ГК вступила в силу с 1 января 2008 года.

Утратили силу:

«О товарных знаках, знаках обслуживания и наименованиях мест происхождения товаров» от 23.09.1992 № 3520-1

«О правовой охране программ для электронных вычислительных машин и баз данных» от 23.09.1992 № 3523-1

«О правовой охране топологий интегральных микросхем» от 23.09. 1992 года № 3526-1

«Об авторском праве и смежных правах» от 9.07.1993 № 5351-1

«Патентный закон» от 23.09.1992 № 3517-1

Гражданский Кодекс. Часть 4.

ПРАВА НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ

Статья 1225 «Результатами интеллектуальной деятельности, которым предоставляется правовая охрана (интеллектуальной собственностью), являются: произведения науки, литературы и искусства; программы для ЭВМ; базы данных; фонограммы. . .»

Статья 1233. Правообладатель может предоставить другому лицу права использования результата интеллектуальной деятельности в установленных договором пределах (лицензионный договор).

Статья 1295. Авторские права на произведение науки, литературы или искусства, созданное в пределах установленных для работника (автора) трудовых обязанностей (служебное произведение), принадлежат автору.

Исключительное право на служебное произведение принадлежит работодателю, если трудовым или иным договором между работодателем и автором не предусмотрено иное.

Если работодатель начнет использование служебного произведения автор имеет право на вознаграждение.

Гражданский Кодекс. Часть 4.

ПРАВА НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ

Статья 1296. **В случае, когда программа для ЭВМ или база данных создана по договору, предметом которого было ее создание, исключительное право на такую программу или такую базу данных принадлежит заказчику, если договором не предусмотрено иное.**

Автор созданных по заказу программы для ЭВМ или базы данных, которому не принадлежит исключительное право, имеет право на вознаграждение.

Статья 1301. **В случаях нарушения исключительного права на произведение автор или иной правообладатель вправе требовать от нарушителя выплаты компенсации:**
в размере от 10 тыс. до 5 млн. рублей, определяемом по усмотрению суда;
в двукратном размере стоимости экземпляров произведения.

Гражданский Кодекс. Часть 4.

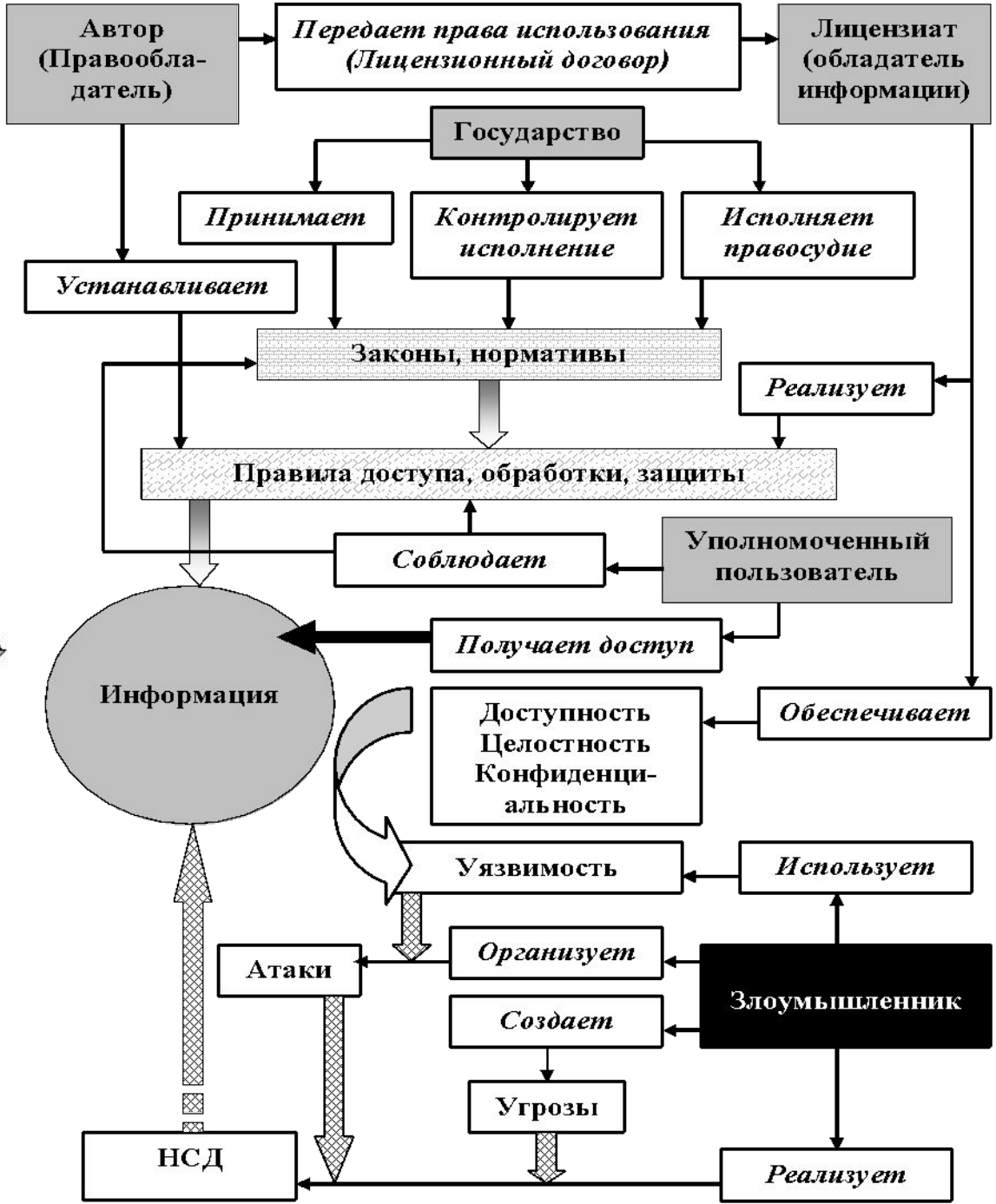
ПРАВА НА РЕЗУЛЬТАТЫ ИНТЕЛЛЕКТУАЛЬНОЙ ДЕЯТЕЛЬНОСТИ И СРЕДСТВА ИНДИВИДУАЛИЗАЦИИ

Статья 1333. Изготовителем базы данных признается лицо, организовавшее создание базы данных и работу по сбору, обработке и расположению составляющих ее материалов.

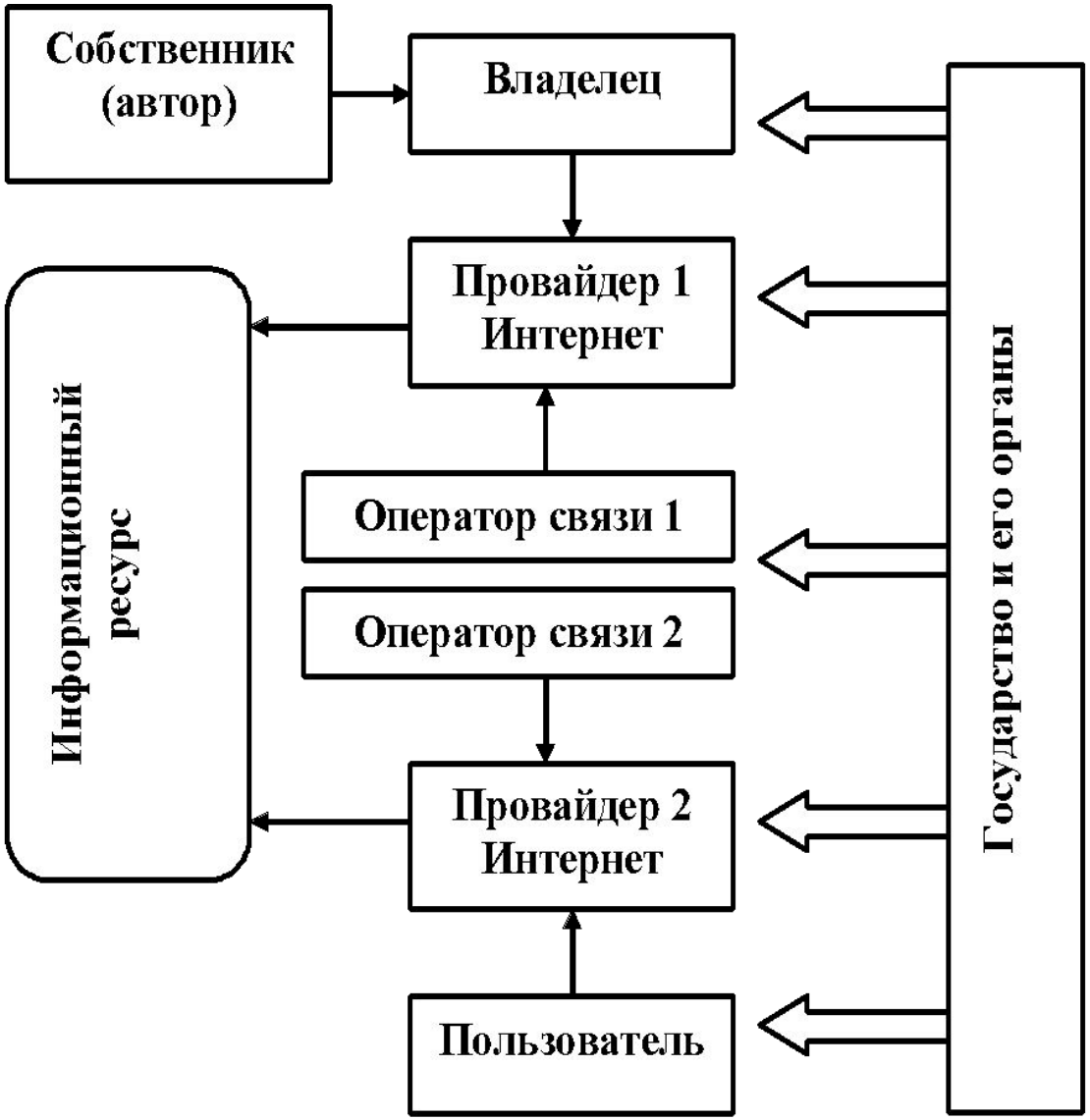
Статья 1334. Никто не вправе извлекать из базы данных материалы и осуществлять их последующее использование без разрешения правообладателя. При этом под извлечением материалов понимается перенос всего содержания базы данных или существенной части составляющих ее материалов на другой информационный носитель с использованием любых технических средств и в любой форме.

Статья 1274. Свободное использование произведения в информационных, научных, учебных или культурных целях. Выраженные в цифровой форме экземпляры произведений, предоставляемые библиотеками во временное безвозмездное пользование, могут предоставляться только в помещениях библиотек при условии исключения возможности создать копии этих произведений в цифровой форме.

Модель отношений субъектов информационных отношений



Модель отношений субъектов информационных отношений в сети Интернет



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»

На сайте http://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 «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.

Система обеспечения безопасности сети (СОБ)

Основные функциональные требования:

Многоуровневость
Распределенность средств защиты по разным элементам сети
Разнородность или разнотипность применяемых средств
Уникальность защиты
Непрерывность развития
Распределение полномочий
Прозрачность и простота
Физическое разделение серверов и рабочих станций
Обеспечение предотвращения несанкционированного доступа
Организация централизованной службы административного управления сети
Организация централизованной службы управления безопасностью сети.

Принципы построения СОБ сети

Две концепции построения защищенной корпоративной сети:

1. Создание СОБ корпоративной сети, построенной на базе каналов связи и средств коммутации общего пользования, в которой применяются открытые протоколы Internet.
2. Отказ от средств Internet, создание корпоративной сети на базе специализированной или выделенной сети связи с использованием конкретной сетевой технологии, в частности ATM, FR, ISDN.

Принцип максимальной дружественности
Принцип прозрачности
Принцип превентивности
Принцип оптимальности
Принцип адекватности
Принцип системного подхода
Принцип адаптивности
Принцип доказательности

Принципы построения СОБ сети

УРОВНИ СОБ:

1. Защита рабочих станций сети.
2. Средства защиты локальной сети.
3. Уровень корпоративной сети (объединение ЛВС).

ЭТАПЫ ПОСТРОЕНИЯ СОБ:

1. Экспертиза защищенности корпоративной информационной системы.
2. Разработка концепции и политики информационной безопасности компании.
3. Проектирование корпоративной системы в защищенном исполнении.
4. Поставка и ввод в опытную эксплуатацию средств защиты.
5. Сопровождение систем информационной безопасности.
6. Модернизация и развитие систем информационной безопасности.

Принципы построения СОБ сети

Общие принципы проектирования СОБ:

Экономическая эффективность
Минимум привилегий
Простота
Постоянство работы
Открытость проектирования и функционирования механизмов защиты
Независимость системы защиты от субъектов защиты
Отчетность и подконтрольность
Личная ответственность лиц, занимающихся обеспечением безопасности
Принцип враждебного окружения
Отсутствие излишней информации