Основы защиты информации и управления интеллектуальной собственностью

Рощупкин Яков Викторович
Кафедра Защиты информации

1. Максимов Ю.Н., Сонников В.Г., Петров В.Г. и др. Технические методы и средства защиты информации. СПб.: Полигон, 2000. – 320 с.
2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам: Учеб. пособие для подготовки экспертов системы Гостехкомиссии России. М.: Горячая линия - Телеком, 2005. – 416 с.
3. Голиков В.Ф., Лыньков Л.М., Прудник А.М., Борботько Т.В. Правовые и организационно-технические методы защиты информации: Учеб. пособие. – Мн.: БГУИР, 2004. – 80 с.
4. Голдовский И. Безопасность платежей в Интернете. – СПб.: Питер, 2001. – 240 с.
5. Деднев М.А., Дыльнов Д.В., Иванов М.А. Защита информации в банковском деле и электронном бизнесе. М.: Кудиц-образ, 2004. – 512 с.
5. Галатенко В.А. Основы информационной безопасности: курс лекций. М.: Интернет-Университет Информационных Технологий, 2003. – 280 с.

http://abitur.bsuir.by/m/12_116608_1_50028.ZIP

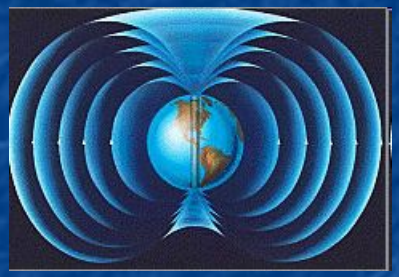
http://abitur.bsuir.by/m/12_116608_1_51479.ZIP

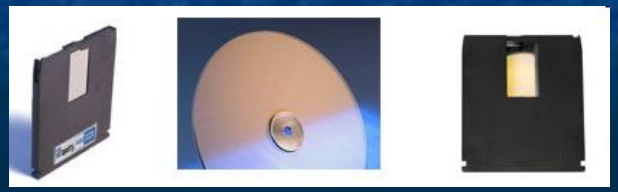
Информационная безопасность. Важность проблемы. Основные понятия.

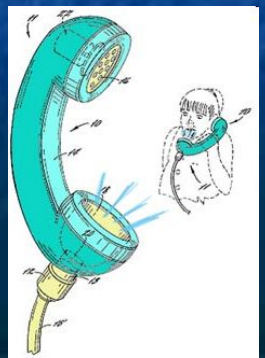
Лекция 1

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах

Информационный объект (ИО) – среда, в которой информация создается, передается, обрабатывается или хранится







Информационная безопасность – защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести **неприемлемый** ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Природа воздействия на информационный объект может быть двух видов:

— **непреднамеренной** (стихийные бедствия, отказы оборудования, ошибки персонала и т.д.);

— **преднамеренной** (действия злоумышленников).

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности

Виды ущерба информационному объекту или поддерживающей инфраструктуре:

Нарушение конфиденциальности — нарушение свойства информации быть известной только определенным субъектам.

Нарушение целостности — несанкционированное изменение, искажение, уничтожение информации.

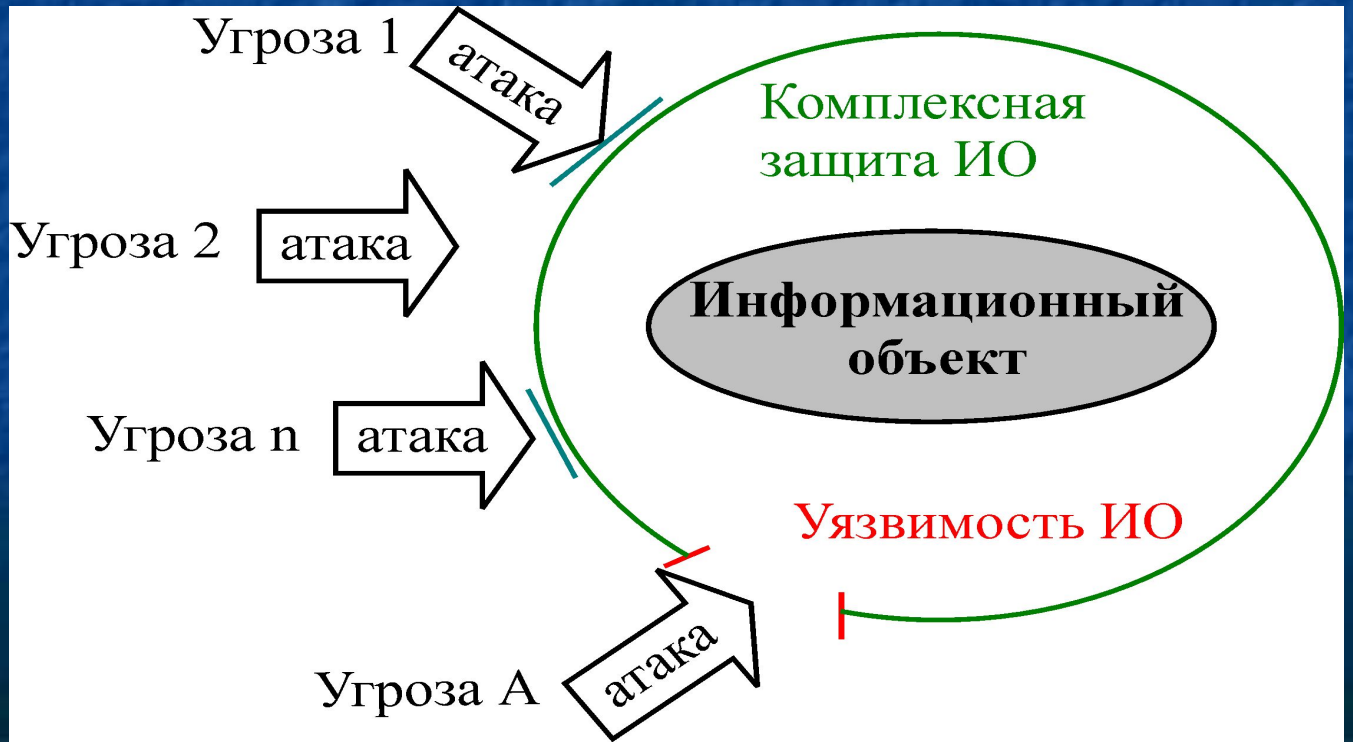
Нарушение доступности (отказ в обслуживании) — нарушаются доступ к информации, работоспособность объекта, доступ в который получил злоумышленник.

Угрозы информационной безопасности

Угроза информационной безопасности объекта – возможные воздействия на ИО, приводящие к ущербу

Уязвимость – свойство объекта, делающее возможным возникновение и реализацию атаки

Атака – действие злоумышленника, заключающееся в поиске и использовании той или иной уязвимости



Классификация угроз

– по аспекту информационной безопасности, против которого угрозы направлены в первую очередь **(доступность, целостность, конфиденциальность, собственность)**;

– по компонентам информационных систем, на которые угрозы нацелены **(данные, программы, аппаратура, поддерживающая инфраструктура)**;

– по способу осуществления **(случайные, природные / техногенного характера; преднамеренные;)**;

– по расположению источника угроз **(внутренние / внешние)**.

Охраняемые сведения и демаскирующие признаки

Охраняемые Сведения – сведения, несанкционированное распространение которых создает или может создать угрозу национальной безопасности Республики Беларусь, а также конституционным правам и свободам граждан. (Закон РБ “О государственных секретах”).

Демаскирующие признаки – любые характеристики ИО, которые можно обнаружить с помощью ТСР, проанализировать и получить информацию об охраняемых сведениях

Первичные ДП представляют собой физические характеристики объектов и среды, непосредственно регистрируемые специальной аппаратурой и содержащие информацию об охраняемых сведениях. Примеры: напряженность электромагнитного поля, амплитуда, частота и фаза тока, уровень излучения и т. п.

Очевидно, что именно первичные ДП являются источниками информации, получаемой с помощью технических средств разведки.

Вторичные ДП — это признаки, которые могут быть получены путем накопления и обработки первичных ДП. Примеры: диаграммы излучения объекта, амплитудно-частотные спектры излучений, химический состав вещества и т.д.

Анализ риска

Процесс анализа риска состоит из 6 последовательных этапов:

1. Идентификация и классификация объектов защиты (ресурсов компании, подлежащих защите);
2. Категорирование ресурсов;
3. Построение модели злоумышленника;
4. Идентификация, классификация и анализ угроз и уязвимостей;
5. Оценка риска;
6. Выбор организационных мер и технических средств защиты.

Идентификация и классификация объектов защиты

- Информационные ресурсы (конфиденциальная и критичная информация компании);
- Программные ресурсы (ОС, СУБД, критичные приложения, например ERP);
- Физические ресурсы (сервера, рабочие станции, сетевое и телекоммуникационное оборудование);
- Сервисные ресурсы (электронная почта, www и т.д.).

Категорирование ресурсов

- Категорирование заключается в определении уровня **конфиденциальности** (секретности) и **критичности** (степень влияния на эффективность производственных процессов) ресурса.

параметр/значение	критичный	существенный	незначительный
строго конфиденциальный	7	6	5
конфиденциальный	6	5	5
для внутреннего пользования	5	4	3
открытый	4	3	2

Построение модели злоумышленника

Основные характеристики, которые позволяют описать основные группы нарушителей:

- **Мотивы;**
- **Цели;**
- **Финансовое обеспечение;**
- Наличие и уровень **профессиональной подготовки;**
- **Техническое обеспечение;**
- Наличие и качество **предварительной подготовки** преступления
- Наличие и уровень **внедрения** нарушителей **на объект;**
- **Время** действия;

Основные классы злоумышленников

- **Класс А** - Действуют злонамеренно и обладают практически неограниченным финансовым обеспечением.
- **Класс Б** - Действуют злонамеренно и обладают ограниченным, но достаточно крупным финансовым обеспечением.
- **Класс В** - Действуют злонамеренно и обладают малым (или вообще не обладают) финансовым обеспечением, но имеют хороший профессиональный уровень подготовки.
- **Класс Г** - Действуют злонамеренно и обладают малым (или вообще не обладают) финансовым обеспечением и имеющие низкий уровень профессиональной подготовки.
- **Класс Д** - Действуют не злонамеренно.

Оценка риска

- Определяется потенциальный ущерб от угроз нарушения информационной безопасности для каждого ресурса или группы ресурсов.

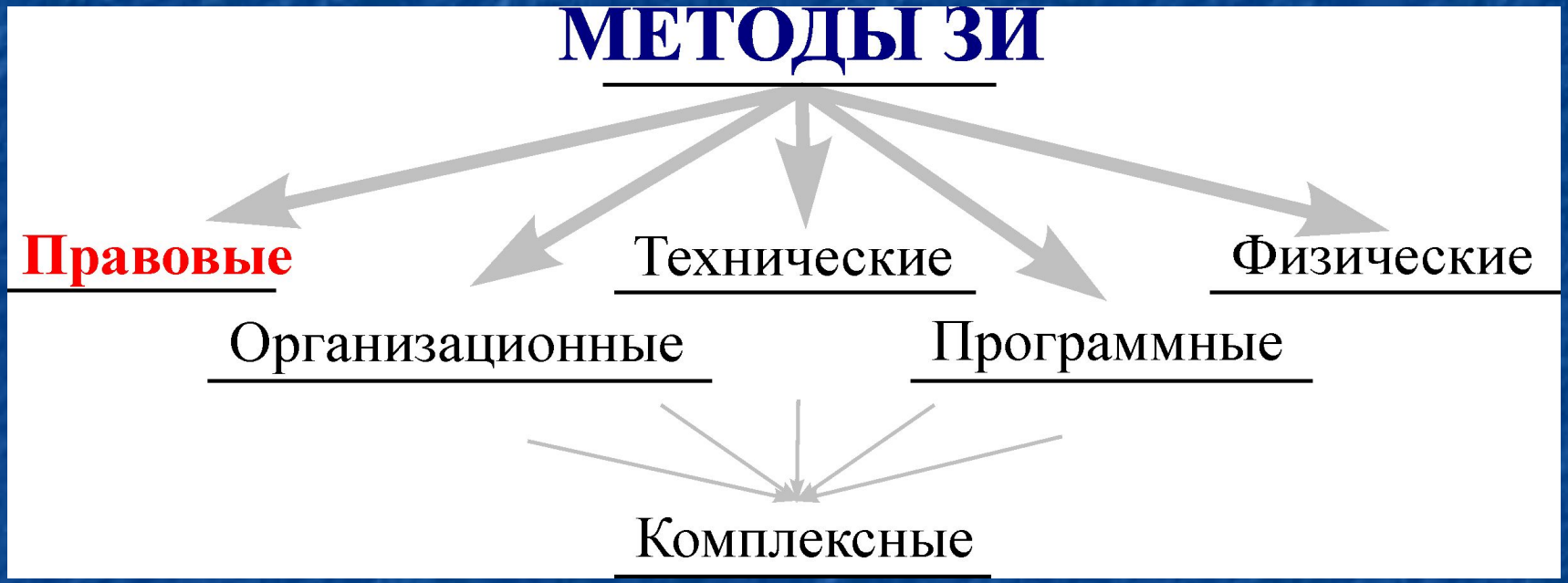
Качественный показатель ущерба зависит от параметров:

- Значимость ресурса;
- Частота реализации угрозы на этот ресурс.

Исходя из полученных оценок ущерба, обоснованно выбираются адекватные организационные меры и технические средства защиты

ЗИ от случайных угроз

КЛАССИФИКАЦИЯ МЕТОДОВ ЗИ



Принципиальным вопросом при определении уровня защищенности объекта является выбор критериев. Рассмотрим один из них - широко известный критерий "эффективность - стоимость".

Пусть имеется информационный объект, который при нормальном функционировании создает положительный эффект (экономический, политический, технический и т.д.). Этот эффект обозначим через E_0. Несанкционированный доступ к объекту уменьшает полезный эффект от его функционирования (нарушается нормальная работа, наносится ущерб из-за утечки информации и т.д.) на величину ΔE. Тогда эффективность функционирования объекта с учетом воздействия несанкционированного доступа:

$$E = E_0 - \Delta E.$$

Относительная эффективность:

$$\delta = \frac{E}{E_0} = \frac{E_0 - \Delta E}{E_0} = 1 - \frac{\Delta E}{E_0}.$$

Уменьшение эффективности функционирования объекта приводит к материальному ущербу для владельца объекта. В общем случае материальный ущерб есть некоторая неубывающая функция от ***ΔE***:

$$U = f(\Delta E).$$

Будем считать, что установка на объект средств защиты информации уменьшает негативное действие несанкционированного доступа на эффективность функционирования объекта. Обозначим снижение эффективности функционирования объекта при наличии средств защиты через $\Delta E_З$, а коэффициент снижения негативного воздействия несанкционированного доступа на эффективность функционирования объект - через ***K***, тогда:

$$\Delta E_З = \frac{\Delta E}{K},$$

где K≥1.

Выражения (1) и (2) примут вид:

$$E_З = E_0 - \Delta E_0 = E - \frac{\Delta E}{K},$$

$$\delta_З = \frac{E_З}{E_0} = \frac{E_0 - \Delta E_З}{E_0} = 1 - \frac{\Delta E_З}{E_0} = 1 - \frac{\Delta E}{K E_0}.$$

Стоимость средств защиты зависит от их эффективности, и в общем случае ***K*** — есть возрастающая функция от стоимости средств защиты:

$$K = f(C).$$

Поскольку затраты на установку средств защиты можно рассматривать как ущерб владельцу объекта от возможности осуществления несанкционированного доступа, то суммарный ущерб объекту:

$$U_\Sigma = \frac{U}{K} + C = \frac{U}{f(C)} + C.$$

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то U_Σ непосредственно изменяет эффективность:

$$E_З = E_0 - \frac{\Delta E}{K - C}.$$

Таким образом, классическая постановка задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа имеет вид:

$$\begin{cases} U_\Sigma \to min \\ C = C_{опт} \end{cases},$$

или

$$\begin{cases} E_З \to max, \\ C = C_{опт} \end{cases} \qquad \begin{cases} \delta_З \to max, \\ C = C_{опт}. \end{cases}$$

Шпионский музей Кита Мэлтона

- ✔ Устройства для скрытого фотографирования

Приемопередатчик в настольной лампе

- Использовались американскими специалистами для камуфлирования в них агентурных радиостанций, при этом в основание лампы были встроены и приемник, и передатчик. В некоторых случаях подобная аппаратура использовалась в качестве подслушивающего устройства с передачей информации по радиоканалу

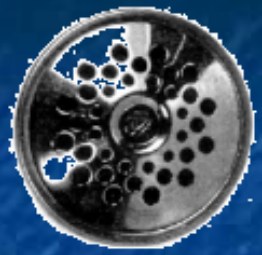
Шифровальные устройства

- В общем случае буквы и цифры сообщения заменяются другими символами, делая его совершенно непонятным.

Шифровальная машина Enigma

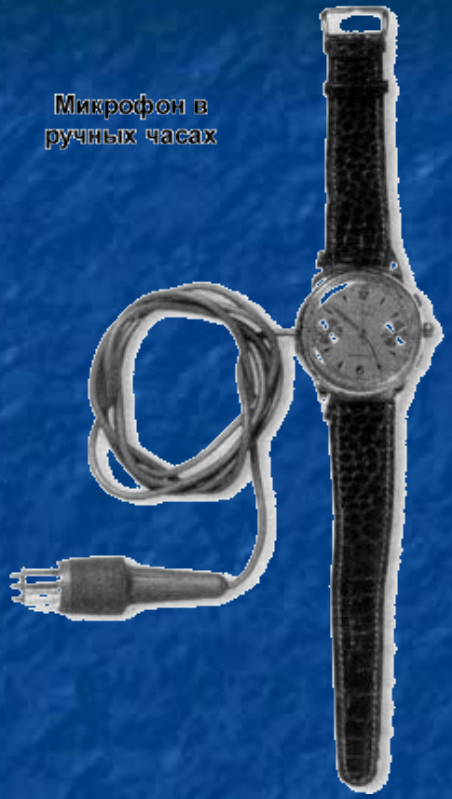
- В ходе войны Enigma подвергалась постоянной модернизации. Только в 1943 году, используя электронно-вычислительную технику, удалось раскрыть применявшийся в ней шифр. По мнению историков этот факт сыграл решающую роль в победе союзников над нацистами во Второй мировой войне. Созданная в 1923 году Enigma представляла собой электромеханическое устройство для зашифровки и расшифровки текстовой информации. Каждая буква сообщения зашифровывалась самостоятельно при помощи целого набора механических роторов и электрических разъемов

Подслушивающие устройства

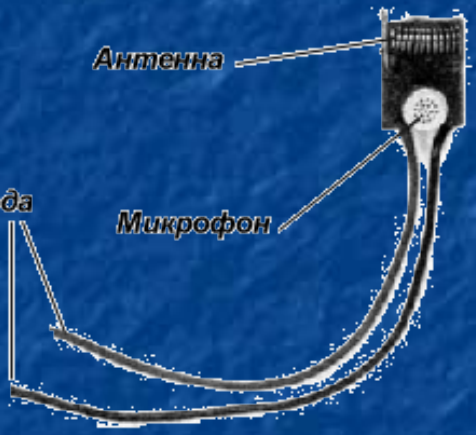


Микрофон обычной телефонной трубки со встроенным передатчиком

Микрофон в ручных часах



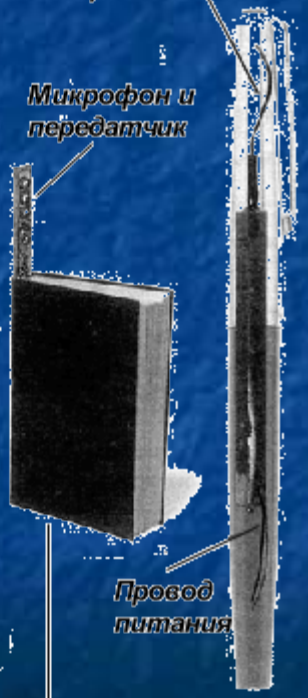
Радиомикрофон универсального назначения



Микрофон с передатчиком в корешке книжного переплета

Антенный провод

Микрофон и передатчик



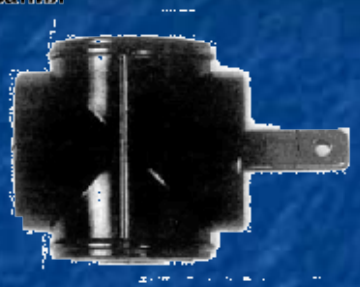
Провод питания

Внедрение средства подслушивания в корешок переплета

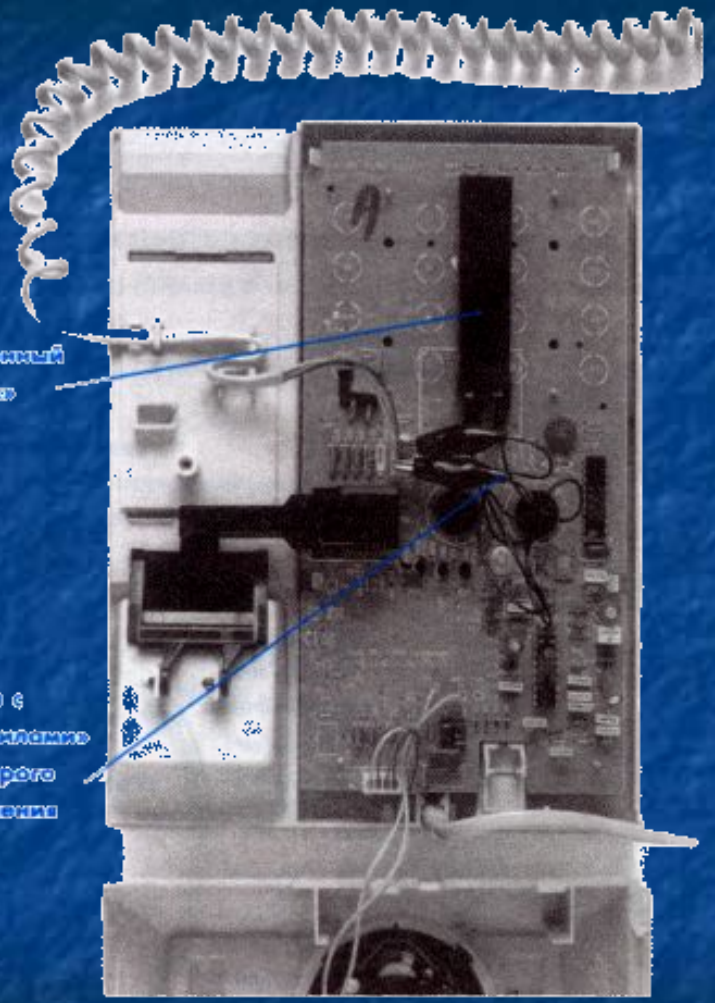
Устройство для подслушивания через стену

Средства подслушивания

Демонстрационная модель разъема с устр-вом подслушивания



Реальный сетевой адаптер, оборудованный устройством подслушивания



Подслушивание телефонов при помощи быстро устанавливаемого устройства

Электромагнитное оружие

- **Электромагнитная бомба** — генератор радиоволн высокой мощности (десятки гигаватт), приводящих к уничтожению электронного оборудования командных пунктов, систем связи и компьютерной техники на расстоянии сотен метров от источника. Создаваемая электрическая наводка по мощности воздействия на электронику оказывается сравнимой с ударом молнии.
- *Низкочастотные* (используют для доставки разрушающего напряжения наводку в линиях электропередачи)
- *Высокочастотные* (вызывают наводку непосредственно в элементах электронных устройств и обладающие высокой проникающей способностью — достаточно мелких щелей для вентиляции для проникновения волн внутрь оборудования).

Доставка электромагнитной бомбы

- Впервые взрыв был произведён в атмосфере над Тихим океаном (1950гг). Результатом было нарушение электроснабжения на Гавайях из-за воздействия электромагнитного импульса высотного ядерного взрыва.

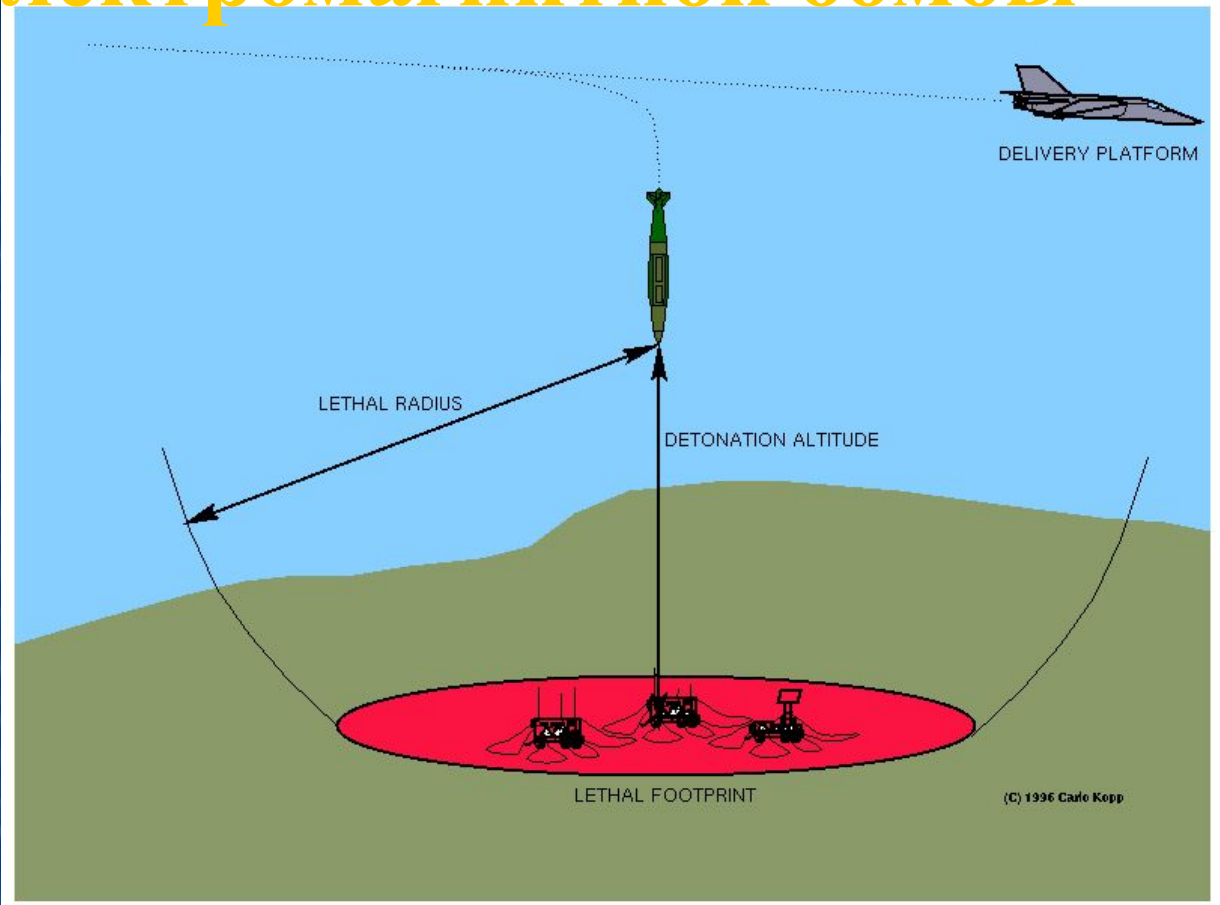


FIG.7 LETHAL FOOTPRINT OF LOW FREQUENCY E– BOMB IN RELATION TO ALTITUDE

- Лучи достигли Гавайских островов, расположенных в сотнях километров от места испытания, и радиопередачи были нарушены до самой Австралии. Взрыв бомбы, помимо мгновенных физических результатов, воздействовал на электромагнитные поля на огромном расстоянии.

Электромагнитный терроризм

- Генератор излучений ЭМИ содержит источник питания, модулятор и полеобразующее устройство – антенну.
- Стоимость – от 5 до 50 тыс. USD.
  Затраты на проведение работ, связанных с обеспечением стойкости РЭС к воздействию ЭМИ, на ранних стадиях проектирования составляют не более 2% от стоимости разработки, а стоимость защищенного РЭС возрастает не более чем на 3 – 5%.
- Воздействие электромагнитного оружия вызывает в цепях РЭС и на клеммах электронной техники импульсы напряжений от 100 до 10000 В. Наблюдаются массовые искрения и пробои в воздушных промежутках размером до 50 мм между составными частями конструкции РЭС. При этом энергия искровых пробоев составляет от 0,1 до 100 мДж.
- Этой энергии достаточно, чтобы в РЭС вызвать отказы электронной техники, замыкания в цепях источников питания, пожары и взрывы горючих веществ,
  энергия инициирования взрыва многих пыле-газо-воздушных смесей находится в пределах от 20 до 0,01 мДж,
  поражения полупроводниковых структур – от 1 до 0,001 мДж