	До	После
Знания о материале		
Полезность материала		

Основные угрозы информационной безопасности

лекция

Учебные вопросы

1.Информация как объект правовых отношений. Перечни сведений ограниченного доступа.

2. Основные угрозы информационной безопасности Российской Федерации.

3. Технические каналы утечки информации.

4. Потенциальный (вероятный) нарушитель информационной безопасности Российской Федерации.

5. Нарушения требований по обеспечению информационной безопасности.

6. Возможные последствия нарушений установленных требований обеспечения информационной безопасности и технической

1.Информация как объект правовых отношений. Перечни сведений ограниченного доступа.

Регулирующая роль государства заключается в формировании правового информационного пространства через систему законодательных актов, определяющих права и ответственность субъектов информационных отношении.

Значительный прорыв за последние десять лет достигнут в сфере разработки национальных стандартов, определяющих процедуры и правила обеспечения информационной безопасности.

Положительным является опыт гармонизации национальных стандартов с ведущими зарубежными стандартами, в первую очередь, со стандартами ISO, отражающими мировой опыт в области информационной безопасности.

Не менее важной является роль общества, которое должно создавать условия нетерпимости к недобросовестным информационным отношениям, в том числе, и тем, которые не попадают под правовое

Защищаемая информация

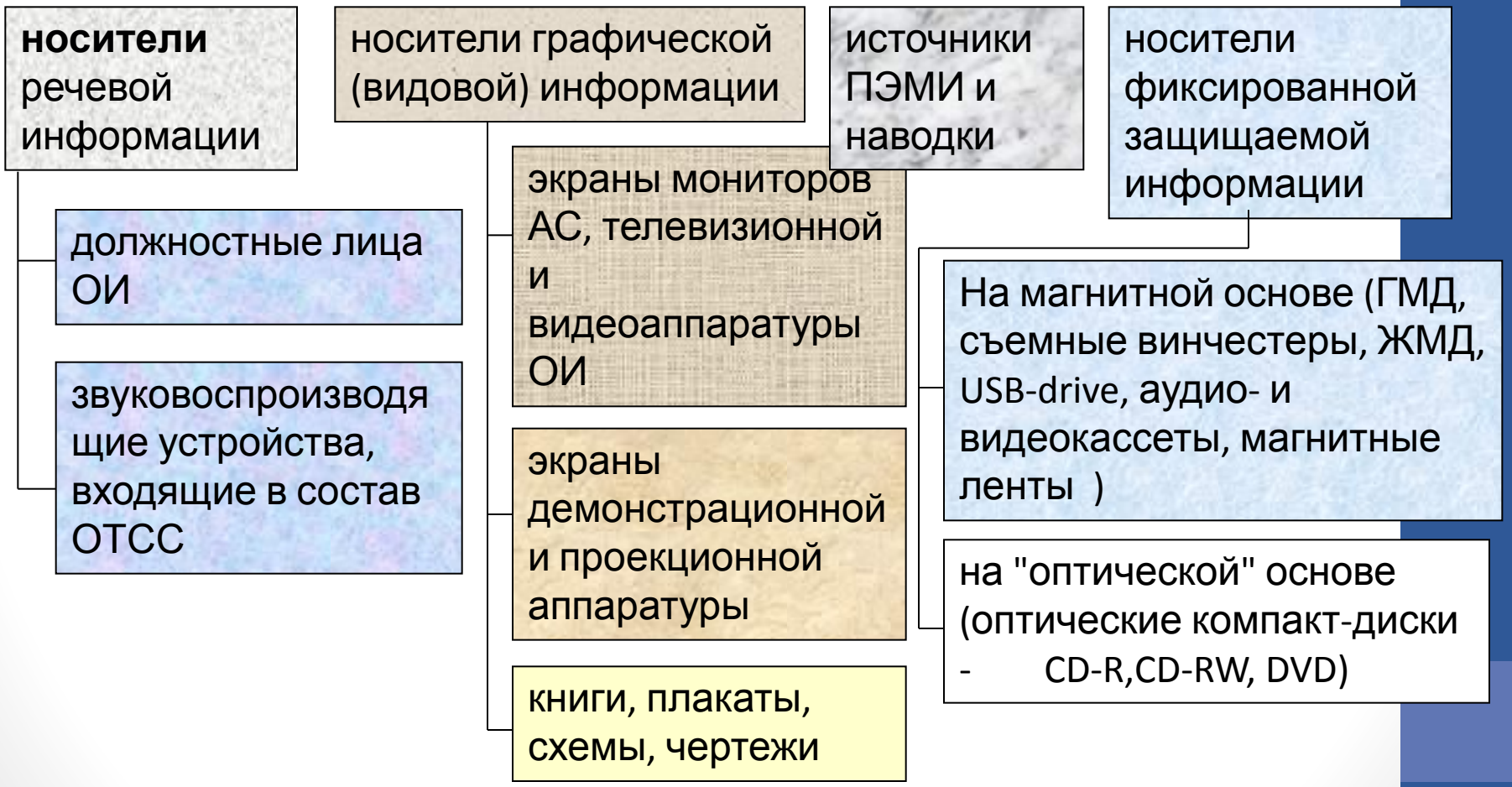
речевая (акустическая) информация

графическая (видовая) информация

информация, обрабатываемая (циркулирующая) непосредственно в АС, представленная в виде файлов, каталогов, баз и хранилищ данных, записей и их полей

информация, обрабатываемая (циркулирующая) в технических средствах обработки информации (ТСОИ) и автоматизированных системах (АС) в виде электрических и оптических сигналов и распространяющуюся от них в виде побочных электромагнитных излучений (ПЭМИ)

Первичные носители защищаемой информации



Вторичные носители, воспроизводящие преобразованную защищаемую информацию

- для речевой (акустической) информации
  - акустические колебания в воздушной среде
  - вибрационные колебания
  - электрические сигналы в токопроводящих цепях
  - собственные ПЭМИ
  - ЭМИ внешних источников
- для графической (видовой) информации
  - отраженное излучение в видимом и ИК диапазоне
  - собственные излучения носителей: электронно-лучевых, жидкокристалли ческих, плазменных и др. экранов и табло
- для информации, циркулирующей в ОТСС
  - модулированные информативным сигналом ПЭМИ ВТСС и средств обеспечения ОИ
  - наведенные электрические сигналы (наводки) в токопроводящих цепях ОТСС, ВТСС и (или) средств обеспечения ОИ
  - отраженные от элементов ОТСС ЭМИ облучающего источника, модулированные информативными сигналами ОТСС

Перечни защищаемых сведений

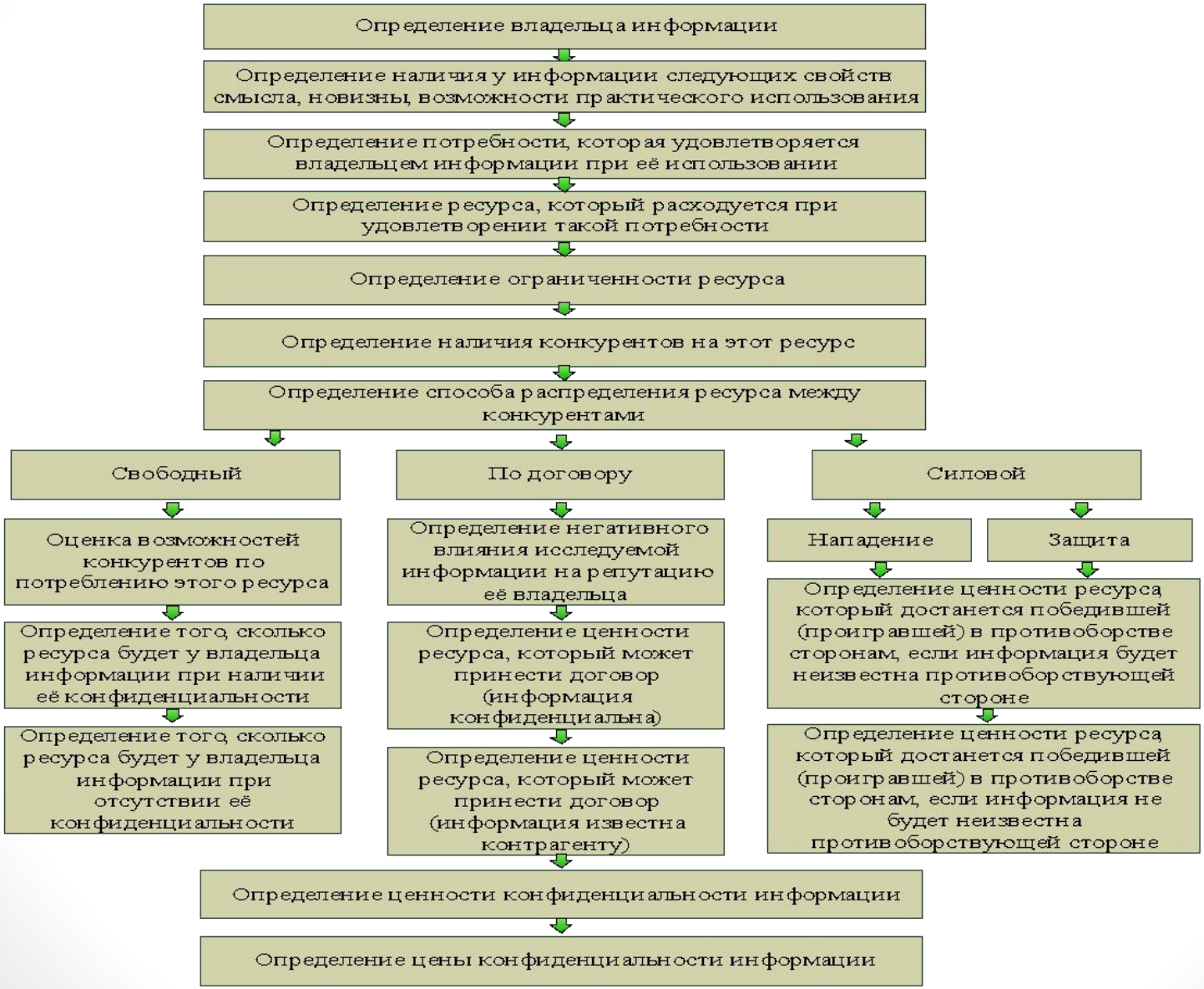
Перечень сведений конфиденциального характера (утв. Указом Президента РФ от 6 марта 1997 г. № 188, ред. от 23.09.2005)// Российская газета. – 1997. – 14 марта (№ 51).

Перечень сведений, подлежащих засекречиванию в ФТС России;

Перечень сведений ограниченного распространения в ФТС России.

1. Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.
2. Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц.
3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).
4. Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).
5. Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).
6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.
7. Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов.

Методический подход к обоснованию конфиденциальности информации



2. Основные угрозы информационной безопасност Российской Федерации.

Угроза – это потенциальная возможность определенным образом нарушить информационную безопасность.

Попытка реализации угрозы называется **атакой,** а тот, кто предпринимает такую попытку, – **злоумышленником.**

Потенциальные злоумышленники

Наиболее уязвимыми с точки зрения защищенности информационных ресурсов являются так называемые критические компьютерные системы, под которыми будем понимать сложные компьютеризированные организационно-технические и технические системы, блокировка или нарушение функционирования которых потенциально приводит к потере устойчивости организационных систем государственного управления и контроля, утрате обороноспособности государства, разрушению системы финансового обращения, дезорганизации систем энергетического и транспортного обеспечения государства, глобальным экологическим и техногенным катастрофам. К критическим компьютерным системам относятся и компьютерные информационные системы таможенных органов.

При решении проблемы повышения уровня защищенности информационных ресурсов КС необходимо исходить из того, что наиболее вероятным информационным объектом воздействия будет выступать программное обеспечение, составляющее основу комплекса средств получения, семантической переработки, распределения и хранения данных, используемых при эксплуатации критических систем.

В настоящее время основными средствами вредоносного (деструктивного) информационного воздействия на компьютерные системы являются компьютерные вирусы, алгоритмические и программные закладки.

Алгоритмическая закладка – это преднамеренное завуалированное искажение какой-либо части алгоритма решения задачи, либо построение его таким образом, что в результате конечной программной реализации этого алгоритма в составе программного компонента или комплекса программ, последние будут иметь ограничения на выполнение требуемых функций, заданных спецификацией, или вовсе их не выполнять при определенных условиях протекания вычислительного процесса, задаваемого семантикой перерабатываемых программой данных.

Программная закладка – это совокупность операторов и (или) операндов, преднамеренно в завуалированной форме включаемую в состав выполняемого кода программного компонента на любом этапе его разработки.

Программная закладка реализует определенный несанкционированный алгоритм с целью ограничения или блокирования выполнения программным компонентом требуемых функций при определенных условиях протекания вычислительного процесса

Действия алгоритмических и программных закладок условно можно разделить на три класса:

- изменение функционирования вычислительной системы (сети);
- несанкционированное считывание информации;
- несанкционированная модификация информации, вплоть до ее уничтожения.

В классе изменения функционирования вычислительной системы (сети) воздействий выделяют следующие:

- уменьшение скорости работы вычислительной системы (сети);
- частичное или полное блокирование работы системы (сети);
- имитация физических (аппаратурных) сбоев работы вычислительных средств и периферийных устройств;
- переадресация сообщений;
- обход программно-аппаратных средств криптографического преобразования информации;
- обеспечение доступа в систему с непредусмотренных периферийных устройств.

Несанкционированное считывание информации, осуществляемое в автоматизированных системах, направлено на:

- считывание паролей и их отождествление с конкретными пользователями;
- получение секретной информации;
- идентификацию информации, запрашиваемой пользователями;
- подмену паролей с целью доступа к информации;
- контроль активности абонентов сети для получения косвенной информации о взаимодействии пользователей и характере информации, которой обмениваются абоненты сети.

Несанкционированная модификация информации является наиболее опасной разновидностью воздействий программных закладок, поскольку приводит к наиболее опасным последствиям. В этом классе воздействий можно выделить следующие:

- разрушение данных и кодов исполняемых программ внесение тонких, трудно обнаруживаемых изменений в информационные массивы;
- внедрение программных закладок в другие программы и подпрограммы (вирусный механизм воздействий);
- искажение или уничтожение собственной информации сервера и тем самым нарушение работы сети;
- модификация пакетов сообщений.

Вредоносные программы называются разрушающими программными средствами (РПС), а их обобщенная классификация может выглядеть следующим образом:

- компьютерные вирусы – программы, способные размножаться, прикрепляться к другим программам, передаваться по линиям связи и сетям передачи данных, проникать в электронные телефонные станции и системы управления и выводить их из строя;

- программные закладки – программные компоненты, заранее внедряемые в компьютерные системы, которые по сигналу или в установленное время приводятся в действие, уничтожая или искажая информацию, или дезорганизуя работу программно-технических средств;

- способы и средства, позволяющие внедрять компьютерные вирусы и программные закладки в компьютерные системы и управлять ими на расстоянии.


Деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере
Стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков
ВНЕШНИЕ ИСТОЧНИКИ
Обострение международной конкуренции за обладание информационными технологиями и ресурсами
Деятельность международных террористических организаций
Увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий
УГРОЗ
Деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств
Разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение

Мобильные устройства как угроза информационной безопасности государственных органов

Использование сотрудниками персональных мобильных устройств, смартфонов, КПК и завтрашних Мобильных Интернет Устройств (Mobile Internet Devices) – определяются воздействием нескольких ключевых факторов:

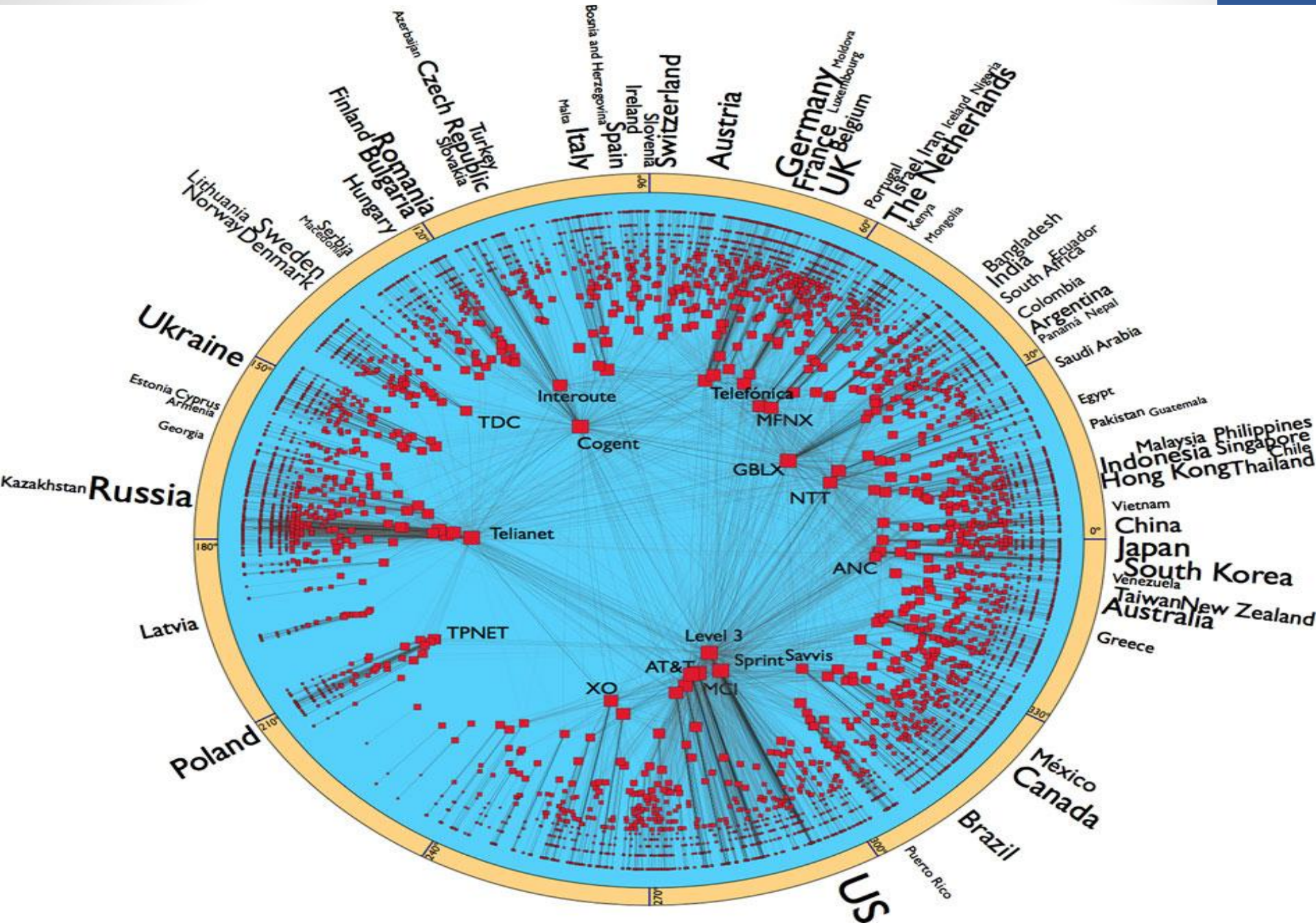
- прогресса микроэлектронных, а также телекоммуникационных технологий;
- опережающего развития потребительской электроники;
- нового социального явления - прихода в государственные структуры подросшего поколения Цифровых Аборигенов (Digital Natives)

К категории наиболее опасных можно отнести:

- для ОС Android: Android.SmsSend, Android.Gongfu, Android.Plankton, Android.GoldDream, Android.Crusewind, Android.SpyEye, Android.DreamExploid, Android.Wukong;
- для ОС iOS: iPhoneOS. HLLW.Ikee, коммерческие программы-шпионы.
- кроме специализированных под конкретные ОС вредоносных программ, существуют троянцы, способные работать на любой мобильной платформе с поддержкой Java (например, Symbian и большинство сотовых телефонов).

СОЦИАЛЬНЫЕ СЕТИ

Карта одного из сайта социальных сетей



Заразив персональный компьютер, злоумышленники могут:

- блокировать зараженное устройство;
- получить доступ к почтовой переписке,
- получить доступ к паролям используемых программ,
- получить доступ системам работы с денежными средствами;
- получить доступ к конфиденциальным данным виде файлов, архивов и фотографиям.

Внедренная в мобильное устройство вредоносная программа может:

- отправлять СМС и звонить на платные номера; включать микрофон без ведома жертвы — и тем самым получать информацию «из первых уст»;

- получать данные от GPS-навигатора о местонахождении жертвы — ее присутствии или отсутствии в определенных местах;

- получать доступ к конфиденциальным данным, сохраненным в виде фотографий и звуковых записей, а также СМС-переписке и истории совершенных звонков.

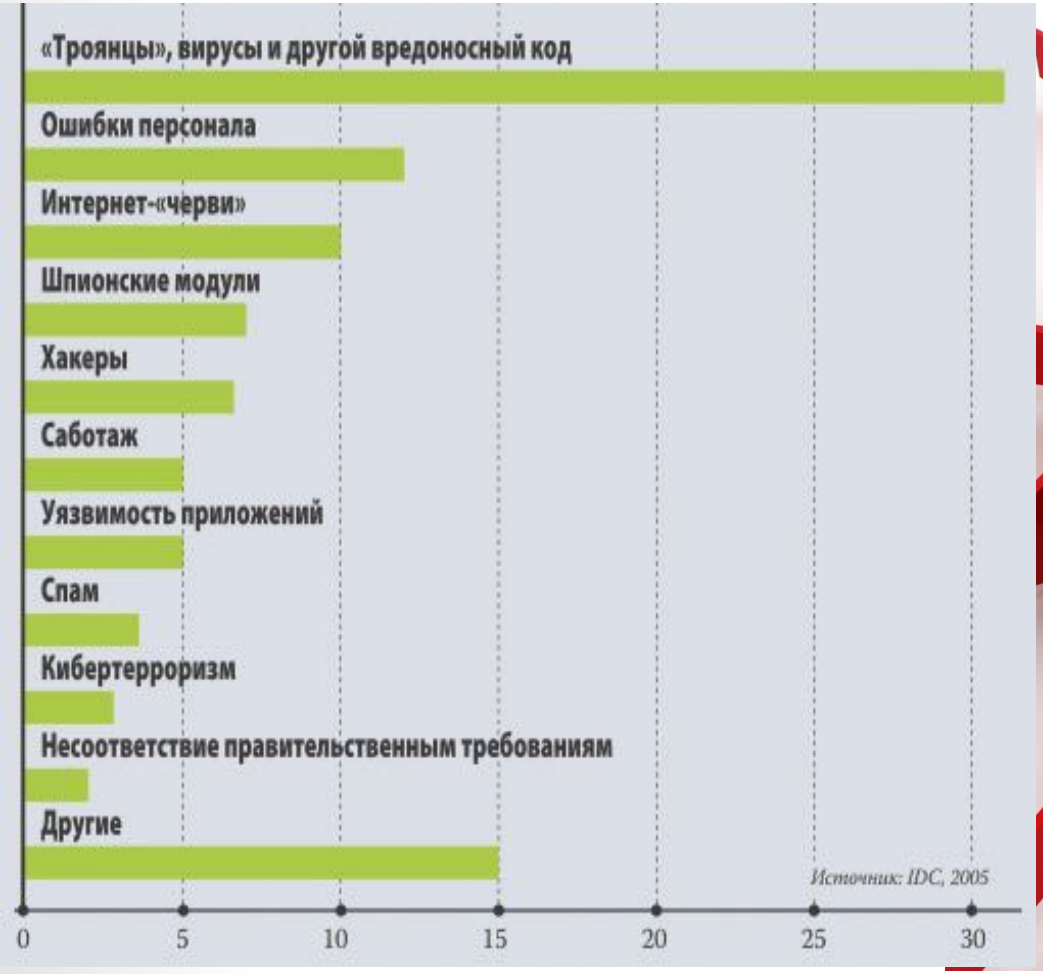
Владелец зараженного устройства отказывается под полным круглосуточным контролем!

Для органов власти заражение мобильных устройств сотрудников представляет особо опасную угрозу их информационной безопасности.

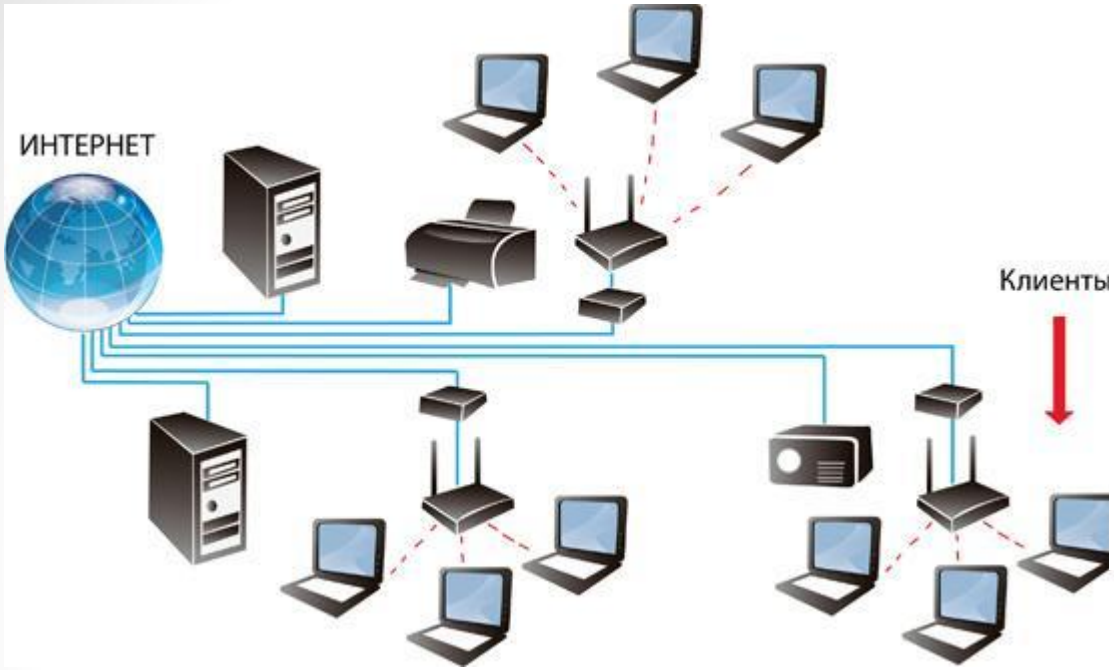
Многие сотрудники работают с внутренней почтой и конфиденциальными данными на своих устройствах.

Зараженные устройства, даже не подключенные к сети, могут быть использованы для атаки на нее — через беспроводные сети.

Проникновение в контролируемую зону



Wi-Fi-сети и угрозы информационной безопасности



Прямые - угрозы информационной безопасности, возникающие при передаче информации по беспроводному интерфейсу.

Косвенные — угрозы, связанные с наличием на объекте и рядом с объектом большого количества WiFi-сетей, которые могут использоваться для передачи информации, в том числе и полученной несанкционированно.

г. Москва

Май 2012 года

2-ой МЕЖДУНАРОДНЫЙ ФОРУМ ПО ПРАКТИЧЕСКОЙ БЕЗОПАСНОСТИ

CTF — международные соревнования по защите информации, проводимые по принципам игры CTF (capture the flag)

Young School - конкурс исследовательских работ студентов, аспирантов и молодых ученых.

hack2own - конкурс позволит участникам продемонстрировать навыки анализа защищенности и взлома мобильных устройств (на базе Apple iOS, Android), наиболее распространенных интернет-браузеров и операционных систем (умение эксплуатировать уязвимости актуальных версий ядра ОС).

Online HackQuest – вплотную примыкающие к CTF соревнования. Участники смогут поработать с множеством реальных уязвимостей и попробовать свои силы в решении небольших заданий по информационной безопасности, а кроме того, повлиять на сюжетную линию очного CTF.

Банковский аппарат – 3 мин 30 сек

ОС планшетных устройств – 5 мин 40 сек

ОС мобильных телефонов – 2 мин 15 сек

Более 200 мобильных телефонов за 1 час

Классификация угроз

Угрозы	Несанкционированные действия		
	Случайные	Преднамеренные	
		Пассивные	Активные
Прямые	Невыявленные ошибки программного обеспечения КС; отказы и сбои технических средств КС; ошибки операторов; неисправность средств шифрования; скачки электропитания на технических средствах; старение носителей информации; разрушение информации под воздействием физических факторов (аварии и т.п.).	Маскировка несанкционированных запросов под запросы ОС; обход программ разграничения доступа; чтение конфиденциальных данных из источников информации; подключение к каналам связи с целью получения информации («подслушивание» и/или «ретрансляция»); при анализе трафика; использование терминалов и ЭВМ других операторов; намеренный вызов случайных факторов	**Включение в программы РПС, выполняющих функции нарушения целостности и конфиденциальности информации и ПО; ввод новых программ, выполняющих функции нарушения безопасности по; незаконное применение ключей разграничения доступа; обход программ разграничения доступа; вывод из строя подсистемы регистрации и учета; уничтожение ключей шифрования и паролей; подключение к каналам связи с целью модификации, уничтожения, задержки и переупорядочивания данных; вывод из строя элементов физических средств защиты информации КС; намеренный вызов случайных факторов.**
Косвенные	**Нарушение пропускного режима и режима секретности; естественные**	**Перехват ЭМИ от технических средств; хищение производственных отходов (распечаток); визуальный канал;**	**Помехи; отключение электропитания; намеренный вызов случайных факторов.**

3. Технические каналы утечки информации.

Структура технического канала утечки информации

Каналы утечки информации образуются:

- низкочастотными электромагнитными полями, возникающими при работе ТС;
- при воздействии на ТС электрических, магнитных и акустических полей;
- при возникновении паразитной высокочастотной (ВЧ) генерации;
- при прохождении информативных (опасных) сигналов в цепи электропитания;
- при взаимном влиянии цепей;
- при прохождении информативных (опасных) сигналов в цепи заземления;
- при паразитной модуляции высокочастотного сигнала;
- вследствие ложных коммутаций и несанкционированных действий.

Перехват акустических сигналов по воздушному каналу направленными микрофонами

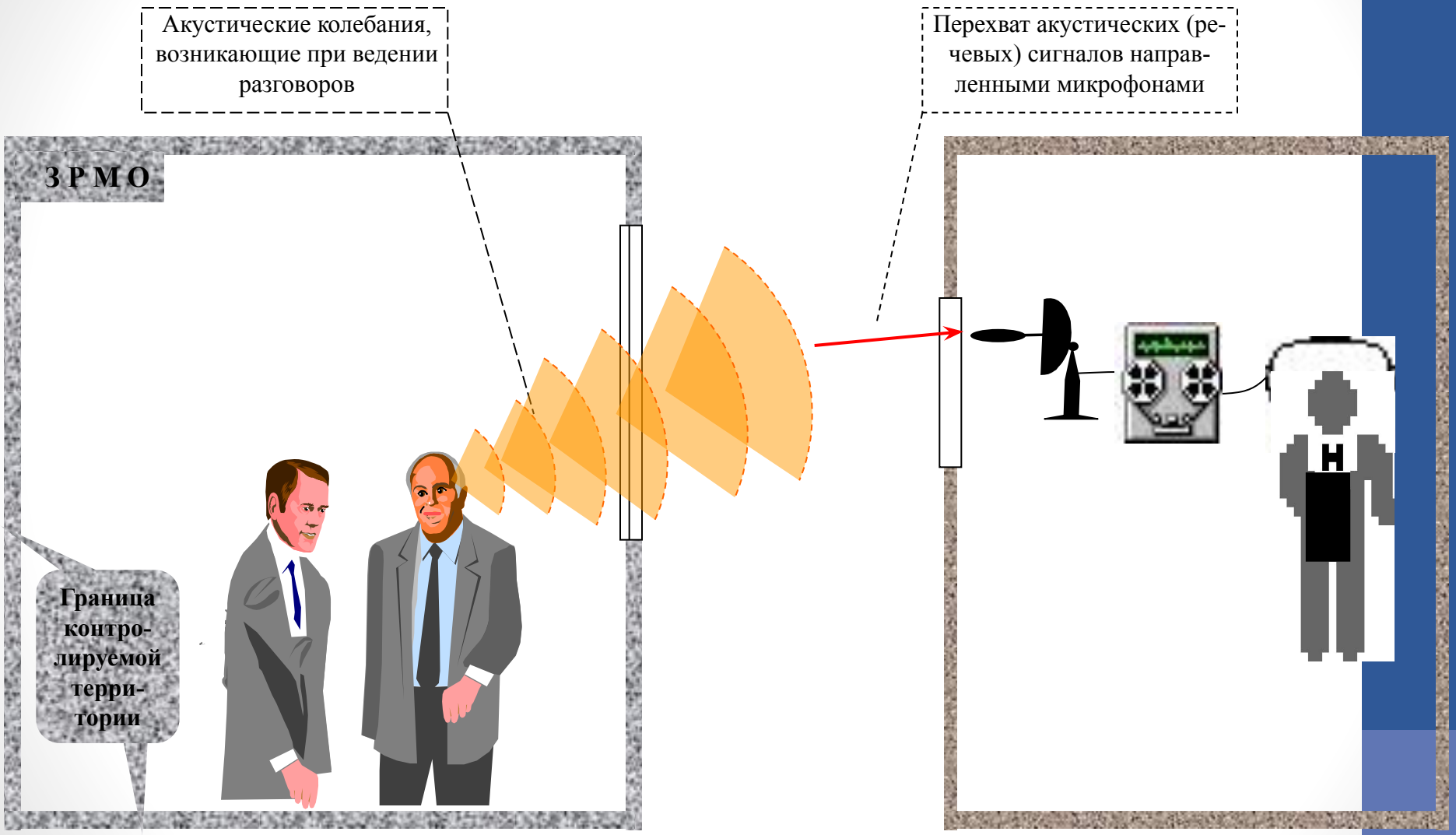


Рис.

Перехват акустических сигналов по воздушному каналу микрофонами, комплексированными с портативными устройствами звукозаписи

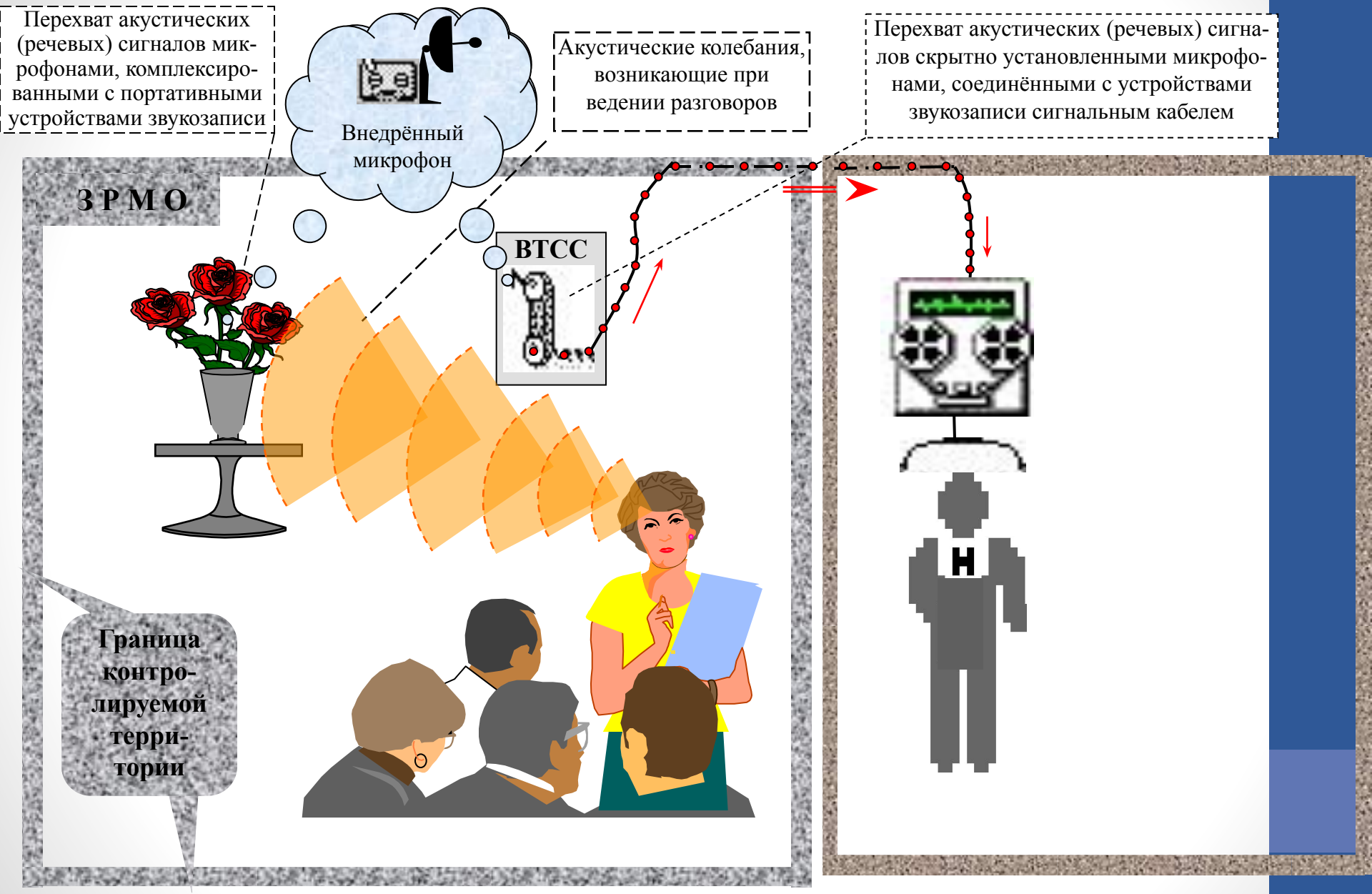


Рис.

Перехват акустических сигналов по воздушному каналу микрофонами, комплексированными с устройствами передачи информации по радиоканалу

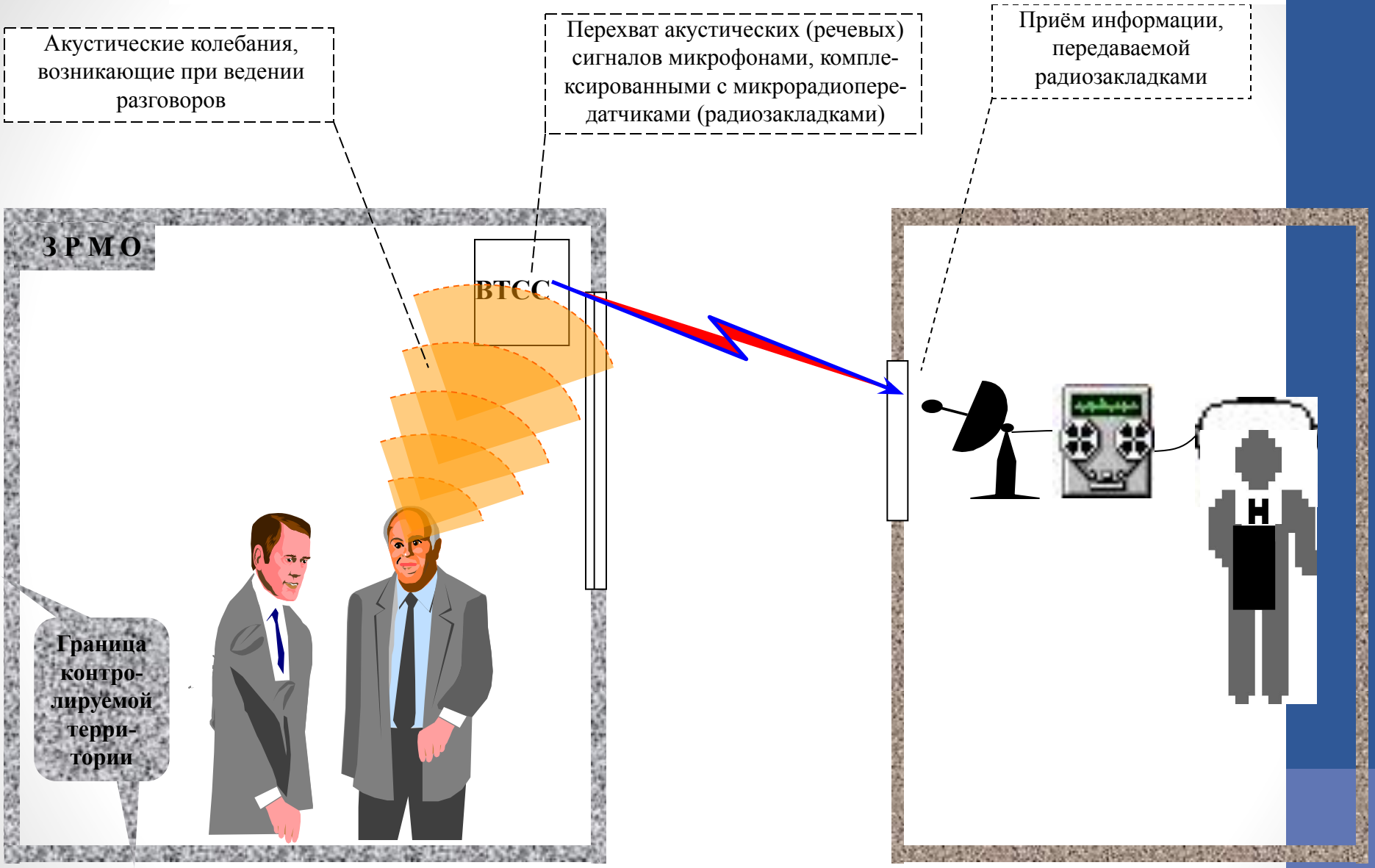


Рис.

Перехват акустических сигналов по воздушному каналу микрофонами (в том числе контактными), комплексированными с устройствами передачи информации по оптическому каналу

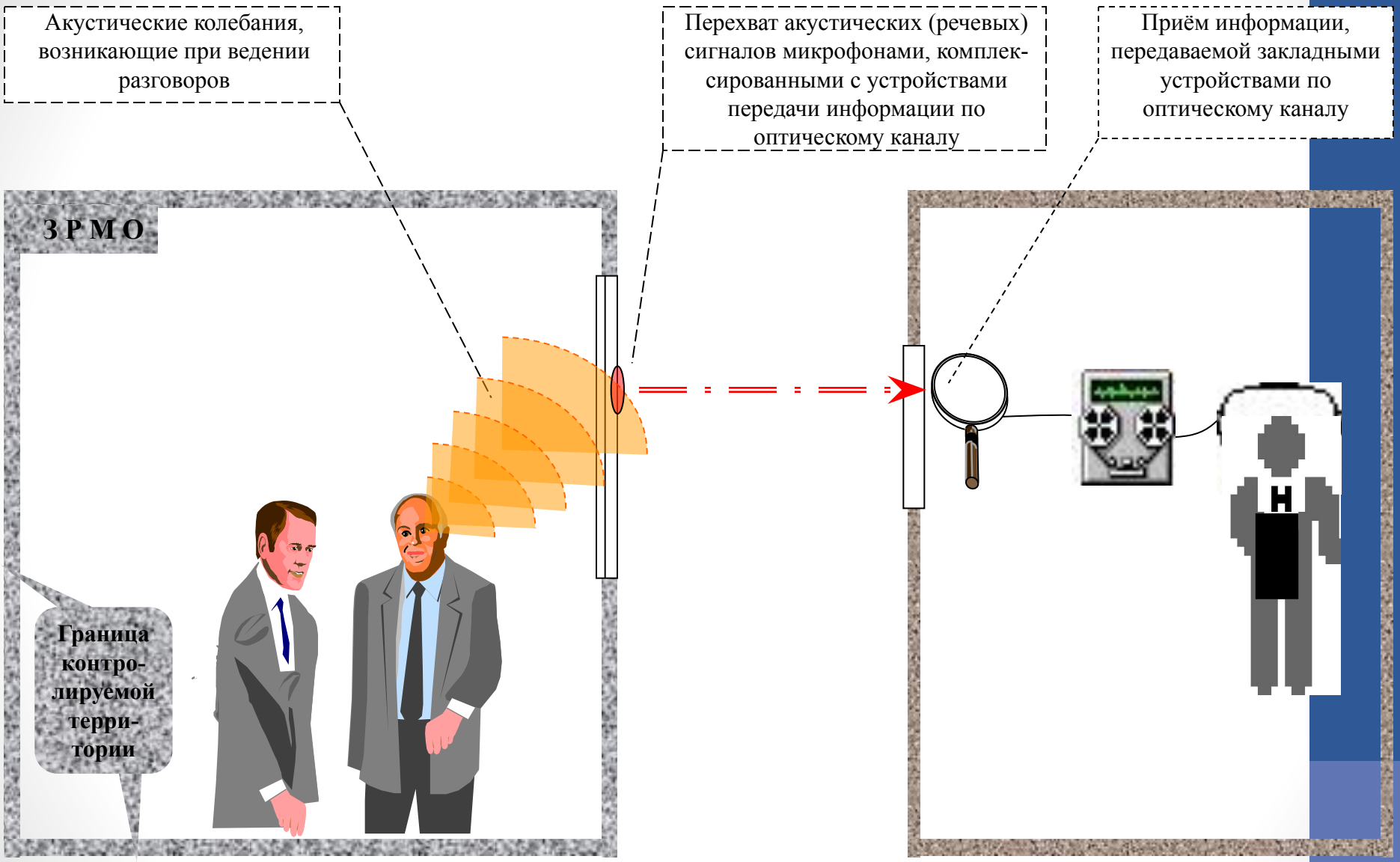


Рис.

Перехват информации по параметрическому каналу путём высокочастотного облучения ТСПИ

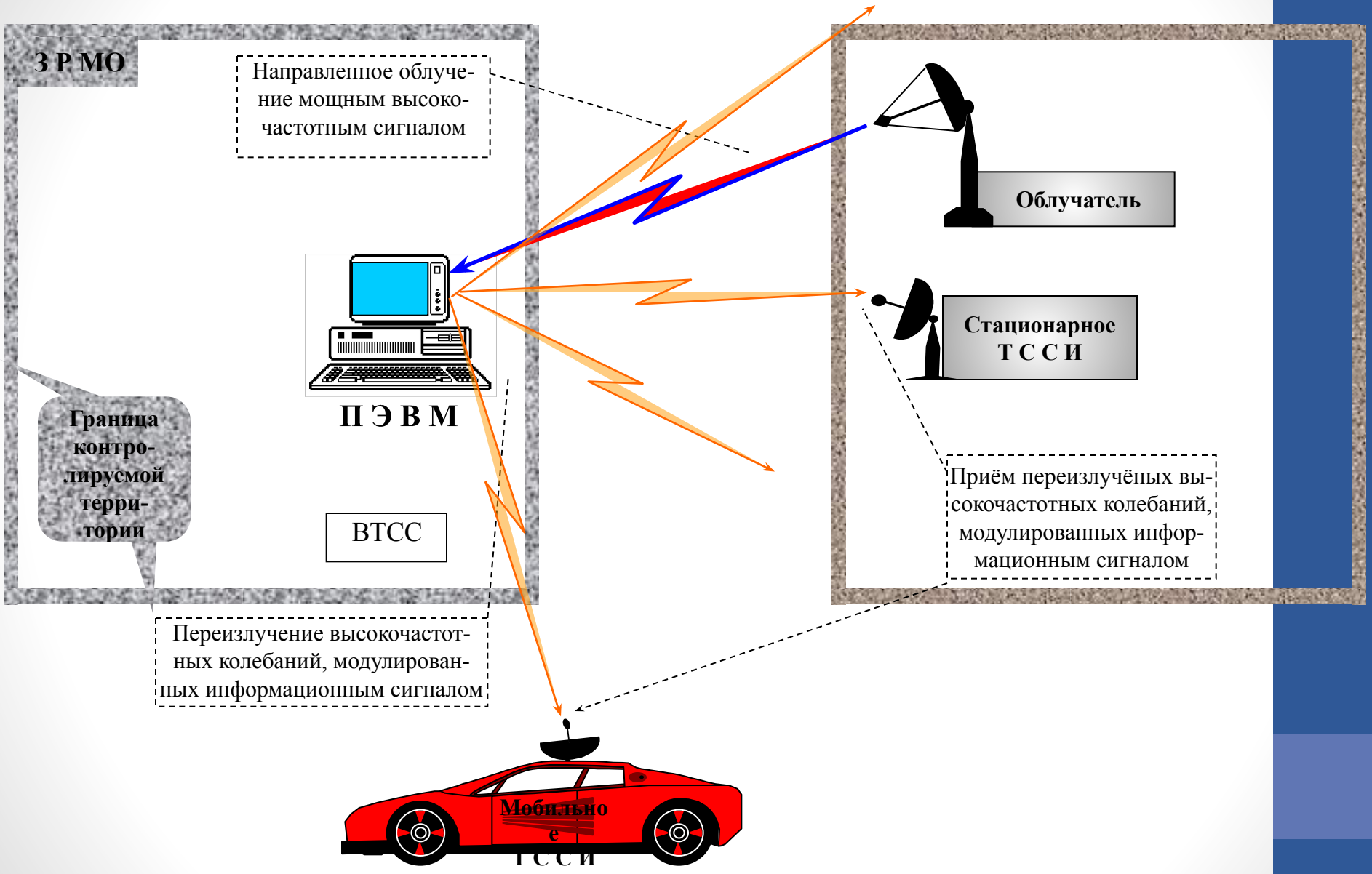


Рис.

4. Потенциальный (вероятный нарушитель информационной безопасности Российской Федерации.

Модель нарушителя и нарушения информационной безопасности

Способ нарушения информационной безопасности	Свойства информации и информационной инфраструктуры, на которые оказывается воздействие
Внедрение программ-вирусов и программных закладок на стадии проектирования или эксплуатации информационной системы, приводящих к компрометации системы защиты информации	Целостность Аутентичность Неотказуемость Конфиденциальность Подотчетность
Воздействие на обслуживающий персонал и пользователей системы с целью создания благоприятных условий для реализации угроз информационной безопасности	Конфиденциальность Доступность Подотчетность
Радиоэлектронное подавление линий связи и систем управления	Доступность Целостность

Модель нарушителя и нарушения информационной безопасности

Способ нарушения информационной безопасности	Свойства информации и информационной инфраструктуры, на которые оказывается воздействие
Нарушение технологии обработки данных и информационного обмена	Конфиденциальность Доступность Целостность
Перехват информации по техническим каналам ее утечки	Конфиденциальность
Перехват и дешифрование информации в сетях передачи данных и линиях связи	Конфиденциальность Целостность

Модель нарушителя и нарушения информационной безопасности

Способ нарушения информационной безопасности	Свойства информации и информационной инфраструктуры, на которые оказывается воздействие
Внедрение электронных устройств перехвата информации в технические средства и помещения	Конфиденциальность Подотчетность
Навязывание ложной информации по сетям передачи данных и линиям связи	Достоверность Целостность Аутентичность Неотказуемость

Модель нарушителя и нарушения информационной безопасности

Способ нарушения информационной безопасности	Свойства информации и информационной инфраструктуры, на которые оказывается воздействие
Манипулирование информацией (дезинформация, сокрытие или искажение информации)	Целостность Достоверность Доступность
Незаконное копирование, уничтожение, хищение данных и программ, уничтожение носителей информации	Конфиденциальность Доступность
Хищение ключей (ключевых документов) средств криптографической защиты информации, программных или аппаратных ключей средств защиты информации от несанкционированного доступа	Конфиденциальность Целостность Аутентичность Неотказуемость

5. Нарушения требований по обеспечению информационной безопасности.

Типовые недостатки в области технической защиты информации

Проведение мероприятий закрытого характера в помещениях, не предназначенных для этих целей

Использование аппаратов правительственной связи в неаттестованных помещениях

Подключение автоматизированных систем, обрабатывающих информацию ограниченного доступа, к сети «Интернет»

Подключение к автоматизированным системам, обрабатывающих информацию ограниченного доступа , неучтенных носителей на основе «Flash-памяти», различных мобильных устройств

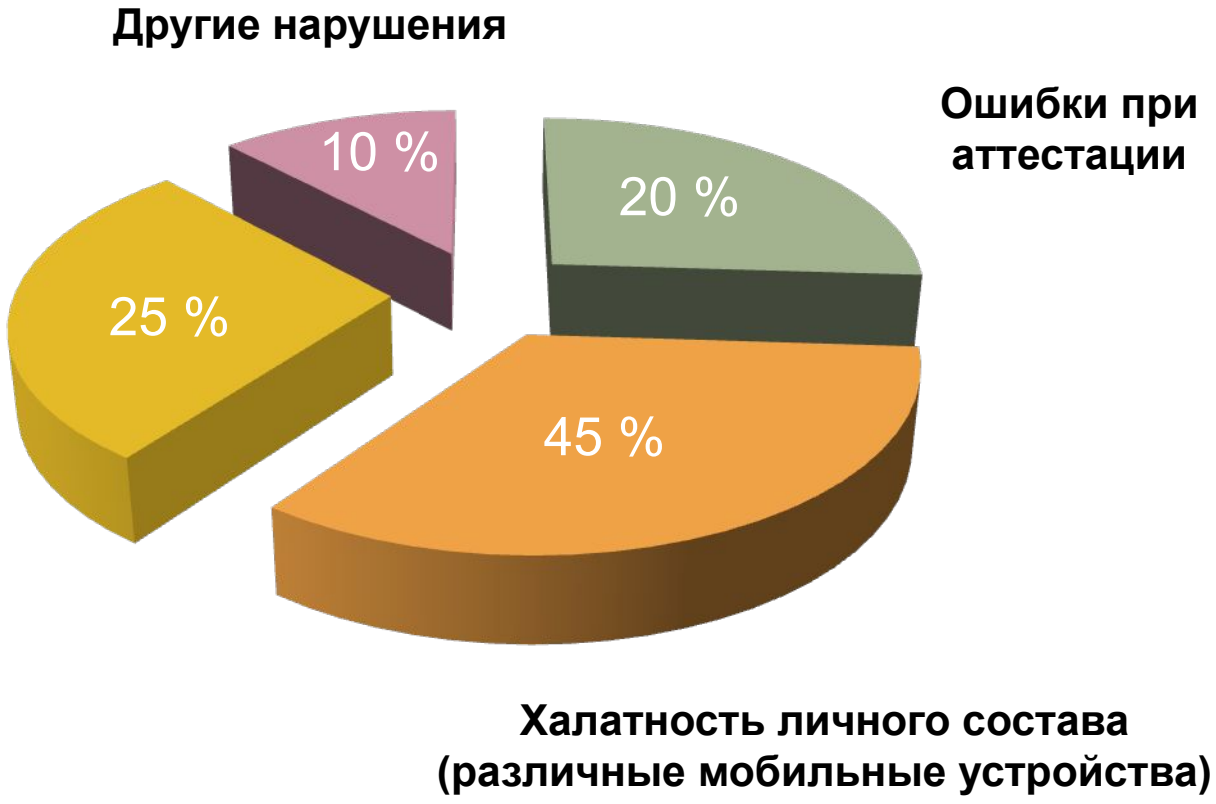
Размещение в помещениях, где обсуждаются закрытые вопросы, технических средств, подключенных к сети «Интернет»

Самовольное изменение состава оборудования и программного обеспечения, аттестованных по требованиям безопасности информации объектов вычислительной техники

Несоответствие настроек средств защиты информации от несанкционированного доступа установленным требованиям, отключение средств защиты информации

Недостаточный уровень воспитательной работы и методического руководства подчиненными по вопросам технической защиты информации со стороны руководителей подразделений ФМС России

Анализ нарушений



6. Возможные последствия нарушений установленных требований обеспечения информационной безопасности и технической защиты информации.

В классе изменения функционирования вычислительной системы (сети) воздействий выделяют следующие:

- уменьшение скорости работы вычислительной системы (сети);
- частичное или полное блокирование работы системы (сети);
- имитация физических (аппаратурных) сбоев работы вычислительных средств и периферийных устройств;
- переадресация сообщений;
- обход программно-аппаратных средств криптографического преобразования информации;
- обеспечение доступа в систему с непредусмотренных периферийных устройств.

Несанкционированное считывание информации, осуществляемое в автоматизированных системах, направлено на:

- считывание паролей и их отождествление с конкретными пользователями;
- получение секретной информации;
- идентификацию информации, запрашиваемой пользователями;
- подмену паролей с целью доступа к информации;
- контроль активности абонентов сети для получения косвенной информации о взаимодействии пользователей и характере информации, которой обмениваются абоненты сети.

Несанкционированная модификация информации является наиболее опасной разновидностью воздействий программных закладок, поскольку приводит к наиболее опасным последствиям. В этом классе воздействий можно выделить следующие:

- разрушение данных и кодов исполняемых программ внесение тонких, трудно обнаруживаемых изменений в информационные массивы;
- внедрение программных закладок в другие программы и подпрограммы (вирусный механизм воздействий);
- искажение или уничтожение собственной информации сервера и тем самым нарушение работы сети;
- модификация пакетов сообщений.

Угрозы для механизмов управления системой защиты

Разрушение функциональных возможностей СЗИ происходит, когда она не может своевременно обеспечить необходимые функциональные возможности. Разрушение может охватывать как один тип функциональных возможностей СЗИ, так и группу возможностей.

Разрушение функциональных возможностей СЗИ может происходить при использовании следующих типов уязвимых мест:

- неспособность обнаружить необычный характер трафика (т.е. намеренное переполнение трафика),
- неспособность перенаправить трафик, выявить отказы аппаратных средств ЭВМ, и т.д.,
- конфигурация ИС, допускающая вероятность выхода из строя в случае отказа в одном месте,
- неавторизованные изменения компонентов аппаратных средств ИС (переконфигурирование адресов на автоматизированных рабочих местах, изменение конфигурации маршрутизаторов или хабов, и т.д.),
- неправильное обслуживание аппаратных средств ИС,
- недостаточная физическая защита аппаратных средств ИС

Модель угроз и принципы обеспечения безопасности ПО

Модель угроз должна включать:

- полный реестр типов возможных программных закладок;
- описание наиболее технологически уязвимых мест компьютерных систем (с точки зрения важности и наличия условий для скрытого внедрения программных закладок);
- описание мест и технологические карты разработки программных средств, а также критических этапов, при которых наиболее вероятно скрытое внедрение программных закладок;
- реконструкцию замысла структур, имеющих своей целью внедрение в ПО заданного типа (класса, вида) программных закладок диверсионного типа;
- психологический портрет потенциального диверсанта в компьютерных системах.

Семинар № 1
«Анализ реализации государственной политики обеспечения информационной безопасности в Российской Федерации»

План семинара:
1. Анализ сущности и значения информации в развитии современного информационного общества. Актуальность обеспечения информационной безопасности в современном обществе.
2. Анализ основных понятий в сфере обеспечения информационной безопасности.
3. Анализ видов тайн, официально признанных в Российской Федерации.
4. Анализ государственной политики Российской Федерации в области обеспечения информационной безопасности.
5. Анализ организации лицензирования и сертификации в области защиты информации.
6. Анализ особенностей организации обеспечения информационной безопасности в таможенных органах