Основы социальной информатики

Информационные ресурсы

«Информационные ресурсы – отдельные документы или отдельные массивы документов, документы или массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах»

Информационные ресурсы – являются стратегическими ресурсами наряду с традиционными.

Однако между информационными ресурсами и всякими иными существует одно важнейшее различие: ***всякий ресурс, кроме информационного, после использования исчезает.***

Традиционными видами общественных ресурсов являются:

- Материальные ресурсы;

Сырьевые (природные)

Энергетические

Трудовые

Финансовые

В основу классификации можно положить:

- Отраслевой принцип (по виду науки, промышленности, социальной сферы и т.п., к чему относится информация);
- Форму представления (по виду носителей, степени формализованности, наличию дополнительного описания и пр.


Национальные информационные ресурсы
Библиотечные ресурсы
Архивные ресурсы
Научно-техническая информация
Правовая информация
Информация государственных (властных) структур
Отраслевая информация
Финансовая и экономическая информация
Информация о природных ресурсах
Информация предприятий и учреждений

Рынок информационных ресурсов

Развитие компьютерных информационных технологий способствует формированию рынка информационных ресурсов.
Товар – информационные продукты и услуги.
Как и на всяком рынке, на рынке информационных товаров и услуг есть свои поставщики(продавцы) и потребители (покупатели).

Поставщики – как правило, это производитель информации или ее собственники.

- **Центры, в которых создаются и хранятся базы данных;**
- **Службы связи и телекоммуникации;**
- **Бытовые службы;**
- **Специализированные коммерческие фирмы, занимающиеся куплей-продажей информацией (рекламные агентства);**
- **Неспециализированные фирм**
  и в качестве дополнительной
- **Консалтинговые фирмы;**
- **Биржи;**
- **Частные лица (программисты**

Потребители это все мы

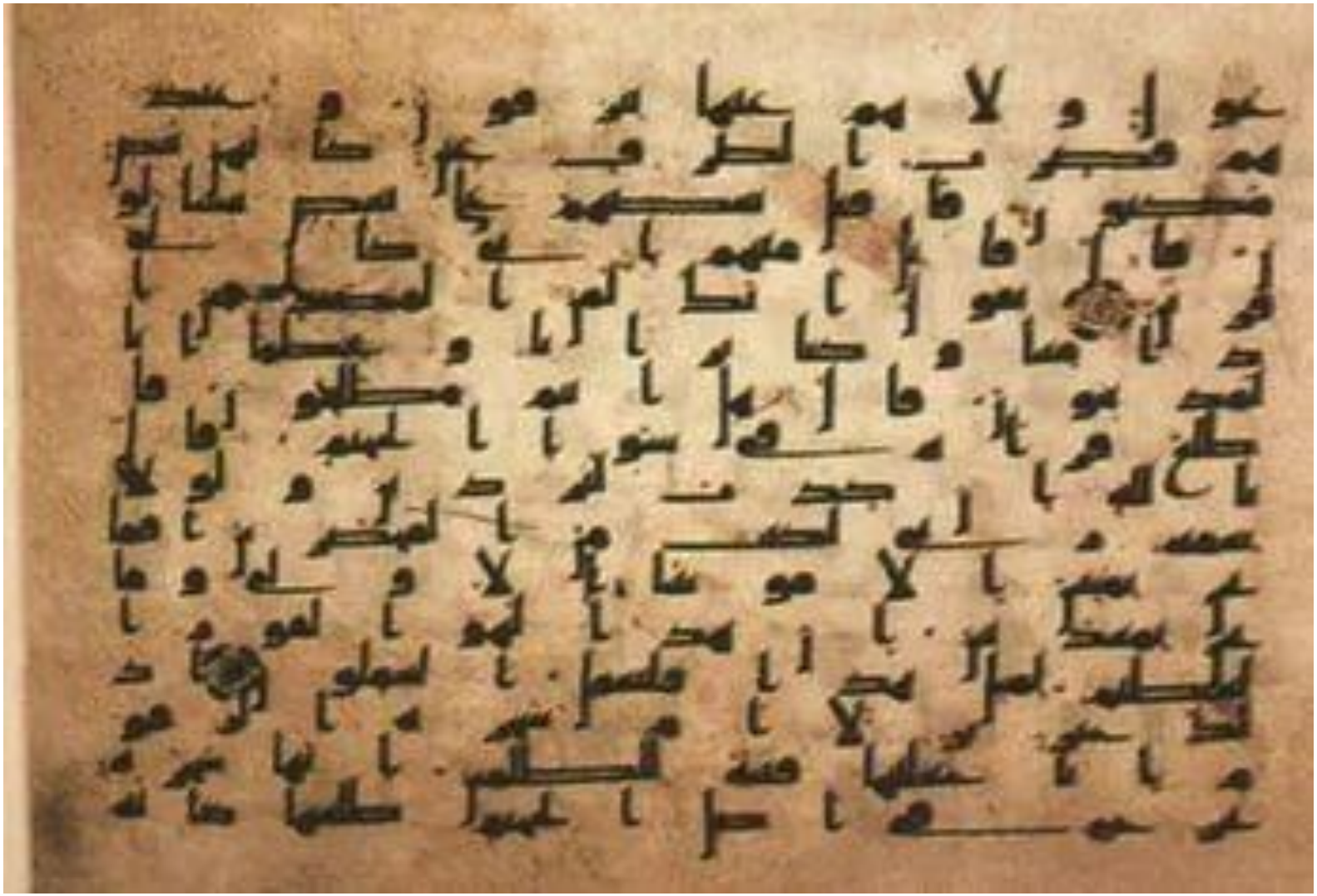
Особый вид товара на информационном рынке – информационные услуги.

- **Поиск и подбор информации;**
- **Консалтинг;**
- **Обучение;**
- **Телекоммуникации;**

Информационное общество.

Информационные революции.

1)Изобретение



2)Изобретением книгопечатания.

3)Прогресс средств связи.

4)Появление микропроцессорной техники и, в частности, ПК…

Основные черты информационного общества.

Четвёртая информационная революция дала толчок к появлению термина – «информационное общество».

Само название впервые возникло в Японии.

Важно, что движение России к информационному обществу реализуется государством как стратегическая, приоритетная цель, достижению которой способствует достаточно высокий кадровый и научно-технический потенциал России.

Развитие и массовое использование информационных и коммуникационных технологий

Бурный рост производства средств вычислительной техники.

- **создание телекоммуникационной инфраструктуры, включающей в себя сети передачи данных;**
- **появление огромных баз данных, доступ к которым через сети получили миллионы людей;**

Скорость роста числа пользователей Сети достаточно устойчиво составляет порядка 20% в год. Первое место по количеству пользователей Интернета занимает США. На втором и третьем местах – Китай и Япония. Россия занимает 11-е место, что является большим прогрессом по сравнению с ситуацией 5 - 10-летней давности.

По некоторым показателям, связанным с Интернетом, наша страна находится в числе лидеров. Так, по числу пользователей оптоволоконными сетями Россия стоит на первом месте в Европе.

Универсализации информационных технологий.

Совершенствование компьютерной техники.

Преодоление информационного кризиса.

Информационный кризис – поток информации, который хлынул на человека, столь велик, что недоступен обработке в приемлемое время.
В результате наступает **информационный кризис**, проявляющийся в следующем:

- информационный поток превосходит ограниченные возможности человека по восприятию и переработке информации;
- возникает большое количество избыточной информации, которая затрудняет восприятие полезной для потребителя информации;
- укрепляются экономические, политические и другие барьеры, которые препятствуют распространению информации.

Частичный выход из информационного кризиса видится в применении новых информационных технологий. Внедрение современных средств и методов хранения, обработки и передачи информации многократно снижает барьер доступа к ней и скорость поиска.

Рост информационной культуры.

Современное понимание информационной культуры заключается в ***умении и потребности человека работать с информацией средствами новых информационных технологий***.

Целенаправленные усилия общества и государства по развитию информационной культуры населения являются обязательными при продвижении по пути к информационному обществу. Одной из важных задач курса информатики является развитие элементов информационной культуры учащихся. Указанная задача носит комплексный характер, она не может быть решена только школой.

Информационная культура должна стать частью общечеловеческой культуры. Культурный человек должен уметь оценивать получаемую информацию качественно, понимать её полезность, достоверность и т.д.

Опасности информационного общества.

Противоречия.

проблемы на пути к информационному обществу:

- **реальная возможность разрушения посредством информационных технологий частной жизни людей и организаций4**
- **опасность всё большего влияния на общество средств массовой информации и тех, кто эти средства контролирует;**
- **проблема отбора качественной и достоверной информации при большом её объёме;**
- **проблема адаптации многих людей к среде информационного общества, к необходимости постоянно повышать свой профессиональный уровень;**
- **столкновение с виртуальной реальностью, в которой трудноразличимы иллюзия и действительность, создаёт у некоторых людей, особенно молодых, малоизученные, но явно неблагоприятные психологические проблемы;**
- **сокращение числа рабочих мест в экономике развитых стран, не компенсируемое полностью созданием новых рабочих мест в**

Правовое регулирование в информационной сфере

Правовое регулирование в информационной сфере является новой и сложной задачей для государства.

В Российской Федерации существует ряд законов в этой области.

Федеральный закон **«0 правовой охране программ для ЭВМ и баз данных »**

принятый в **1996 г.**

Автор имеет право на выпуск в свет программ и баз данных , их распространение , модификацию и иное использование .

Федеральный закон **«0б информации, информационных технологиях и защите информации »**

Принятый в **2006 г.**

регулирует отношения , возникающие при осуществлении права на поиск , получение, передачу, производство и распространение информации; при применении информационных технологий ; обеспечении защиты информации .

Закон разрешает :

1) свобода поиска, получения , передачи, производства и распространения информации любым законным способом ;
2)установление ограничений доступа к информации только федеральными законами;
3)открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации , кроме случаев, установленных федеральными законами ;
4) равноправие языков народов Российской Федерации.
5) неприкосновенность частной жизни.

Федеральный закон **«Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления »**
(2009 г.).

Принципы:

1) открытость и доступность информации о деятельности государственных органов и органов местного самоуправления, за исключением случаев, предусмотренных федеральным законом ;

2) достоверность информации
3) свободу поиска

4) соблюдение прав граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту их чести и деловой репутации

Федеральный закон **« 0 персональных данных »** (2006 г.)

регулирует отношения , связанные с обработкой персональных данных

Согласно закону, сбор и обработка персональных данных каждого гражданина в подавляющем большинстве случаев могут осуществляться только с его письменного согласия . Цель закона - обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных.

Федеральный закон **«Об электронной подписи »**

Как известно , любой документ недействителен без подписи ответственных лиц, однако в электронном виде (путем передачи, например , отсканированного текста) такая подпись не может быть полноценной заменой подписи на бумажном документе. При электронной подписи используются : **а)** ключ электронной подписи - уникальная последовательность символов , предназначенная для создания электронной подписи;

б) ключ проверки электронной подписи - уникальная последовательность сим волов, однозначно связанная с ключом электронной подписи и предназначенная для проверки подлинности электронной подписи. Право на выдачу таких ключей имеют только специально уполномоченные государством органы.

Нарушения законов в сфере информации предусматривают как гражданско-правовую, так и уголовную ответственность.

В 1996 г. в Уголовный кодекс был впервые внесен раздел **«Преступления в сфере компьютерной информации ».** Он определил меру наказания за некоторые виды преступлений , ставших , к сожалению, распространенными:

За неправомерный доступ к компьютерной информации , повлекший уничтожение , блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети , предусматривается наказание в виде штрафа в размере до пятисот минимальных размеров оплаты труда либо лишения свободы на срок до двух лет . То же деяние, совершенное организованной группой либо лицом с использованием своего служебного положения , наказывается штрафом в размере до восьмисот минимальных размеров оплаты труда либо лишением свободы на срок до пяти лет.

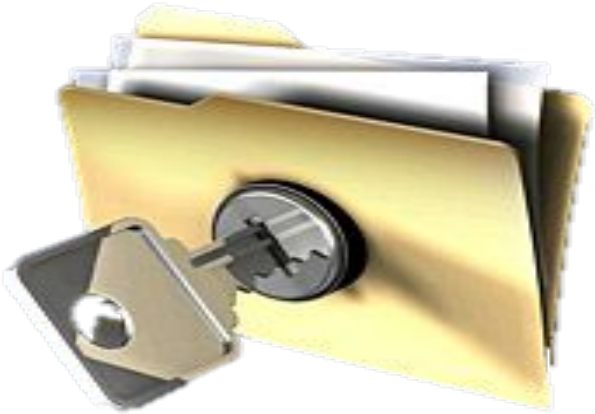
За создание вредоносных программ для ЭВМ можно получить лишение свободы на срок до 3 лет , а при наличии тяжких последствий - до 7 лет .

Указанными преступлениями уголовно наказуемая деятельность в сфере информационных технологий не ограничивается.

Взлом паролей , кража номеров кредитных карточек и других банковских реквизитов, распространение противоправной информации (клеветы , материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т. п.) **через Интернет** - всё это преступная деятельность , наказание за которую может быть гораздо более жестким, чем перечисленные выше.

Информационная безопасность

Под ***информационной безопасностью*** понимается защищенность информационной системы от случайного или преднамеренного вмешательства, наносящего ущерб владельцам или пользователям информации.

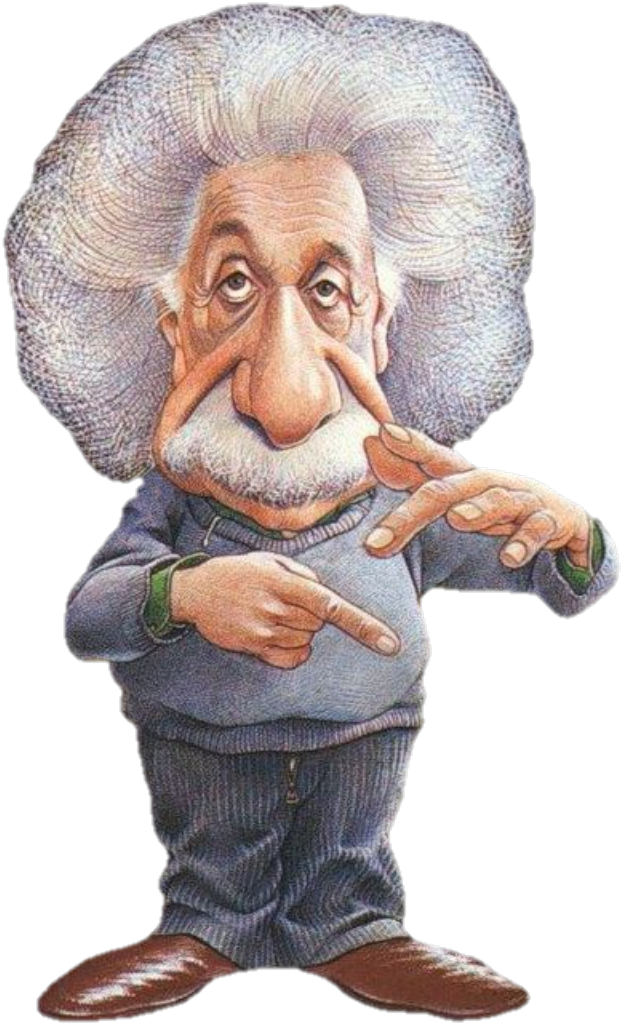


На практике важнейшими являются **три аспекта** информационной безопасности:

- **доступность** (возможность за разумное время получить требуемую информационную услугу);
- **целостность** (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);
- **конфиденциальность** (защита от несанкционированного прочтения).

Методы и средства информационной безопасности

Методами обеспечения защиты информации в организации являются:



- **Препятствие** – метод физического преграждения пути злоумышленнику к защищаемой информации (сигнализация, замки и т. д.).

- **Управление доступом** – метод защиты информации, связанный с регулированием использования всех ресурсов информационной системы. УД включает следующие функции защиты:
  - ***идентификацию сотрудников*** и ресурсов информационной системы;
  - ***аутентификацию*** (установления подлинности) объекта по предъявленному им идентификатору (имени). Как правило, к таким средствам относятся пароли;
  - ***проверку полномочий*** - авторизация пользователей;

- **Маскировка** – метод защиты информации в информационной системе организации путем ее криптографического закрытия.
- **Регламентация** – метод защиты информации, создающий определенные условия автоматизированной обработки, хранения и передачи информации, при которых возможность несанкционированного доступа к ней (сетевых атак) сводилась бы к минимуму.

- **Принуждение** – метод защиты, при котором пользователи системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной и уголовной ответственности.
- **Побуждение** – метод защиты информации, который мотивирует сотрудников не нарушать установленные правила за счет соблюдения сложившихся моральных и этических норм.

Средства защиты информации

Основными средствами защиты являются: физические, аппаратные, программные, аппаратно-программные, криптографические, организационные, законодательные и морально-этические.

Физические средства защиты предназначены для внешней охраны территории объектов и защиты компонентов информационной системы организации.

Аппаратные средства защиты – это устройства, встроенные в блоки информационной системы (сервера, компьютеры и т.д.). Они предназначены для внутренней защиты элементов вычислительной техники и средств связи

Программные средства защиты предназначены для выполнения функций защиты информационной системы с помощью программных средств (Антивирусная защита, Межсетевые экраны и т.д.)

Аппаратно-программные средства защиты.

- *Криптографические средства* – средства защиты информации, связанные с применением инструментов шифрования.
- *Организационные средства* – мероприятия регламентирующие поведение сотрудника организации.
- *Законодательные средства* – правовые акты, которые регламентирующие правила использования, обработки и передачи информации и устанавливающие меры ответственности.
- *Морально-этические средства* – правила и нормы поведения сотрудников в коллективе.

Аппаратно-программные средства защиты

можно разбить на пять групп:

1. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.
2. Системы шифрования дисковых данных.
3. Системы шифрования данных, передаваемых по сетям.
4. Системы аутентификации электронных данных.
5. Средства управления криптографическими

1. Системы идентификации (распознавания) и аутентификации (проверки подлинности) пользователей.

Применяются для ограничения доступа случайных и незаконных пользователей к ресурсам компьютерной системы. Общий алгоритм работы заключается в полчении от пользователя информацию, удостоверяющую его личность, проверить ее подлинность и затем предоставить (или не предоставить) этому пользователю возможность работы с системой.

Выделяют следующие типы:

- секретная информация, которой обладает пользователь (*пароль, секретный ключ*, персональный идентификатор и т.п.); пользователь должен запомнить эту информацию или же для нее могут быть применены специальные средства хранения;
- физиологические параметры человека (*отпечатки пальцев*, рисунок радужной оболочки глаза и т.п.) или особенности поведения (особенности работы на

2. Системы шифрования дисковых данных

Чтобы сделать информацию бесполезной для противника, используется совокупность методов преобразования данных, называемая криптографией [от греч. **kryptos** - скрытый и grapho - пишу].

- Системы шифрования могут осуществлять криптографические преобразования данных на уровне файлов или на уровне дисков. К программам первого типа можно отнести архиваторы типа ARJ и RAR, которые позволяют использовать криптографические методы для защиты архивных файлов. Примером систем второго типа может служить программа шифрования Diskreet, входящая в состав популярного программного пакета Norton Utilities, Best Crypt.

Большинство систем, предлагающих установить пароль на документ, *не шифрует информацию*, а только обеспечивает запрос пароля при доступе к документу.

К таким системам относится MS Office, 1С и многие другие.

3. Системы шифрования данных, передаваемых по сетям

Различают два основных способа шифрования:

- *канальное шифрование*
- *Оконечное* (абонентское) шифрование.

В случае канального шифрования

защищается вся информация, передаваемая по каналу связи, включая служебную. Этот способ шифрования обладает следующим достоинством - встраивание процедур шифрования на канальный уровень позволяет использовать аппаратные средства, что способствует повышению производительности системы.

Однако у  меются и существенные недостатки.

Оконечное (абонентское) шифрование

позволяет обеспечить конфиденциальность данных, передаваемых между двумя абонентами.

В этом случае защищается только содер сообщений, вся служебная информация остается открытой.

Недостатком является возможность анализировать информацию о структуре обмена сообщениями, например об отправителе и получателе, о времени и

4. Системы аутентификации электронных данных

При обмене данными по сетям возникает проблема аутентификации автора документа и самого документа, т.е. установление подлинности автора и проверка отсутствия изменений в полученном документе. Для аутентификации данных применяют код аутентификации сообщения (имитовставку) или электронную подпись.

- **Имитовставка** вырабатывается из открытых данных посредством специального преобразования шифрования с использованием секретного ключа и передается по каналу связи в конце зашифрованных данных. Имитовставка проверяется получателем, владеющим секретным ключом, путем повторения процедуры, выполненной ранее отправителем, над полученными открытыми данными.
- **Электронная цифровая подпись** представляет собой относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом. Отправитель формирует цифровую подпись, используя секретный ключ отправителя. Получатель проверяет подпись, используя открытый ключ отправителя.

Таким образом, для реализации имитовставки используются принципы симметричного шифрования, а для реализации электронной подписи - асимметричного. Подробнее эти две системы шифрования будем изучать позже.

5. Средства управления криптографическими ключами

Безопасность любой криптосистемы определяется используемыми криптографическими ключами. В случае ненадежного управления ключами злоумышленник может завладеть ключевой информацией и получить полный доступ ко всей информации в системе или сети. Различают следующие виды функций управления ключами: **генерация, хранение, и распределение ключей.**

- Способы генерации ключей для симметричных и асимметричных криптосистем различны. Для генерации ключей симметричных криптосистем используются аппаратные и программные средства генерации случайных чисел. Генерация ключей для асимметричных криптосистем более сложна, так как ключи должны обладать определенными математическими свойствами. Подробнее на этом вопросе остановимся при изучении симметричных и асимметричных криптосистем.
- Функция хранения предполагает организацию безопасного хранения, учета и удаления ключевой информации. Для обеспечения безопасного хранения ключей применяют их шифрование с помощью других ключей. Такой подход приводит к концепции иерархии ключей. В иерархию ключей обычно входит главный ключ (т.е. мастер-ключ), ключ шифрования ключей и ключ шифрования данных. Следует отметить, что генерация и хранение мастер-ключа является критическим вопросом криптозащиты.
- Распределение - самый ответственный процесс в управлении ключами. Этот процесс должен гарантировать скрытность распределяемых ключей, а также быть оперативным и точным.

Между пользователями сети ключи распределяют двумя способами:

- с помощью прямого обмена сеансовыми ключами;

Перечень документов

1. О ГОСУДАРСТВЕННОЙ ТАЙНЕ. Закон Российской Федерации от 21 июля 1993 года № 5485-1 (в ред. Федерального закона от 6 октября 1997 года № 131-ФЗ).

2. ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ. Федеральный закон Российской Федерации от 20 февраля 1995 года № 24-ФЗ. Принят Государственной Думой 25 января 1995 года.

3. О ПРАВОВОЙ ОХРАНЕ ПРОГРАММ ДЛЯ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН И БАЗ ДАННЫХ. Закон Российской Федерации от 23 февраля 1992 года № 3524-1.

4. ОБ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ. Федеральный закон Российской Федерации от 10 января 2002 года № 1-ФЗ.

5. ОБ АВТОРСКОМ ПРАВЕ И СМЕЖНЫХ ПРАВАХ. Закон Российской Федерации от 9 июля 1993 года № 5351-1.

6. О ФЕДЕРАЛЬНЫХ ОРГАНАХ ПРАВИТЕЛЬСТВЕННОЙ СВЯЗИ И ИНФОРМАЦИИ. Закон Российской Федерации (в ред. Указа Президента РФ от 24.12.1993 № 2288; Федерального закона от 07.11.2000 № 135-ФЗ.

7. Положение об аккредитации испытательных лабораторий и органов по сертификации средств защиты информации по требованиям безопасности информации / Государственная техническая комиссия при Президенте Российской Федерации

9. Положение по аттестации объектов информатизации по требованиям безопасности информации / Государственная техническая комиссия при Президенте Российской Федерации.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации: с дополнениями в соответствии с Постановлением Правительства Российской Федерации от 26 июня 1995 года № 608 "О сертификации средств защиты информации" / Государственная техническая комиссия при Президенте Российской Федерации.

11. Положение о государственном лицензировании деятельности в области защиты информации / Государственная техническая комиссия при Президенте Российской Федерации.

12. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Руководящий документ / Государственная техническая комиссия при Президенте Российской Федерации.

13. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации: Руководящий документ / Государственная техническая комиссия при Президенте Российской Федерации.

14. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: Руководящий документ / Государственная техническая комиссия при Президенте Российской Федерации.

15. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации: Руководящий документ / Государственная техническая комиссия при Президенте Российской Федерации.

16. Защита информации. Специальные защитные знаки. Классификация и общие требования: Руководящий документ / Государственная техническая комиссия при Президенте Российской