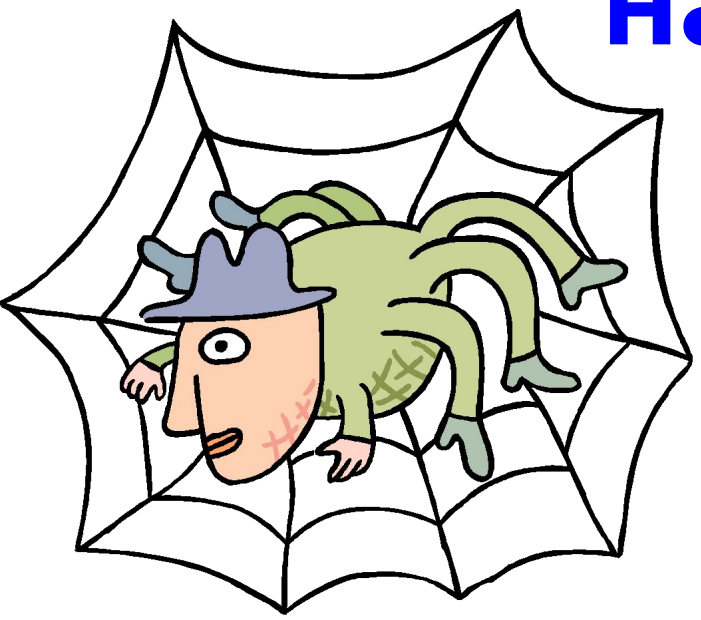
Модели информационных нарушителей



Модель нарушителя информационной безопасности – это формализованное (математическая модель) или неформализованное (вербальная модель) описание возможностей, ресурсов и характерных способов действий лиц, являющихся носителями информационных угроз.

Информационных нарушителей классифицируют по степени их осведомленности об объекте преступных посягательств, наличию опыта неправомерного доступа и по их технической оснащенности.

Модель нарушителя включает:

- Описание целей и мотивов противоправных действий
- Степень подготовленности и оснащенности нарушителей, их возможная специализация
- Описание орудий преступления и их признаков
- Описание конкретных способов совершения преступлений, включая модели поведения
- Демаскирующие признаки преступной деятельности
- Механизмы следообразования и используемые способы сокрытия следов преступления
- Способы имитации воздействий нарушителя при проверке средств защиты

Виды атак на информационные системы

- **Неправомерный доступ к информации** - любая форма проникновения в систему, позволяющая манипулировать информацией против воли ее собственника
- **Перехват информации** – несанкционированный процесс добывания информации из информационных систем, каналов связи, зон информационной утечки с использованием специальных технических средств

Виды атак на информационные системы

- **Блокирование информации –** воспрепятствование нормальным процессам передачи, приема, отображения, хранения информации с использованием аппаратных и/или программных средств
- **Хищение** - скрытая форма присвоения вещественных ценностей и носителей информации
- **Вандализм** - преднамеренная порча вещественных ценностей, данных и программного обеспечения

Цели нарушителей

- Шутки
- Любопытство (проникновение как головоломка, работа для ума)
- Любопытство по отношению к чужим секретам
- Известность и слава
- Идеологические соображения и политические цели
- Финансовая выгода
- Месть
- Жажда уничтожения
- Другие мотивы

Размышления о риске (Брюс Шнайер)

- Террористы бывают счастливы умереть за свои убеждения
- Ищущие славы не хотят попасть в тюрьму
- Грабители банков не желают быть привлеченными к ответственности за шпионаж
- Для снижения риска могут использоваться более подготовленные и более дорогостоящие атаки
- Рациональный нарушитель выбирает атаку, которая с лихвой окупит понесенные расходы с учетом квалификации, доступа, истраченных ресурсов, времени и риска
- Действия преступников не всегда рациональны, т.к. некоторые из низ психически ненормальны

«Внутренние» нарушители

«Внутренними» нарушителями информационной безопасности считаются лица из числа персонала, допущенного к обработке защищаемой информации, обслуживанию информационных систем и прочих лиц, допущенных для проведения работ в помещения, где хранится и обрабатывается защищаемая информация

Иерархия «внутренних» нарушителей

- Болтливые сотрудники
- Пользователи с низкой квалификацией
- Излишне любопытные и сверхинициативные пользователи
- Некомпетентный или недобросовестный инженерно-технический персонал
- Программисты - «любители»
- Нелояльные программисты и проектировщики системы
- Нелояльные администраторы

Нарушение работы ЭВМ

- Пользователем, оператором, диспетчером - по причине использования компьютеров, управляющих производственным процессом или движением транспорта, не по назначению, а также по причине пренебрежения правилами антивирусной защиты
- Инженером, техником - пренебрежение правилами размещения, подключения и эксплуатации компьютерной техники
- Администратором - несоблюдение требований информационной безопасности, использование нелицензионного программного обеспечения

Пользователи как источники угроз

- Большая часть ущерба вызывается беспечностью и небрежностью пользователей
- Интересы пользователя не всегда совпадают с интересами организации
- «Хуже всего не те люди, которые бросают работу и уходят, а те, которые бросают работу и остаются. Они фактически вредят больше всего»

Нарушение работы ЭВМ со стороны пользователя

- Случайная порча носителей информации
- Ввод неверных (ошибочных) данных
- Пересылка данных по неверному адресу
- Случайное повреждение каналов связи
- Отключение или некомпетентное применение средств защиты информации
- Некомпетентное включение или изменение режима работы аппаратуры

Сравнительный анализ опасностей

Кракер, без сомнения, более опасен для компьютерной системы, чем обычный пользователь.

Однако пользователь работает за компьютером постоянно, а хакер может «удостоить» атакой систему один раз в несколько лет

«На каждого подлого кракера находится один обозленный на организацию сотрудник и восемь небрежных»

Corporate Computer Security Issues and Strategies

Портрет подозрительного сотрудника

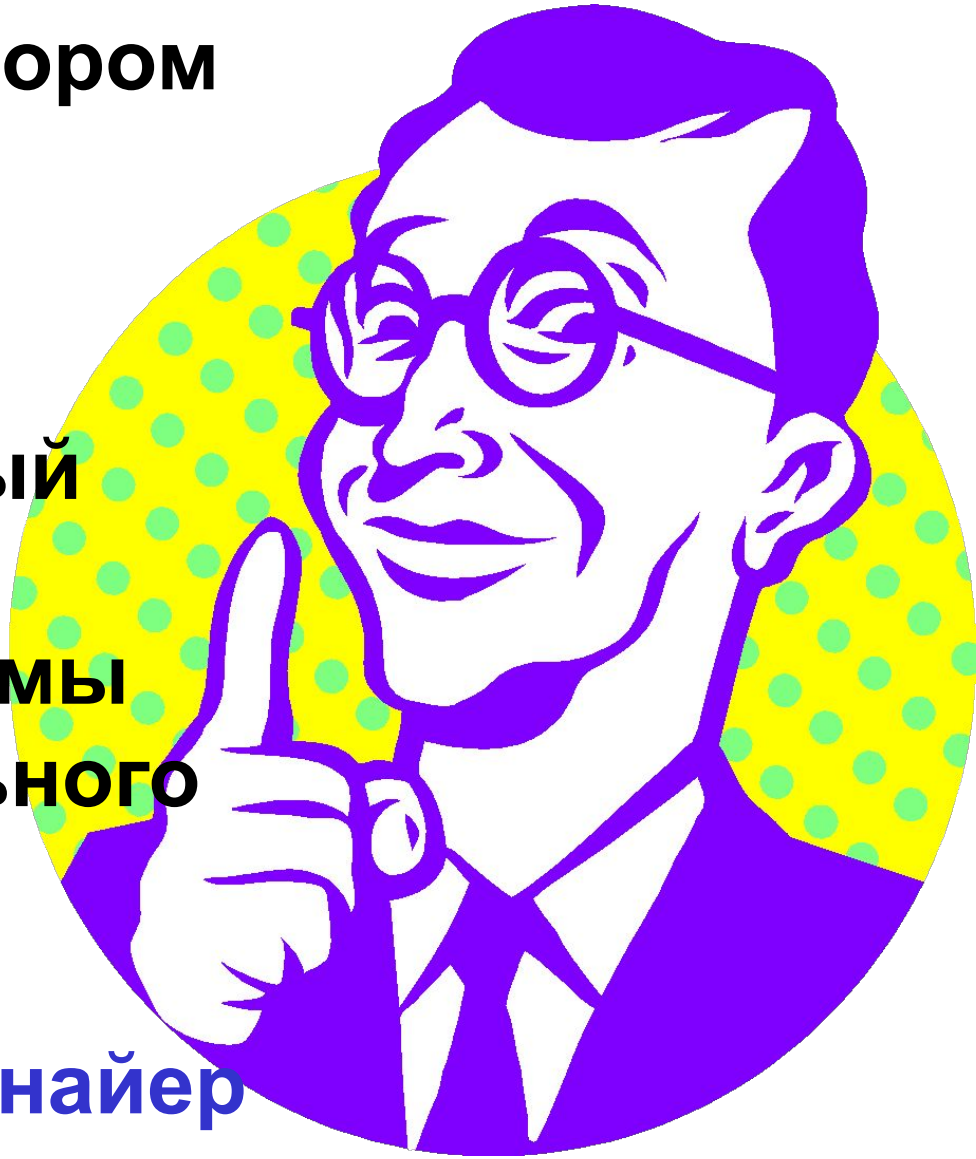
- Хорошо знает, как работает система охранной сигнализации
- Имеет ключи ото всех основных замков в служебные помещения
- Приходит на работу очень рано, задерживается дольше других, иногда работает в выходные дни
- Делает все возможное для завоевания доверия руководства и самостоятельной бесконтрольной работы
- Не поддерживает дружеских и деловых отношений с другими сотрудниками, предпочитает работать самостоятельно

«Внешние» нарушители

Хакерские специальности

- **Хакеры** - лица, удаленно внедряющиеся в чужие системы с целью выявления их уязвимостей и уведомления компьютерного сообщества
- **Кракеры** - взломщики систем и программ с защитой с меркантильными целями
- **Кардеры** - лица, живущие за счет чужих кредитных карточек
- **Фрикеры** - лица, использующие средства телефонной связи без оплаты
- **Вирмейкеры** - программисты, создающие вредоносные программы

- **Хакер - человек со специфическим набором навыков и неспецифической моралью. Это индивидуум, который экспериментирует с недостатками системы ради интеллектуального любопытства или собственного удовольствия - Б.Шнайер**



Хакеры (HACKER сущ.)

1. Индивидуум, который получает удовольствие от изучения деталей функционирования компьютерных систем и от расширения их возможностей, в отличие от большинства пользователей компьютеров, которые предпочитают знать только необходимый минимум.
2. Энтузиаст программирования; индивидуум, получающий удовольствие от самого процесса программирования, а не от

Благородные цели хакеров

- Исследуя компьютерную систему, обнаружить слабые места в системе безопасности и *информировать об этом* пользователей и разработчиков системы
- Проанализировав существующую безопасность компьютерной системы, *сформулировать* необходимые требования и условия повышения уровня защищенности

Хакеры часто имеют более высокую квалификацию, чем проектировщики системы. Хакеры смотрят на систему с внешней стороны, с позиции нападающего, а не с внутренней - с позиции проектировщика

Цели кракеров

Непосредственное осуществление взлома системы с целью *получения несанкционированного доступа* к чужой информации:

- **кража,**
- **подмена,**
- **объявление факта взлома,**

с последующим извлечением материальной выгоды

Взгляд на информационного нарушителя с позиций РД Гостехкомиссии

- Нарушитель может запускать программы из фиксированного набора, реализующего заранее определенные функции
- Нарушитель может создавать и запускать собственные программы
- Нарушитель может воздействовать на конфигурацию оборудования и базовое программное обеспечение
- Нарушитель относится к числу проектировщиков, программистов, инженеров

Степени осведомленности информационных нарушителей

- Неосведомленный нарушитель: не имеет навыков программирования, не знает принципа работы устройств охраны, управления доступом и СЗИ
- Осведомленный нарушитель (знает, но не имеет собственного опыта)
- Осведомленный нарушитель, имеющий опыт взлома систем

Виды осведомленности нарушителей

- **Осведомленность об объекте преступных посягательств (информационных ресурсах, платежных системах)**
- **Осведомленность о способах и средствах защиты информации на атакуемом объекте**
- **Осведомленность о методах скрытого доступа к информации**

Подготовленный нарушитель:

- Имеет необходимые знания об информационных технологиях, средствах и методах защиты информации, психологии людей (пользователей и администраторов)
- Имеет опыт неправомерного доступа к защищаемой информации
- Оснащен необходимыми аппаратными и программными средствами для ведения разведки, доступа и перехвата, умеет их создавать или программировать

Описание удавшихся способов совершения преступлений наряду с возможностью распро-странения орудий преступления в виде компьютерных программ. Первому нападающему приходится быть изобретательным, остальные могут просто использовать его программы.

Причины вовлечения КТ в противоправную деятельность

- **Компьютерные технологии входят в обиход человека как в быту, так и на рабочем месте, и их использование не нуждается в каком-либо разрешении или обосновании**
- **Создание и развитие системы электронной коммерции, глубокое проникновение компьютерных технологий в кредитно-финансовую сферу, виртуализация общественных отношений в сфере предоставления услуг и их оплаты**
- **Развитие программных средств электронного синтеза и обработки аудиозаписей, фото- и видеоизображений**

Влияние КТ на преступность

- Благодаря автоматизации существенно увеличивается вероятность очень редких событий, благоприятных для нарушителя
- Появляется возможность успешной реализации удаленных атак с очень низкой вероятностью успеха
- Реализуется возможность быстрого добывания и фильтрации данных об объектах преступного посягательства
- Расстояние и возможность скрывать свое реальное местонахождение делает преступника безнаказанным

Причины, способствующие сокрытию следов преступной деятельности

- **Развитые формы криптографического и стеганографического скрытия компьютерной информации**
- **Возможность использования компьютерных сетей в качестве каналов скрытой связи**
- **Возможность скрытия следов удаленного доступа, работа в сети через компьютер-посредник, от чужого имени**

Ограбление магазина или угон автомобиля требует присутствия и участия преступника на месте преступления. Потерпевшему следует опасаться только тех преступников, которые находятся неподалеку. Благодаря Интернету каждому владельцу сетевого компьютера приходится принимать во внимание информационную преступность всего мира

Влияние компьютерных технологий на преступность

- Проблемы с поиском преступников и привлечением их к ответственности
- Информационный нарушитель почти всегда имеет преимущество перед защищающейся стороной
- Фактор времени: ответные меры хронически отстают
- Имеет место широчайшее распространение технических приемов и средств совершения преступлений

Особенности компьютерных преступлений

- **Совершаются образованными людьми с использованием «интеллектуальных» средств и орудий преступления**
- **Отличаются высокой латентностью, низкой раскрываемостью, практически полной безнаказанностью**
- **Расследование преступлений требует высокой квалификации специалистов, использования дорогостоящей аппаратуры и программного обеспечения**

Ресурсы нарушителя

- трудозатраты на подготовку и реализацию доступа (временной ресурс)
- аппаратные и/или программные средства доступа (материальный ресурс)
- специальные познания в сфере компьютерных и иных технологий, а также опыт доступа (мыслительный ресурс)

За нормированное время нарушитель может:

- добиться положительного результата (реализовать доступ и совершить необходимые манипуляции с информацией),
- отказаться от проникновения,
- отложить попытку до следующих благоприятных обстоятельств (попутно получив дополнительную информацию о системе защиты)

Формы представления компьютерной информации на этапах ее обработки и хранения в большинстве случаев не позволяют человеку-нарушителю получать ее с помощью органов чувств. Для реализации основных видов доступа ему приходится использовать различные аппаратные и программные средства.

Орудия и средства преступления

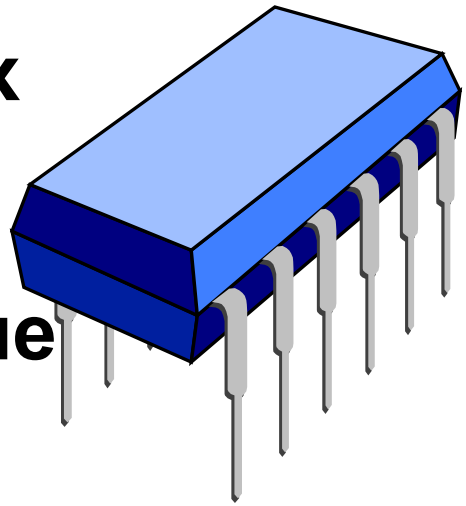
- штатные аппаратно-программные средства компьютерной системы
- добытые или подобранные пароли, похищенные или изготовленные носители (имитаторы) ключевой и биометрической информации
- компьютерные программы, предназначенные для сбора информации об объекте доступа и проникновения в него
- машинные носители для копирования компьютерной информации

Орудия и средства преступления

- "компьютеризированные" устройства с памятью или собственным каналом связи (цифровые диктофоны, плееры, фото-видеокамеры, мобильные устройства связи)
- аппаратные закладки
- устройства для снятия информации по каналам утечки
- монтажный инструмент для доступа в аппаратные отсеки атакуемого компьютера

Нарушитель может использовать свою компьютерную систему:

- в общей компьютерной сети с атакуемым компьютером
- подключаемую к физическому каналу локальной сети, в которой работает атакуемый компьютер
- подключаемую к доступным интерфейсам атакуемого компьютера
- подключаемую к компонентам атакуемой системы (выносному терминалу, демонтированному внешнему носителю)



В некоторых случаях разработанные, изготовленные, запрограммированные средства могут выполнять задачу доступа автоматически, без участия человека. По этой причине автономные аппаратные программные закладки можно рассматривать в качестве самостоятельных “нарушителей”.

Обнаружение человека-нарушителя техническими средствами основано на ряде демаскирующих признаков, которые образуют его физическую информационную модель

Демаскирующими признаки подразделяются на опознавательные, которые описывают нарушителя в статическом состоянии и признаки деятельности, которые характеризуют его в динамике, в ходе преступных действий.

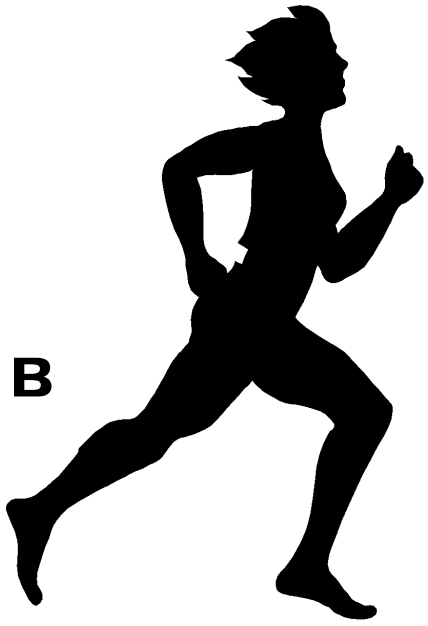
К модели нарушителя относятся также характерные информационные признаки состояния или деятельности, по которым присутствие нарушителя на объекте информатизации или его неправомерная деятельность по доступу к защищаемой информации может быть обнаружена и зафиксирована техническими средствами охраны

Модели человека-нарушителя

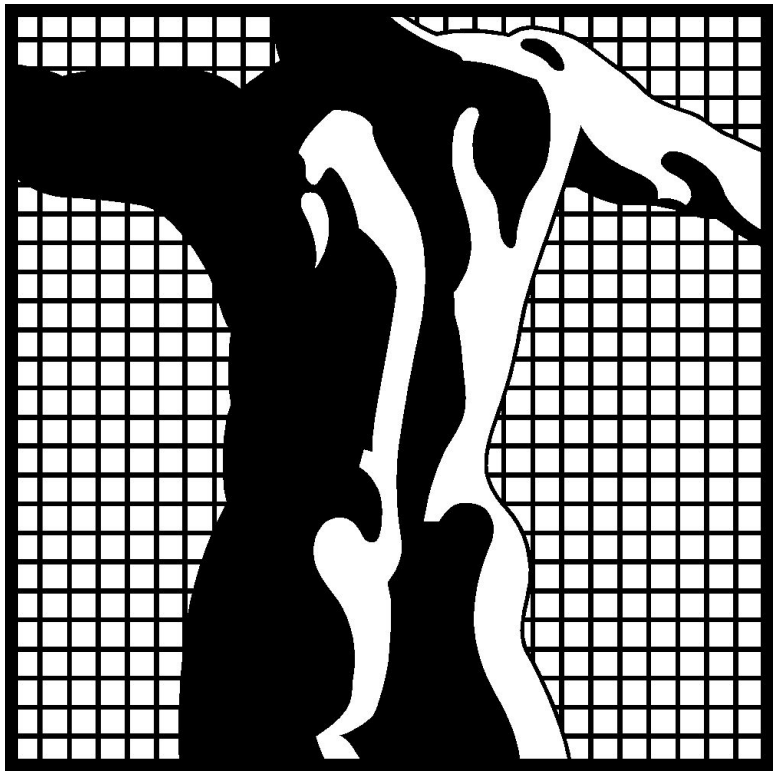
- Геометрическая модель
- Биомеханическая модель
- Физико-химическая модель
- Социальная модель

Геометрическая модель

Человек может передвигаться в пространстве в различных положениях: в рост, согнувшись, на четвереньках, ползком, перекатом и др. В каждом случае его тело представляет сложную геометрическую фигуру с определенными размерами



Геометрическая модель

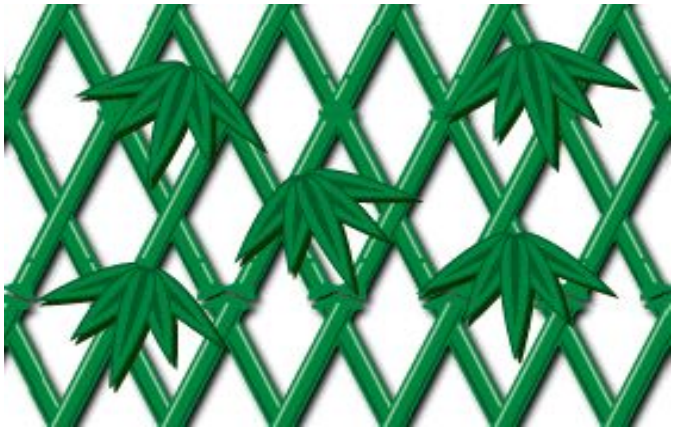


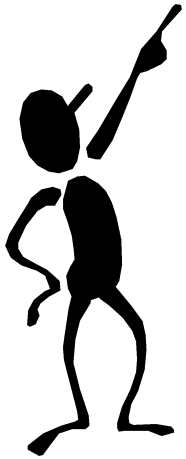
Благодаря антропометрии известны характерные размеры человеческого тела и его частей при различных способах передвижения в пространстве

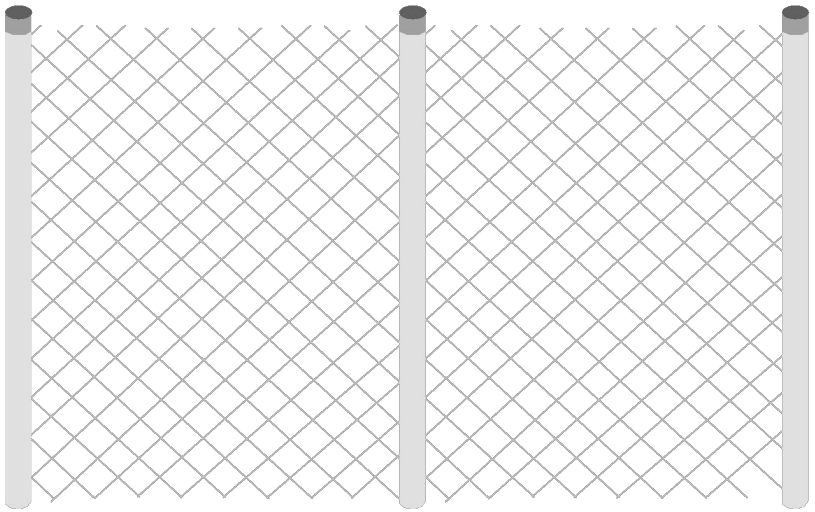
Большинство характерных размеров человеческого тела подчиняются нормальному закону распределения

Геометрическая модель

Характерные размеры человеческого тела служат исходными данными при определении размеров инженерных и сигнализационных заграждений, а также зон обнаружения







Биомеханическая модель

В соответствии с данной моделью нарушитель представляет собой активную физическую массу, перемещающуюся в пространстве методом локомоций и оказывающую силовое воздействие на окружающие тела (предметы)

Механическое воздействие человека

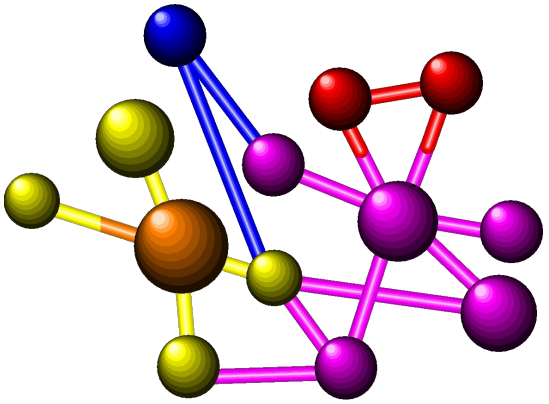
- Мускульная энергия (в том числе с использованием приспособлений, увеличивающих мускульную силу: рычагов, гидравлических и пневматических устройств, блоков)
- Возбуждение в окружающей среде механических колебаний (при ходьбе, беге, прыжках, плавании)
- Вибрации, возбуждаемые при поддержании равновесия (при перелазе)
- Вибрации при дыхании и сердцебиении

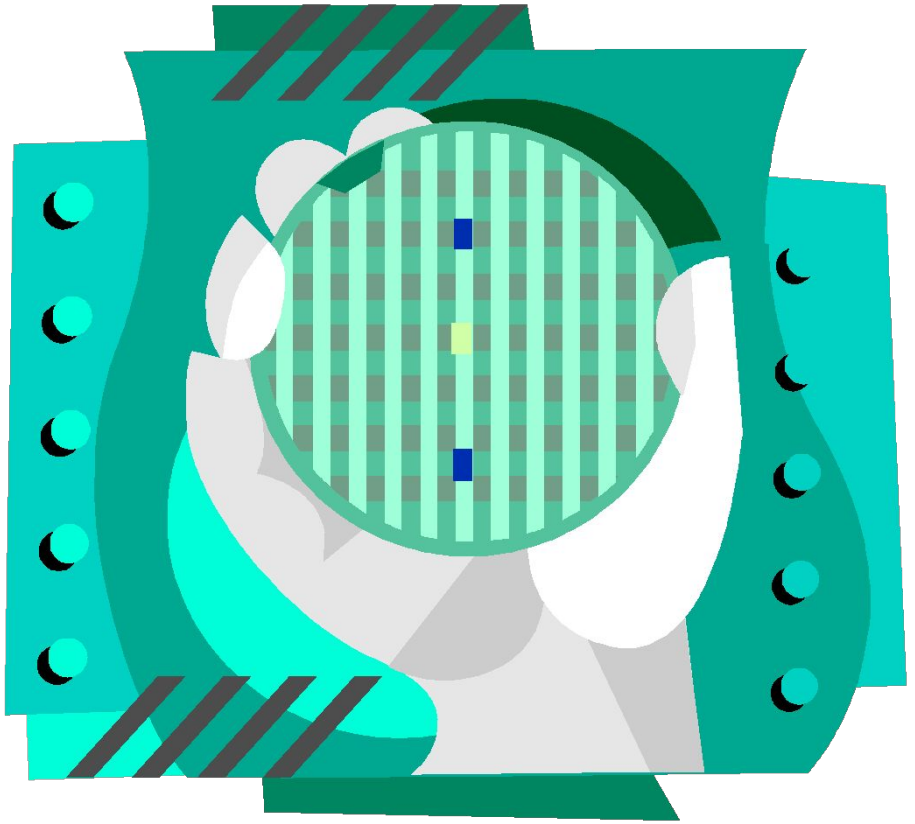
Биомеханическая модель

При движении по опорной поверхности нарушитель воздействует на нее с силой, пропорциональной его массе и квадрату скорости

Физико-химическая модель

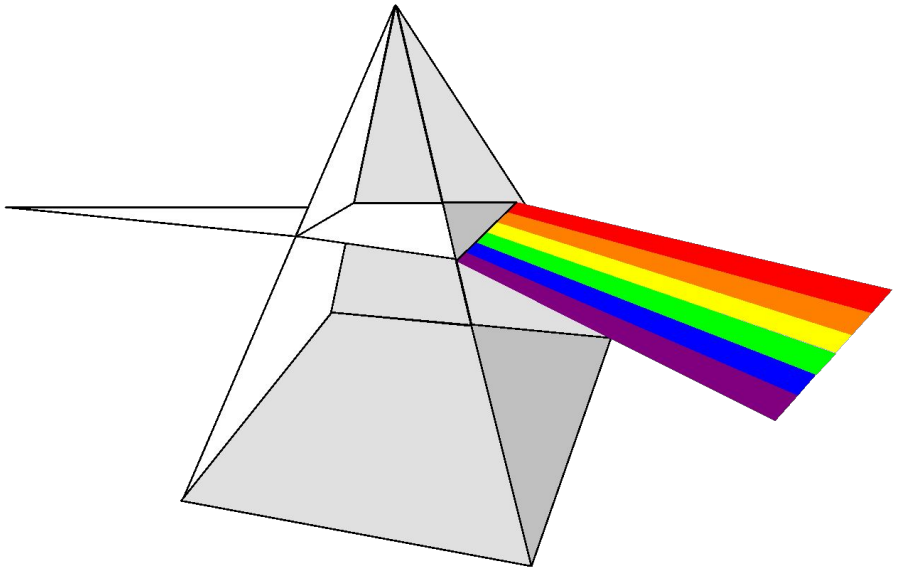
Человеческое тело обладает электрическими проводимостью и емкостью, благодаря чему может являться элементом электрической цепи

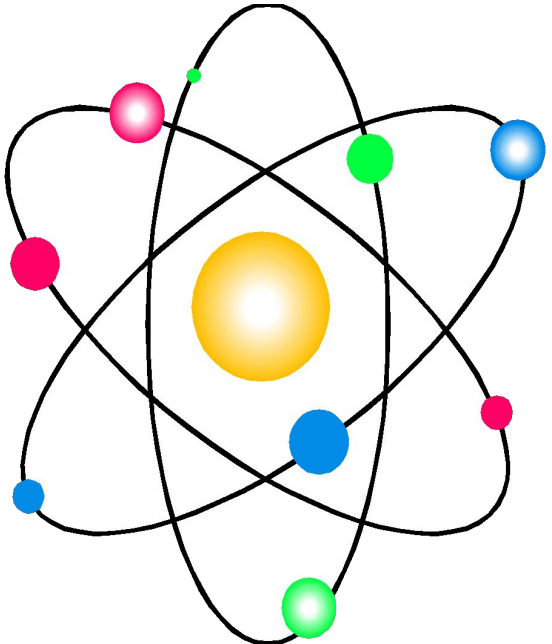




Физико-химическая модель

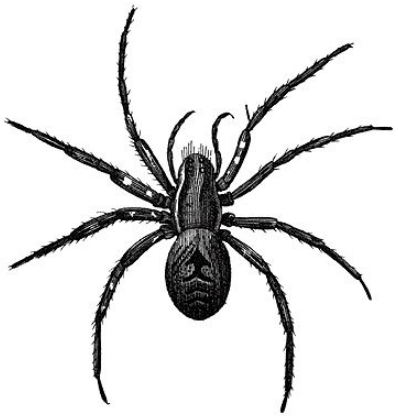
Человеческое тело способно отражать, рассеивать и поглощать электромагнитные и акустические волны





Физико-химическая модель

Человеческое тело способно генерировать собственные электростатические, электромагнитные и тепловые излучения



Человеческий организм в процессе жизнедеятельности выделяет с потом характерные химические вещества, которые можно зафиксировать с помощью газоанализаторов или биологических организмов

Энергетическое воздействие человека

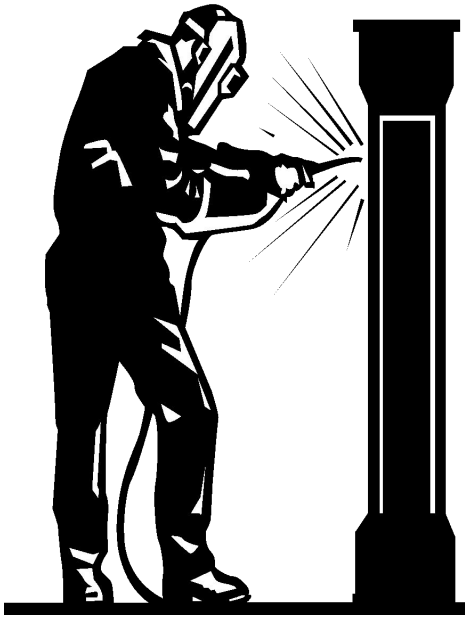
- Излучение тепловой энергии в «дальнем» ИК диапазоне
- Генерация электростатического заряда, движущегося с телом человека
- Излучение электромагнитных полей, связанных с биоритмами

Признаки состояния

- Выделение продуктов метаболизма
- Электрическое сопротивление тела (в частности - кожного покрова)
- Электрические параметры человеческого тела (удельное сопротивление, относительная диэлектрическая проницаемость, оптическая прозрачность)
- Способность поглощать, отражать и рассеивать электромагнитные и акустические волны)

Социальная модель

Человек умеет изготовлять и использовать предметы искусственного происхождения, в том числе и с целью проникновения на охраняемый объект



Социальная модель нарушителя

- **Постоянное наличие при себе предметов искусственного происхождения (одежды, обуви, предметов обихода)**
- **Умение находить и приспосабливать подручные средства**
- **Наличие при себе специально сконструированных средств проникновения и взлома (отмычки, слесарный инструмент)**

Демаскирующие признаки электронных закладок

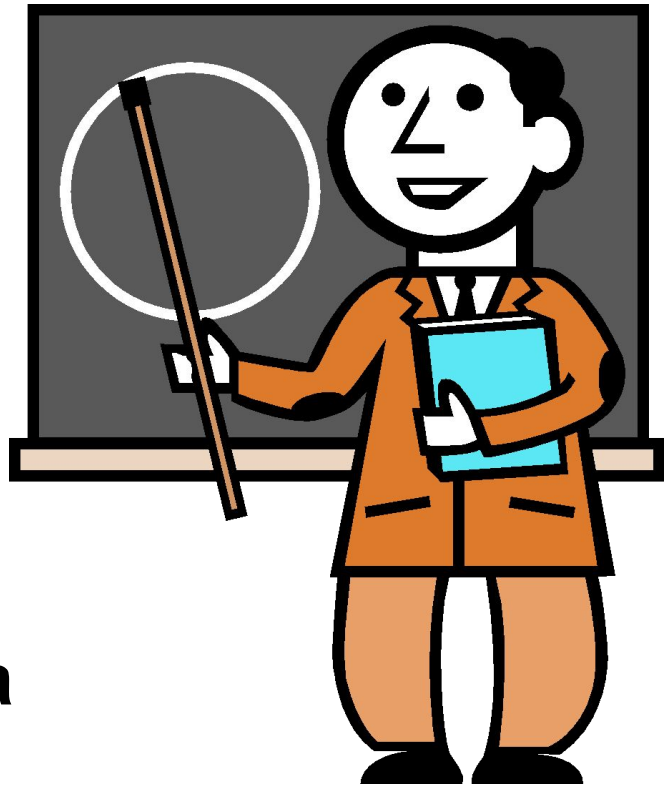
- Признаки внешнего вида – малогабаритный предмет неизвестного назначения
- Тонкий провод, проложенный от микрофона в другое помещение
- Наличие в предмете автономных источников питания (батарей, аккумуляторов)
- Наличие полупроводниковых элементов
- Наличие сосредоточенных источников модулированного радиоизлучения из помещения

Демаскирующие признаки вредоносного программного кода на этапе хранения

- Наличие сигнатуры - уникальной комбинации определенных байт
- Размещение программного кода в определенных областях памяти машинного носителя (например, загрузочные сектора)
- Размещение интерпретируемого кода (скриптов) в документах, изначально созданных без сценариев и макросов

Сигнатура - это последователь-ность байт, однозначно характерная для конкретной вредоносной программы

Сигнатура - это множество N пар $\{P_i, B_i\}$, i = 1...N, где P_i - расположение i-го байта, B_i - значение i-го байта. На практике чаще используют непрерывные сигнатуры, для которых можно задать длину сигнатуры и расположение (смещение) для первого байта



Демаскирующие признаки вредоносного программного кода на этапе исполнения

- Обращение к определенным портам транспортного уровня
- Попытка исполнения привилегированных команд
- Обращение к занятым или заблокированным устройствам ввода-вывода, файлам
- Обращение к физической памяти за пределами выделенного сегмента

Признаки подготовки программы к исполнению

- Помещение полного имени исполняемого файла в соответствующие разделы системного реестра
- Установление ассоциативной связи конкретных неисполняемых файлов с конкретными приложениями (через реестр)
- Использование ссылок (ярлыков) на исполняемые программы
- Помещение имени программы в папку «Автозагрузка»

Демаскирующие признаки вредоносного кода

- Присутствие интерпретируемого кода в шаблонах, документах и временных файлах
- Замедление или неестественное выполнение операций при работе с файлами, текстом, таблицами, рисунками
- Генерация сообщений об ошибках при некорректном выполнении программы

Демаскирующие признаки удаленных атак

- Повтор определенных действий (сканирование портов в поисках доступных сетевых сервисов, подбор пароля и др.)
- Неправильные или некорректные команды
- Несоответствующие параметры сетевого трафика (нестандартные комбинации бит, полуоткрытые соединения, признаки подмены адресов)
- Иные формы аномального поведения

Правила составления модели нарушителя

- Оценить объект защиты с воображаемой позиции противника, конкурента, злоумышленника. Для кого может представлять интерес защищаемая информация?
- Сколько стоит защищаемая информация и сколько готов за нее заплатить воображаемый или реальный противник?
- Обладает ли организация такой информацией, на которую может покушаться подготовленный и оснащенный нарушитель?

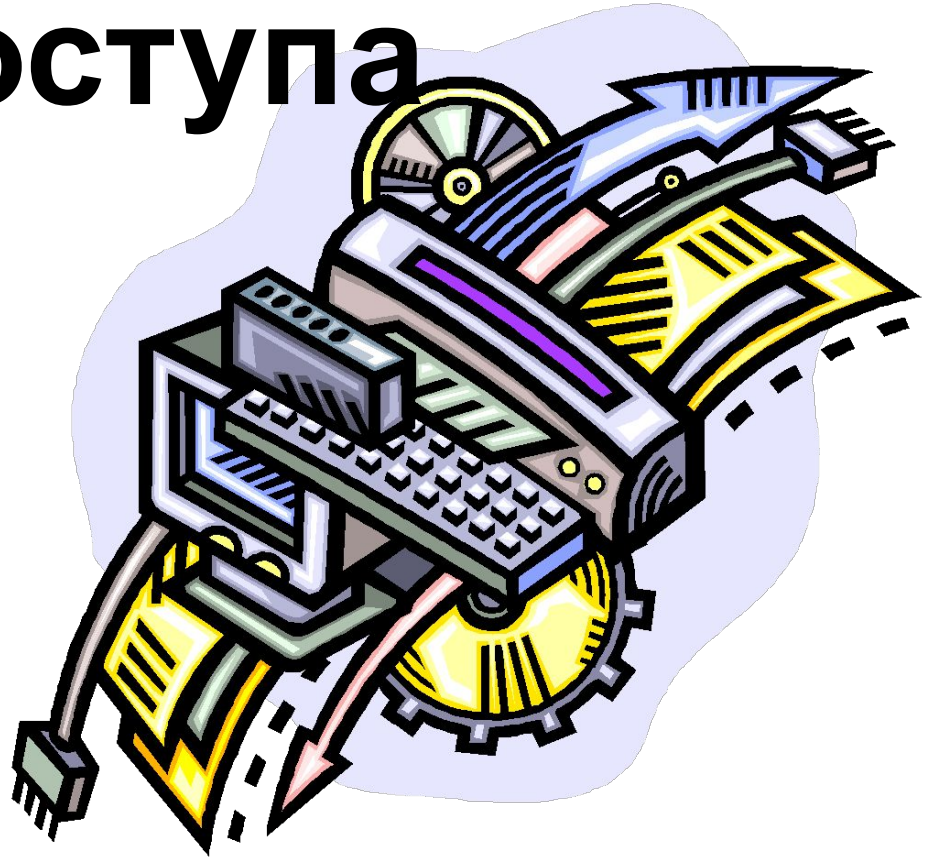
Правила проведения контроля защищенности информационного объекта

- **Проверка должна проводиться организациями, которым Вы безусловно доверяете**
- **Организация, производящая проверку защищенности, должна иметь соответствующую лицензию**
- **Проверка должна производиться скрытно, под легендой (чтобы ею не воспользовались настоящие злоумышленники)**
- **Контролируемый объект в период проведения проверки должен функционировать в обычном режиме**

Правила проведения контроля защищенности информационного объекта

- Воздействие на систему защиты такими же способами, какие будет использовать реальный нарушитель
- Проверка системы защиты в условиях, гарантирующих ее целостность или возможность восстановления
- Использование безопасных воздействий, имитирующих реальную атаку
- Оценка защищенности на основе измерений и расчетов

Модель комплексной защиты от несанкционированного доступа



Если на Ваш объект никто не вторгается, значит:

- Вы живете в государстве с хорошей законодательной и правоохранительной системой
- Или: Вас окружают только добропорядочные граждане
- Или: Ваши секреты и имущество не представляют ценности для посторонних
- Или: Ваш объект неприступен
- Или: Вы сами являетесь авторитетом преступного мира

Характеристика несанкционированного доступа

- **НСД – это любая форма проникновения нарушителя извне на объект информатизации, позволяющая ему манипулировать защищаемой информацией**
- **Доступ – это процесс физического или логического перемещения нарушителя к источнику, вещественным носителям или каналам передачи информации, либо к средствам управления информационной системой**

НСД сопровождается:

- Хищением вещественных носителей информации
- Перехватом управления системой
- Внедрением вредоносной компьютерной программы с обеспечением условий для ее запуска на исполнение
- Внедрением аппаратных закладок
- Перехватом сигналов в каналах связи
- Ознакомлением с информацией, ее отбором и копированием на собственные носители, блокированием обработки и др

Непосредственный доступ человека-нарушителя

Открытое или скрытое физическое проникновение на объект с целью:

- **внедрения аппаратной или программной закладки**
- **хищения вещественных носителей информации**
- **копирования документов или ознакомления с ними**
- **диверсии или вандализма**

Удаленный доступ:

- Используется работоспособный канал связи
- Реализуется, если нарушитель может подключить к этому каналу свой приемопередатчик
- Связан с передачей на расстояние сигналов (как правило - электрических)
- Нет существенной разницы в том, что передает нарушитель: команду или данные. Это зависит только от аппаратного и/или программного устройства на другом конце

Удаленный доступ:

- В компьютерных сетях используются сетевые протоколы и сервисные программы, запущенные на атакуемом компьютере
- Удаленному доступу предшествует разведка сети, ее отдельных узлов, запущенных программ

Этапы удаленного доступа

- Разведка топологии сети (пассивный и активный этапы)
- Поиск жертвы
- Оценка уязвимостей системы, поиск ее защитных механизмов
- Поиск или подбор аутентифицирующей информации
- Проникновение в систему (с преодолением защиты или без него)
- Поиск (копирование | модификация | блокирование) необходимой информации

Этапы удаленного доступа

- [Демонстративные деструктивные действия (deface и др.)]
- Стирание «электронных» следов доступа
- Подготовка «люка» для последующего вторжения
- [Использование взломанной системы для атаки на следующий узел сети]
- Выход из системы

Комплексная защита должна состоять из:

- Рубежа сопротивления вторжению
- Рубежа контроля и предупреждения о вторжении
- Средств и мер защитного реагирования

Этапы комплексной защиты

- Сделать защищаемую информацию непривлекательной для посторонних
- Создать фальшивые объекты
- Сделать объект неприступным
- Оборудовать на подступах к вещественным носителям и каналам передачи информации рубежи контроля
- Предусмотреть оценку достоверности обнаружения вторжения
- Оборудовать рубежи сдерживания нарушителя
- Содержать и тренировать персонал охраны

Этапы комплексной защиты

- **Рассчитать и составить план реагирования на вторжение**
- **Предусмотреть защитное блокирование, резервирование, эвакуацию или уничтожение защищаемой информации**
- **Зафиксировать следы преступной деятельности**

Способы снижения привлекательности защищаемой информации для посторонних

- Ограничение числа людей, осведомленных о ценности, месте и способах хранения и обработки информации
- Сокращение до необходимого минимума численности и осведомленности сил реагирования
- Разделение внешней и внутренней зон реагирования (охрана дипломатических представительств, объектов, на которых обрабатываются сведения, содержащие государственную тайну)
- Легендирование, дезинформация потенциального противника

Рубеж сопротивления вторжению

- Представляет собой разновидность внешнего слоя пассивной защиты (стратегия изоляции)
- Обеспечивает физическую, логическую или смысловую защиту от НСД
- Сортирует потенциальных злоумышленников по степени их квалификации, решительности и способности к риску
- Защищает от большинства людей и их преступных действий (но не от самых опасных)

Рубеж сопротивления физическому вторжению нарушителя

- Ограждение периметра объекта информатизации
- Ограждающие конструкции зданий и помещений
- Двери и замковые устройства
- Оконные решетки, защитные стекла
- Сейфы и хранилища
- Барьер, шлагбаум, кабина, шлюз в системе управления доступом

Рубеж сопротивления логическому вторжению нарушителя

- Межсетевой экран (без функций контроля)
- Зашифрованный документ
- Стеганографический контейнер
- Компьютерная программа с фрагментами защиты от несанкционированного запуска и копирования
- Обычная парольная система (без процедуры контроля и блокирования)

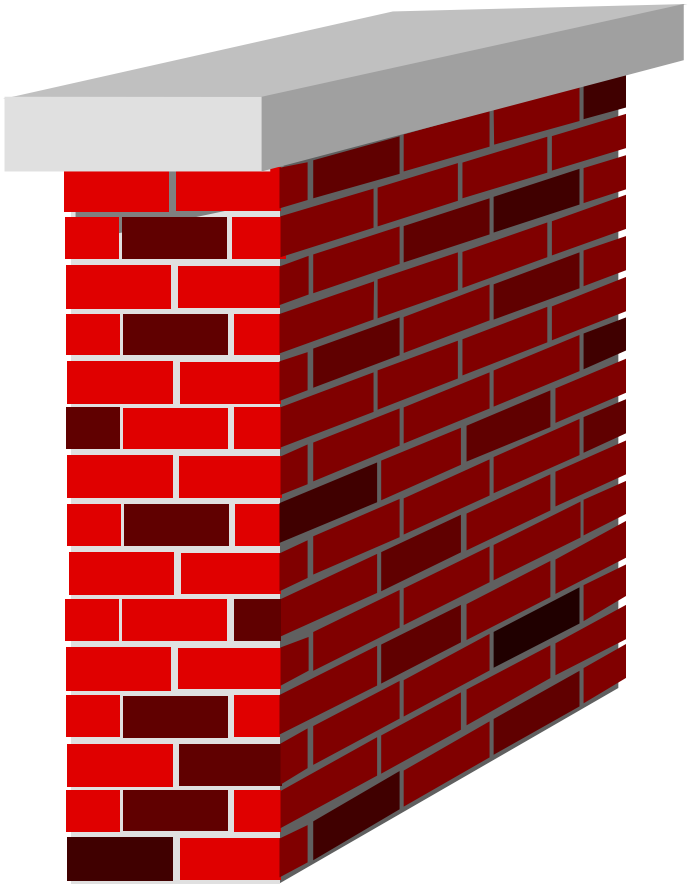
Защита периметра

- Установление видимой законной границы вокруг объекта
- Воспрепятствование доступа посторонних в охраняемое пространство (физическое или логическое)
- Предупреждение потенциальных нарушителей о мерах противодействия, в т.ч. о угрозе их жизни или здоровью
- Защита периметра наиболее целесообразна, если приходится охранять много объектов (зданий, помещений, компьютеров в ЛВС)

Пассивная система защиты должна сопротивляться вторжению, пока защищаемая информация не перестанет быть актуальной для нарушителя (принцип временной защиты)

Примеры успешно преодоленных рубежей сопротивления вторжению (Великая Китайская стена, линия Мажино, немецкая шифровальная система «Энигма»)

Показатели эффективности рубежа сопротивления вторжению



- Непрерывность рубежа по месту и времени
- Прочность
- Длительность сопротивления взлому
- % потенциальных нарушителей, отказавшихся от попыток доступа

Рубеж сопротивления вторжению редко применяется в одиночку. Но существуют способы защиты, в которых контроль и реагирование не предусматриваются

- **Зашифрованный документ**
- **Компьютерная программа с элементами защиты от несанкционированного запуска и копирования**

Рубеж контроля

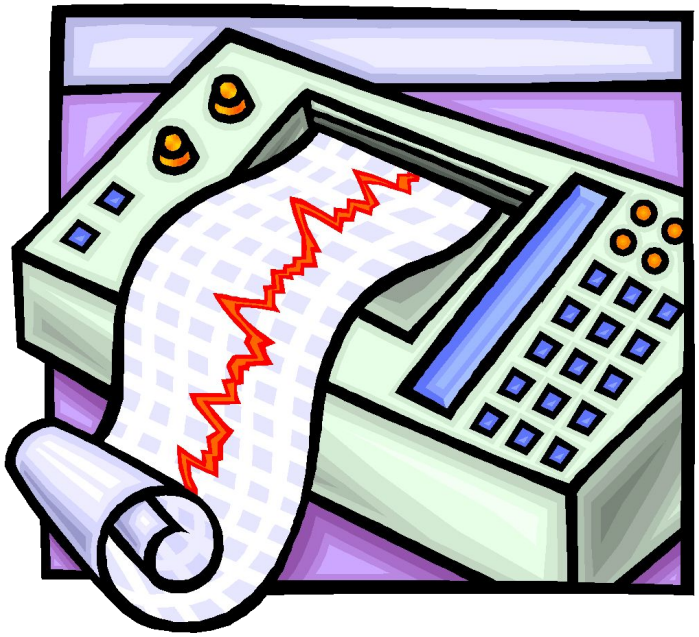
В основе – определение пространства признаков угроз (опасных сущностей), их описание, сравнение с признаками фоновой среды и установление наборов признаков, позволяющих идентифицировать объект (угрозу).

Контролирующие мероприятия фиксируют

- **Попытки несанкционированного доступа (проникновения)**
- **Наличие нарушителя в контролируемом пространстве**
- **Активные действия нарушителя по доступу к информации**
- **Последствия действий (нанесенный ущерб)**

Этапы контроля

- обнаружение (сигнала, цели) на окружающем фоне, среди помех,
- распознавание класса цели (классификация) – человек, транспортное средство, программа из семейства вирусов, средство удаленного подслушивания и др.
- идентификация конкретного объекта из класса (символа, сигнатуры, вида модуляции, конкретного лица и др.)



Объекты контроля

- известная сигнатура в массиве (последовательности) двоичных сигналов
- вызовы определенных, заведомо опасных или привилегированных системных функций
- вызовы иных функций с заданием «цепочки» вызовов,
- открытие определенного файла или каталога
- обращение к определенному устройству
- радиосигнал с известной (неизвестной) модуляцией, спектром, амплитудой
- сетевой пакет с известной сигнатурой в заголовке (тип и назначение пакета)

Объекты контроля

- большое число заявок на обслуживание (сетевых или локальных)
- контрольная сумма файла, сетевого пакета или сектора
- атрибуты файла (владелец, права доступа, временные отметки и др.),
- ВЧ-сигнал в телефонной линии (там, где его быть не должно)
- скачок входного сопротивления телефонной линии или падения питающего напряжения
- открытие запертой двери, сворки, форточки, фрамуги окна

Объекты контроля

- **неожиданные успехи конкурентов**
- **признаки нелояльности собственных сотрудников**
- **подозрительные лица, транспортные средства, работы или иные виды деятельности вблизи охраняемого объекта и др.**

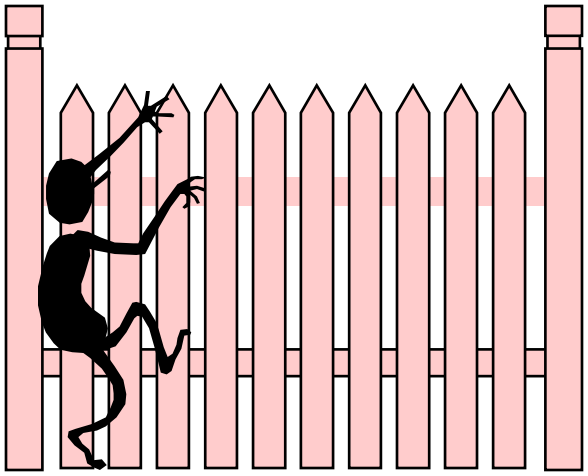
Формы активности «нарушителей»

- Перемещение нарушителя в пространстве. Например, человек-нарушитель с целью доступа к объекту преступных посягательств должен пересечь охраняемое пространство и войти в соприкосновение с охраняемой ценностью
- Внеполосный высокочастотный сигнал в телефонной линии
- Внешнее электромагнитное излучение, которое модулируется параметрами здания
- Луч инфракрасной энергии на остекленной поверхности

Формы активности «нарушителей»

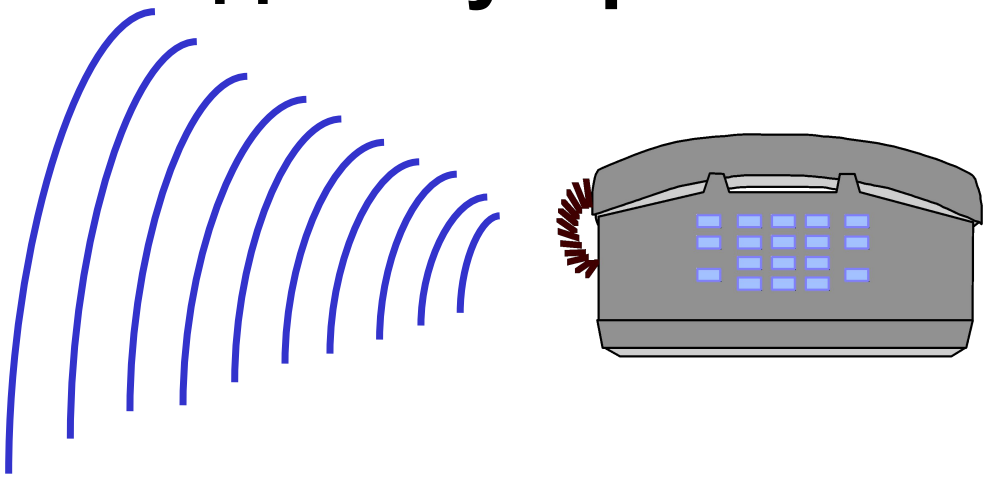
- Сетевой пакет (пакеты) с определенной сигнатурой, поступившие на приемник определенной сетевой карты (приемник идентифицируется уникальным аппаратным адресом)
- Излучение энергии (как правило, электромагнитной или акустической). Таким образом проявляет себя замаскированная радиозакладка
- Обращение к файлу, устройству ввода-вывода информации
- Вызов привилегированной или заведомо опасной системной функции

Пассивные способы обнаружения



Фиксация факта и места преодоления периметра объекта

Обнаружение активности закладных устройств



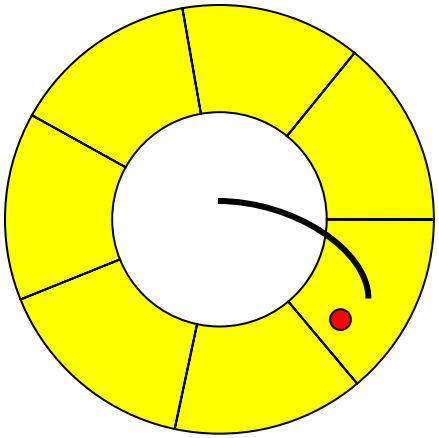
Пассивные рубежи контроля

- Предназначены для обнаружения признаков действия активного нарушителя
- Обнаруживаемые виды активности: движение тела в пространстве, характерные локомоции, наличие радиоизлучения с определенными параметрами, создание нового процесса в оперативной памяти, его обращение к файловым объектам и устройствам
- Рубеж оборудуется вокруг защищаемого объекта
- Средства обнаружения должны обладать пространственной чувствительной зоной

Пассивные «нарушители»

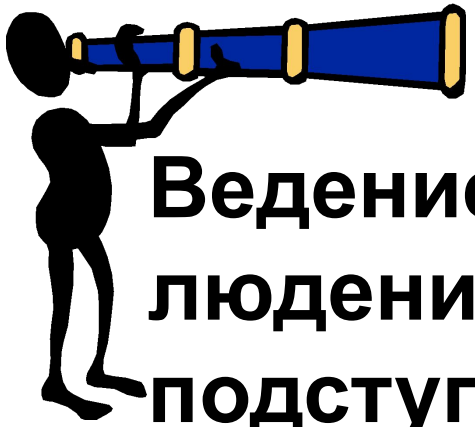
- Файл вредоносной программы, записанный в определенных секторах дискового пространства или загруженный в определенный диапазон оперативной памяти
- Процесс (исполняемая программа), ожидающий очереди на запуск
- Электронное устройство подслушивания, скрытно размещенное в помещении и не демаскирующее себя радиопередачей
- Человек-нарушитель, замаскировавшийся после проникновения на объект
- Оператор, ведущий технический перехват информации
- Телефонная закладка или скрытно подключенный параллельный телефон

Активные способы обнаружения



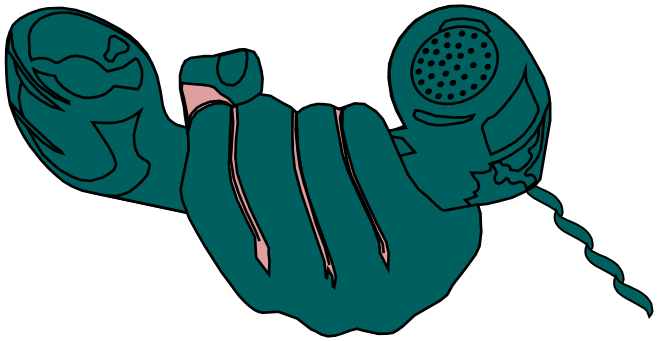
Сканирование памяти компьютера

BA 27 01 CD 21 C3 43
52 41 4B 20 78 31 AE
AB A5 E3 20 E1 .. ..



Ведение наблюдения за подступами к объекту

Поиск замаскированных устройств подслушивания



Активные рубежи контроля

- Предназначены для обнаружения признаков состояния пассивного нарушителя
- Рубеж представляет собой активный процесс в режиме поиска (наблюдения, сканирования)
- Пассивный нарушитель считается проникшим на объект и скрывающимся в ожидании удобных условий для дальнейших действий
- Поиск (сканирование) ведется путем поочередного контроля (сосредоточения энергии или внимания) всех элементов пространства

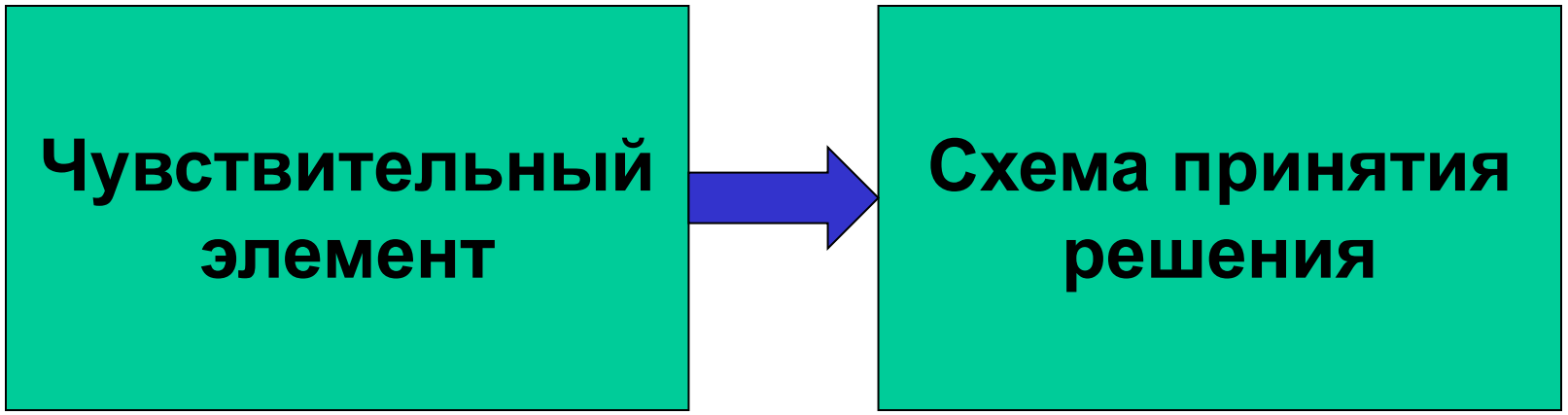
В качестве контролируемого пространства могут выступать

физическое пространство

пространство памяти

диапазон частот

временное пространство



- **Правильное обнаружение**
- **Пропуск сигнала**
- **Правильное не обнаружение**
- **Ложная тревога**

Характеристики системы контроля

- контролируемое пространство (физическое трехмерное пространство, трехмерное или одномерное дисковое пространство, одномерное пространство длин волн или частот, пространство модуляционных признаков, одномерное пространство двоичных сигналов в последовательном канале, древовидная структура файлов и пр.)
- размер элемента контролируемого пространства
- дискретность контролируемого пространства (можно ли проникнуть сквозь элементы контроля?)

Характеристики системы контроля

- алгоритм сканирования пространства
- период сканирования каждого элемента
- размер тела воздействия (размер нарушителя по сравнению с однократно контролируемым объемом пространства)
- что подлежит контролю: непосредственное воздействия нарушителя или какой-нибудь вторичный признак (например, электрический сигнал в канале связи)
- минимально необходимое количество информации о состоянии объекта контроля
- ошибки первого и второго рода и др.

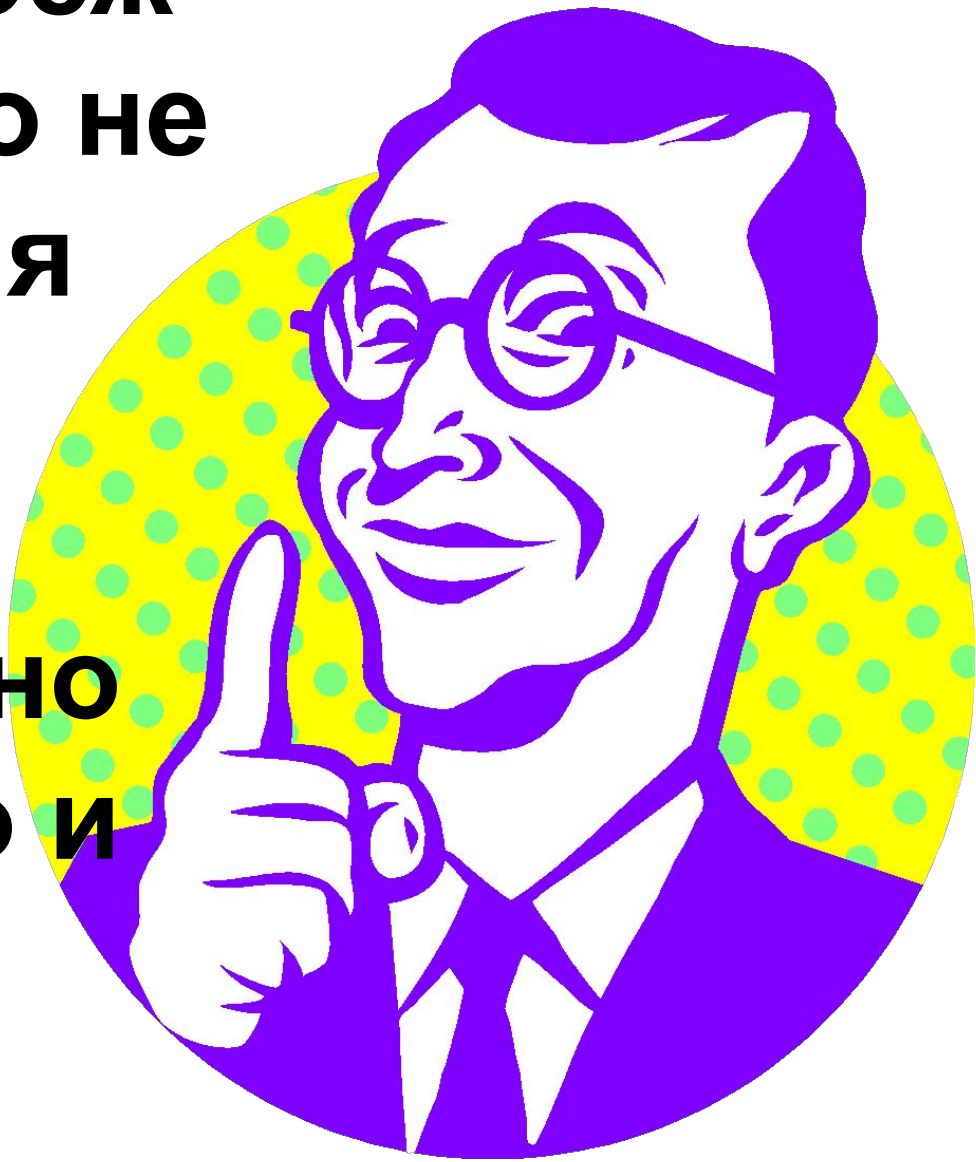
Характеристики технических средств обнаружения (ТСО)

- Вероятность обнаружения нарушителя
- Наработка на ложную тревогу
- Точность указания места нарушения
- Информация о количестве нарушителей, направлении их движения

Способы повышения достоверности тревожной информации

- Применение нескольких рубежей контроля
- Использование чувствительных элементов с различными принципами действия
- Средства визуального и технического наблюдения за объектом и рубежами охраны
- Периодическая проверка работоспособности рубежей контроля
- Использование составной сигнатуры вредоносного программного кода
- Использование дополнительных информативных признаков нарушителя (например, 3-й гармоники в нелинейных локаторах)

Сам по себе рубеж контроля ничего не значит. Действия нарушителя не только должны быть немедленно обнаружены, но и своевременно пресечены

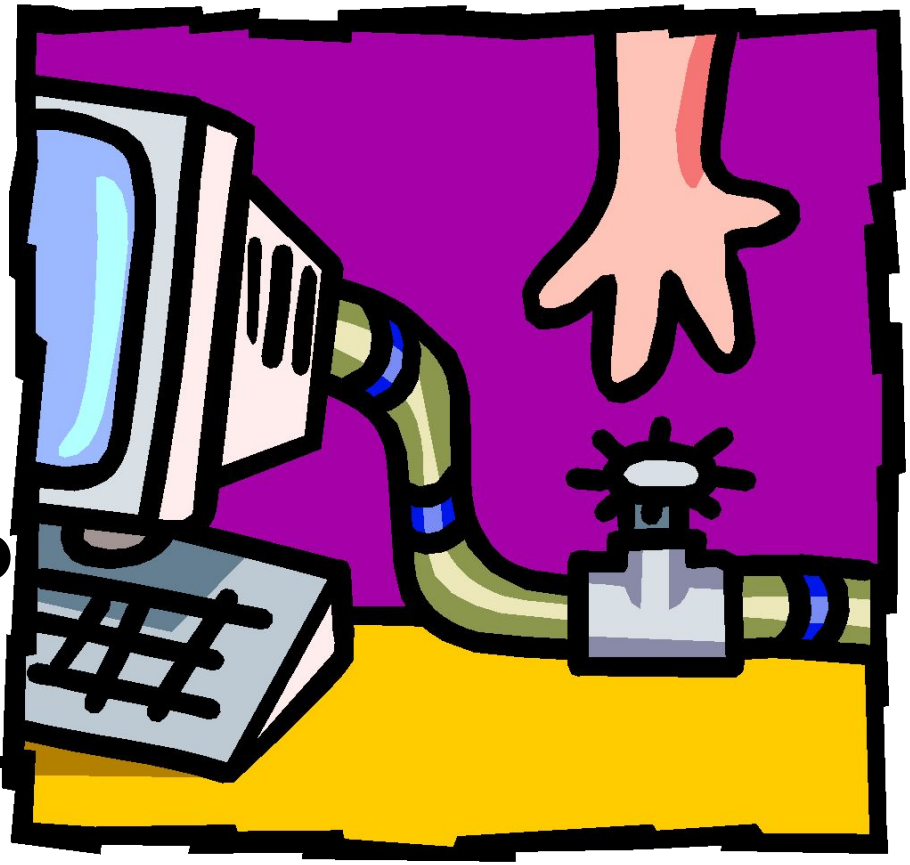


Формы реагирования на сигнал о вторжении

- Защитное блокирование возможности физического или логического доступа
- Отключение анализирующего устройства от источника подозрительных сигналов (аппаратное и программное)

- Силовое блокирование и задержание нарушителя персоналом охраны
- Сбор доказательств и привлечение нарушителя к юридической ответственности

- **Защитное блокирование - спосо воспрепятствования доступу к компьютер- ной информации со стороны посторонних лиц и непривилегиро- ванного кода**



Формы защитного блокирования

- Отключение запроса пароля на вход в систему (после N-кратного ошибочного ввода)
- Блокирование учетной записи пользователя
- Блокирование физического носителя ключевой информации (например, электронной карточки в банкомате)
- Блокирование человека-нарушителя на пункте пропуска (в шлюзе, кабине, тамбуре)

В случае поступления сигнала о вторжении или неисправности системы данные должны «глухо» блокироваться и от нарушителя, и от владельца

Виды защитного блокирования

- Отключение управления устройст-вами записи/считывания машинного носителя через контроллер
- Блокирование экрана и клавиатуры
- Замедление повторного запроса после ввода серии неверных паролей
- Имитация «зависания» операцион-ной системы, требующая перезаг-рузки

Формы защитного уничтожения информации

- Импульсное размагничивание машинных носителей на магнитной основе
- Уничтожение вещественных носителей информации при транспортировке с помощью специальных кейсов
- Защитное стирание данных с помощью контроллера HDD

Устройство стирания информации с ЖМД «Стек-НС2м»

Изделие «Стек-НС2м» монтируется в стандартный компьютерный корпус, компьютер полностью сохраняет свою функциональность и внешний вид.

Система может быть настроена на автоматическое стирание информации по ряду признаков: длительное отключение питания, нетипичные перемещения корпуса в пространстве, внеурочное включение питания.

Имеется защита полного разряда аккумулятора

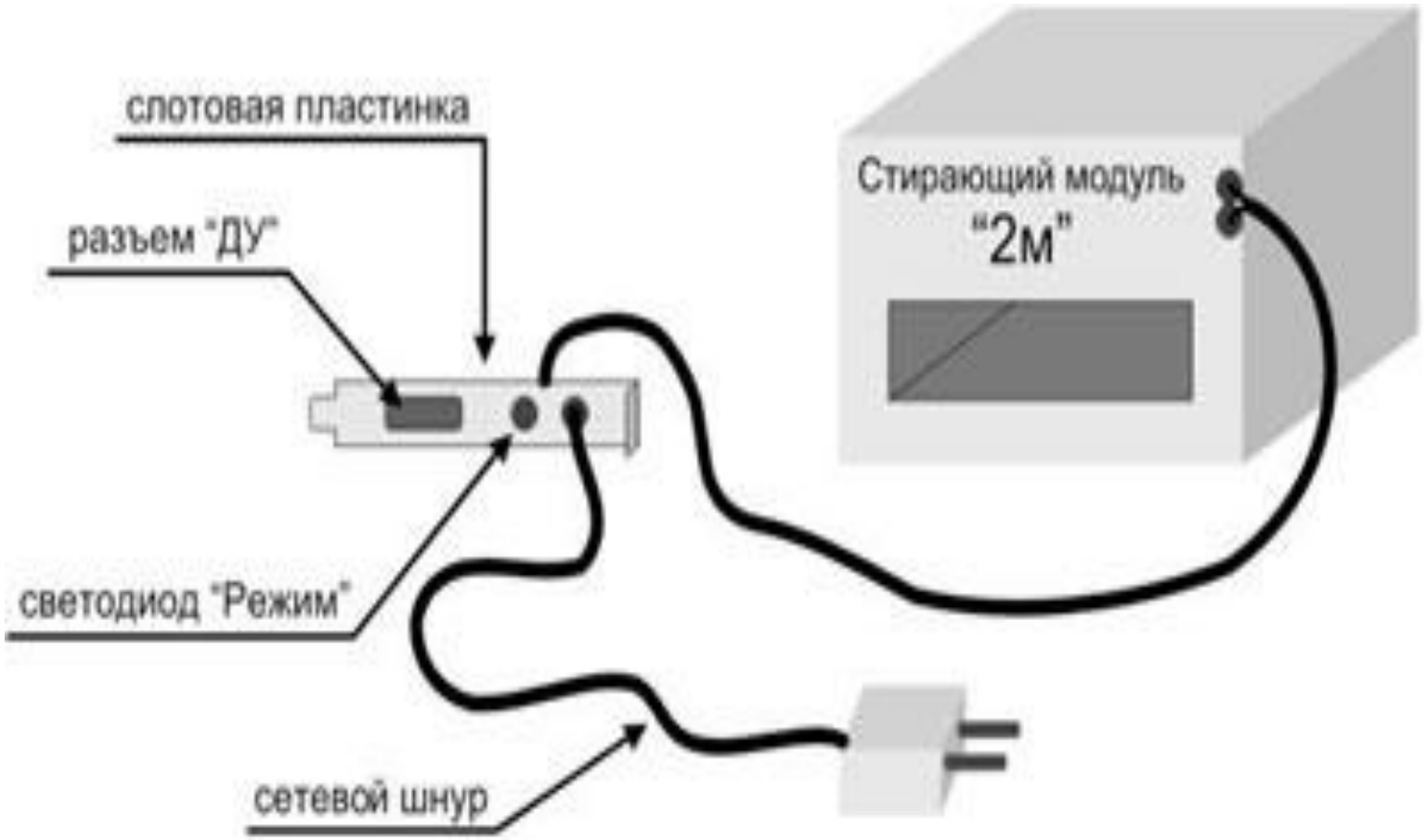
Устройство стирания информации с ЖМД «Стек-НС2м»

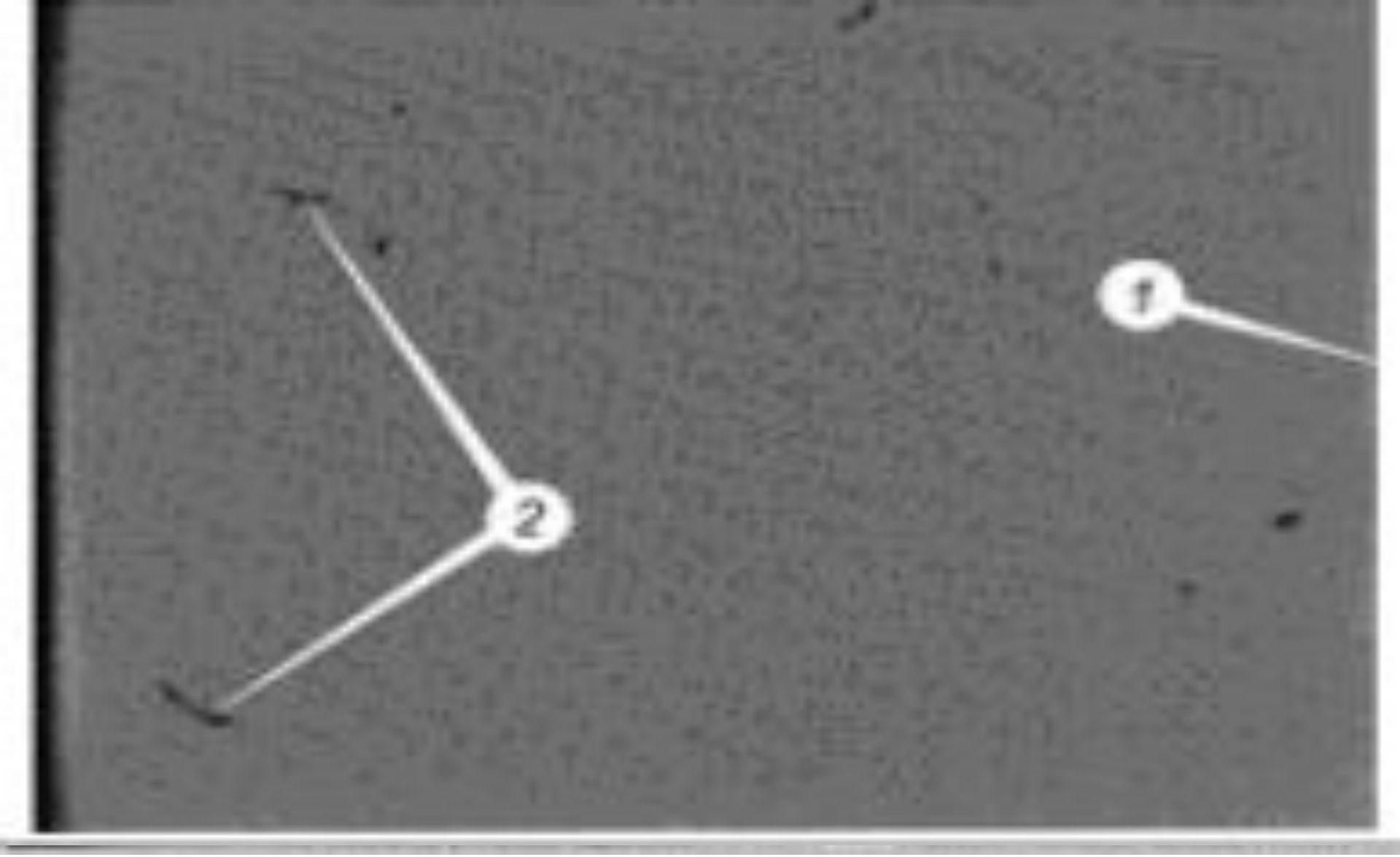
Устройство стирания информации с ЖМД «Стек-НС2м»

Используется для гарантийного стирания информации с жесткого диска, установленного в системный блок компьютера. Гарантии на возможность продолжения эксплуатации носителя после стирания информации нет

Устройство может включаться вручную с помощью кнопки, дистанционно по радиоканалу (блок радиоуправления автомобильной сигнализации, пейджер, сотовая связь), либо при срабатывании датчика контроля вскрытия системного блока

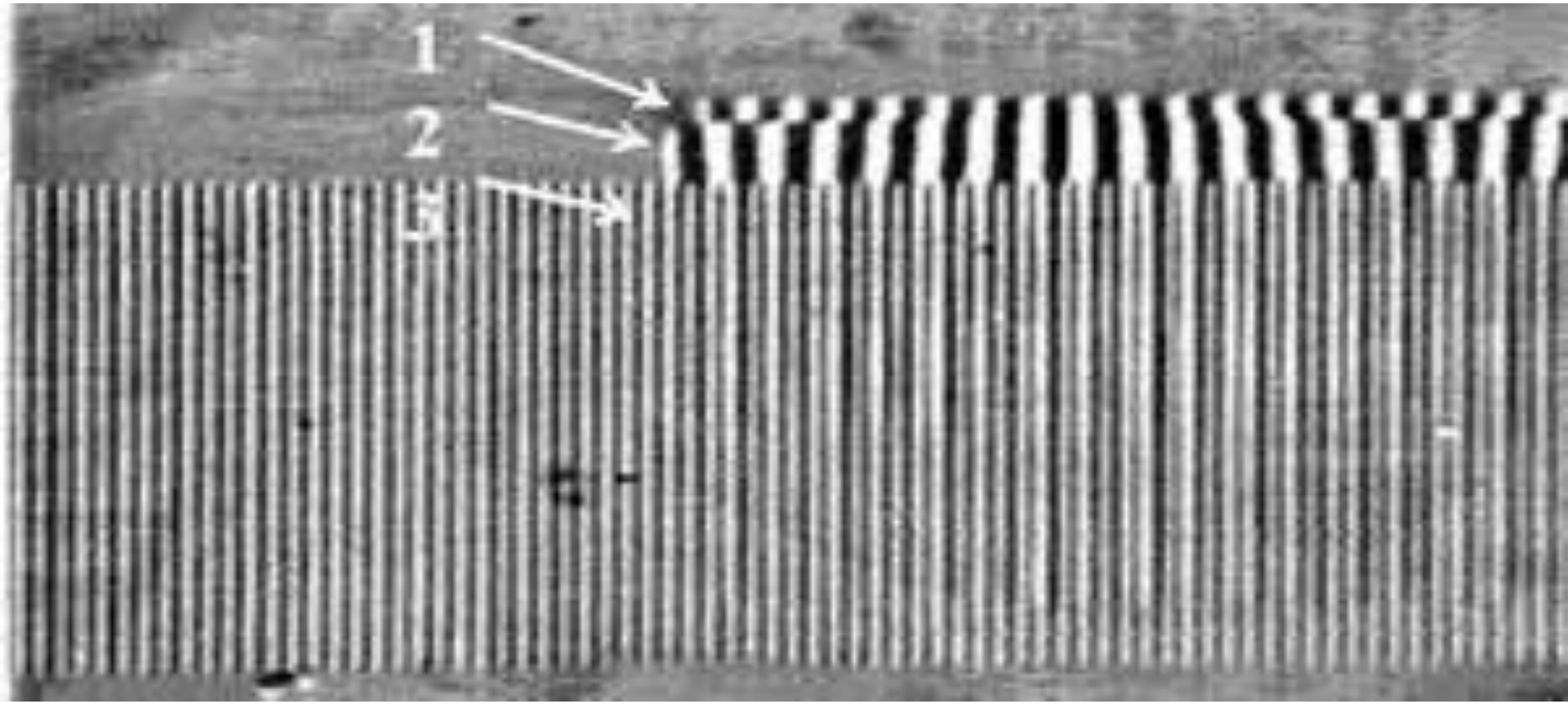
Устройство стирания информации с ЖМД «Стек-НС2м»





1 – внешний край ЖМГ; 2 – дефекты поверхности магнитного носителя; 3 – разметка ЖМД

Программное уничтожение информации



1,2 - остатки предыдущих записей;
3 - новая запись

Правильно организованная защита должна содержать элементы неожиданности для нарушителя и ложные объекты, для того, чтобы израсходовать ресурсы нарушителя и вынудить его оставить больше следов

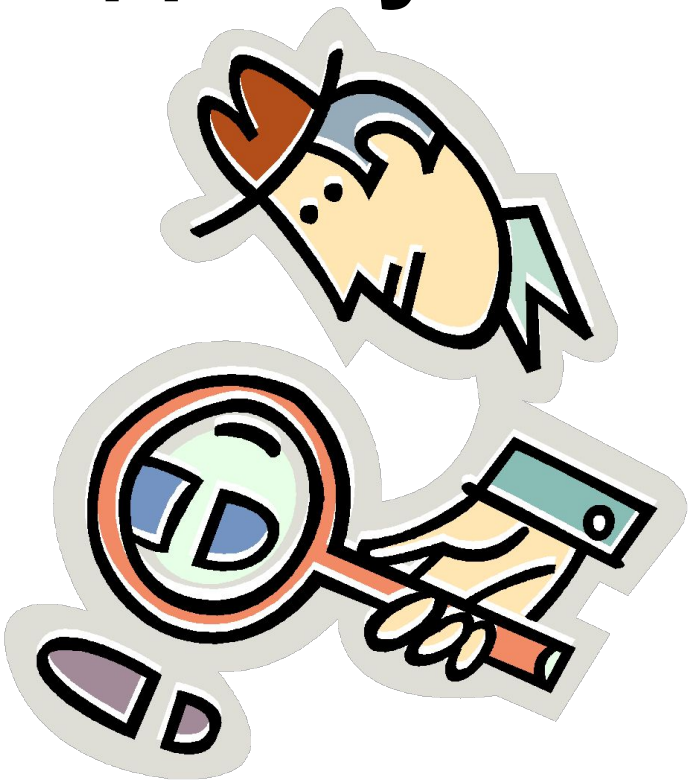
Последний рубеж защиты от НСД должен представлять собой систему документирования преступной деятельности с целью ее расследования и привлечения виновного к ответственности

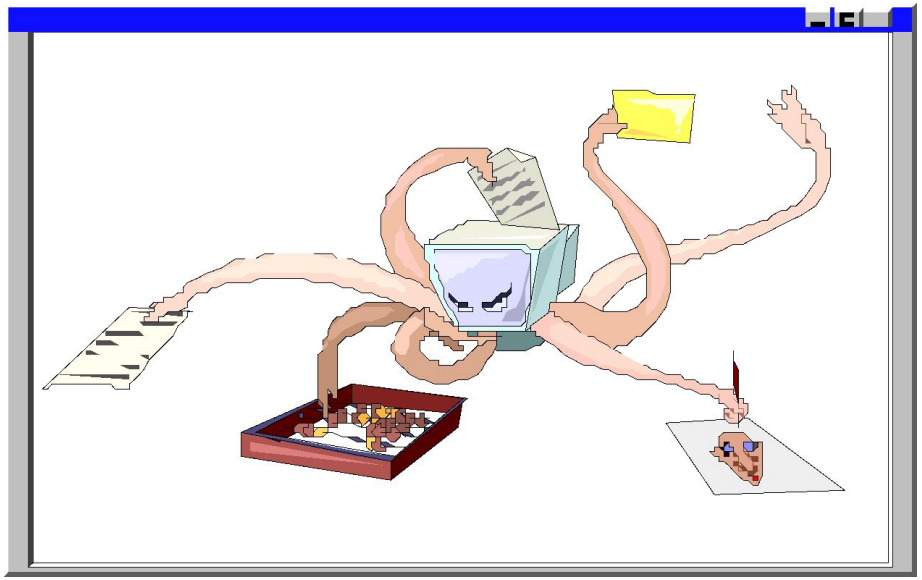
Виды документирования следов НСД

- Внешний осмотр места происшествия
- Снятие отпечатков пальцев
- Фотографирование и видеосъемка
- Поиск и извлечение аппаратной закладки
- Копирование файла вредоносной программы и передача ее для исследования
- Анализ записей в журналах аудита

Следы физического доступа

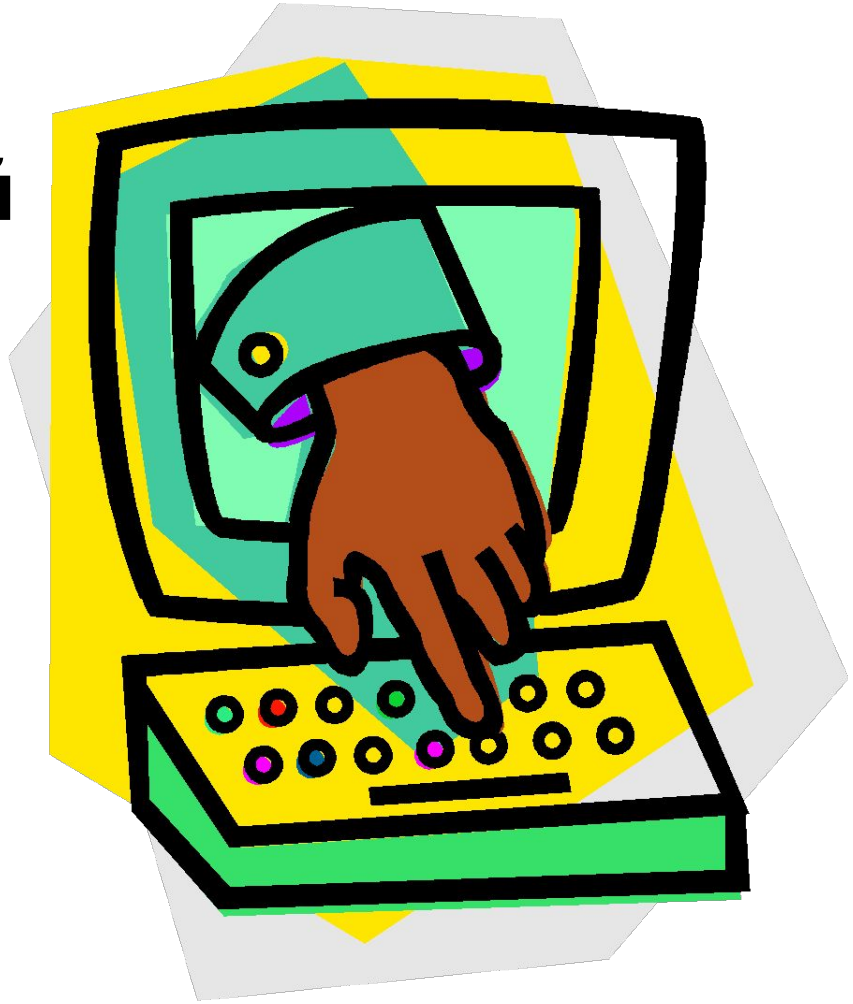
- Следы взлома или отпирания двери
- Забытые нарушителем инструменты, машинные носители, личные вещи
- Следы вскрытия блоков аппаратуры
- Изменение расположения блоков компьютера на рабочем месте
- Компьютер, оставленный включенным нарушителем
- Признаки поспешного выключения компьютера





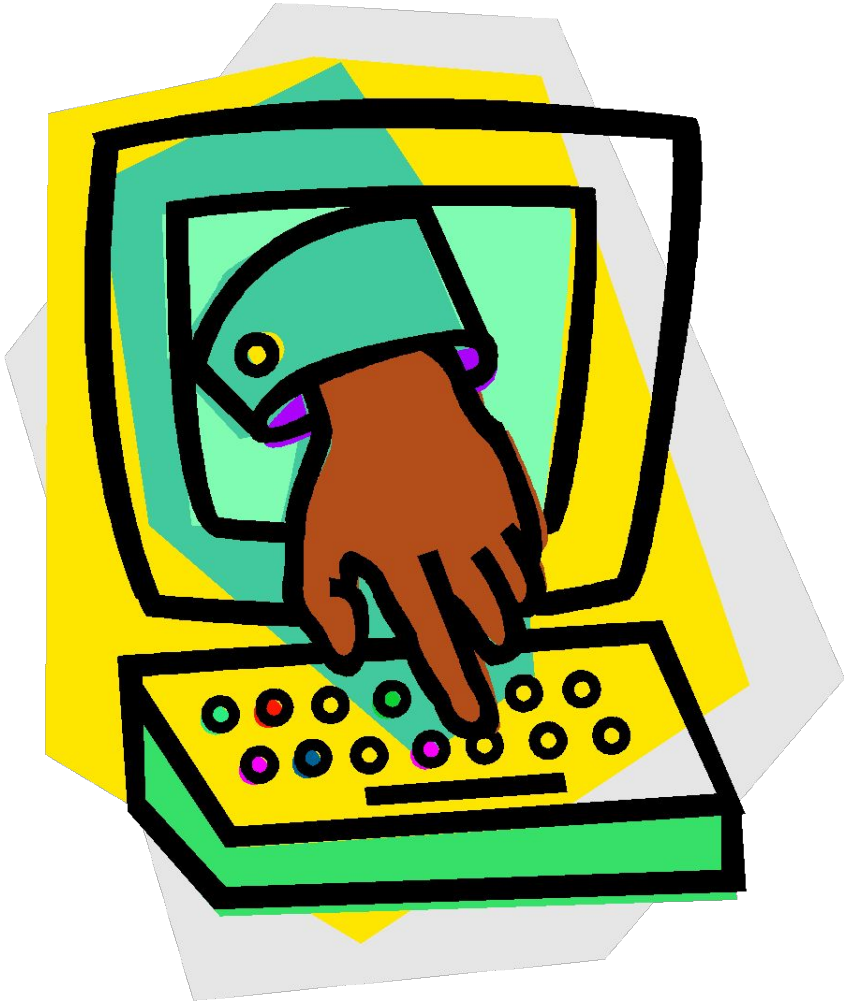
В отличие от вещественных следов, оставляемых преступником, в памяти компьютера фиксируются опосредованные воздействия человека, а механизм следообразования определяется только устройствами ввода-вывода

Между пальцами преступника, воздействующего на клавиатуру или манипулятор, и внешней памятью компьютера, в которой остаются его следы, располагается множество аппаратных узлов и компьютерных программ, которые стирают многие идентифицирующие признаки



Следы, свидетельствующие об авторизации пользователя

- Записи о факте и времени попытки доступа в журнале аудита
- Регистрация новых пользователей в системном реестре



Следы, свидетельствующие о внедрении и/или запуске вредоносной программы

- Названия неизвестных файлов в каталогах, а также в списках программ, предназначенных для автоматического запуска
- Появление новых программ
- Преобразование файлов (типа, размера, временных отметок и др.)
- Отсутствие доступа к файловой системе, либо к отдельным файлам и каталогам
- Нарушение разметки машинных носителей

Следы, свидетельствующие о внедрении и/или запуске вредоносной программы

- Изменение настроек CMOS-памяти
- Отключение существующих или подключение новых устройств
- Невозможность загрузки или полное блокирование ЭВМ
- Уменьшение доступного дискового пространства
- Уменьшение доступной оперативной памяти и др.