МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ОРЛОВСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МВД РОССИЙСКОЙ ФЕДЕРАЦИИ»

Д.С. Мишин, Н.Г. Подчерняев

Основы информационной безопасности в органах внутренних дел

А Л Ь Б О М С Х Е М

ОРЕЛ
ОрЮИ МВД России
2008

УДК 6Ф.3+34С33
ББК 32.97+67.99(2)116
М71

Авторский коллектив:

Мишин Д. С. (темы 1-5, Приложение), Подчерняев Н.Г. (темы 1, 4, Приложение).

Мишин, Д.С.

М71 **Информационная безопасность и применение информационных технологий в борьбе с преступностью:** Альбом схем / Д.С. Мишин, Н.Г. Подчерняев. Орел: Орловский юридический институт МВД России, 2008. 48 с.

Альбом схем подготовлен в соответствии с содержанием и структурой программы учебной дисциплины «Основы информационной безопасности в ОВД». Альбом включает в себя основную часть и приложения. Основная часть содержит материал по 5 темам курса, в частности: правовое обеспечение информационной безопасности, концепция комплексной защиты компьютерной информации, основы организации противодействия НСД в сфере информационных технологий, обеспечение информационной безопасности в каналах связи, модели систем обеспечения информационной безопасности.

Альбом подготовлен для курсантов и слушателей образовательных учреждении МВД России, а также может быть использован студентами и преподавателями юридических вузов.

УДК 6Ф.3+34С33
ББК 32.97+67.99(2)116

С О Д Е Р Ж А Н И Е

ТЕМА № 1. ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

БАЗОВЫЕ ПОНЯТИЯ ДИСЦИПЛИНЫ

СТРУКТУРА ИНФОРМАЦИОННЫХ СИСТЕМ

ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

есть совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации

Доктрина служит основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового и методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

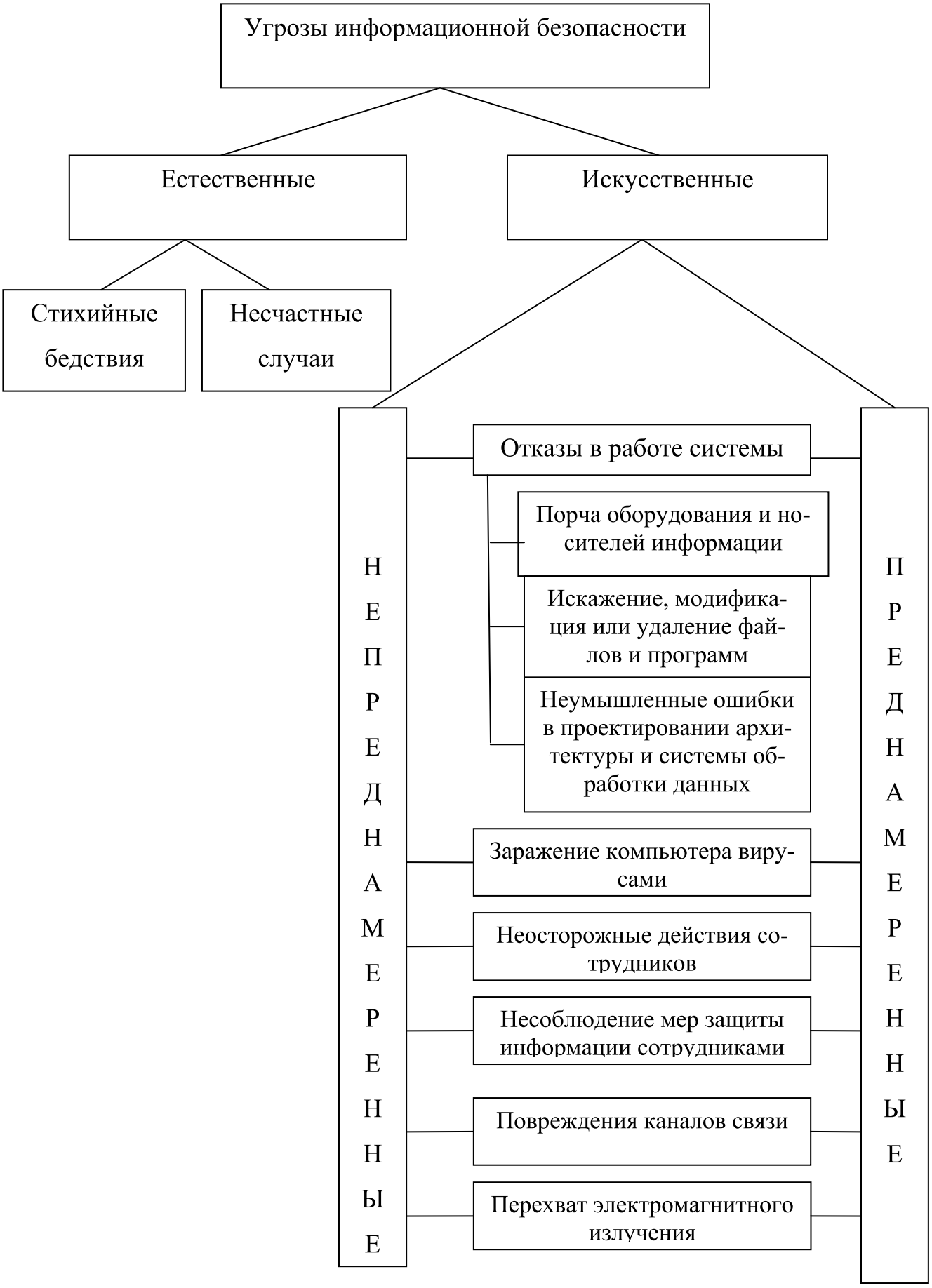
ПРАВОВЫЕ МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

(разработка нормативных правовых актов, регламентирующих отношения в информационной сфере, и нормативных методических документов)

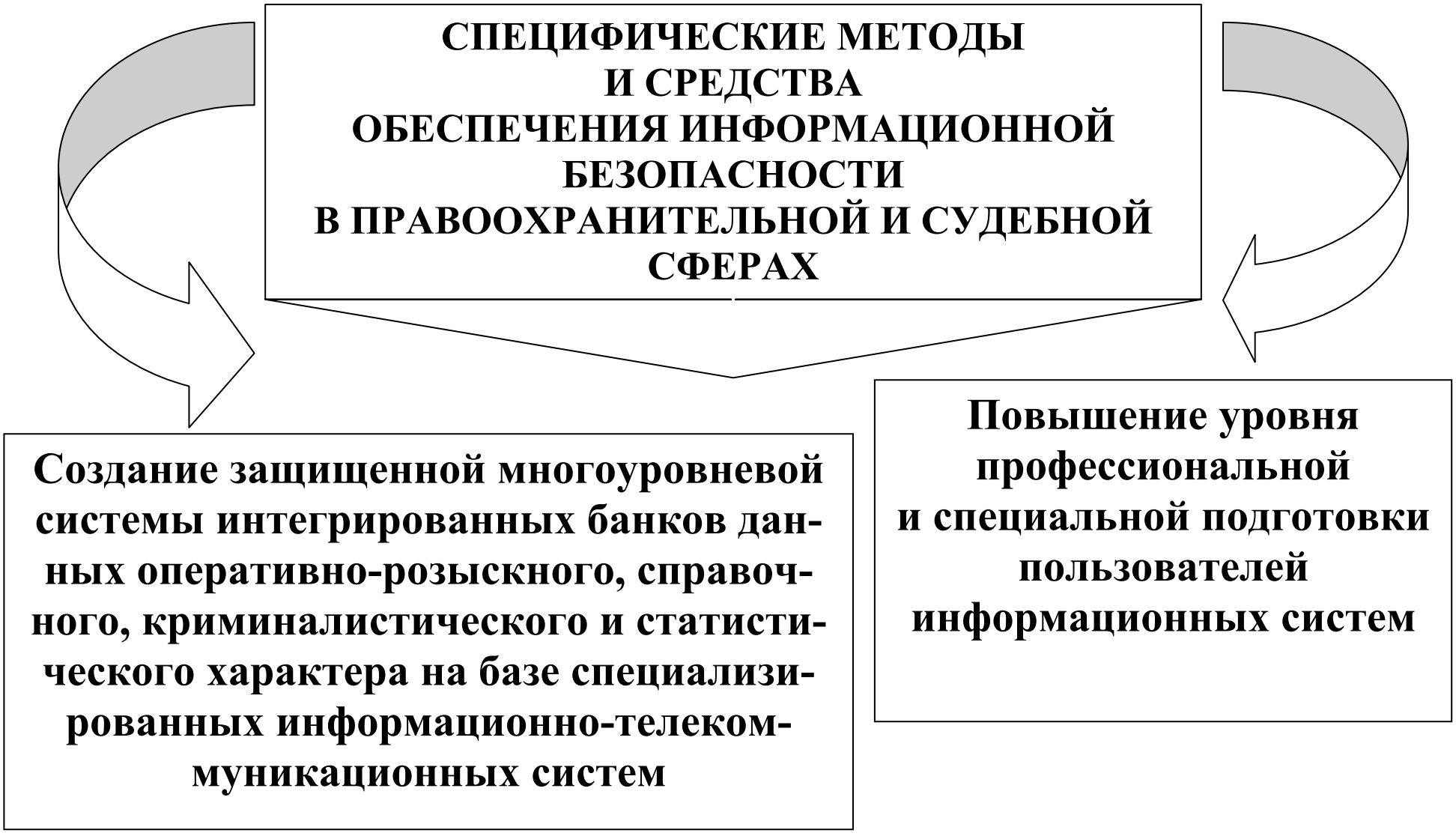
ОСНОВНЫЕ НАПРАВЛЕНИЯ

- **внесение изменений и дополнений в законодательство РФ, устранения внутренних противоречий в федеральном законодательстве, противоречий, связанных с международными соглашениями, конкретизации правовых норм;**
- **уточнение статуса иностранных информационных агентств, средств массовой информации и журналистов;**
- **законодательное закрепление приоритета развития национальных сетей связи и отечественного производства космических спутников связи;**
- **определение статуса организаций, предоставляющих услуги глобальных информационно-телекоммуникационных сетей на территории РФ;**
- **создание правовой базы для формирования в РФ региональных структур обеспечения, информационной безопасности.**
- **законодательное разграничение полномочий между федеральными органами государственной власти и органами государственной власти субъектов РФ;**

ТЕМА № 2. КОНЦЕПЦИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ


Угрозы информационной безопасности
Естественные
Искусственные
Стихийные бедствия
Несчастные случаи
НЕПРЕДНАМЕРЕННЫЕ
Отказы в работе системы
Порча оборудования и носителей информации
Искажение, модификация или удаление файлов и программ
Неумышленные ошибки в проектировании архитектуры и системы обработки данных
Заражение компьютера вирусами
Неосторожные действия сотрудников
Несоблюдение мер защиты информации сотрудниками
Повреждения каналов связи
Перехват электромагнитного излучения
ПРЕДНАМЕРЕННЫЕ

ОБЪЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ПРАВООХРАНИТЕЛЬНОЙ И СУДЕБНОЙ СФЕРАХ:


СПЕЦИФИЧЕСКИЕ МЕТОДЫ
И СРЕДСТВА
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
В ПРАВООХРАНИТЕЛЬНОЙ И СУДЕБНОЙ
СФЕРАХ
Создание защищенной многоуровневой системы интегрированных банков данных оперативно-розыскного, справочного, криминалистического и статистического характера на базе специализированных информационно-телекоммуникационных систем
Повышение уровня профессиональной и специальной подготовки пользователей информационных систем

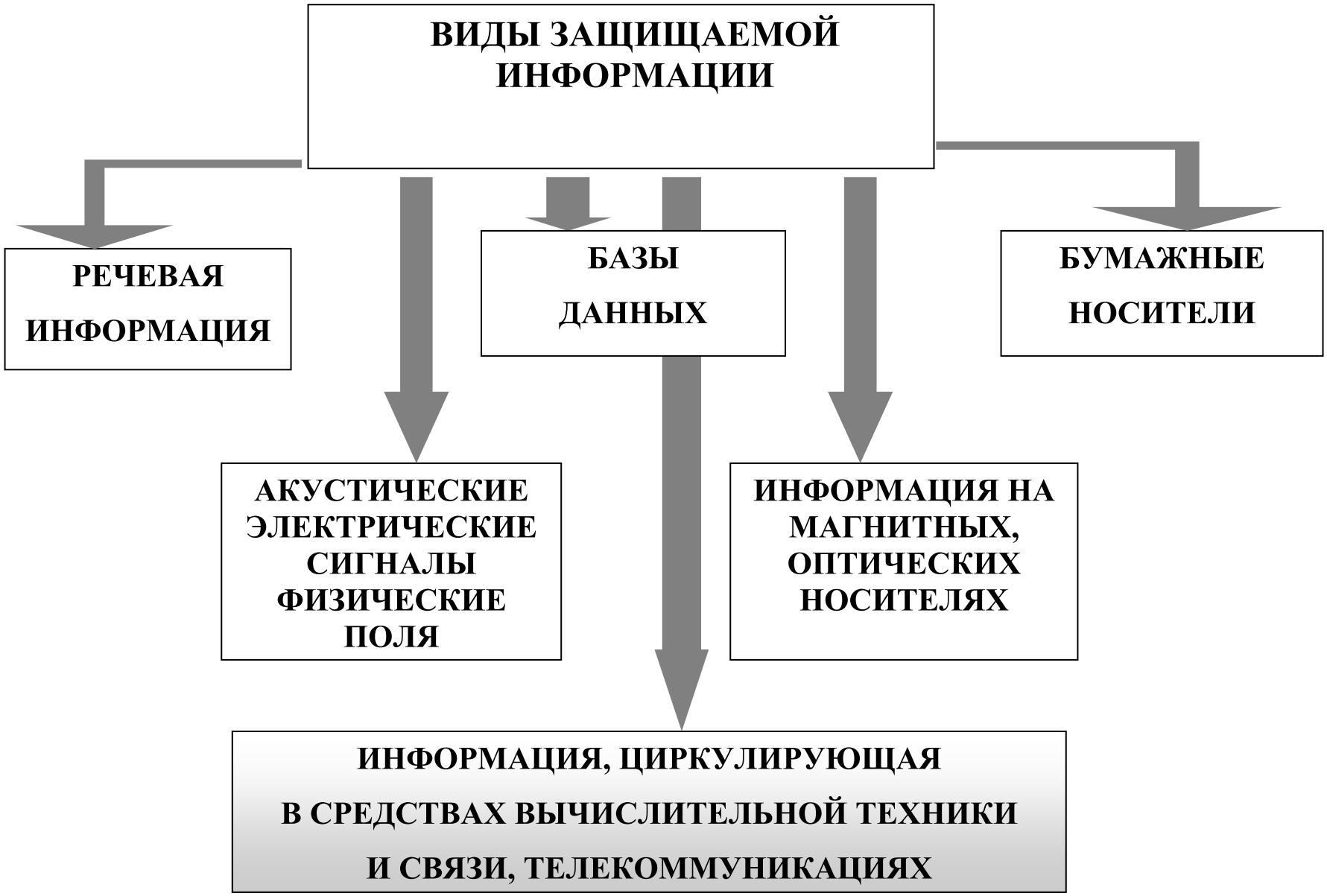
ДОСТИЖЕНИЕ АБСОЛЮТНОЙ БЕЗОПАСНОСТИ НЕВОЗМОЖНО

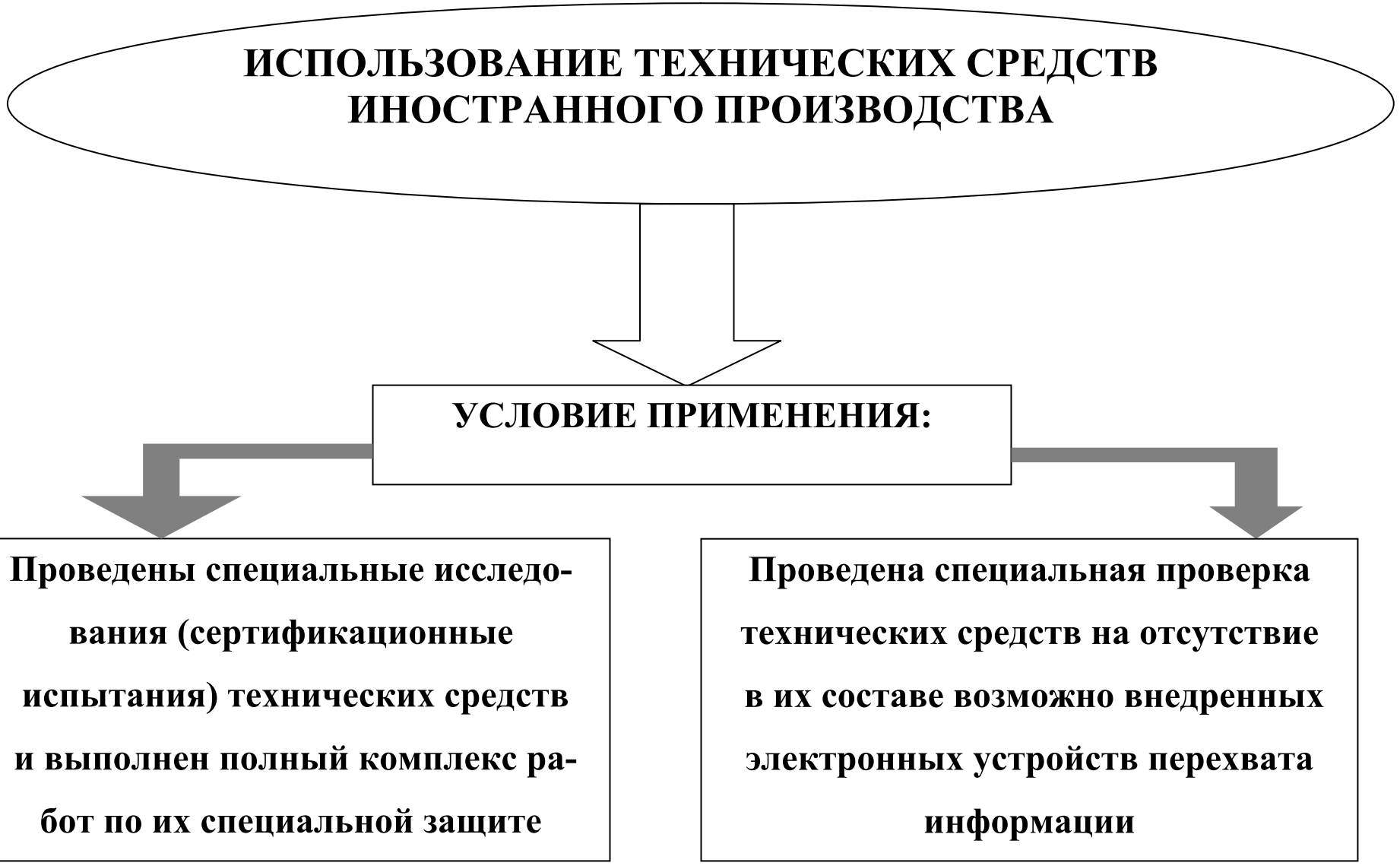
ПРИЧИНЫ:

Абсолютная защита сделает систему недоступной не только для взломщика, но и для хозяина

Система безопасности не может противостоять всем угрозам

Безопасность системы во многом зависит от “человеческого фактора”


ВИДЫ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ
РЕЧЕВАЯ ИНФОРМАЦИЯ
БАЗЫ ДАННЫХ
БУМАЖНЫЕ НОСИТЕЛИ
АКУСТИЧЕСКИЕ ЭЛЕКТРИЧЕСКИЕ СИГНАЛЫ ФИЗИЧЕСКИЕ ПОЛЯ
ИНФОРМАЦИЯ НА МАГНИТНЫХ, ОПТИЧЕСКИХ НОСИТЕЛЯХ
ИНФОРМАЦИЯ, ЦИРКУЛИРУЮЩАЯ В СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И СВЯЗИ, ТЕЛЕКОММУНИКАЦИЯХ


ИСПОЛЬЗОВАНИЕ ТЕХНИЧЕСКИХ СРЕДСТВ ИНОСТРАННОГО ПРОИЗВОДСТВА
УСЛОВИЕ ПРИМЕНЕНИЯ:
Проведены специальные исследования (сертификационные испытания) технических средств и выполнен полный комплекс работ по их специальной защите
Проведена специальная проверка технических средств на отсутствие в их составе возможно внедренных электронных устройств перехвата информации


ОБЪЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ
Выделенные помещения, предназначенные для ведения секретных переговоров
Средства и системы информатизации, программные средства, используемые для обработки секретной информации
Технические средства и системы, не обрабатывающие непосредственно секретную информацию, но размещенные в помещениях, где обрабатывается секретная информация


СРЕДА БЕЗОПАСНОСТИ
Область физической безопасности
Безопасность оборудования
Безопасность персонала
Безопасность программного обеспечения
Правовая безопасность
Безопасность телекоммуникационной среды

ПОКАЗАТЕЛИ КЛАССОВ ЗАЩИЩЕННОСТИ

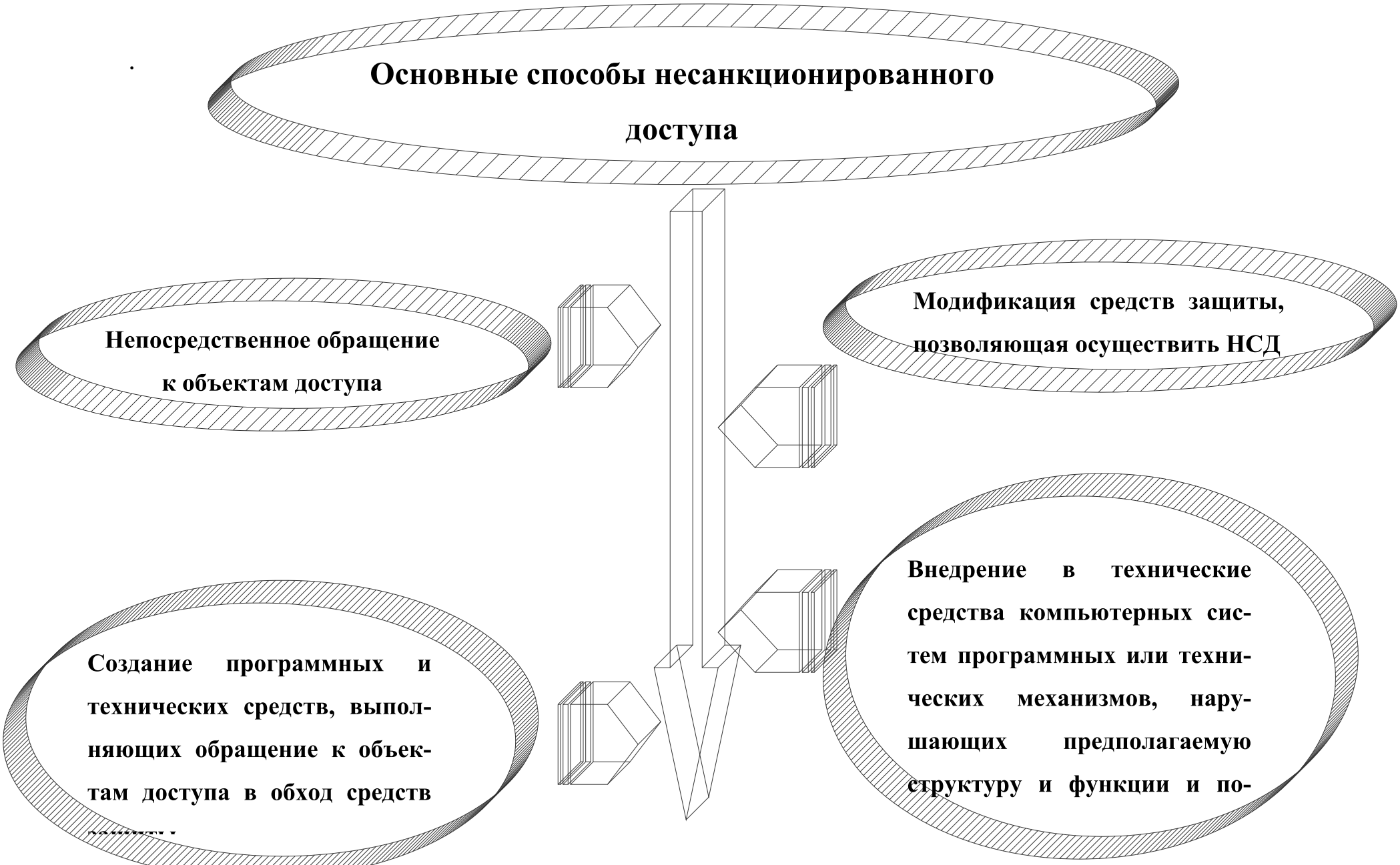
НАИМЕНОВАНИЕ ПОКАЗАТЕЛЯ	КЛАСС ЗАЩИЩЕННОСТИ					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	⮟	⮟	⮟	☑	⮟	☑
Мандатный принцип контроля доступа	▭	▭	⮟	☑	☑	☑
Очистка памяти	▭	⮟	⮟	⮟	☑	☑
Изоляция модулей	▭	▭	⮟	☑	⮟	☑
Маркировка документов	▭	▭	⮟	☑	☑	☑
Защита ввода вывода на отчуждаемый физический носитель информации	▭	▭	⮟	☑	☑	☑
Сопоставление пользователя с устройством	▭	▭	⮟	☑	☑	☑
Идентификация и аутентификация	⮟	☑	⮟	☑	☑	☑
Гарантии проектирования	▭	⮟	⮟	⮟	⮟	⮟
Регистрация	▭	⮟	⮟	⮟	☑	☑
Взаимодействие пользователя с комплексом средств защиты	▭	▭	▭	⮟	☑	☑
Надежное восстановление	▭	▭	▭	⮟	☑	☑
Целостность комплекса средств защиты	▭	⮟	⮟	⮟	☑	☑
Контроль модификации	▭	▭	▭	▭	⮟	☑

▭ - нет требований к данному классу;
⮟ - новые или дополнительные требования,
☑ - требования совпадают с требованиями к СВТ предыдущего класса.

ТЕМА № 3. ОСНОВЫ ОРГАНИЗАЦИИ ПРОТИВОДЕЙСТВИЯ НСД В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Меры по противодействию несанкционированному доступу к компьютерной информации

ТЕХНИЧЕСКИЕ	ОРГАНИЗАЦИОННЫЕ	ПРАВОВЫЕ
• Защита от несанкционированного доступа к информации криминалистических учетов • Резервирование компьютерных систем • Конструкционные меры защиты от хищений и диверсий • Использование резервного электропитания • Использование специальных программно-аппаратных комплексов	• Охрана компьютерных сетей • Подбор персонала • Программа восстановления работоспособности • Определение лиц ответственных за безопасность • Приказы и инструкции регламентирующие информационные технологии в ОВД	• **ЗАКОНЫ;** • закон «Об информации, информационных технологиях и о защите информации» • закон «О государственной тайне» • закон «Об оперативно-розыскной деятельности» • закон «О правовой охране топологий интегральных микросхем» • закон «О связи» • закон «О средствах массовой информации» • закон «Об авторском праве и смежных правах» • закон «О правовой охране программ для электронных вычислительных машин и баз данных» • Основы законодательства об Архивном фонде РФ и архивах • закон «Об обязательном экземпляре документов» • УК РФ • КоАП РФ и др. • Подзаконные акты; • **Судебная практика.**


Основные способы несанкционированного доступа
Непосредственное обращение к объектам доступа
Модификация средств защиты, позволяющая осуществить НСД
Создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств
Внедрение в технические средства компьютерных систем программных или технических механизмов, нарушающих предполагаемую структуру и функции и по-

МЕТОДЫ ОБНАРУЖЕНИЯ АТАК НА КОМПЬЮТЕРНУЮ ИНФОРМАЦИЮ

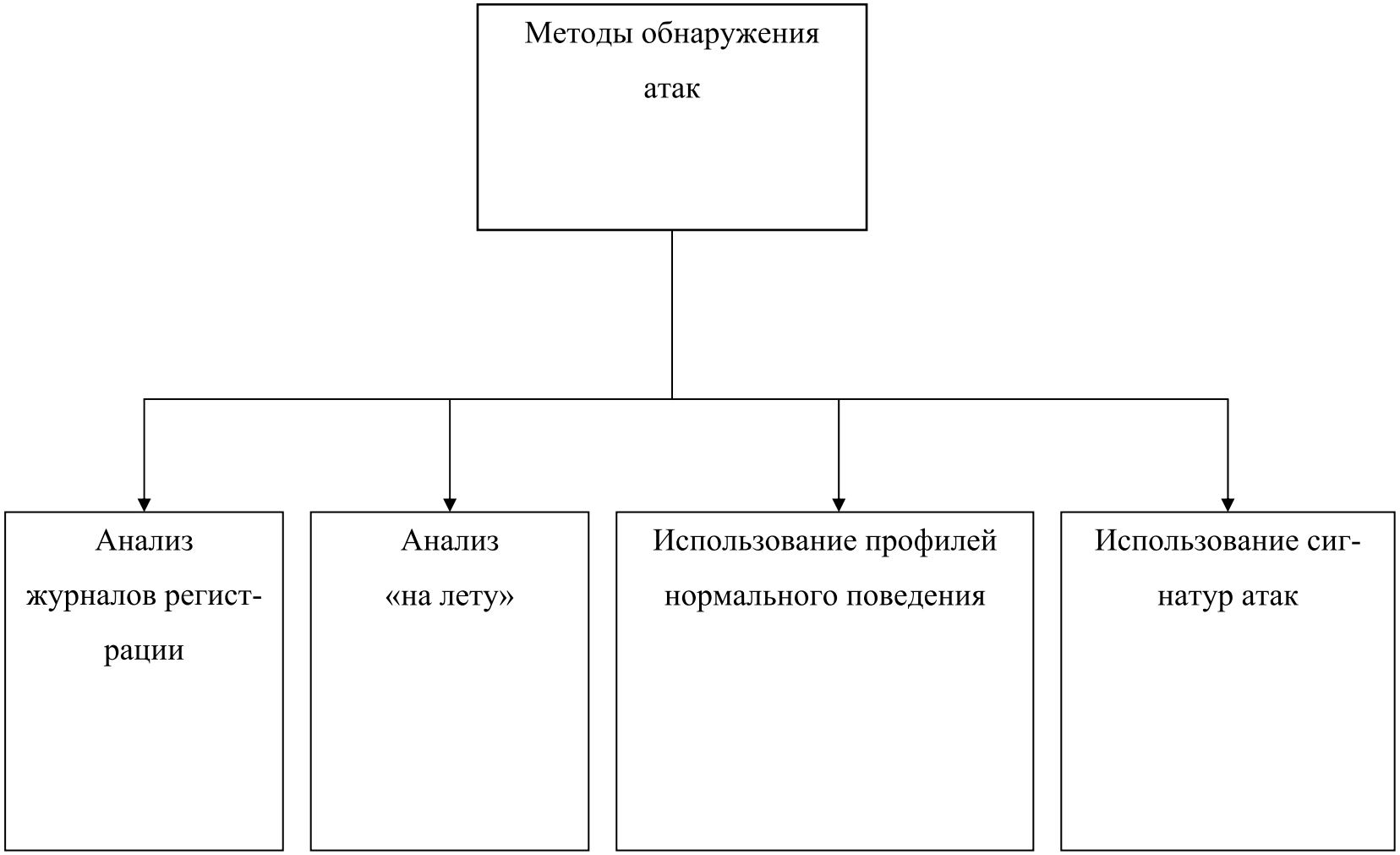
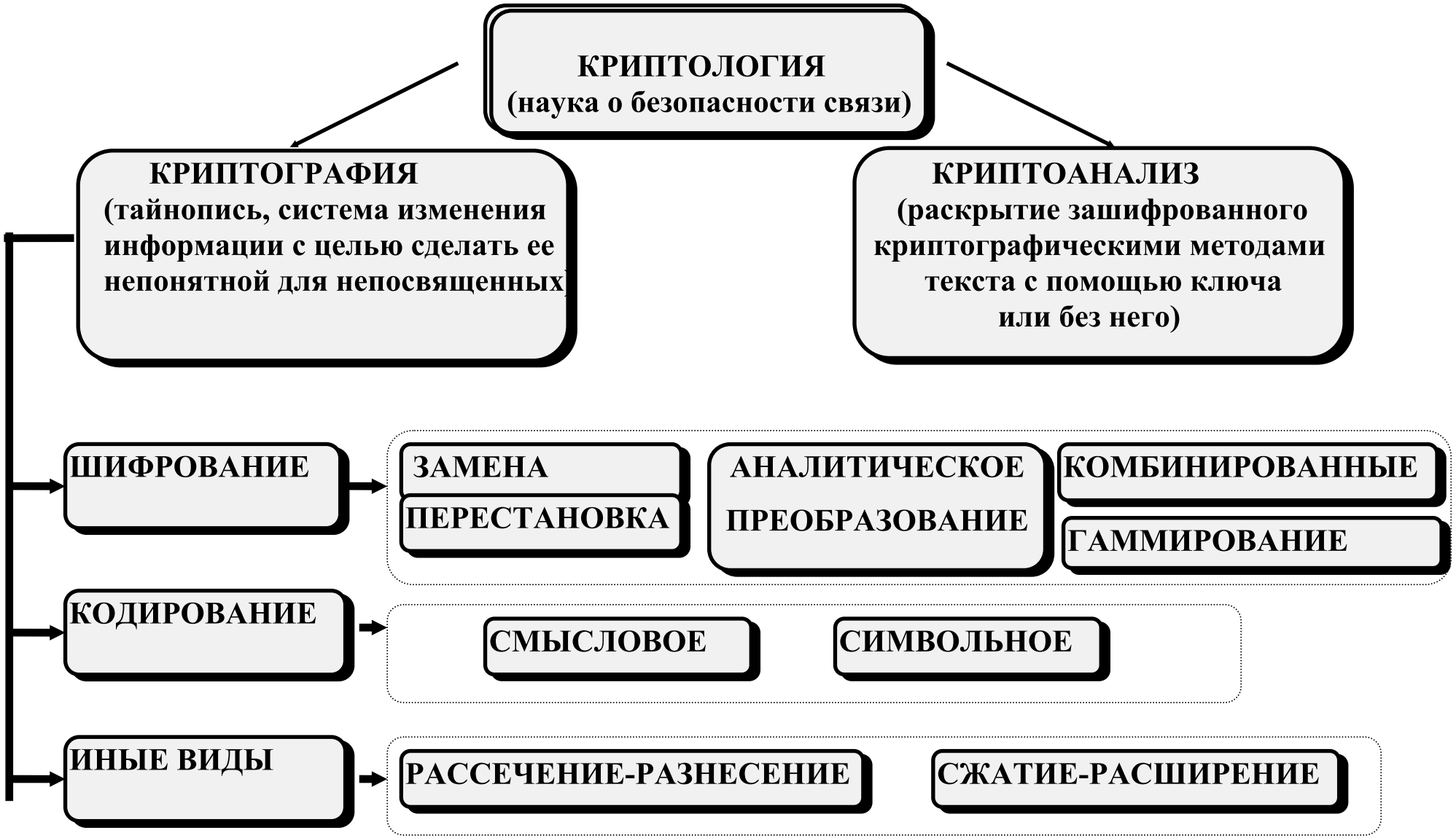


СХЕМА НАЗНАЧЕНИЙ ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

КЛАССИФИКАЦИЯ ВИДОВ НАРУШЕНИЯ РАБОТОСПОСОБНОСТИ СЕТИ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ ПО СПОСОБАМ НАНЕСЕНИЯ И ОБЪЕКТАМ ВОЗДЕЙСТВИЯ.

Способы нанесения	Объекты воздействия			
	Оборудование	Программы	Данные	Персонал
Раскрытие (утечка) информации	Хищение носителей информации, подключение к линии связи, несанкционированное использование ресурсов	Несанкционированное копирование, перехват	Хищение, копирование, перехват	Передача сведений о защите, разглашение, халатность
Потеря целостности информации	Подключение, модификация, спец. вложения, изменение режимов работы, несанкционированное использование ресурсов	Введение «троянских коней» и «жучков»	Искажение, модификация	Вербовка персонала
Нарушение работоспособности автоматизированной информационной сети	Изменение режимов функционирования, выход из строя, хищение, разрушение	Искажение, удаление, подмена	Искажение, удаление, навязывание ложных данных	Уход, физическое устранение


КРИПТОЛОГИЯ
(наука о безопасности связи)
КРИПТОГРАФИЯ
(тайнопись, система изменения информации с целью сделать ее непонятной для непосвященных)
КРИПТОАНАЛИЗ
(раскрытие зашифрованного криптографическими методами текста с помощью ключа или без него)
ШИФРОВАНИЕ
ЗАМЕНА
ПЕРЕСТАНОВКА
АНАЛИТИЧЕСКОЕ ПРЕОБРАЗОВАНИЕ
КОМБИНИРОВАННЫЕ
ГАММИРОВАНИЕ
КОДИРОВАНИЕ
СМЫСЛОВОЕ
СИМВОЛЬНОЕ
ИНЫЕ ВИДЫ
РАССЕЧЕНИЕ-РАЗНЕСЕНИЕ
СЖАТИЕ-РАСШИРЕНИЕ


СТАНДАРТНЫЕ ЗАЩИТНЫЕ СРЕДСТВА
АВТОНОМНОГО ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА
Средства защиты вычислительных ресурсов, использующие парольную идентификацию и ограничивающие доступ несанкционированного пользователя
Применение различных методов шифрования, независящих от контекста информации
средства защиты от копирования
защита от компьютерных вирусов

ТЕМА 4. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КАНАЛАХ СВЯЗИ.

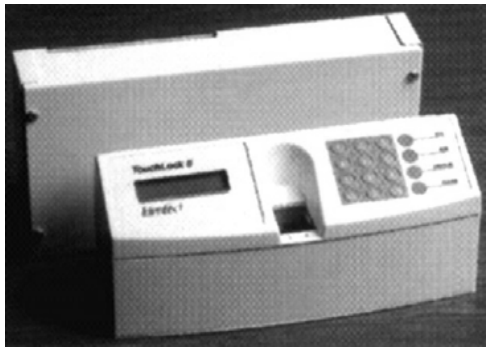
ТЕХНИЧЕСКИЕ СРЕДСТВА РАЗВЕДКИ.

РАДИО МИКРОФОНЫ	ЭЛЕКТРОННЫЕ «УШИ»	СРЕДСТВА ПЕРЕХВАТА ТЕЛЕФОННОЙ СВЯЗИ	СРЕДСТВА СКРЫТОГО НАБЛЮДЕНИЯ И ПОИСКА	СРЕДСТВА КОНТРОЛЯ КОМПЬЮТЕРА И СЕТЕЙ	СРЕДСТВА ПРИЕМА ЗАПИСИ, УПРАВЛЕНИЯ.
с автономным питанием	микрофоны с проводами	с непосредственным подключением	Оптические	пассивные средства контроля монитора	приемники для радиозакладок
с питанием от телефонной сети	электронные стетоскопы	с индукционным датчиком	фотографические	активные средства контроля монитора	устройства накопления и записи
с питанием от электросети	направленные микрофоны	с датчиками внутри телефонного аппарата	тепловизионные и ночного видения	пассивные средства контроля шины (магистрали)	средства переприема (ретрансляторы)
управляемые дистанционно	лазерные микрофоны	телефонной радиотрансляции	телевизионные	активные средства контроля шины (магистрали)	средства ускоренной передачи
с функцией включения по голосу	микрофоны с передачей по электросети	перехвата сотовой, телефонной связи	определения местоположения	аппаратные закладки	устройства дистанционного управления
Полуактивные	с использованием микрофона аппарата	перехвата пейджинговых сообщений	маркирования и целеуказания	программные закладки	источники питания
с накоплением и быстрой передачей	гидро-акустические микрофоны	много-канального перехвата	видео закладочные	компьютерные вирусы	вспомогательные и другие средства

ТЕХНИЧЕСКИЕ УСТРОЙСТВА КОНТРОЛЯ ДОСТУПА

- доступ по отпечатку пальца, идентификационному номеру и паролю
- использование оптического метода

Сканер



Контролирующее устройство

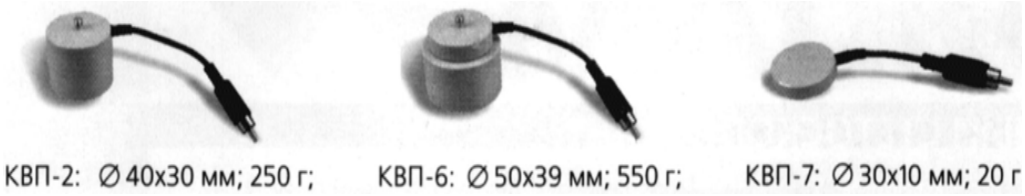
ВИБРОАКУСТИЧЕСКАЯ ЗАЩИТА

ШОРОХ-2

ШОРОХ-1

КОНТРОЛЬНЫЙ СТЕТОСКОП «СКИН»

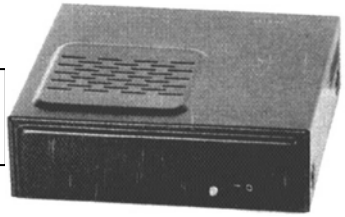
ВИБРОПРЕОБРАЗОВАТЕЛИ



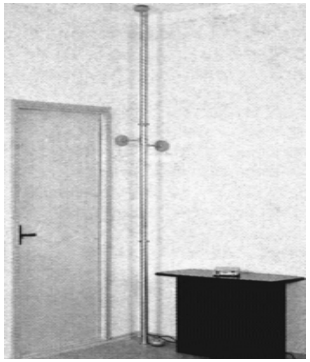
КВП-2: ∅40х30 мм; 250 г; КВП-6: ∅50х39 мм; 550 г; КВП-7: ∅30х10 мм; 20 г

СИСТЕМЫ ВИБРОАКУСТИЧЕСКОГО ЗАШУМЛЕНИЯ

VNG-006DM

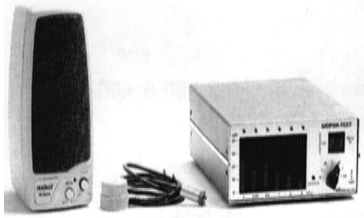


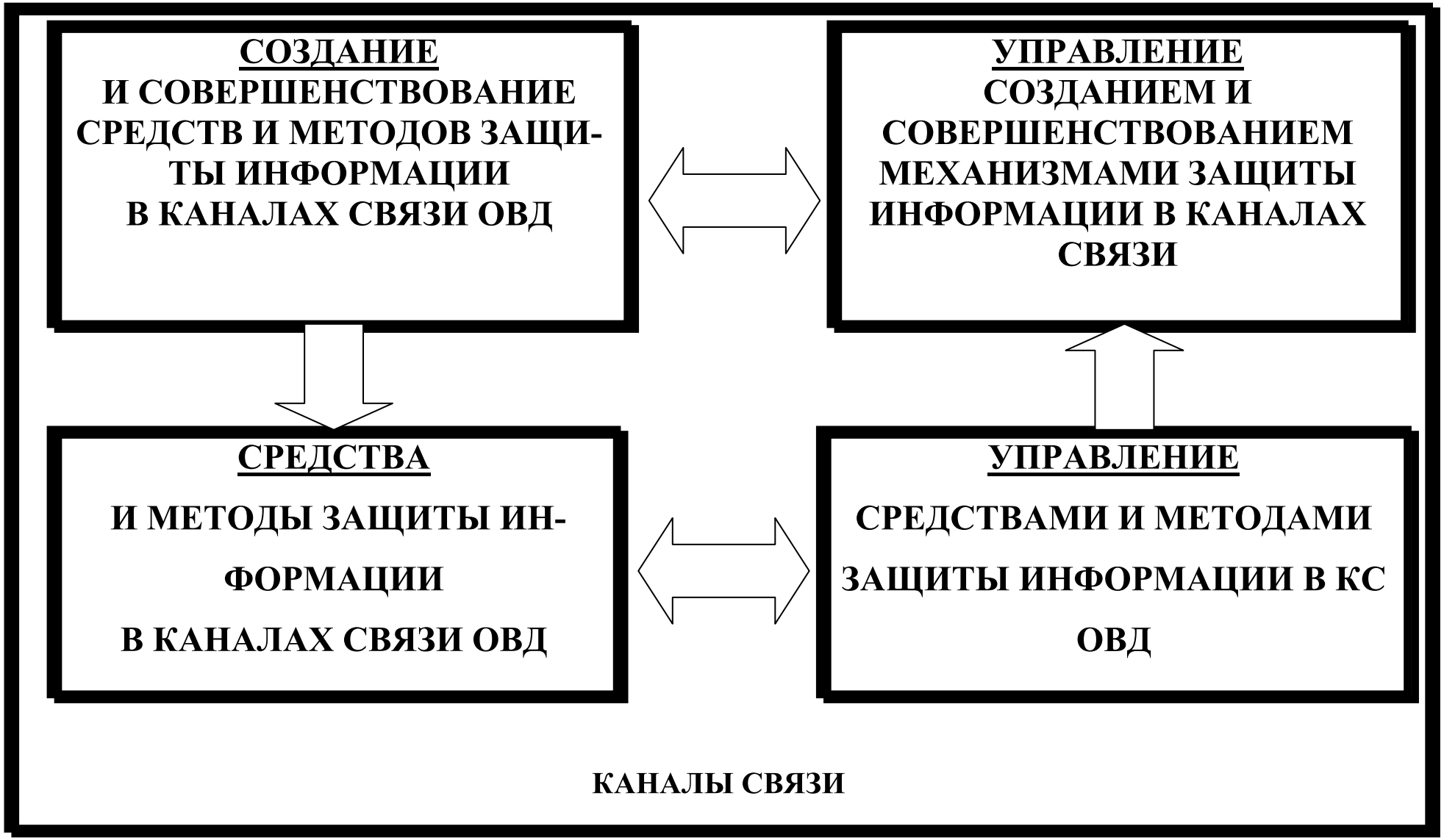
ФОН-В МОБИЛЬНАЯ



ИЗМЕРИТЕЛЬНЫЕ КОМПЛЕКСЫ

ШОРОХ-ТЕСТ




СОЗДАНИЕ
И СОВЕРШЕНСТВОВАНИЕ СРЕДСТВ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ ОВД
УПРАВЛЕНИЕ СОЗДАНИЕМ И СОВЕРШЕНСТВОВАНИЕМ МЕХАНИЗМАМИ ЗАЩИТЫ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ
СРЕДСТВА
И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ ОВД
УПРАВЛЕНИЕ
СРЕДСТВАМИ И МЕТОДАМИ ЗАЩИТЫ ИНФОРМАЦИИ В КС ОВД
КАНАЛЫ СВЯЗИ

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В КАНАЛАХ СВЯЗИ

ЗАЩИТА ТЕЛЕФОННЫХ ЛИНИЙ

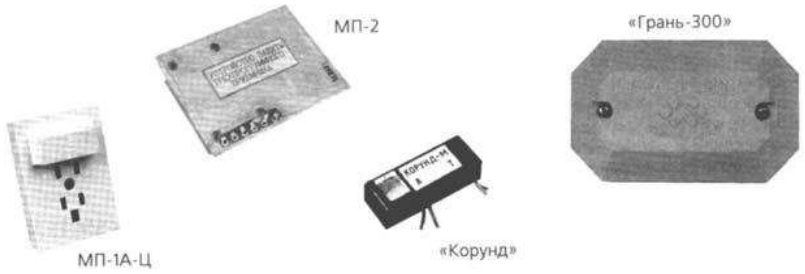
TF-012

ПРОКРУСТ-2000

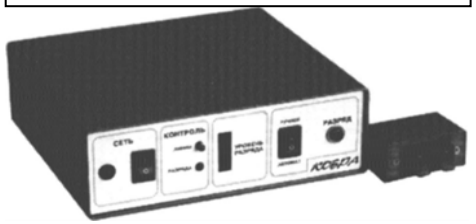
ГРОТ SCR-M1

Защита ТЛФ линии от закладок, предотвращение съема по этим линиям и передачи информации до АТС

Защита средств от утечки информации за счет микрофонного эффекта и ВЧ-навязывания



КОБРА



СКРЕМБЛЕРЫ

Шифрация речевого сети сигнала и защита факсимильных сообщений, передаваемых по телефонной

ТЕМА № 5. МОДЕЛИ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ОПРЕДЕЛЯЕМЫЕ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ВНЕШНИЕ УГРОЗЫ
(представляющие наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах)

- разведывательная деятельность специальных служб иностранных государств, международных преступных сообществ, организаций и групп, связанная со сбором сведений, раскрывающих задачи, планы деятельности, техническое оснащение, методы работы и места дислокации специальных подразделений и органов внутренних дел Российской Федерации;
- деятельность иностранных государственных и частных коммерческих структур, стремящихся получить несанкционированный доступ к информационным ресурсам правоохранительных и судебных органов.

ВНУТРЕННИЕ УГРОЗЫ
(представляющими наибольшую опасность для объектов обеспечения информационной безопасности в правоохранительной и судебной сферах):

- нарушение установленного регламента сбора, обработки, хранения и передачи информации, содержащейся в картотеках и автоматизированных банках данных и использующейся для расследования преступлений;
- недостаточность законодательного и нормативного регулирования информационного обмена в правоохранительной и судебной сферах;
- отсутствие единой методологии сбора, обработки и хранения информации оперативно-розыскного. справочного, криминалистического и статистического характера;
- отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах;

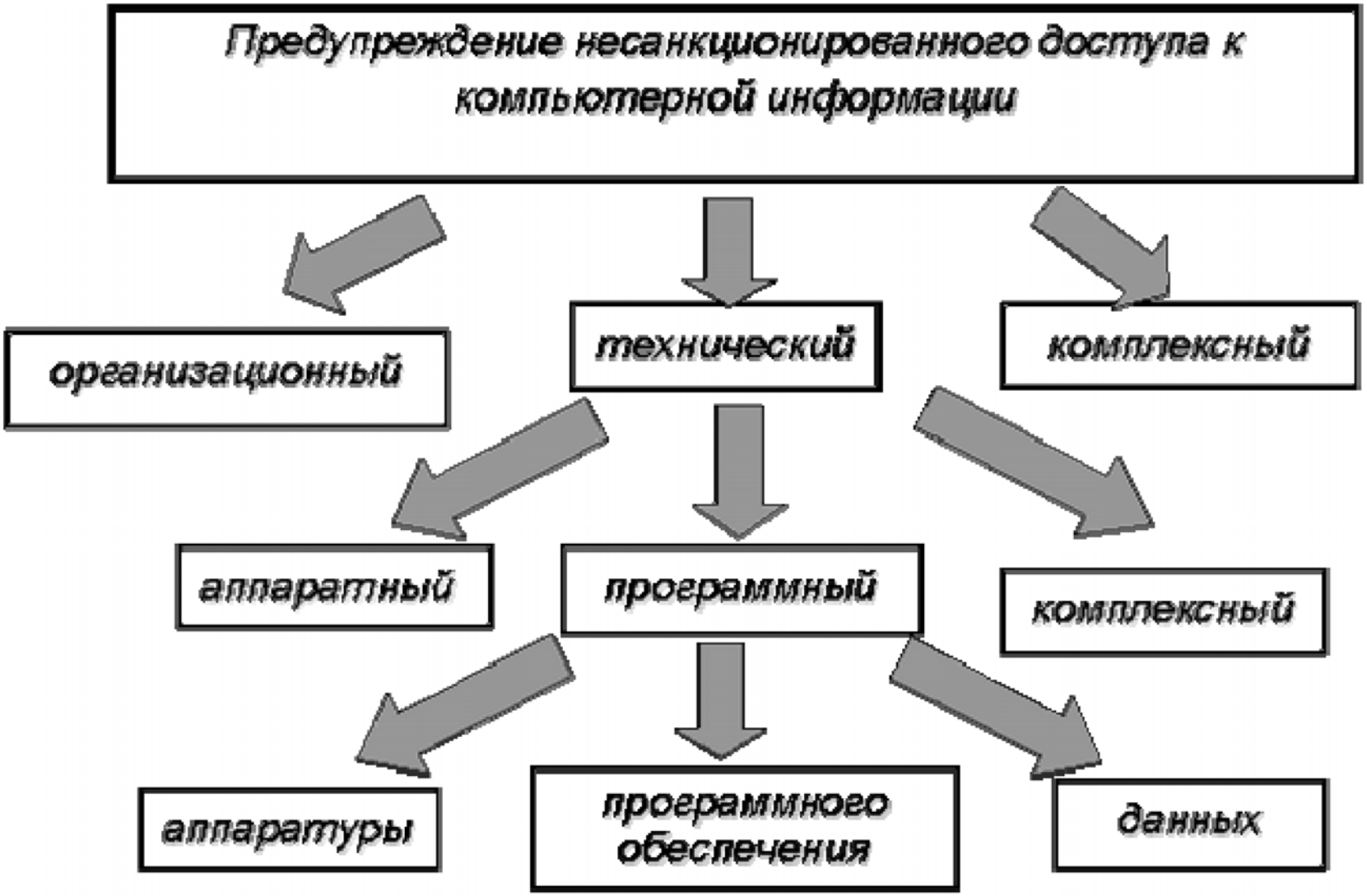
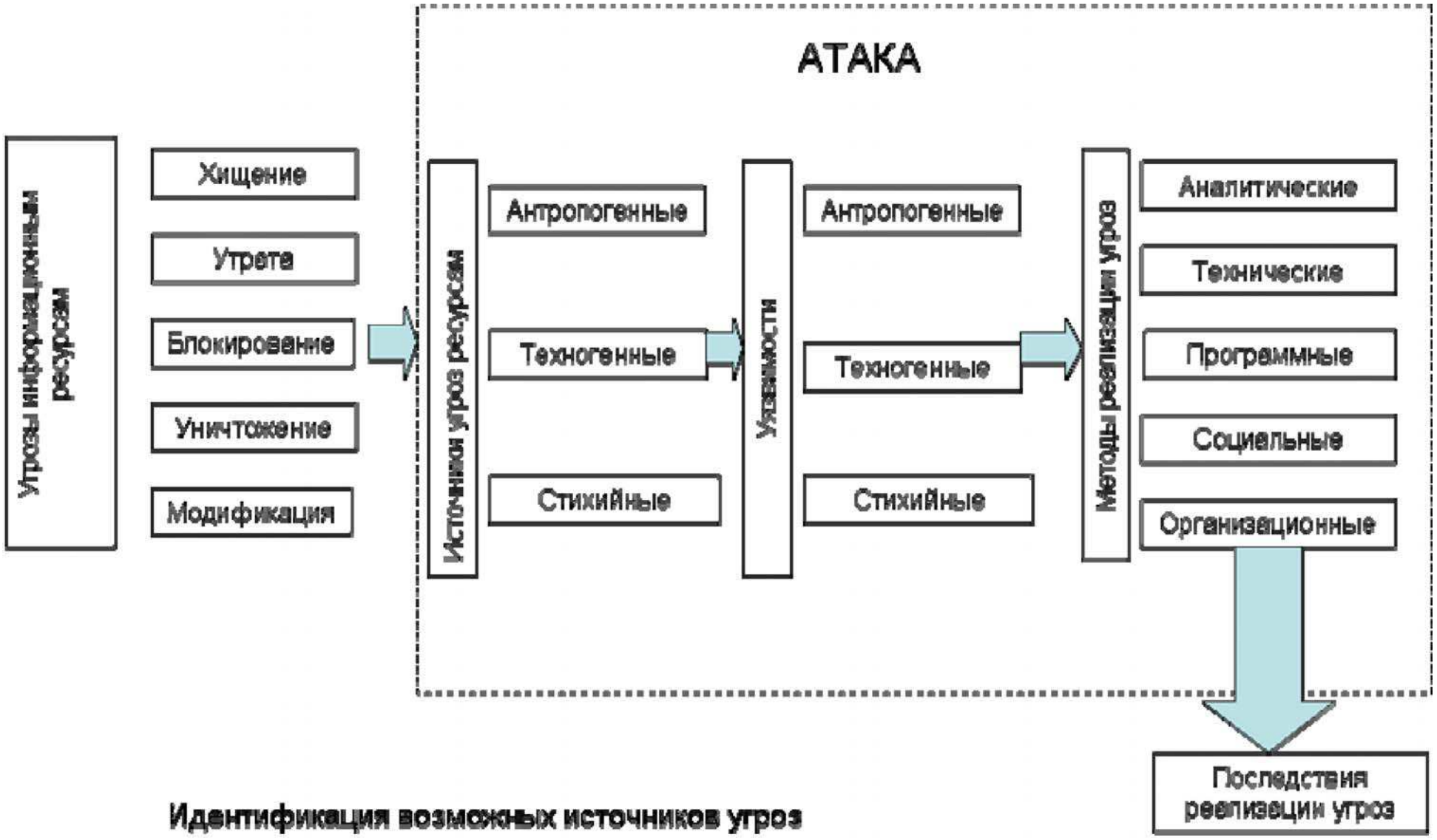
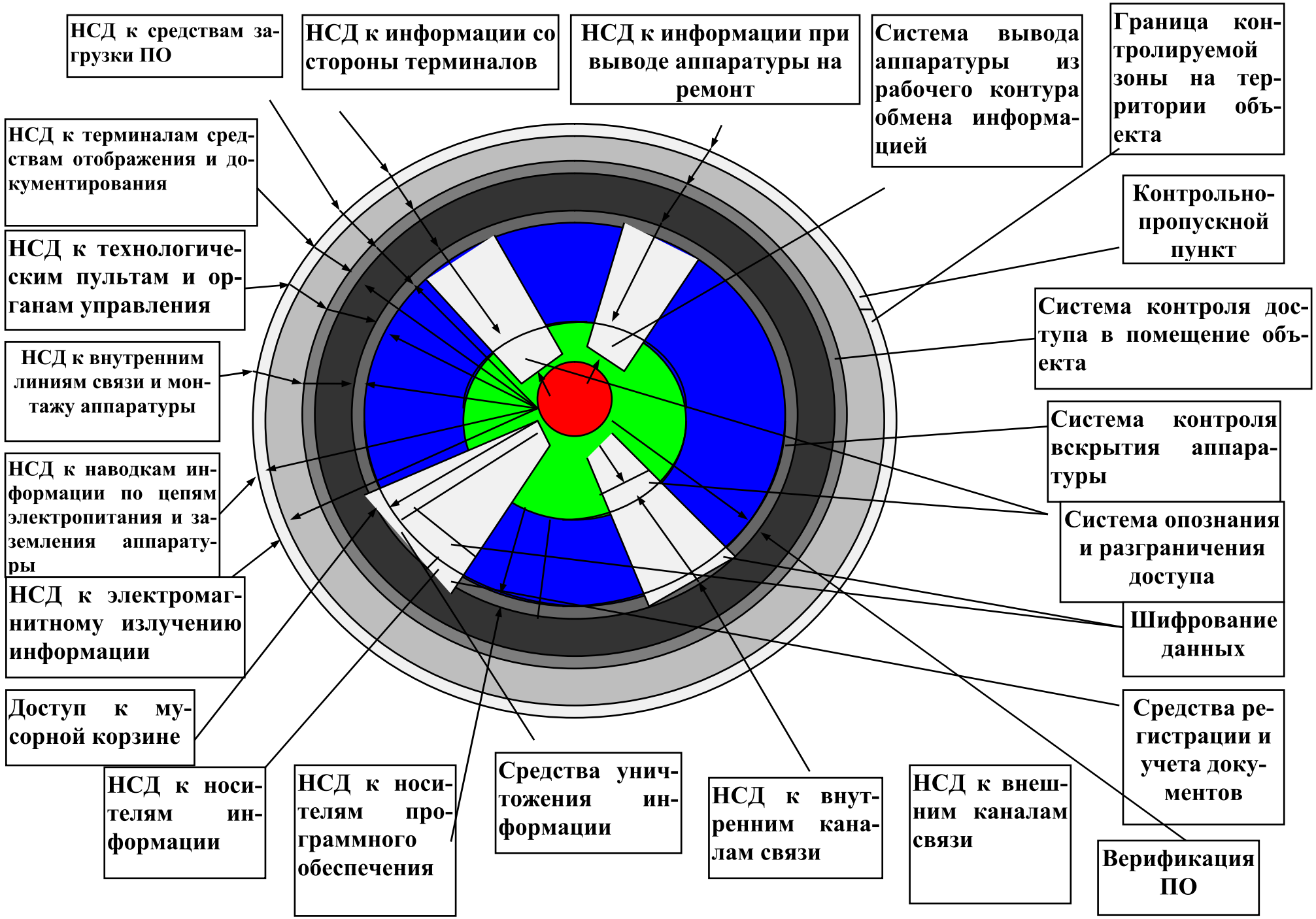


Рисунок 3.6. *Предупреждение несанкционированного доступа к компьютерной информации криминалистических учетов ОВД*

МОДЕЛЬ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНОЙ СЕТИ




НСД к средствам загрузки ПО
НСД к информации со стороны терминалов
НСД к информации при выводе аппаратуры на ремонт
Система вывода аппаратуры из рабочего контура обмена информацией
Граница контролируемой зоны на территории объекта
НСД к терминалам средствам отображения и документирования
Контрольно-пропускной пункт
НСД к технологическим пультам и органам управления
Система контроля доступа в помещение объекта
НСД к внутренним линиям связи и монтажу аппаратуры
Система контроля вскрытия аппаратуры
НСД к наводкам информации по цепям электропитания и заземления аппаратуры
Система опознания и разграничения доступа
НСД к электромагнитному излучению информации
Шифрование данных
Доступ к мусорной корзине
Средства регистрации и учета документов
НСД к носителям информации
НСД к носителям программного обеспечения
Средства уничтожения информации
НСД к внутренним каналам связи
НСД к внешним каналам связи
Верификация ПО

№	У Г Р О З Ы	ПОТЕНЦИАЛЬНО ВОЗМОЖНЫЕ СРЕДСТВА ПРОТИВОДЕЙСТВИЯ		
	Наименование	Технические	Программные	Организационные
1	хищение носителей информации на неисправных компьютерах	установки уничтожения информации		организация уничтожения информации, контроль надежности уничтожения, документальное оформление актов уничтожения
2	подслушивание разговоров	оборудование помещений шумопоглащающими средствами		
4	использование визуальных оптических средств наблюдения	использование специальных стекол в окнах, установка экранов и штор		расположение надлежащим образом устройств
7	перехват ЭМИ линий связи	использование экранирующих кабелей, шифрующей аппаратура	программное шифрование	организация охраны территории вокруг помещения, использование технических средств в защищенном исполнении
10	нарушения режима работы путем подключения генератора помех		программный комплекс контроля аппаратуры	организационный контроль состава аппаратуры
11	сбор отходов	установка измельчающих устройств		организация контролируемого сбора и уничтожения
12	несанкционированное копирование информации устройств отображения	установка экранов	программы гашения экранов	

ПРИЛОЖЕНИЕ 1

Основные термины и определения:

А

Администратор защиты - субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации

Активное средство защиты - средство, обеспечивающее создание активных помех средствам технической разведки (промышленного шпионажа) или разрушение нормального функционирования этих системы средств.

Акустический канал утечки информации - это физический путь от источника акустических сигналов (человек, техника) к нарушителю за счет механических колебаний среды распространения (воздух, жесткие среды, вода, жидкости).

Анализ риска – процесс определения угроз безопасности системы и отдельным ее компонентам, определения их характеристик и потенциального ущерба, а также разработка мер защиты.

Антивирус - программа, обнаруживающая или обнаруживающая и удаляющая вирусы. Если вирус удалить невозможно, зараженная программа уничтожается.

Аппаратные средства защиты -механические, электромеханические, электронные, оптические, лазерные, радио-, радиотехнические, радиолокационные и другие устройства, системы и сооружения, предназначенные для защиты информации от несанкционированного доступа, копирования, кражи или модификации. анализа

Аппаратура засекречивания - специальные технические устройства для автоматического шифрования (дешифрования) телефонных и телеграфных переговоров (сообщений). см. Скремблер

Аттестация - оценка на соответствие определенным требованиям. С точки зрения защиты аттестации подлежат объекты, помещения, технические средства, программы, алгоритмы на предмет соответствия требованиям зашиты информации по соответствующим классам безопасности.

Аудит – форма независимого, нейтрального контроля какого-либо направления деятельности коммерческого предприятия.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности

Б

Безопасность - состояние защищенности жизненно важных интересов личности, предприятия, общества и государства от внутренних и внешних угроз. Безопасность достигается проведением единой государственной политики в области обеспечения безопасности, системой мер экономического, политического, организационного и иного характера, адекватных угрозам жизненно важным интересам личности, общества и государства.

Безопасность информационная - это проведение правовых, организационных и инженерно-технических мероприятий пи формировании и использовании информационных технологий, инфраструктуры и информационных ресурсов, защите информации высокой значимости и прав субъектов, участвующих в информационной деятельности.

Безопасность информационной сети - меры, предохраняющие информационную сеть от несанкционированного доступа, случайного или преднамеренного вмешательства в нормальные действия ли попыток разрушения ее компонентов.

Включает защиту оборудования, программного обеспечения, данных.

Блокировка, блокирование - изоляция или приведение объекта в состояние, препятствующее выполнению определенных несанкционированных действий.

Бомба - тайное встраивание в программу команд, которые должны срабатывать один или несколько раз при определенных условиях. Существуют варианты с "логической" или "временной" бомбой.

В

Верификация - процесс сравнения двух уровней спецификации средств вычислительной техники или автоматизированных систем на надлежащее соответствие

Визуально-оптический канал утечки информации - это физический путь от источника излучения отражения электромагнитной энергии в ультрафиолетовом, видимом или инфракрасном спектре через воздушное пространство к злоумышленнику.

Вирус компьютерный - небольшая, достаточно сложная, тщательно составленная и опасная программа, которая может самостоятельно размножаться, переносить себя на диски, прикрепляться к чужим программам и передаваться по информационным сетям.

Г

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

Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России) является органом государственного управления Российской Федерации и в пределах своей компетенции осуществляет руководство органами защиты информации, составляющей государственную и служебную тайну в политической, научно-технической и других сферах.

Гриф секретности - реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставленные на самом носителе и (или) в сопроводительной документации на него. Установлено три степени секретности сведений, составляющих гостайну, и соответствующие грифы секретности: "особой важности", "совершенно секретно" и "секретно".

Д

Данные - сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их проявления, отображенные на материальном носителе, используемые в целях сохранения знаний.

Дешифратор - устройство для автоматической расшифровки сообщения (сигнала). Применяется в системах криптографической защиты информации.

Дешифрование - процесс, противоположный шифрованию. Широко используется для снятия шифров сигналов (сообщений) и распознавания результатов фотосъемки объектов разведки.

Дискреционное управление доступом - разграничение доступа между поименованными субъектами и поименованными объектами. Субъект с определенным правом доступа может передать это право любому другому субъекту

Документированная информация -(документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Допуск к государственной тайне - процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений.

Достоверность - оценка вероятности отсутствия ошибок в информации (документах, схемах, данных).

Достоверность информации - соответствие полученной информации действительной обстановке. Достигается: обозначением времени свершения событий, сведения о которых передаются; тщательным изучением и сопоставлением данных, полученных из различных источников; проверкой сомнительных сведений; своевременным скрытном дезинформационных и маскировочных мероприятий; исключением искаженной информации, передаваемой по техническим средствам.

Доступ к информации - ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение

Ж

Жалюзи - ставни, шторы и т.п. из параллельных пластинок (неподвижных или поворачивающихся). Устанавливаются для защиты от визуального наблюдения и акустического подслушивания на окнах.

Жучок – установка радиомикрофона в помещение, технические средства, бытовую технику различного назначения с целью перехвата разговоров.

З

Закрытые данные - данные, доступные ограниченному кругу пользователей. Как правило, ограничение доступа осуществляется системой разграничения с помощью определенных правил (паролей).

Засекреченная связь - связь, при которой информация, передаваемая по телефону, телеграфу, фототелеграфу, шифруется (дешифруется) аппаратурой засекречивания в процессе передачи (приема). Имеет целью скрыть информацию от ознакомления с ее содержанием.

Зашифрованные данные - данные, хранящиеся в шифрованном виде (в документах, в памяти ЭВМ и т.п.), т.е. данные, к которым применен способ криптографической защиты.

Защита вычислительной сети - исключение несанкционированного доступа пользователей к элементам и ресурсам сети путем использования организационных мероприятий, аппаратных, программных и методов и средств.

Защита государственных секретов - принятие предусмотренных законами и подзаконными актами правовых, организационных, инженерно-технических и иных мер по ограничению распространения сведений, отнесенных к государственным секретам.

Защита данных - меры сохранения данных от нежелательных последствий, которые неумышленно или преднамеренно ведут к их модификации, раскрытию или разрушению.

Защита информации - комплекс мероприятий, проводимых с целью предотвращения утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), несанкционированного копирования, блокирования информации и т.п.

Защищенное средство вычислительной техники - средство (автоматизированная система), в котором реализован комплекс средств защиты

Защищенность - способность системы противостоять несанкционированному доступу к конфиденциальной информации, ее искажению или разрушению. Защищенность информации можно рассматривать как с позиций технической защиты от несанкционированного доступа (свойство недоступности), так и социально-психологических по степени конфиденциальности и секретности (свойство конфиденциальности).

Звукомаскировка – комплекс мероприятий, направленных на снижение уровня демаскирующих шумов, снижения уровня речевых сигналов, а также создание помех, затрудняющих ведение акустической разведки.

И

Идентификатор объекта доступа - уникальный признак субъекта или доступа

Идентификация - присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов

Инженерно-техническая защита - совокупность организационных, организационно-технических и технических мероприятий, обеспечивающих защиту физических

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

Информация конфиденциальная – документированная информация, доступ к которой ограничивается в соответствии с законами о коммерческой, промышленной и профессиональной тайне, государственной службе.

Информация ограниченного доступа - подразделяется на секретную и конфиденциальную.

Информация секретная - информация, содержащая в соответствии с Законом Российской Федерации "О государственных секретах" сведения, составляющие государственную тайну.

Информационная безопасность - состояние информации, информационных ресурсов, информационных систем, при котором с требуемой вероятностью обеспечивается защита информации от утечки, хищения, утраты, несанкционированного уничтожения, искажения , модификации (подделки), копирования, блокирования и т.п.

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах), являющиеся предметом отношений юридических и физических лиц, государства.

Источник конфиденциальной информации (ИКИ) – обладатель (носитель) охраняемый сведений, представленных в определенной физической форме. ИКИ выступают люди, документы, публикации, издания, изделия, продукция, технические средства обеспечения производственной деятельности, производственные и промышленные отходы.

К

Канал проникновения - физический путь от нарушителя к конфиденциальной информации, посредством которого возможен несанкционированный доступ к охраняемым сведениям.

Канал распространения информации - физический путь от источника конфиденциальной информации к субъекту (субъектам) общения, посредством которого возможно разглашение охраняемых сведений. К каналам распространения относятся средства информационной коммуникации и массовой информации, такие как связь, почта, выставки, радио, телевидение, пресса и т.д. и т.п.

Канал связи - физическая среда, аппаратные и в некоторых каналах программные средства передачи информации.

Канал утечки информации - неконтролируемый физический путь от источника информации за пределы организации или круга лиц, обладающих охраняемыми сведениями, посредством которого возможно неправомерное овладение злоумышленниками конфиденциальной информацией. Для образования канала утечки необходимы определенные пространственные, временные и энергетические условия и соответствующие средства приема, накопления и обработки информации на стороне злоумышленников.

Канальное шифрование - применение процедур шифрования информации (данных) в каждом канале их передачи.

Класс защищенности средств вычислительной техники (автоматизированной системы) - определенная совокупность требований по защите средств вычислительной техники (автоматизированной системы) от несанкционированного доступа к информации

Ключ защиты - ключ, присваиваемый операционной системой программе и используемый для сравнения с ключом памяти при обращении этой программы с целью защиты памяти.

Ключ криптографический – последовательность символов, которые управляют процедурами шифрования и дешифрования.

Ключевая система - совокупность правил, определяющих порядок генерации, распределения, использования, хранения, смены, уничтожения, восстановления крипта графических ключей.

Код - система условных обозначений (группа цифр, букв или других символов) для и, передачи сведений конфиденциального характера по техническим средствам связи.

Кодирование информации - преобразование информации в целях ее цифрового представления при обработке на технических средствах.

Коммерческая тайна - не являющиеся государственными секретами сведения, связанные с производством, технологической информацией, управлением, финансами и другой деятельностью предприятия, разглашение или утечка которых может нанести ущерб его интересам. Не могут составлять коммерческую тайну учредительные документы и устав; документы, дающие право заниматься предпринимательской деятельностью; сведения по установленным формам отчетности о финансово-хозяйственной деятельности; сведения о численности, составе работающих, их заработной плате и условиях труда, а также о наличии свободных мест; документы об уплате налогов и обязательных платежей; сведения о загрязнении окружающей среды; сведения об участии должностных лиц предприятий в кооперативах, малых предприятиях, товариществах и т.д.

Комплекс средств защиты - совокупность программных и технических средств, создаваемая и поддерживаемая для обеспечения защиты средств вычислительной техники или автоматизированных систем от несанкционированного доступа к информации.

Компьютерное мошенничество - преступное искажение программы, а также запись и использование искаженных данных. Целью компьютерного мошенничества является, как правило, незаконное получение имущественных выгод для себя или других лиц. Особое распространение получило за рубежом.

Компьютерный вирус см. Вирус компьютерный.

Компьютерный саботаж - нарушение функционирования информационной системы посредством манипуляций с программным обеспечением (уничтожение или фальсификация информации) или аппаратурой (повреждение или разрушение средств информационной техники).

Компьютерный червь - специальная программа, предназначенная для преодоления разнообразных форм защиты. Эти программы в отличие от ВИРУСОВ размножаются сами по себе (для размножения вирусов требуется носитель).

Контроль доступа - предупреждение несанкционированного доступа к защищенным данным.

Контроль доступа к информации вычислительной системы (ВС) реализуется последовательным применением трех процедур:

- идентификации (присвоения объектам ВС конкретных имен или кодов с целью последующего опознания и учета факторов обращения, объединяемых в виде записей в так называемой «таблице авторизации», которая хранится в памяти ВС);
- установления аутентичности (проверки подлинности объекта с помощью определенной информации, содержащейся в «матрице доступа» (списке ЛВК и запрещаемых объектов) и позволяющей убедиться в истинности обращения);
- проверки полномочий (проверки информации, содержащейся в «матрице полномочий» по каждому объекту, о допустимых процедурах со стороны запрашиваемого).

Контроль электромагнитных излучений – определение уровня (мощности) электромагнитного излучения в пределах контролируемой зоны и сравнение с допустимыми нормами.

Конфиденциальность – правовой режим информации, не подлежащей огласке.

Концепция защиты информации - система взглядов, требований и условий организации защиты охраняемых сведений от разглашения, утечки и несанкционированного доступа к ним через различные каналы.

Кража программного обеспечения - незаконное приобретение или использование программ, записанных в памяти ЭВМ. Эти преступления затрагивают интересы как отдельных лиц, так и государства.

Криптоанализ - раскрытие зашифрованного криптографическими методами текста с помощь известного ключа или без него (за счет вскрытия неизвестного ключа).

Криптография - тайнопись, система изменения информации (текста, речи) с целью сделать ее непонятной для непосвященных лиц.

Криптология - наука о безопасности (секретности) связи. Включает криптографию (шифрование) и криптоанализ.

Криптопреобразование - совокупность операций шифрования и дешифрования информации.

Крэкер - разновидность хэкеров, занимающаяся воровством чужой информации.

Л

Лазерная разведка – добывает информацию об объектах разведки с помощью лазерных систем. Лазерные локационные системы используют оптические сигналы и работают в режиме импульсного зондирования. Их важным достоинством является возможность высокоточного измерения угловых координат и дальности до цели при сравнительно небольших габаритных размерах и массе. Лазерные устройства в определенных условиях позволяют обнаруживать и подслушивать на расстоянии переговоры, ведущиеся в помещениях.

Люк - способ, обеспечивающий вставку в программу дополнительно одной или нескольких программ. Обычно это делается за счет "разрыва" программы.

М

Мандатное управление доступом разграничение доступа субъектов к объектам, основанное на использовании метки конфиденциальности информации, дающей право доступа к информации заданного уровня конфиденциальности.

Маскарад - незаконное проникновение в компьютерную систему по кодам и другим идентификаторам законных пользователей.

Маскировка – комплекс мероприятий по введению противника в заблуждение относительно наличия и расположения объектов, их деятельности и намерений. Способы маскировки: скрытие, имитация, демонстративные действия и дезинформация.

Математическая защита информации – математические и криптографические средства, используемые для кодирования, шифрования или иного преобразования информации, в результате которого содержание становится недоступным без предъявления некоторой специальной информации и ее обратного использования.

Математическое обеспечение СЗИ совокупность математических методов, моделей и алгоритмов для решения задач оценки опасности и мер защиты информации.

Материально-вещественный канал утечки информации - это физический путь от источника (носителя) к злоумышленнику в виде ′жестких масс, жидкостей или газообразных веществ.

Матрица полномочий – прямоугольная матрица, элемент которой означает право (полномочия) соответствующего объекта (субъекта) относительно соответствующего элемента защищаемых сведений.

Методологические основы защиты информации – а) совокупность научных принципов, обеспечивающих соблюдение требований системно-концептуального подхода при исследовании и разработки проблем защиты информации; б) совокупность методов, необходимых и достаточных для оптимальной реализации этих принципов.

Многоуровневая защита - защита, обеспечивающая разграничение доступа субъектов с различными ¦правами доступа к объектам различных уровней конфиденциальности

Модель - система объектов или процессов, свойства которых в каком-либо смысле подобны свойствам другой системы или процесса.

Модель защиты - абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств и/или организационных мер от несанкционированного доступа

Модель нарушителя правил разграничения доступа - абстрактное (формализованное или ¦неформализованное) описание нарушителя правил разграничения доступа

Модели общие систем и процессов защиты информации модели определяющие (оценивающие) общие характеристики указанных систем и процессов в отличие от моделей локальных и частных, которые обеспечивают определение (оценки) некоторых локальных или частных характеристик систем или процессов.

Н

Нарушение - попытка несанкционированного доступа к любой части подлежащей защите информации, хранимой, обрабатываемой и передаваемой в автоматизированных системах управления.

Нарушитель - субъект, имеющий доступ к работе со штатными средствами АС и СВТ как части АС. Нарушители классифицируются по уровню возможностей, предоставляемых им штатными средствами АС и СВТ.

Несанкционированный доступ - доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Носители сведений, с**оставляющие государственную тайну,** - материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образцов, сигналов, технических решений и процессов.

О

Обоснованность засекречивания сведений – установление путем экспертной оценки целесообразности засекречивания конкретных сведений, вероятных экологических или иных последствий этого акта, исходя из баланса жизненно важных интересов государства, общества и граждан.

Обследование - изучение реальных объектов (помещений, оборудования, технических средств) как возможных источников конфиденциальной информации. В процессе обследования определяются структура, тип объекта (помещение, оборудование, технические средства) на предмет отнесения его к какой-либо группе конфиденциальности, выявляются возможные каналы утечки коммерческих секретов и вырабатываются необходимые защитные мероприятия.

Объект доступа - единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Ограждения - средства физического ограничения доступа на охраняемые территории, зоны, помещения. Применяются средства охраны по периметру в виде многорядных сетчатых или

проволочных заграждений. С внутренней стороны заграждений сооружаются препятствия, исключающие возможность протаранивания заграждения транспортными средствами.

Ограничения на ПЭМИН - организационные мероприятия, уменьшающие мощность, дальность и направления распространения побочных электромагнитных излучений и наводок (ПЭМИН). Реализуются в виде пространственных, территориальных, временных и энергетических ограничений.

Опознавание - установление типа, вида обнаруженного объекта его государственной или ведомственной принадлежности. Опознавание может быть визуальным, акустическим, радиоэлектронным. визуальное опознавание осуществляется невооруженным глазом или с помощью оптических приборов по опознавательным (демаскирующим) признакам, обозначающим государственную принадлежность объектов или по характерным признакам.

Организационная защита - регламентация производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, что разглашение, утечка и несанкционированный доступ к конфиденциальной информации становится невозможным или существенно затрудняется за счет организационных мероприятий.

Организационно-правовое обеспечение защиты информации - представляет собой упорядоченную совокупность организационных решений, законов, нормативов и правил, регламентирующих как общую организацию работ по защите информации, так и создание и функционирование систем защиты информации в конкретных автоматизированных системах обработки информации.

Организационно-технические мероприятия – мероприятия, обеспечивающие блокирование возможных каналов утечки информации через технические средства обеспечения производственной и трудовой деятельности с помощью специальных технических средств.

Организационные мероприятия – мероприятия ограничительного характера, сводящиеся в основном к регламентации доступа к конфиденциальности информации или режиму использования технических средств.

Охраняемая зона – территория объекта, на которой исключено неконтролируемое пребывание лиц, не имеющих на это права.

П

Паразитное излучение (ПИ) -побочное излучение, возникающее в результате самовозбуждения электронного устройства из-за паразитных связей в генераторных и усилительных приборах или каскадах. ПИ ведет к образованию неконтролируемого канала утечки информации.

Пароль - идентификатор субъекта доступа, который является его (субъекта) секретом

Пассивное средство защиты - средство, обеспечивающее закрытие объекта защиты путем поглощения, отражения или рассеивания излучений объекта.

Перехват (П) - способ несанкционированного получения конфиденциальной информации. П бывает непосредственный (НП) и электромагнитный (ЭП). НП информации за счет непосредственного подключения к телефонным каналам или каналам подслушивания. ЭП производится с помощью средств радиоразведки за счет приема излучаемой электромагнитной энергии.

Побочное излучение - нежелательное радиоизлучение, возникающее в результате любых нелинейных процессов в радиопередающем устройстве, кроме процесса модуляции.

Побочные электромагнитные излучения и наводки – нежелательные излучения и наводки, проявляющиеся в виде побочных, внеполосных, шумовых и наводимых сигналов, потенциально образующих неконтролируемые каналы утечки конфиденциальной информации.

Подделка (модификация, фальсификация) документа - это изготовление полностью фиктивного документа (письмо, авизо, вексель), либо незаконное изменение подлинного документа: исправление, замена или уничтожение части текста, внесение дополнительных данных, воспроизводство подписи за другое лицо, помещение оттиска поддельного штампа и другие.

Показатель защищенности средств вычислительной техники - характеристика средств вычислительной техники, влияющая на защищенность и описываемая определенной группой требований, варьируемых по уровню, глубине в зависимости от класса защищенности средств вычислительной техники

Получение (добывание) информации – действия, связанные со сбором, обработкой и анализом фактов, связанных со структурой, свойствами и взаимодействием объектов и явлений, извлекаемых из поступающих сигналов и знаков.

Помехи (П) – обширная область явлений, препятствующих нормальной работе аппаратуры, устройств комплексов и вызывающих отклонение от расчетных (номинальных) значений параметров работы различных технических средств.

Р

Помехозащищенность – показатель эффективности комплекса мер, направленных на обеспечение надежности работы технических устройств (комплексов) в условиях помех.

Помехоустойчивость – способность технического устройства выполнять свои функции с требуемым качеством в условиях воздействия помех.

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам доступа

Правовая защита информации - специальные правовые акты, правила, процедуры и мероприятия, обеспечивающие защиту информации на правовой основе.

Правовое обеспечение СЗИ - совокупность нормативных документов, положений, инструкций, руководств, требования которых являются обязательными в рамках сферы их деятельности в системе защиты информации

Препятствие – преграды и сооружения, элементы рельефа и местные предметы, вызывающие замедление или остановку движения субъекта, пытающегося проникнуть к охраняемому объекту, конкретному помещению объекта или расположению охраняемого устройства.

Преступление компьютерное – преступление, совершенное средствами вычислительной техники и вычислительных сетей, направленное на незаконное похищение информации или приводящее к ее модификации или разрушению.

Программное обеспечение – совокупность программ для ЭВМ определенного типа.

Программные методы защиты информации - комплекс специальных алгоритмов и компонентов общего программного обеспечения ВС, предназначенных для выполнения функций контроля, разграничения доступа

Проникновение – успешное преодоление механизмов защиты.

Р

Радиозакладка – миниатюрное электронное устройство, состоящее из микрофона и миниатюрного радиопередатчика, обеспечивающего передачу подслушиваемых переговоров на достаточно значительное расстояние с помощью электромагнитных волн.

Радиоразведка – добывание сведений путем приема радиоизлучений средств радиосвязи, телеметрии, информатики и оргтехники, их анализа и восстановления передаваемых сообщений.

Радиотехническая разведка- добывание сведений путем приема и анализа радиоизлучений радиоэлектронных средств технических устройств и технологического оборудования.

Радиоэлектронная защита - комплекс мероприятий по обеспечению устойчивой работы радиоэлектронных средств и систем от подавления, поражения, нарушения их работы, несанк-

ционированного подслушивания и исключения возникновения неконтролируемых каналов за счет ПЭМИН.

Радиоэлектронная разведка – добывание сведений о противнике с помощью радиоэлектронных средств. Подразделяется на радиоразведку, радиотехническую, радиолокационную, радиотепловую (тепловизионная), тепловую (инфракрасная), лазерную, телевизионную, звуковую, гидроакустическую разведку.

Разглашение - умышленные или неосторожные действия должностных лиц и граждан, которым соответствующие сведения в установленном порядке были доверены по службе или работе, приведшие к ознакомлению с ними лиц, не допущенных к этим сведениям.

Разграничение доступа - система мероприятий, обеспечивающих предоставление пользователям только той информации, которая необходима им для выполнения работы.

Разрешительная система - совокупность правил, регулирующих порядок доступа сотрудников организации (предприятия) и других лиц к сведениям (работам, документам, изделиям, продукции), являющимся коммерческой тайной.

Режим конфиденциальности - защищенный законодательством страны порядок обеспечения безопасности носителей конфиденциальной информации.

Риск - возможность (опасность) потерь предприятия при наступлении определенных событий.

Рубежи защиты информации представляют собой совокупность методов и средств, обеспечивающих многоуровневую, иерархическую систему допуска к информации с помощью различных средств, таких как физические, технические, программные и т.п.

С

Сертификат защиты - документ, удостоверяющий соответствие средств вычислительной техники средств управления и связи, автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование или распространение как защищенных.

Сертификация уровня защиты - процесс установления соответствия средства вычислительной техники или автоматизированной системы набору определенных требований по защите.

Система защиты информации - организованная совокупность мероприятий, методов, органов и средств, создаваемых с целью защиты информации.

Система контроля доступа - совокупность мероприятий и технических средств, исключающих неконтролируемое проникновение злоумышленника на охраняемую территорию, помещение.

Система обеспечения безопасности -совокупность средств, методов и мероприятий, создаваемая и поддерживаемая для предупреждения или исключения случайного или преднамеренного доступа, получения, раскрытия, модификации или разрушения информации.

Скремблер – аналоговый речевой шифратор, осуществляет перестановку отдельных «вырезок» входного сигнала, и за счет этого создает шифрованный сигнал.

Сохранность информации - свойство, характеризующее степень готовности определенных ИМ к целевому применению и заключающееся в способности обеспечивать постоянное наличие и своевременное предоставление ИМ, необходимых для автоматизированного решения целевых и функциональных задач ВС.

Способы действий по защите информации – выявление возможных каналов утечки информации, поиск и обнаружение реальных каналов утечки информации, оценка степени опасности каждого реального канала, локализации (подавление) опасных каналов и контроль надежности защитных мероприятий.

Средства вычислительной техники - совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Средства защиты от несанкционированного доступа – программные, технические или программно-технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа.

Средства криптографической защиты – средства, осуществляющие криптографические преобразования информации для обеспечения ее безопасности.

Старение информации - свойство информации утрачивать со временем свою практическую ценность, обусловленное изменением состояния отображаемой ею предметной области.

Стойкость криптографического закрытия - минимальная длина закрытого текста, на которой могут быть выявлены такие статистические закономерности, на основе которых может быть восстановлена.

Субъект доступа - лицо или процесс, действия которых регламентируются правилами разграничения доступа.

Т

Тайна военная - особой важности, совершенно секретные и секретные сведения военного характера, составляющие тайну государственную и тайну служебную, охраняемые государством.

Тайна государственная - особой важности, совершенно секретные и секретные сведения военного, экономического, политического и иного характера, охраняемые государством.

Тайна переписки - правовая неприкосновенность почтовой и иной корреспонденции, а также телефонных переговоров и телеграфных сообщений.

Тайна служебная - см. Служебная тайна.

Техническая защита информации совокупность мероприятий, технических средств (механических, оптических, электрических и радиотехнических), обеспечивающих защиту информации. Реализуется физическими, аппаратными и программными средствами и математическими (криптографическими) методами.

Технические мероприятия – мероприятия, обеспечивающие приобретение, установку и использование в процессе производственной деятельности –специальных защищенных от побочных излучений (безопасных) технических средств обработки конфиденциальной информации или средств, ПЭМИН, которых не превышают допустимые нормы.

Технические средства защиты - аппаратные (встроенные в аппаратуру) и функционирующие автономно (независимо от аппаратуры) технические средства, обеспечивающие техническую защиту конфиденциальной информации.

Технические средства контроля доступа - средства систем контроля доступа на охраняемые территории, в помещения, хранилища и другие пространства и емкости.

Технические средства радиоэлектронной разведки включают радиоприемники с соответствующими антеннами; радиопеленгаторы; устройства панорамного обзора сигналов и анализа спектра частот; выходные устройства для выделения и перехвата сигналов многоканальных передач; оконечные устройства приема и отображения добываемых данных; устройства документирования и обработки – информации; аппаратуру рассекречивания зашифрованных и закодированных радиопередач; средства управления, связи, сбора и передачи добываемой информации.

Техническое обеспечение СЗИ – комплекс технических средств обнаружения, измерения, контроля и защиты информации.

Троянский конь – способ, основанный на тайном введении в функциональную программу таких команд, которые позволяют ей осуществлять новые, не планировавшиеся владельцем программ функций.

У

Уборка мусора – метод поиска информации, оставленной пользователем после работы с компьютером. Подразделяется на простые способы – от просмотра корзин с мусором до сбора оставляемых листингов и более серьезные, связанные с исследованием данных, оставленных в памяти ЭВМ.

Уведомление – разновидность сообщения отправителя, используемое для информирования получателя об отправке ему конфиденциальной информации.

Угроза - реально или потенциально возможные действия или условия преднамеренного или случайного (неумышленного) нарушения режима функционирования предприятия путем нанесения материального (прямого или косвенного) ущерба, приводящие к финансовым потерям, включая и упущенную выгоду.

Угроза безопасности активная – угроза намеренного несанкционированного изменения состояния системы.

Управление безопасностью – система регулярных защитных мероприятий, направленных на обеспечение безопасности в соответствии с изменяющимися условиями внутренней и внешней среды.

Управление доступом способ защиты информации путем регулирования использования ресурсов (документов, технических и программных средств, элементов баз данных и т.п.). Управление доступом включает следующие функции защиты: идентификацию пользователей, персонала и ресурсов; проверку полномочий; разрешение и создание условий работы в пределах установленного регламента; регистрацию (протоколирование) обращения к защищаемой информации; реагирование при попытках несанкционированного действия.

Управление ключами - построение ключей, их хранение распространение, удаление, учет и применение в соответствии с методикой безопасности.

Уровень безопасности - компоненты иерархической структуры информации, которая состоит из подсистем одного ранга.

Уровень полномочий - максимальный уровень секретности сведений, к которым разрешен доступ соответствующему субъекту (объекту).

Утечка информации - неконтролируемый выход конфиденциальной информации за пределы организации или круга лиц, которым эта информация доверена.

Уязвимость - слабость в средствах защиты, вызванная ошибками или слабостями в процедурах, проекте, реализации, внутреннем контроле системы, которая может быть использована для проникновения в систему.

Ф

Федеральные органы правительственной связи и информации - являются составной частью сил обеспечения безопасности Российской Федерации и входят в систему органов федеральной исполнительной власти. Единую систему федеральных органов правительственной связи и информации составляют: Федеральное агентство правительственной связи и информации (ФАПСИ) при Президенте Российской Федерации; органы защиты правительственной связи и информации в субъектах Российской Федерации; войска; учебные заведения, научно-исследовательские организации, предприятия.

Физическая безопасность - реализация физических барьеров и контрольных процедур, как превентивная или контрмера, против физических угроз (взлома, кражи, террористического

акта, а также пожара, подтопления и т.д.) ресурсам системы и конфиденциальной информации.

Физическая изоляция - использование физических систем охраны в целях исключения возможности неконтролируемого доступа на охраняемую территорию, зону, помещение.

Физические средства защиты информации - технические устройства, инженерные сооружения и организационные мероприятия, исключающие проникновение потенциальных нарушителей в места, где они могут иметь доступ к защищаемой информации. К ним относятся: физическая изоляция сооружений и помещений, ограждение территории на расстояниях, исключающих эффективную регистрацию электромагнитных излучений аппаратуры; развертывание систем управления доступом у входов в охраняемые помещения; использование специальных запирающих устройств; наблюдение за охраняемыми помещениями и развертывание системы охранной сигнализации.

Физическая структура канала утечки информации - представление канала утечки информации виде взаимосвязанных аппаратных средств и физических элементов, его образующих.

Х

Хэкер - компьютерный хулиган, незаконно (без разрешения) подключающийся к чужим сетям и проникающий в чужие ЭВМ.

Ц

Целостность информации - Способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и(или) преднамеренного искажения(разрушения)

Ч

Червь – это специально написанная программа, предназначенная для преодоления разнообразных мер защиты. Программа, как правило, узко специализирована и взламывает только определенный тип защиты.

Ш

Шифр - совокупность условных знаков, используемых для преобразования открытой информации в вид, исключающий ее восстановление (дешифрование), если наблюдающий (перехватывающий) не имеет сведений (ключа) для раскрытия шифра.

Шифраппаратура - криптографические средств различных видов (технических и программно-технических), предназначенных для защиты информации, передаваемой за пределы контролируемой зоны по незащищенным каналам связи, регламентируется "Положением о разработке, изготовлении и обеспечении эксплуатации шифровальной техники, государственных и ведомственных систем связи и управления и комплексов вооружения, использующих шифровальную технику"

Шифратор – устройство для автоматического шифрования информации.

Шифрование - математическое, алгоритмическое (криптографическое) преобразование данных с целью получения шифрованного текста. Шифрование может быть предварительное (шифруется текст документа) и линейное (шифруется разговор). Кроме того, бывает шифрование блочное (каждый очередной блок шифруется независимо) и поточное (каждый знак шифруется независимо от других.

Э

Экранирование - способ снижения мощности нежелательных излучений, способных образовать неконтролируемый канал утечки информации.

Электромагнитный канал утечки информации - это физический путь от источника побочных электромагнитных излучений и наводок (ПЭМИН) различных технических средств к злоумышленнику за счет распространения электромагнитной энергии в воздушном пространстве и направляющих системах.

Альбом схем

Основы информационной безопасности в органах внутренних дел

Мишин Дмитрий Станиславович, к.ю.н.

Подченяев Николай Григорьевич, к.т.н., доцент

Свидетельство о государственной аккредитации
Рег. № 0440 от 22.12.06 г.
Подписано в печать _____ г. Формат 60x90 1/16.
Учет.-изд.л. - _____. Тираж _____. Заказ № _____.

Орловский юридический институт МВД РФ.
302027, Орел, Игнатова, 2.