6. Технические каналы утечки информации, возникающие при работе вычислительной техники за счет ПЭМИН

При выявлении технических каналов утечки информации СВТ целесообразно рассматривать как систему, включающую основное (стационарное) оборудование, оконечные устройства, соединительные линии (совокупность проводов и кабелей, прокладываемых между отдельными СВТ и их элементами), системы электропитания, системы заземления.

Отдельные технические средства (ТС) или группа технических средств, предназначенных для обработки информации ограниченного доступа, вместе с помещениями, в которых они размещаются, составляют объект СВТ.

Наряду с СВТ в помещениях устанавливаются технические средства и системы, непосредственно не участвующие в обработке информации ограниченного доступа, но использующиеся совместно с СВТ и находящиеся в зоне электромагнитного поля, создаваемого ими. Такие технические средства и системы называются вспомогательными техническим средствами и системами (ВТСС). К ним относятся: технические средства открытой телефонной, громкоговорящей связи, системы пожарной и охранной сигнализации, электрификации, радиофикации, часофикации, электробытовые приборы и т.д.

В качестве канала утечки информации наибольший интерес представляют ВТСС, имеющие выход за пределы контролируемой зоны (КЗ), т.е. зоны, в которой исключено появление лиц и транспортных средств, не имеющих постоянных или временных пропусков на объект.

Кроме соединительных линий ТСПИ и ВТСС за пределы контролируемой зоны могут выходить провода, к ним не относящиеся, но проходящие через помещения, где установлены технические средства, а также трубы систем отопления, водоснабжения и другие токопроводящие металлоконструкции и пластмассовые и композитные конструкции. Такие провода, кабели и токопроводящие элементы называют посторонними проводниками.

В зависимости от физической природы возникновения информационных сигналов, а также среды их распространения и способов перехвата, технические каналы утечки информации можно разделить на электромагнитные, электрические.

6.1. Электромагнитные поля - основной канал утечки информационных сигналов со средств вычислительной техники.

К электромагнитным каналам утечки информации относятся:

- излучение элементов СВТ;
- излучение на частотах работы высокочастотных генераторов СВТ, промодулированных информационными сигналами;
- излучение на частотах самовозбуждения СВТ.

6.1.1. Электромагнитный канал утечки информации.

Этот канал утечки информации со средств вычислительной техники охватывает диапазон работы СВТ на скоростях до 6 Гбит и диапазон частот излучений 100 Гц … 100 ГГц.

Основные закономерности и свойства электромагнитного поля описываются уравнениями Максвелла.

$$\begin{cases} rot\bar{H} = \sigma\bar{E} + \varepsilon_0\varepsilon_2 \dfrac{dE}{Dt} \\ rot\bar{E} = -\mu_0\mu_2 \dfrac{dH}{Dt} \quad \text{где } \varepsilon_0 = \dfrac{10^{-9}}{36\pi} \left(\Phi/_{\text{м}}\right) \quad \mu_0 = 4\pi 10^{-7} \ (\text{Г} \\ div\bar{E} = \dfrac{\rho}{\varepsilon\varepsilon_0} \end{cases} \tag{3}$$

Для гармонического сигнала

$$\dot{E} = Ee^{iwt}$$
$$\dot{H} = He^{iwt} \tag{4}$$

Система уравнений Максвелла будет выглядеть как:

$$\begin{cases} rot\dot{H} = (\sigma + i\omega\varepsilon_0)\dot{E} \\ rot\dot{E} = -i\omega\mu_0 H \\ div\dot{E} = \dfrac{\rho}{\varepsilon_0} \\ div\dot{H} = 0 \end{cases} \quad \text{, где } rot\ \text{E} = \lim_{\Delta S} \frac{\oint_S \bar{A}\, dl}{\Delta S} \tag{5}$$

Для решения приведенных уравнений Максвелла вводятся дополнительные параметры электромагнитного поля – электрический и магнитный запаздывающие потенциалы φ и A:

$$\varphi = \frac{1}{4\pi\varepsilon_0}\int_v \frac{\rho(t-\frac{r}{i})dv}{r};$$

$$A = \frac{\mu}{4\pi}\int_v \frac{\delta_i(t-\frac{r}{i})dv}{r}, \qquad (6)$$

Гд ρ δ_i - объемные плотности заряда и тока; r – расстояние до точки наблюдения. Для линейного тока векторный потенциал соответственно равен:

$$A = \frac{\mu_0}{4\pi}\int_e \frac{\delta dl}{r} \qquad (7)$$

С учетом введенных параметров A и φ

$$\begin{cases} \bar{E} = -(grad\varphi + \dfrac{d\bar{A}}{dt}) \\ \bar{H} = \dfrac{1}{\mu_0} rot\bar{A} \end{cases} \qquad (8)$$

$$grad\varphi = \begin{cases} \frac{d\varphi}{dx} \\ \frac{d\varphi}{dy} \\ \frac{d\varphi}{dz} \end{cases}$$

Реальные излучатели СВТ можно рассматривать как совокупность элементарных электрических и магнитных излучателей (диполей).

6.1.2. Элементарный электрический излучатель (ближняя зона от источника)

В полярной системе координат элементарный электрический излучатель можно представить в виде изображенном на рисунке 6.

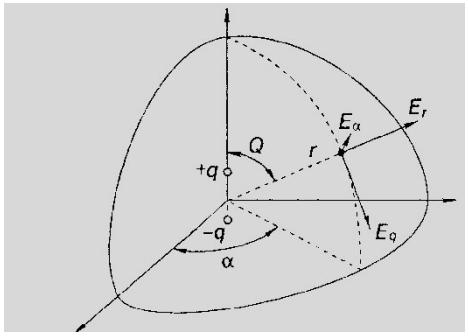


Рис. 6. Элементарный электрический излучатель

$$\begin{cases} \dot{\bar{E}}_r = \dfrac{2\dot{J}l\cos\theta}{4\pi j\omega\varepsilon_0 r^3}(1+j\alpha r^2)e^{-j\alpha r} \\ \dot{\bar{E}}_\theta = \dfrac{\dot{J}l\sin\theta}{4\pi j\omega\varepsilon_0 r^3}(1+j\alpha r-\alpha^2 r^2)e^{-j\alpha r} \\ \dot{\bar{H}}_\alpha = \dfrac{\dot{J}l\sin\theta}{4\pi r^2}(1-j\alpha r)e^{-j\alpha r} \end{cases} \qquad (9)$$

где $\alpha = \frac{2\pi}{\lambda} = \frac{\omega}{c}$ $\quad j = i\omega\dot{q}$

В экваториальной плоскости (горизонтальная плоскость) имеем:

$$\begin{cases} \dot{\vec{E}}_\theta = M_э\left(\dfrac{1}{(\alpha r^3)} + \dfrac{j}{(\alpha r)^2} - \dfrac{1}{\alpha r}\right) \\ \dot{\vec{H}}_\alpha = \dfrac{\dot{M}_э}{\rho}\left\{\dfrac{j}{(\alpha r)^2} - \dfrac{1}{\alpha r}\right\} \end{cases} \qquad (10)$$

где $M_Э = \frac{ql}{4\pi\varepsilon\varepsilon_0}a^3$ (в/м) – параметр излучателя; $\rho = \sqrt{\frac{\mu_0}{\varepsilon_0}} = \frac{1}{\varepsilon_0 c_0}$; $c = \frac{1}{\sqrt{\mu_0\varepsilon_0}}$ скорость света в вакууме.

Первые два члена в выражении $\dot{\vec{E}}_0$ обязаны gradφ, а последний $\frac{dA}{dt}$. При αr < 1 $\left(r \le \frac{\lambda}{2\pi}\right)$ –в ближней зоне излучения напряженность электрического поля определяется по формуле: $\dot{E}_\theta = \dfrac{\dot{q}l}{4\pi\varepsilon_0}\dfrac{1}{r^3}$ эта формула квазистатики, электрическое поле имеет потенциальный характер.

Для потенциального электрического поля: $\oint E dl = 0$ (rot $E = 0$).

Отношение $\frac{E_0}{H_\alpha} = \frac{1}{j\alpha r}\rho, \qquad \rho = 377\,\text{Ом} = \sqrt{\frac{\mu_0}{\varepsilon_0}}$

Волновое сопротивление электрического поля - высокоомное (десятки и сотни килоом), источники поля – открытые электрические заряды.

Учитывая, что соотношение компонент поля атмосферных помех $\frac{E_m}{H_m} = \rho$, то зона R_2 определяется только электрическим полем E_θ. В дальней зоне $\alpha r >> 1$ (волновая зона):

$$\left|\dot{\bar{E}}_\theta\right| = \frac{M_э}{\alpha r} = \frac{qla^3}{4\pi\varepsilon\varepsilon_0}\frac{1}{\alpha r} = \frac{qla^2}{4\pi\varepsilon\varepsilon_0}\frac{1}{r}. \qquad (11)$$

Отношение $\frac{E_0}{H_a} = \rho = 377$ Ом. Так как отношение компонент поля нормированных шумов в эфире составляет $\frac{E_0}{H_a} = \rho = 377$ Ом., следовательно, зона R_2 будет одинаковой как по магнитной, так и электрической составляющей.

Ниже приведены графики законов убывания компонент поля для элементарного электрического излучателя.

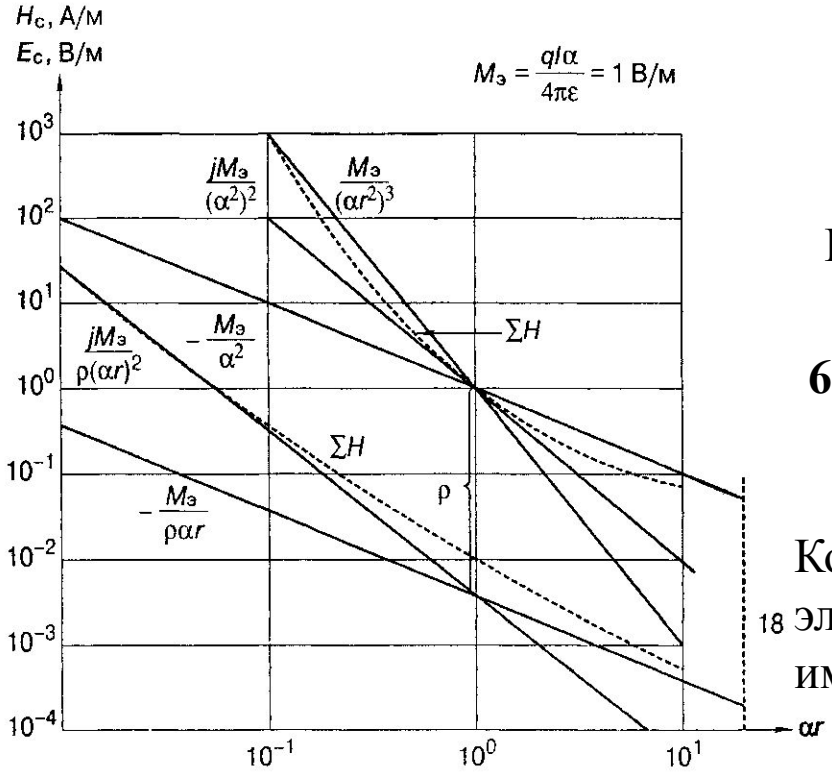


Рис 7. Составляющие поля элементарного электрического излучателя

6.1.3. Решение уравнений Максвелла для элементарного магнитного излучателя

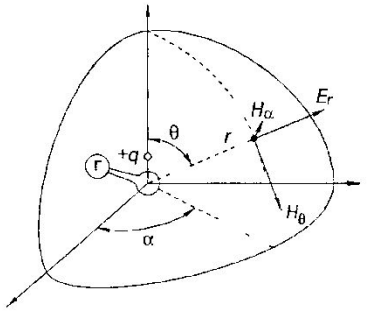
Компоненты электромагнитного поля элементарного магнитного излучателя имеют следующий вид:

$$\overline{H}_2 = \frac{2JS\cos\theta}{4\pi\varepsilon^3}(1+j\alpha r)e^{-j\alpha r}$$

$$\overline{H}_\theta = \frac{JS\sin\theta}{4\pi r^3}(1+j\alpha r-\alpha^2 r^2)e^{-j\alpha r} \qquad (12)$$

$$\overline{E}_\alpha = \frac{j\omega\mu_0 JS\sin\theta}{4\pi r^2}(1-j\alpha r)e^{-j\alpha r}$$

В полярной системе координат элементарный магнитный излучатель представлен на рис. 8.



Введем обозначения

$$\dot{M}_m = \frac{jS}{4\pi}\alpha^3,$$

$$\rho = \sqrt{\frac{\mu_0}{\varepsilon_0}} = \mu_0 C,$$

$$C = \frac{1}{\sqrt{\mu_0 \varepsilon_0}}.$$

В экваториальной плоскости

$$\dot{H}_\theta = M_m\left\{\frac{1}{(\alpha r)^3} + \frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right\}e^{-j\alpha r};$$

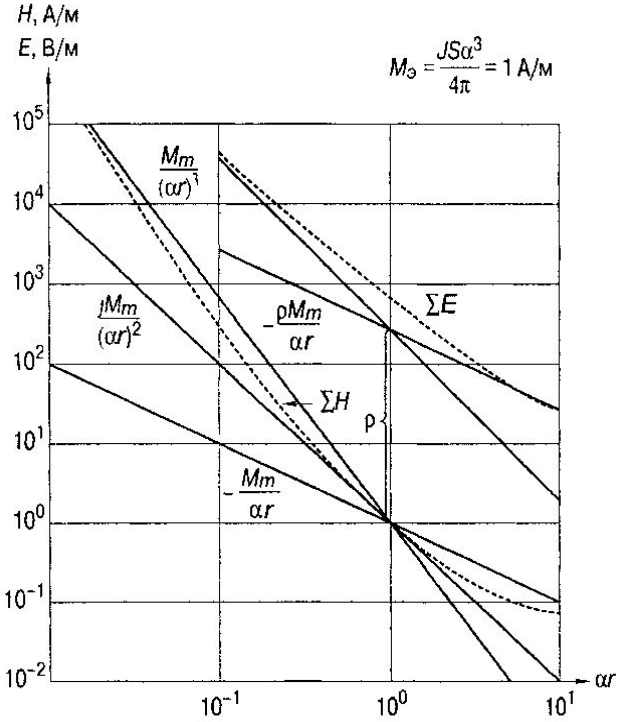
$$\dot{E}_\alpha = \rho M_m\left\{\frac{j}{(\alpha r)^2} - \frac{1}{\alpha r}\right\}e^{-j\alpha r}.$$

Для ближней зоны $\alpha r < 1$ $(r < 0{,}16\lambda)$ $\dot{H}_\theta = \frac{JS}{4\pi r^3}$ ние магнитостатики, (13)

Электрическое поле E_α незначительно и имеет вихревой характер (обусловлено членом уравнения $\frac{dA}{dt}$). Для него $\oint E dt \neq 0$. Волновое сопротивление $\frac{E_\alpha}{H_\theta} = j\alpha r\rho$ – поле низкоомное (доли Ома, либо единицы Ом). Если принять, что $\frac{E_ш}{H_ш} = \rho$, то размер зоны R_2 по H_θ будет намного больше, чем по E_α. Поле H_θ является определяющим при оценке защищенности при расчете R_2. Для дальней зоны излучателя $\alpha r >> 1$

$$(r \geq 3\lambda)\quad H_\theta = \frac{M_m}{\alpha r},\quad \frac{E_\alpha}{H_\theta} = \rho.$$

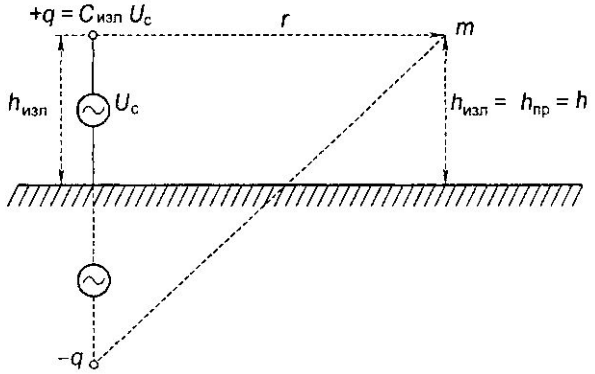
Так как отношение компонент поля нормированных шумов в эфире составляет $\frac{E_m}{H_m} = \rho = 377$ Ом, следовательно, зона R_2 ,будет одинаковой как по магнитной, так и электрической составляющей. Ниже приводятся графики законов, убывания компонент поля для элементарного излучателя (см. рис. 9)



6.1.4. Электрические излучатели электромагнитного поля

Физической моделью излучателя электрического поля СВТ для частот до 100 МГц является несимметричный излучатель с зарядом q. Этот переменный во времени заряд приподнят над проводящей поверхностью раздела электрических средств (пол, межэтажные перекрытия). Для решения задач вычисления электрического поля проводящая поверхность раздела электрических средств заменяется на зеркальное изображение этого заряда.

Физическая модель излучателя электрического поля представлена на рис. 10
Для этой модели в ближней зоне излучателя:



$$E = -\left(\operatorname{grad}\varphi + \frac{dA}{dt}\right);$$

$$\varphi_c = \frac{q}{4\pi\varepsilon_0}\left(\frac{1}{x} - \frac{1}{\sqrt{x^2+4}}\right) \qquad (14)$$

Где x = r/h

Полный вектор E_c электрического поля излучателя равен: $E_c = \sqrt[2]{E_{вер}^2 + E_{гор}^2}$ (15)

где $E_{вер} = \frac{q}{4\pi\varepsilon_0 h^2}\frac{2}{\left(x^2+4\right)^{3/2}}$; $E_{гор} = \frac{q}{4\pi\varepsilon_0 h^2}\left\{\frac{1}{x^2} - \frac{x^2}{\left(x^2+4\right)^{3/2}}\right\}$

средневертикальная составляющая электрического поля СВТ (при измерении несимметричной электрической антенной): $E_{св} = \frac{\varphi_c}{h_{пр}} = \frac{q_{изл}}{4\pi\varepsilon_0 h^2}\left\{\frac{1}{x} - \frac{1}{\left(x^2+4\right)\frac{1}{2}}\right\}$

Для частот свыше 100 МГц физической моделью излучателя электрического поля ТС является элементарный электрический диполь.

6.1.5. Излучатели электромагнитного поля

Физической моделью излучателя магнитного поля является рамка с площадью S, обтекаемой током I, изменяющимся по закону информационного сигнала (рис. 11).

Напряженность магнитного поля в непосредственной близости от излучателя определяется законами квазимагнитостатики. В направлении оси рамки на расстоянии r (направление максимального поля H_m)

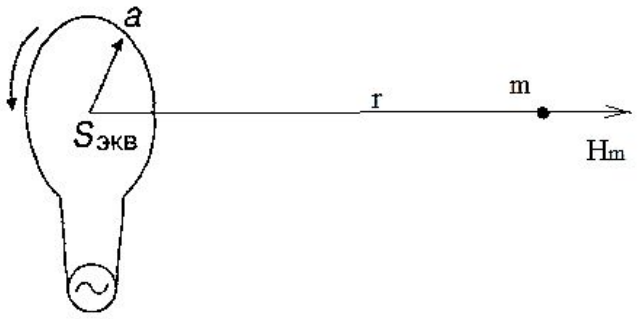


Рис. 11 Физическая модель излучателя магнитного поля

$$H_m = \frac{Ia}{2\left(a^2 + r^2\right)^{3/2}} \quad (17) \qquad \text{или} \qquad H_m = \frac{IS_{экв}}{2\pi\left(a^2 + r^2\right)^{3/2}}$$

где a – радиус излучающей рамки, r – расстояние до точки m. При r >> a, что обычно выполняется при пробных замерах поля при испытаниях ТС (d=1 м)

$$H_m = \frac{IS_{экв}}{2\pi r^3}$$

то есть магнитное поле убывает с расстоянием по закону $(1/r)^3$.

Вихревые составляющие электрического поля излучающей рамки в ближней зоне равны

$$E_{вых} = \alpha_{гр} H = \alpha_{гр} \frac{H_m}{2}.$$

Оно не является определяющим при расчете радиуса зоны радиоперехвата. Ввиду того, что при работе технических средств вычислительной техники возникают электрические и магнитные целесообразно измерять вблизи излучателя отдельно электрическое и магнитное поля (диполь, рамка) и отдельно рассчитывать R_2 по Е и по Н и выбирать из них максимальное значение.

При измерении электрического поля (штыревая антенна или диполь) необходимо учитывать потенциальный характер электрического поля, исключать возможную ошибку за счет конечного значения затухания асимметрии согласующего устройства симметричной антенны (диполя).

6.1.6. Электрические каналы утечки информации

Электрические каналы утечки информации возникают за счет:

1. Наводок электромагнитных излучений СВТ на ВТСС и их соединительные линии, выходящие за пределы контролируемой зоны. Уровень наведенного сигнала зависит от интенсивности излучения ОТСС, расстояния до него, а также от длины транспортирующей цепи до границы КЗ в диапазоне частот 100 Гц … 100МГц.
2. модуляции информационными сигналами цепей электропитания и заземления. Эти сигналы обусловлены как влиянием собственного электромагнитного поля СВТ на провода электропитания, так и модуляцией информационными сигналами цепей блока питания СВТ.
3. Неравномерности потребления тока в сети электропитания. Требования по этому каналу зависят от скорости работы $S_{бод}$ источника опасного сигнала. Предельная скорость работы $S_{бод}$ не более 1200 бод.

Наводки электромагнитных излучений СВТ возникают при излучении информационных сигналов элементами ТС, а также при наличии гальванических связей со средствами ВТ.

Пространство вокруг СВТ, в пределах которого на случайные антенны наводится информационный сигнал выше допустимого (нормированного) уровня, называется зоной 1.

Случайные антенны могут быть сосредоточенными и распределенными. Сосредоточенные случайные антенны (ССА) представляют собой компактное техническое средство, например телефонный аппарат, громкоговоритель трансляционной сети. К распределенным случайным антеннам (РСА) относятся случайные антенны с протяженными параметрами: кабели, провода, металлические трубы и другие токопроводящие коммуникации.

Модулирование сигналов в сети электропитания возможно при наличии реакции выпрямителя на работу устройств с информационными сигналами.

Наводки (модулирование) токов в цепях питания и заземления объекта возможно при работе локальной вычислительной сети по кабелям при значительной их протяженности, а также при наличии гальванической связи в элементах вторичной и первичной цепях.

6.2. Защита информации в компьютерных системах (см. презентацию Л2013ТКУИ слайды 17-25)

Защита информации в компьютерных системах может производиться следующими методами:

- экранирование ТСПИ и их соединительных линий;
- заземление ТСПИ и экранов соединительных линий приборов;
- встраивание в ВТСС, обладающие “микрофонным” эффектом и имеющие выход за пределы контролируемой зоны, специальных фильтров;
- ввод автономных и стабилизированных источников, а также устройств гарантированного питания в цепи электроснабжения ТСПИ;
- монтаж в цепях электропитания ТСПИ, а также в электросетях выделенных помещений помехоподавляющих фильтров.

Активное воздействие на каналы утечки осуществляют путем реализации:

- пространственного зашумления, создаваемого генераторами электромагнитного шума;
- прицельных помех, генерируемых на рабочих частотах радиоканалов подслушивающих устройств специальными передатчиками;
- зашумления электросетей, посторонних проводников и соединительных линий ВТСС, имеющих выход за пределы контролируемой зоны;

6.2.1. Экранирование

Ослабление побочных электромагнитных излучений ТСПИ и их наводок осуществляется экранированием и заземлением средств и их соединительных линий.

Просачивание в цепи электропитания предотвращается фильтрацией информационных сигналов, а для маскирования ПЭМИН используются системы зашумления.

Различают электростатическое, магнитостатическое и электромагнитное экранирования.

Основная задача электростатического экранирования состоит в уменьшении емкостных связей между защищаемыми элементами и сводится к обеспечению накопления статического электричества на экране с последующим отводом зарядов на землю. Применение металлических экранов позволяет полностью устранить влияние электростатического поля.

Эффективность магнитного экранирования зависит от частоты и электрических свойств материала экрана. Начиная со средневолнового диапазона эффективен экран из любого металла толщиной от 0,5 до 1,5 мм, для частот свыше 10 МГц подобный же результат дает металлическая пленка толщиной около 0,1 мм. Заземление экрана не влияет на эффективность экранирования.

Высокочастотное электромагнитное поле ослабляется полем обратного направления, создаваемым вихревыми токами, наведенными в металлическом сплошном или сетчатом экране. Экран из медной сетки 2х2 мм ослабляет сигнал на 30 - 35 дБ, двойной экран на 50 – 60 дБ.

Наряду с узлами приборов экранируются монтажные провода и соединительные линии. Длина экранированного монтажного провода не должна превышать четверти длины самой короткой волны в составе спектра сигнала, передаваемого по проводу.
Высокую степень защиты обеспечивают витая пара в экранированной оболочке и высокочастотные коаксиальные кабели. Наилучшую защиту как от электрического, так и от магнитного полей гарантируют линии типа бифиляра, трифиляра, изолированного коаксиального кабеля в электрическом экране, металлизированного плоского многопроводного кабеля.

В помещении экранируют стены, двери, окна. Двери оборудуют пружинной гребенкой, обеспечивающей надежный электрический контакт со стенами помещения. Окна затягивают медной сеткой с ячейкой 2х2 мм, обеспечивая надежный электрический контакт съемной рамки со стенами помещения.

6.2.2. Защита сети электропитания и заземления

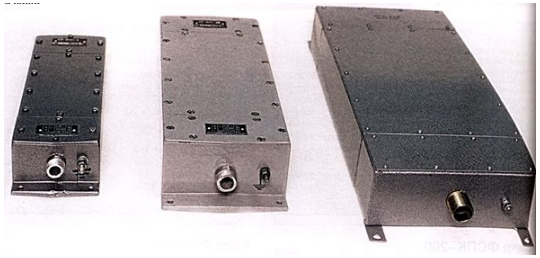
Фильтрация

Для фильтрации применяются разделительные трансформаторы и помехоподавляющие фильтры.

Разделительные трансформаторы предотвращают проникновение сигналов, появляющихся в первичной обмотке, во вторичную. Нежелательные резистивные и емкостные связи между обмотками устраняют с помощью внутренних экранов и элементов, имеющих высокое сопротивление изоляции. Степень снижения уровня наводок достигает 40 дБ.

Основное назначение помехоподавляющих фильтров пропускать без ослабления сигналы, частоты которых находятся в пределах рабочего диапазона, и подавлять сигналы, частоты которых находятся вне этих пределов. Фильтры нижних частот, пропускают сигналы с частотами ниже его граничной частоты. Рабочее напряжение конденсаторов фильтра не должно превышать максимальных значений допускаемых скачков напряжения цепи питания, а ток через фильтр не должен вызывать насыщения катушек индуктивности.

Внешний вид помехоподавляющих фильтров серии ФП



Применяются также активные устройства для защиты линий электропитания, заземления от утечки информации объектов ВТ (вычислительной техники) от утечки информации за счёт наводок на линии электропитания и заземления. Для защиты линий электропитания, заземления от утечки информации используются генераторы шума.

Устройство для защиты линий электропитания, заземления от утечки информации "Соната РС1" предназначено для активной защиты объектов ВТ (вычислительной техники) от утечки информации за счёт наводок на линии электропитания и заземления. Генератор шума по сети электропитания и линиям заземления "Соната РС1" является техническим средством защиты информации, обрабатываемой на объектах вычислительной техники 1, 2 и 3-й категорий от утечки за счёт наводок информативных сигналов в линии электропитания и заземления, соответствует требованиям документов:

“Сборник норм защиты информации за счёт побочных электромагнитных излучений и наводок”, “Средства активной защиты объектов ЭВТ от утечки информации по побочным электромагнитным излучениям и наводкам. Основные технические требования”.

Изделие рассчитано на подключение к 3-х проводной сети энергоснабжения («Фаза», «Ноль» и «Защитное заземление») и обеспечивает формирование несинфазных токов и синфазных и парафазных составляющих шумового напряжения во всех проводниках. При нарушении схемы подключения наличие всех составляющих, а так же значение интегрального уровня шума может не обеспечиваться.

Наиболее частые отклонения в схеме подключения:

1. При подключении изделия к зашумляемой линии 220 В контакт «фазного» провода вилки не соответствует «фазному» контакту розетки. Необходимо исправить:

штырь вилки, помеченный точкой, должен подключаться к "фазному" контакту розетки (для определения «фазного» контакта розетки следует воспользоваться указателем фазы);

2. В розетке к соответствующему контакту не подключено защитное заземление. При невозможности подключить его, необходимо к контакту «земля» розетки подключить проводник длиной не менее 5 м и уложить его вдоль линии электропитания. Для обеспечения электробезопасности необходимо в месте окончания вновь проложенного проводника соединить его с «нулевым» проводом зашумляемой линии 220 В.

6.2.3. Защита от несанкционированного доступа обрабатываемой в автоматизированных системах информации конфиденциального характера.

Система защиты Secret Net 5.0

Secret Net 5.0 – это система защиты конфиденциальной информации от несанкционированного доступа, которая реализует требования руководящих документов и ГОСТ по защите информации и функционирует под управлением современных ОС MS Windows 2000, Windows XP и Windows 2003. Существует в автономном и сетевом вариантах. За счёт интеграции собственных защитных механизмов с механизмами управления сетевой инфраструктуры защищаемой сети Secret Net 5.0 повышает защищенность всей автоматизированной информационной системы в целом и при этом:

- обеспечивает централизованное управление настройками политики безопасности;
- работает совместно с ОС Windows, расширяя, дополняя и усиливая стандартные механизмы защиты;
- осуществляет мониторинг и аудит политики безопасности в режиме реального времени;
- позволяет оперативно реагировать на события НСД;
- поддерживает терминальный режим работы пользователей с рабочей станцией.

Рис. Структура Secret Net 5.0

Система обеспечивает:

- оперативное реагирование на действия злоумышленников;
- централизованный просмотр событий безопасности;
- контроль вывода конфиденциальной информации на внешние носители;
- аппаратную идентификацию пользователей;
- централизованное управление;
- контроль целостности файлов;
- разграничение доступа к устройствам (CD\DVD, USB, Wi-Fi и т.д.).

Secret Net 5.0 (сетевой вариант) содержит следующие компоненты:
• клиент Secret Net 5.0;
• сервер безопасности Secret Net 5.0;
• программу оперативного управления, мониторинга и аудита («Монитор»);
• модификатор схемы Active Directory.

Клиент

Клиент Secret Net 5.0 следит за соблюдением настроенной политики безопасности на рабочих станциях и серверах, обеспечивает регистрацию событий безопасности и передачу журналов на Сервер Безопасности, а также приём от него оперативных команд и их выполнение.

Сервер безопасности

Сервер безопасности производит сбор журналов от зарегистрированных на нем агентов, накапливает полученную информацию в базе данных и обеспечивает выдачу команд оперативного управления клиентам (например, блокировку рабочей станции при выявлении попытки НСД).

Программа оперативного управления, мониторинга и аудита («Монитор») Монитор является программой, которая отображает администратору оперативную информацию от Сервера Безопасности о состоянии рабочих станций и дает возможность отслеживать:

• какие компьютеры сети в данный момент включены;

• какие пользователи на них работают (как локально, так и в терминальном режиме).

«Монитор» в режиме реального времени отображает оперативную информацию о происходящих событиях НСД, позволяет осуществлять просмотр журналов всех рабочих станций, а также выдавать на защищаемыерабочие станции команды оперативного управления.

Модификатор схемы Active Directory Модификатор схемы Active Directory (AD) используется для подготовки схемы ОС Windows к развертыванию Secret Net 5.0. Так как в качестве хранилища информации о настройках безопасности Secret Net 5.0 использует AD, данный модуль создаёт новые объекты и изменяет параметры существующих. Программы управления объектами и параметрами групповых политик, входящие в состав этого модуля, обеспечивают управление параметрами работы доменных пользователей и применение централизованных настроек безопасности Secret Net 5.0.

Управление системой Secret Net 5.0

Система централизованного управления

В качестве хранилища информации в системе централизованного управления используется Active Directory (AD). Для нужд централизованного управления Secret Net 5.0 схема Active Directory расширяется – создаются новые объекты и изменяются параметры существующих.

Для выполнения этих действий используется специальный модуль изменения схемы AD, который устанавливается и запускается на контроллере домена при установке системы централизованного управления. Для приведения параметров работы защитных средств компьютера в соответствие настройкам безопасности Secret Net 5.0, задаваемым с помощью групповых политик, используется агент Secret Net 5.0, установленный на каждом сервере или рабочей станции защищаемой сети.

Столь тесная интеграция системы управления с Active Directory позволяет легко использовать Secret Net 5.0 для организации защиты сети, использующей многодоменную структуру.

Оперативный мониторинг и аудит

В Secret Net 5.0 предусмотрена функция оперативного мониторинга и аудита безопасности информационной системы предприятия, которая позволяет решать такие задачи, как:

• оперативный контроль состояния автоматизированной системы предприятия (получение информация о состоянии рабочих станций и о работающих на них пользователях);

• централизованный сбор журналов с возможностью оперативного просмотра в любой момент времени, а также хранение и архивирование журналов;

• оповещение администратора о событиях НСД в режиме реального времени;

• оперативное реагирование на события НСД – выключение, перезагрузка или блокировка контролируемых компьютеров;

• ведение журнала НСД.

Система оперативного управления имеет свою базу данных, в которой хранится вся информация, связанная с работой сервера по обеспечению взаимодействия компонентов, а также журналы, поступающие от агентов.

В качестве базы данных используется СУБД Oracle 9i.

Мониторинг

С помощью программы мониторинга администратор может управлять сбором журналов с рабочих станций. Предусмотрено два варианта. Первый – сервер оперативного управления собирает журналы по команде администратора. Второй – администратор составляет расписание и передает его серверу, далее сервер собирает журналы в соответствии с этим расписанием.

Также предусмотрена возможность создать удобный для администратора вид представления сети – так называемый «срез» (например, по отделам, по территориальному размещению и т.п.). В случае крупной распределённой сети эта функция делегируется другим администраторам для управления выделенными им сегментами сети.

Аудит

Программа работы с журналами устанавливается на рабочем месте сотрудника, уполномоченного проводить аудит системы защиты. Если функции мониторинга и аудита совмещает один сотрудник, программа устанавливается на том же компьютере, который является рабочим местом администратора оперативного управления.

В системе Secret Net 5.0 для проведения аудита используются 4 журнала:
• журнал приложений;
• журнал безопасности;
• журнал системы;
• журнал Secret Net.

Первые три из перечисленных журналов – штатные, входящие в состав средств операционной системы. В журнале Secret Net хранятся сведения о событиях, происходящих в системе Secret Net 5.0.

Журналы ведутся на каждом защищаемом компьютере сети и хранятся в его локальной базе данных. Сбор журналов осуществляется по команде аудитора или по расписанию.

Программа работы с журналами позволяет аудитору просматривать записи журналов и тем самым отслеживать действия пользователей, связанные с безопасностью автоматизированной информационной системы предприятия. В программе управления журналами предусмотрена настраиваемая выборка записей, используя которую аудитор может просматривать не весь журнал целиком, а только часть записей, удовлетворяющих определенным критериям. Это значительно ускоряет и упрощает работу, связанную с поиском и анализом событий.

С помощью программы работы с журналами аудитор может выдавать команды серверу на архивацию журналов, а также на восстановление журналов из архива. Предусмотрена возможность просмотра архивов, а также сохранения журнала в файл для последующей передачи и анализа записей вне системы Secret Net 5.0.

Защитные механизмы

Усиленная идентификация и аутентификация пользователей Система Secret Net 5.0 совместно с ОС Windows обеспечивает усиленную идентификацию и аутентификацию пользователя с помощью средств аппаратной поддержки при его входе в систему, а также позволяет существенно снизить риски того, что пользователь загрузит компьютер с отчуждаемых внешних носителей и получит доступ к важной информации в обход схемы защиты.

В качестве аппаратной поддержки система Secret Net 5.0 использует: программно-аппаратный комплекс «Соболь» и Secret Net Touch Memory Card. Плату аппаратной поддержки невозможно обойти средствами BIOS. Если в течение определённого времени после включения питания на плату не было передано управление, она блокирует работу всей системы.

Полномочное управление доступом

Каждому информационному ресурсу назначается один их трёх уровней конфиденциальности: «Не конфиденциально», «Конфиденциально», «Строго конфиденциально», а каждому пользователю – уровень допуска. Доступ осуществляется по результатам сравнения уровня допуска с категорией конфиденциальности информации.

Разграничение доступа к устройствам

Функция обеспечивает разграничение доступа к устройствам с целью предотвращения несанкционированного копирования информации с защищаемого компьютера. Существует возможность запретить, либо разрешить пользователям работу с любыми портами\устройствами.

Разграничивается доступ к следующим портам/устройствам:
• последовательным и параллельным портам;
• сменным, логическим и оптическим дискам;
• USB – портам.

Также поддерживается контроль подключения устройств на шинах USB, PCMCIA, IEEE1394 по типу и серийному номеру, права доступа на эти устройства задаются не только для отдельных пользователей, но и для групп пользователей.

Существует возможность запретить использование сетевых интерфейсов – Ethernet, 1394 FireWire, Bluetooth, IrDA, WiFi.

Замкнутая программная среда

Для каждого пользователя компьютера формируется определённый перечень программ, разрешенных для запуска. Он может быть задан как индивидуально для каждого пользователя, так и определен на уровне групп пользователей. Применение этого режима позволяет исключить распространение вирусов, «червей» и шпионского ПО, а также использования ПК в качестве игровой приставки.

Контроль целостности

Используется для слежения за неизменностью контролируемых объектов с целью защиты их от модификации. Контроль проводится в автоматическом режиме в соответствии с некоторым заданным расписанием.

Объектами контроля могут быть файлы, каталоги, элементы системного реестра и секторы дисков. Каждый тип объектов имеет свой набор контролируемых параметров. Так, файлы могут контролироваться на целостность содержимого, прав доступа, атрибутов, а также на их существование, т.е. на наличие файлов по заданному пути.

При обнаружении несоответствия предусмотрены следующие варианты реакции на возникающие ситуации нарушения целостности:

- регистрация события в журнале Secret Net;
- блокировка компьютера;
- восстановление повреждённой/модифицированной информации;
- отклонение или принятие изменений.

Гарантированное уничтожение данных

Уничтожение достигается путем записи случайной последовательности на место удаленной информации в освобождаемую область диска. Для большей надежности может быть выполнено до 10 циклов (проходов) затирания.

Контроль аппаратной конфигурации компьютера

Осуществляет своевременное обнаружение изменений в аппаратной конфигурации компьютера и реагирования на эти изменения.

Предусмотрено два вида реакций:

- регистрация события в журнале Secret Net;
- блокировка компьютера.

Контроль печати конфиденциальной информации

Администратор безопасности имеет возможность запретить вывод конфиденциальной информации на печать, либо разрешить эту операцию некоторым пользователям, при этом распечатанные документы могут автоматически маркироваться в соответствии с правилами оформления документов. Также сам факт печати (или попытки несанкционированного вывода на печать) отображается в журнале защиты Secret Net 5.0.

Регистрация событий

Система Secret Net 5.0 регистрирует все события, происходящие на компьютере: включение\выключение компьютера, вход\выход пользователей, события НСД, запуск приложений, обращения к конфиденциальной информации, контроль вывода конфиденциальной информации на печать и отчуждаемые носители и т.п.

Функциональный самоконтроль подсистем

Самоконтроль производится перед входом пользователя в систему и предназначен для обеспечения гарантии того, что к моменту завершения загрузки ОС все ключевые компоненты Secret Net 5.0 загружены и функционируют.

Импорт и экспорт параметров

В Secret Net 5.0 реализована возможность экспорта и импорта различных параметров системы. После проверки корректности работы защитных механизмов на компьютере, принимаемом за эталонный, выполняется экспорт значений параметров в файл. Далее значения импортируются на необходимое количество компьютеров.

4.11.2. Электронный замок «СОБОЛЬ»

Среди средств, так называемых AAA (authentication, authorization, administration – аутентификация, авторизация, администрирование) важное место занимают программно-аппаратные инструменты контроля доступа к компьютерам – электронные замки, устройства ввода идентификационных признаков (УВИП) и соответствующее программное обеспечение (ПО). В этих средствах контроля доступа к компьютерам идентификация и аутентификация, а также ряд других защитных функций, выполняются с помощью электронного замка и УВИП до загрузки ОС.

По способу считывания современные УВИП подразделяются на контактные, дистанционные и комбинированные.

Контактное считывание идентификационных признаков осуществляется непосредственным взаимодействием идентификатора и считывателя. При бесконтактном способе считывания идентификатор может располагаться на некотором расстоянии от считывателя, а сам процесс считывания осуществляется радиочастотным или инфракрасным методом.

УВИП могут быть электронными, биометрическими и комбинированными.

Электронные УВИП содержат микросхему памяти идентификационного признака. Примером электронного замка может служить устройство «СОБОЛЬ» (рис. 4.47).

Назначение

Применяется для защиты ресурсов компьютера от несанкционированного доступа. Электронный замок «Соболь-PCI» сертифицирован Гостехкомиссией России. Сертификат подтверждает соответствие данного изделия требованиям Руководящего документа Гостехкомиссии России «Автоматизированные системы. Классификация автоматизированных систем и требования по защите информации» и позволяет использовать данный продукт при разработке систем защиты для автоматизированных систем с классом защищенности до 1В включительно.

Рис. 4.47. Электронный замок «Соболь-PCI»

Применение

Электронный замок «Соболь» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети. Электронный замок «Соболь» обладает следующими возможностями:

- идентификация и аутентификация пользователей;
- регистрация попыток доступа к ПЭВМ;
- запрет загрузки ОС со съемных носителей;
- контроль целостности программной среды.

Возможности по идентификации и аутентификации пользователей, а также регистрация попыток доступа к ПЭВМ не зависят от типа использующейся ОС.

Идентификация и аутентификация пользователей

Каждый пользователь компьютера регистрируется в системе электронный замок «Соболь», установленной на данном компьютере. Регистрация пользователя осуществляется администратором и состоит в определении имени регистрируемого пользователя, присвоении ему персонального идентификатора и назначении пароля. Действие электронного замка «Соболь» состоит в проверке персонального идентификатора и пароля пользователя при попытке входа в систему. В случае попытки входа в систему не зарегистрированного пользователя электронный замок «Соболь» регистрирует попытку НСД и осуществляется аппаратная блокировка до 4-х устройств (например: FDD, CD-ROM, ZIP, LPT, SCSI-порты).

В электронном замке «Соболь» используются идентификаторы Touch Memory фирмы Dallas Semiconductor. Загрузка операционной системы с жесткого диска осуществляется только после предъявления зарегистрированного идентификатора. Служебная информация о регистрации пользователя (имя, номер присвоенного персонального идентификатора и т.д.) хранится в энергонезависимой памяти электронного замка.

Регистрация попыток доступа к ПЭВМ

Электронный замок «Соболь» осуществляет ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти. Электронный замок «Соболь» фиксирует в системном журнале вход пользователей, попытки входа, попытки НСД и другие события, связанные с безопасностью системы.

В системном журнале хранится следующая информация: дата и время события, имя пользователя и информация о типе события, например:

- факт входа пользователя;
- введение неправильного пароля;
- предъявление не зарегистрированного идентификатора пользователя;
- превышение числа попыток входа в систему;
- другие события.

Таким образом, электронный замок «Соболь» предоставляет информацию администратору о всех попытках доступа к ПЭВМ.

Контроль целостности программной среды и запрет загрузки со съемных носителей

Подсистема контроля целостности расширяет возможности электронного замка «Соболь». Контроль целостности системных областей дисков и наиболее критичных файлов производится по алгоритму ГОСТ 28147-89 в режиме имитовставки. Администратор имеет возможность задать режим работы электронного замка, при котором будет блокирован вход пользователей в систему при нарушении целостности контролируемых файлов.

Подсистема запрета загрузки с гибкого диска и CD ROM диска обеспечивает запрет загрузки операционной системы с этих съемных носителей для всех пользователей компьютера, кроме администратора. Администратор может разрешить отдельным пользователям компьютера выполнять загрузку операционной системы со съемных носителей. Подсистемы контроля целостности и подсистемы запрета загрузки со съемных носителей функционируют под управлением следующих ОС: MS DOS версий 5.0-6.22 (только ЭЗ «Соболь» для стандарта ISA); ОС семейства Windows'9x (FAT12, FAT16 или FAT32); Windows NT версий 3.51 и 4.0 с файловой системой NTFS; Windows 2000 с файловой системой NTFS (только «Соболь-PCI»); UNIX FreeBCD (только «Соболь-PCI»).

Возможности по администрированию

Для настройки электронного замка «Соболь» администратор имеет возможность:

- определять минимальную длину пароля пользователя;
- определять предельное число неудачных входов пользователя;
- добавлять и удалять пользователей;
- блокировать работу пользователя на компьютере;
- создавать резервные копии персональных идентификаторов.

Использование

Электронный замок «Соболь» может применяться в составе системы защиты информации Secret Net для генерации ключей шифрования и электронно-цифровой подписи. Кроме того, при использовании ЭЗ «Соболь» в составе СЗИ Secret Net обеспечивается единое централизованное управление его возможностями. С помощью подсистемы управления Secret Net администратор безопасности имеет возможность управлять статусом персональных идентификаторов сотрудников: присваивать электронные идентификаторы, временно блокировать, делать их недействительными, что позволяет управлять доступом сотрудников к компьютерам автоматизированной системы организации.

4.11.3. USB-ключ

Основное технологическое отличие USB-ключа от смарт-карты заключается в том, что хранимая в памяти USB-ключа информация не привязана жестко к ячейкам памяти, а располагается в специальной файловой системе. Поэтому один и тот же ключ можно использовать для разных целей: для входа в компьютер, авторизации электронной почты, создания канала виртуальной частной сети (VPN – virtual private network) и многого другого. Таким образом, с помощью одного аппаратного ключа можно комплексно решить задачу идентификации пользователя для всего комплекса офисного программного обеспечения. При этом человек не должен знать пароли и ключи шифрования для всех приложений, достаточно одного пароля для работы с ключом.

Для повышения надежности защиты некоторые аппаратные ключи выполнены в герметичном, влагостойком и пыленепроницаемом корпусе, что гарантирует защищенность данных от многих внешних воздействий. При разгерметизации корпуса информация из памяти ключа стирается. Это сделано для того, чтобы блокировать копирование или подделку ключа и обеспечить достаточно надежное хранение информации внутри аппаратного идентификатора при более жестких требованиях к его конструктиву. Реализовать те же самые требования для всего компьютера значительно сложнее.

Назначение USB-ключа:

• строгая двухфакторная аутентификация пользователей при доступе к защищённым ресурсам (компьютерам, сетям, приложениям);

• аппаратное выполнение криптографических операций в доверенной среде (в электронном ключе: генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функции, выработка ЭЦП);

• безопасное хранение криптографических ключей, профилей пользователей, настроек приложений, цифровых сертификатов и пр. в энергонезависимой памяти ключа;

• поддержка большинством современных операционных систем, бизнес приложений и продуктов по информационной безопасности в качестве средства аутентификации и авторизации.

Возможности применения USB-ключа:

• строгая аутентификация пользователей при доступе к серверам, базам данных, разделам веб сайтов;

• безопасное хранение секретной информации: паролей, ключей ЭЦП и шифрования, цифровых сертификатов;

• защита электронной почты (цифровая подпись и шифрование, доступ);

• защита компьютеров;

• защита сетей, VPN;

• клиент-банк, домашний банк;

• электронная торговля.

Преимущества

USB-ключ, может использоваться в любых приложениях для замены парольной защиты на более надежную двухфакторную аутентификацию (когда пользователь имеет нечто – USB-ключ, и знает нечто – PIN код).

USB-ключ обеспечивает:

• строгую аутентификацию пользователей за счет использования криптографических методов;

• безопасное хранение ключей шифрования и ЭЦП (электронной цифровой подписи), а также цифровых сертификатов для доступа к защищенным корпоративным сетям и информационным ресурсам;

• мобильность для пользователя и возможность работы в «не доверенной среде» (например, с чужого компьютера) – за счет того, что ключи шифрования и ЭЦП генерируются в памяти USB-ключа аппаратно и не могут быть перехвачены;

• безопасное использование – воспользоваться им может только его владелец, знающий PIN-код;
• реализацию как российских, так и западных стандартов шифрования и ЭЦП;
• удобство работы – USB-ключ выполнен в виде брелока со световой индикацией режимов работы и напрямую подключается к USB-портам, которыми сейчас оснащаются 100% компьютеров, не требует специальных считывателей, блоков питания, проводов и т.п.;
• использование одного ключа для решения множества различных задач – входа в компьютер, входа в сеть, защиты канала, шифрования информации, ЭЦП, безопасного доступа к защищённым разделам Web-сайтов, информационных порталов и т.п.

USB-ключ имеет (рис. 4.48):
• микросхему (1);
• защищенный микроконтроллер (2);
• разъем USB (3);
• световой индикатор режимов работы (4);
• герметичный полупрозрачный пластиковый корпус.

Микроконтроллер в составе USB-ключа обеспечивает:
• коммуникационные функции (поддержку протокола USB);
• хранение микрокода для управления протоколом передачи (firmware).

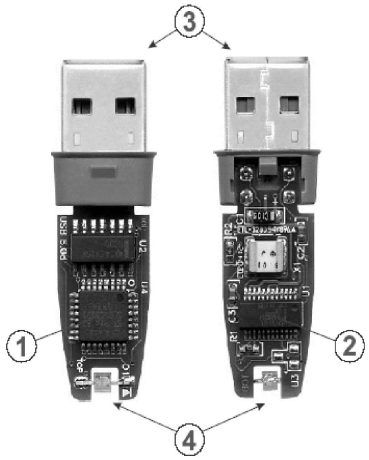


Рис. 4.48 . USB-ключ

В состав микросхемы входят:

- 16-ти битный центральный процессор с набором инструкций;
- память только для чтения (ROM, Read Only Memory), содержащая операционную систему;
- оперативная память (RAM, Random Access Memory), предназначенная для использования операционной системой;
- электрически стираемая программируемая память только для чтения (EEPROM, Electrically Erasable Programable Read Only Memory), предназначенная для хранения пользовательских данных;
- аппаратный генератор случайных чисел;
- криптопроцессор для ускорения выполнения криптографических операций.

4.11.4. Считыватели «Proximity»

Технология Proximity прочно завоевала ведущее место в профессиональных системах управления доступом, потеснив магнитные и Wiegand считыватели и практически полностью вытеснив Touch memory. Устройства ввода идентификационных признаков на базе идентификаторов Proximity (от английского слова proximity – близость, соседство) относится к классу электронных бесконтактных радиочастотных устройств. Они выпускаются в виде карточек, ключей, брелоков и т.п. Каждый из них имеет собственный уникальный серийный номер. Основными составляющими устройств являются интегральная микросхема для связи со считывателем и встроенная антенна. В составе микросхемы находятся приемо-передатчик и запоминающее устройство, хранящее идентификационный код и другие данные. Внутри Proximity может быть встроена литиевая батарейка (активные идентификаторы). Активные идентификаторы могут считывать информацию на расстоянии нескольких метров. Расстояние считывания пассивными идентификаторами (не имеющих батарейки) составляет десятки сантиметров. Устройство считывания постоянно излучает радиосигнал, который принимается антенной и передается на микросхему. За счет принятой энергии идентификатор излучает идентификационные данные, принимаемые считывателем.

Считыватели Proximity в своей работе опираются на широко известные физические принципы. Правда, того же нельзя сказать об алгоритмах обработки сигналов в схеме считывателя, что обычно и составляет «ноу хау» производителей. Рис. 4.49 поясняет взаимодействие карты и считывателя в процессе получения кода, заносимого в карту при ее производстве.

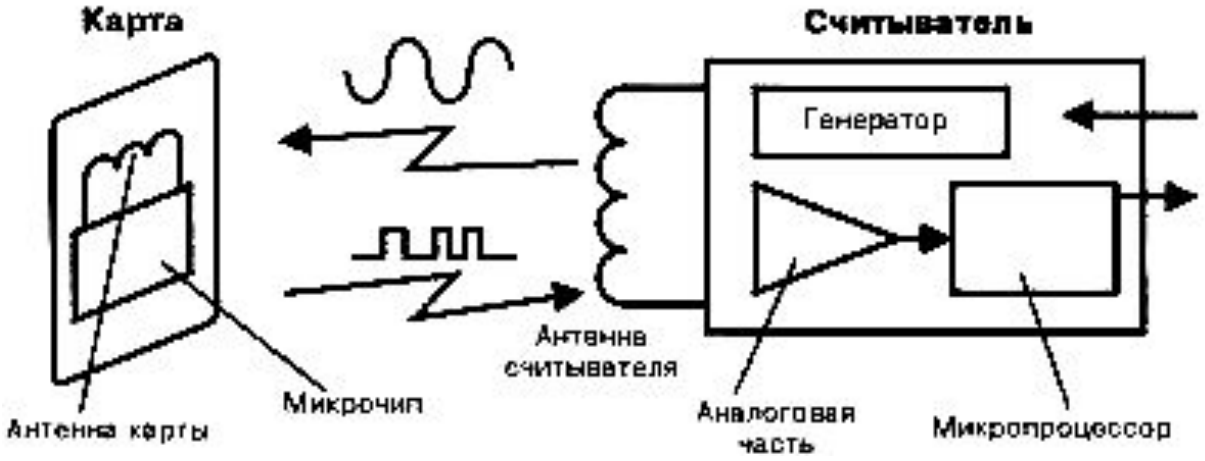


Рис. 4.49. Принцип работы Proximity считывателя

Считыватель содержит генератор, работающий, как правило, на частоте 125 кГц, и нагруженный на антенну считывателя. Излучаемая антенной считывателя энергия принимается антенной карты и запитывает расположенный в карте микрочип. Последний модулирует сигнал в антенне карты кодом, занесенным в микрочип на заводе-изготовителе.

Излученный картой сигнал воспринимается антенной считывателя, обрабатывается сначала
аналоговой частью схемы считывателя, а затем расположенным в считывателе микропроцессором. Микропроцессор проверяет корректность кода, преобразовывает его к требуемому формату и выдает на выход считывателя, то есть на вход контроллера системы управления доступом.

При всем многообразии форматов данных, обрабатываемых контроллерами систем управления доступом, более 80% систем ориентируются в качестве основного или дополнительного на формат Wiegand 26 бит.

Другой популярный формат интерфейса систем управления доступом – формат шины Micro LAN американской фирмы Dallas, в соответствии с которым работают ключи Touch memory. В отличие от Wiegand 26 этот формат хорошо документирован фирмой в литературе, поэтому не будем приводить его описание.

Почти все российские разработчики систем управления доступом ориентировались именно на использование протокола Micro LAN в своих контроллерах.

Считыватели «Parsec»

Рассмотрим принципы работы считывателей «Parsec».

Под торговой маркой «Parsec» производится достаточно широкий спектр оборудования систем управления доступом. В частности, это автономные контроллеры серии ASC-xx и сетевая компьютеризированная система управления доступом ParsecLight. Вместе с тем под этой торговой маркой продается целая гамма Proximity считывателей для применения в существующих системах как отечественного, так и зарубежного производства. Внешний вид считывателей APR-O3xx, APR-04xx и APR-05xx показан на рис. 4.50.

Особо следует сказать о считывателе APR-05xx, который выполнен в корпусе из нержавеющей стали и предназначен для уличной установки в случаях, когда требуется повышенная защита от вандализма.

Рис. 4.50. Внешний вид считывателей «Parsec»

4.11.5. Технология защиты информации на основе смарт-карт

Появление информационной технологии смарт-карт (СК), основанной на картах со встроенным микропроцессором, позволило удобнее решать вопросы использования пластиковых денег. Однако уникальные возможности СК с микропроцессором, состоящие в высокой степени защиты от подделки, поддержке базовых операций по обработке информации, обеспечении высоких эксплуатационных характеристик, сделали СК одним из лидеров среди носителей конфиденциальной информации. Следует отметить отличительные особенности таких карт. СК содержит микропроцессор и ОС, которые обеспечивают уникальные свойства защиты, имеют контактное и бесконтактное исполнение (на рис. 4.51 показана бесконтактная смарт-карта).

Таким образом, технология СК обеспечивает надежное хранение ключей и доступ к различным информационным ресурсам. Персональные идентификаторы iKey компании Rainbow являются недорогими брелоками, которые могут использоваться на любой рабочей станции, имеющей универсальную последовательную шину (USB). Они обеспечивают надежность, простоту и безопасность в такой же степени, как и смарт-карты, но без сложностей и лишних затрат, связанных с использованием считывателя.

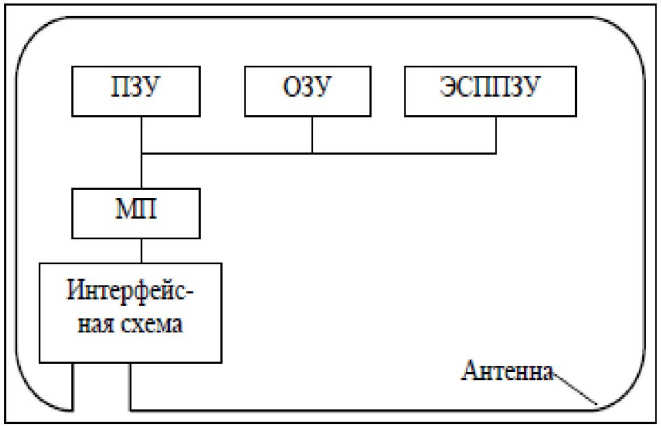


Рис. 4.51. Схема бесконтактной смарт-карты

iKey являются идеальным инструментом для контроля доступа к сетевым службам. iKey 2000 поддерживает и интегрируется со всеми основными прикладными системами, работающими по технологии PKI и используемыми в сетях отдельной организации, нескольких взаимодействующих организаций. Указанные системы включают Microsoft Internet Exolorer и Outlook, Netscape, Entrust, Baltimore, Xcert, Verisign и др. iKey 2000 разрабатывался для защиты цифровой идентичности в рамках инфраструктуры открытых ключей (PKI). iKey 2000 способен с помощью аппаратных средств генерировать и сохранять в памяти пары открытых ключей и цифровые сертификаты, а также производить цифровую подпись. Личный PKI-ключ недоступен компьютеру клиента.

iKey 2000 создает мощную систему защиты и криптографического кодирования непосредственно внутри аппаратного устройства. Для iKey 2000 пользователю поставляется программное обеспечение. Устройство содержит полный набор криптографических библиотек для броузеров Netscape и Internet Exolorer, а также для клиентов электронной почты. iKey 2000 действует одновременно как смарт-карта и считыватель, находящиеся в едином устройстве с конструктивом USB. Для активизации прикладной программы достаточно вставить iKey 2000 в USB-порт.

iKey 2000 реализует более простой метод обеспечения привилегий пользователя, чем пароли или чисто программные сертификаты. Чтобы запрограммировать ключ, администратору потребуется всего несколько минут. Потерянные ключи могут быть дезактивированы и изменены.

АПМДЗ «КРИПТОН-ЗАМОК

Назначение:

АПМДЗ «КРИПТОН-ЗАМОК» - это сертифицированные комплексы аппаратно-программных средств, которые предназначены для обеспечения разграничения и контроля доступа пользователей к техническим средствам вычислительной сети (сервера и рабочие станции), на которых будет обрабатываться информация, в том числе и с высоким грифом секретности. Также изделия семейства АПМДЗ «КРИПТОН-ЗАМОК» выполняют функции разграничения доступа к аппаратным ресурсам компьютеров, а также контроля целостности установленной на компьютере программной среды под любые ОС, использующие файловые системы FAT12, FAT16, FAT32 и NTFS , а так же EXT2, EXT3.

Основные возможности:

- Идентификация пользователя до запуска BIOS компьютера.
- Аутентификация пользователя по паролю.
- Создание нескольких профилей защиты, надежное разграничение ресурсов компьютера, принудительная загрузка операционной системы (ОС) с выбранного устройства в соответствии с индивидуальными настройками администратора для каждого пользователя.
- Блокировка компьютера при НСД, накопление и ведение электронного журнала событий (в собственной энергонезависимой памяти).

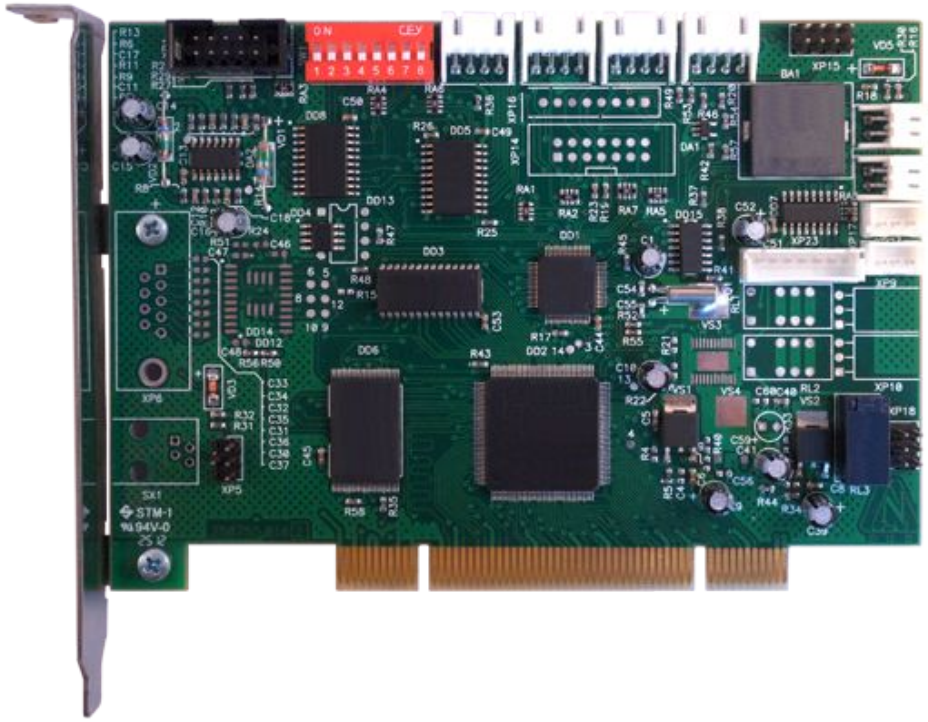
- Подсчет эталонных значений контрольных сумм объектов и проверка текущих значений контрольных сумм (рассчитываются по алгоритму вычисления хэш-функции по ГОСТ Р34.11-94), экспорт/импорт списка проверяемых объектов на гибкий магнитный диск.
- Интеграция в другие системы безопасности (сигнализация, пожарная охрана и пр.).
- Организация бездисковых рабочих мест на основе встроенного Флеш-диска.

Преимущества:

- Алгоритм кодирования аутентифицирующей информации в Изделиях «КРИПТОН-ЗАМОК» - в соответствии с требованиями ГОСТ 28147-89;
- Возможность разрешить некоторым пользователям осуществлять загрузку ОС с накопителя на гибком магнитном диске (НГМД) или CD ROM. Во всех других случаях Изделия «КРИПТОН-ЗАМОК» загружают ОС только через сетевой адаптер, произведенный фирмой «АНКАД», или с одного из накопителей на жёстком диске компьютера, который специально подготовлен администратором;
- Модульная структура, которая позволяет настраивать и дорабатывать изделия «КРИПТОН-ЗАМОК» под разнообразные требования заказчиков.

Сертификат ФСБ России № СФ/527-2047 от 25 января 2013г

АПМДЗ "КРИПТОН-ЗАМОК/К" (М-526А) - многоконтурная модель, предназначенная для создания нескольких контуров безопасности, т. е. осуществляется загрузка конфигурации компьютера в соответствии с индивидуальными настройками системы для каждого пользователя, разделение пользователей по физическим дискам (информация одного пользователя не доступна другому) и сетевым контурам.



Характеристики:

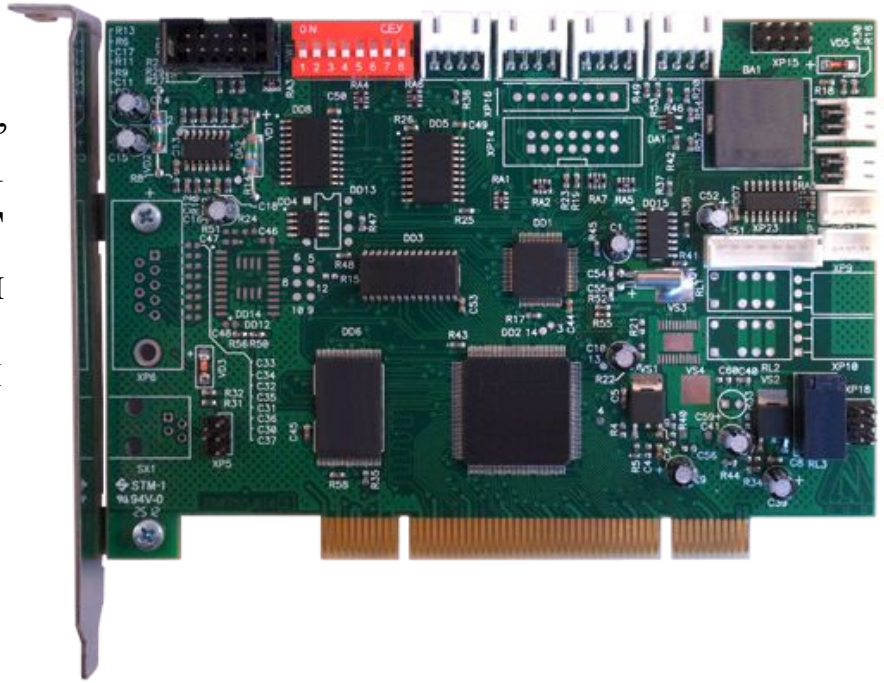
Наименование параметра	Характеристика
Стандарт средств идентификации, аутентификации и контроля целостности загружаемой ОС	Требования к аппаратно-программным модулям доверенной загрузки ЭВМ и дополнению к ним по классу защиты 1Б.
Поддерживаемые файловые системы (при контроле целостности):	FAT 12, FAT 16, FAT 32,
	NTFS
	EXT2
Максимальное количество регистрируемых пользователей	32
Стандарт интерфейса расширения компьютера	PCI Local BUS Revision 2.1, 2.2
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Носитель аутентифицирующей информации	Устройство памяти Touch Memory
Коммутируемые каналы	4 канала управления IDE или SATA;
	2 канала управления работой сетевыми адаптерами Ethernet;
	1 канал управления НГМД или приводом CD/DVD
Потребляемая мощность, не более, Вт	5
Габариты модуля КРИПТОН-ЗАМОК/К, мм	156,3 x 121 x 22
Масса модуля КРИПТОН-ЗАМОК/К, не более, г	

КРИПТОН-ЗАМОК/У (М-526Б)

Сертификат ФСБ России №СФ/027-1346 выдан 18.09.2009 г., действителен до 13.04.2013 г.

Положительное заключение ФСБ России от 14 августа 2014 года

АПМДЗ "КРИПТОН-ЗАМОК/У"(М-526Б, сертификат ФСТЭК России (в составе СРД "КРИПТОН-ЩИТ") - предназначен для работы с модулями криптографической защиты информации.



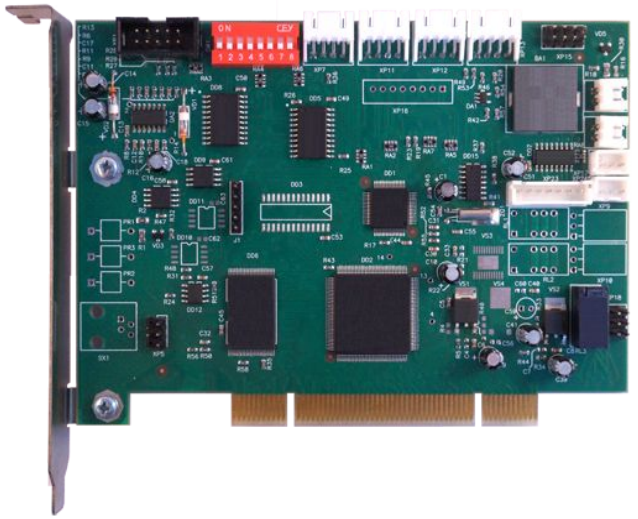
Характеристики:

Наименование параметра	Характеристика
Файловые системы, используемые при контроле целостности загружаемого ПО	FAT 12, FAT 16, FAT 32, NTFS, EXT2, EXT3 (Linux, кодировка KOI-8R).
Максимальное количество регистрируемых пользователей	32
Стандарт интерфейса расширения компьютера	PCI Local BUS Revision 2.1, 2.2
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Носитель аутентифицирующей информации	Устройство памяти Touch Memory
Потребляемая мощность, не более, Вт	5
Масса, не более, г	100
Габариты модуля АПМДЗ-У, мм	156,3 x 121 x 22

Сертификат ФСБ России №СФ/527-2048 от 21.01.2013г. (М-526В)
Сертификат ФСБ России №СФ/527-2049 от 20.03.2013г. (М-526В1)

Характеристики:

Наименование параметра	Характеристика
Стандарт средств идентификации, аутентификации и контроля целостности загружаемой ОС	Требования к аппаратно-программным модулям доверенной загрузки ЭВМ и дополнению к ним по классу защиты 1Б
Файловые системы, используемые при контроле целостности, загружаемого ПО	FAT 12, FAT 16, FAT 32, NTFS , EXT2, EXT3 (Linux, кодировка KOI-8R).
Максимальное количество регистрируемых пользователей	32
Стандарт интерфейса расширения компьютера	PCI Local BUS Revision 2.1, 2.2;
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Носитель аутентифицирующей информации	Устройство памяти Touch Memory
Потребляемая мощность, не более, Вт	5
Масса модуля КРИПТОН-ЗАМОК/УМ , не более, г	100
Габариты модуля КРИПТОН-ЗАМОК/УМ , мм	156,3 x 121 x 22

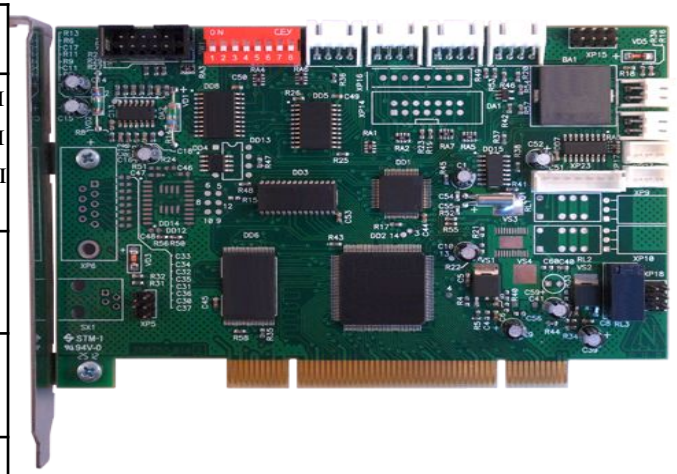


КРИПТОН-ЗАМОК/УМ (М-526В1) - модель, предназначенная для создания нескольких контуров безопасности и работы с модулями криптографической защиты информации.

Характеристики

Технические средства защиты информации

Наименование параметра	Характеристика
Класс стандарта средств идентификации, аутентификации и контроля целостности загружаемой ОС	Требования к аппаратно-программным модулям доверенной загрузки ЭВМ и дополнению к ним по классу защиты 1Б.
Файловые системы, используемые при контроле целостности загружаемого ПО	FAT 12, FAT 16, FAT 32, NTFS , EXT2, EXT3 (Linux, кодировка KOI-8R).
Максимальное количество регистрируемых пользователей	32
Стандарт интерфейса расширения компьютера	PCI Local BUS Revision 2.1, 2.2;
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Носитель ключевой информации	Устройство памяти Touch Memory
Коммутируемые каналы	- 4 канала управления IDE или SATA ЖД;
	- 2 канала управления работой сетевыми адаптерами Ethernet;
	- 1 канал управления НГМД или приводом CD/DVD-ROM.
Потребляемая мощность, не более, Вт	5
Габариты модуля КРИПТОН-ЗАМОК/УК	156,3x121x22
Масса модуля КРИПТОН-ЗАМОК/УК, не более, г	100



КРИПТОН-ЗАМОК/УК

Сертификат ФСТЭК России №2364 от 9 июня 2011г.

АПМДЗ "КРИПТОН-ЗАМОК/УК" - предназначен для создания нескольких контуров безопасности и работы с модулями криптографической защиты информации.

КРИПТОН-ЗАМОК/Е (М-526Е1)

Сертификат ФСБ России № СФ/527-2050 от 21 января 2013г. (М-526Е)
Сертификат ФСБ России № СФ/527-2051 от 20 марта 2013г. (М-526Е1)

АПМДЗ "КРИПТОН-ЗАМОК/Е" - модификация изделия для шины PCI Express. В ней реализован ряд новых возможностей, включая удаленное управление:

- Половинный форм-фактор платы, что позволяет использовать устройство в системных блоках уменьшенного размера;
- Шина PCI Express x1 Rev.1.1;
- Встроенный процессор с тактовой частотой 200МГц, обеспечивающий более быструю загрузку и работу устройства;
- Встроенная память не менее 256Мб;
- Независимый USB-интерфейс для подключения ключевых носителей и осуществления других функций.

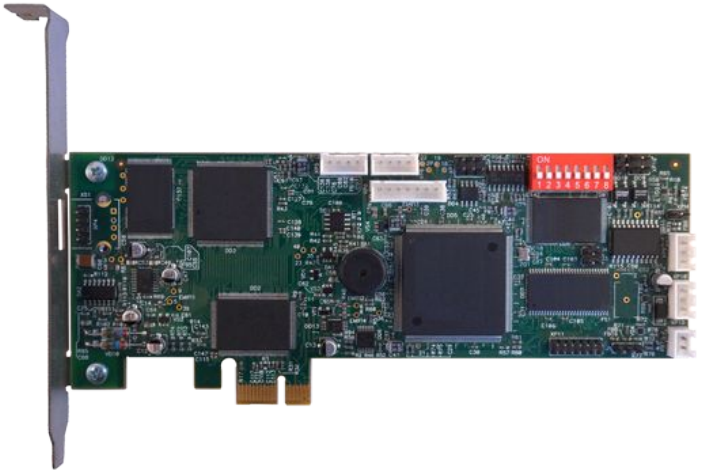
Обеспечение включения компьютера только после предъявления зарегистрированного ключевого носителя. Информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Характеристики:

Наименование параметра	Характеристика
Класс стандарта средств идентификации, аутентификации и контроля целостности загружаемой ОС	Требования к АПМДЗ по классу 1Б
Максимальное количество регистрируемых пользователей	32
Носитель аутентифицирующей информации	Устройство памяти Touch Memory
Файловые системы, используемые при контроле целостности, загружаемого ПО	FAT 12, FAT 16, FAT 32, NTFS , EXT2, EXT3 (Linux, кодировка KOI-8R).
Стандарт интерфейса расширения компьютера	PCI Express x1
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Потребляемая мощность, не более, Вт,	5
Масса модуля КРИПТОН-ЗАМОК/E, не более, г	100
Габариты модуля КРИПТОН-ЗАМОК/E, мм	180 x 120 x 25

Характеристики:

Наименование параметра	Характеристика
Класс стандарта средств идентификации, аутентификации и контроля целостности загружаемой ОС	Требования к АПМДЗ по классу 1Б
Максимальное количество регистрируемых пользователей	32
Носитель аутентифицирующей информации	Смарт-карта
Файловые системы, используемые при контроле целостности, загружаемого ПО	FAT 12, FAT 16, FAT 32, NTFS , EXT2, EXT3 (Linux, кодировка KOI-8R).
Стандарт интерфейса расширения компьютера	PCI Express x1
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Потребляемая мощность, не более, Вт	5
Масса модуля КРИПТОН-ЗАМОК/СК, не более, г	100
Габариты модуля КРИПТОН-ЗАМОК/СК, мм	180 x 120 x 25



КРИПТОН-ЗАМОК/СК (М-526СК)

Заключение ФСБ России является модификацией изделий КРИПТОН-ЗАМОК/Е, КРИПТОН-ЗАМОК/УМ, в которой реализована возможность использования в качестве носителей аутентифицирующей информации смарт-карт.

Шифраторы

Абонентские шифраторы

Устройства криптографической защиты данных (УКЗД) серии КРИПТОН — это аппаратные шифраторы для PC-совместимых компьютеров. Устройства применяются в составе средств и систем криптографической защиты данных для обеспечения информационной безопасности (в том числе защиты с высоким уровнем секретности) в государственных и коммерческих структурах. Они гарантируют защиту информации, обрабатываемой на персональном компьютере и/или передаваемой по открытым каналам связи.

Изделия выполнены в виде плат расширения PCI и PCIe для персонального компьютера.

Устройства КРИПТОН разработаны, производятся и реализуются Фирмой АНКАД. Они построены на разработанных Фирмой АНКАД специализированных 32-разрядных шифрпроцессорах серии БЛЮМИНГ.

Изделия поставляются заказчикам в Центральном Банке, ФСБ России, СВР России и Службе специальной связи и информации ФСО России министерствах обороны и внутренних дел, Министерстве по налогам и сборам, Федеральном казначействе, коммерческих банках, финансовых и страховых компаниях, многим корпоративным клиентам.

Все модели серии КРИПТОН имеют сертификаты соответствия требованиям ФСБ России (в составе абонентских пунктов и автоматизированных рабочих мест для защиты информации, содержащей сведения, составляющие государственную тайну).

Основные возможности:

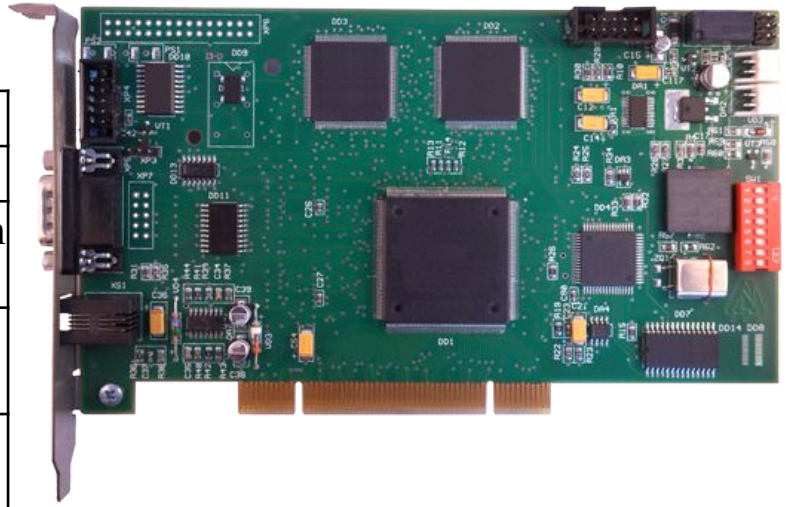
- Шифрование информации (файлы, группы файлов и разделы дисков), обеспечивая их конфиденциальность;
- Осуществление электронной цифровой подписи файлов, проверка их целостность и авторство;
- Создание прозрачно шифруемых логических дисков, максимально облегчая и упрощая работу пользователя с конфиденциальной информацией;
- Формирование криптографически защищенных виртуальных сетей, шифрование IP-трафика и обеспечение защищенного доступа к ресурсам сети мобильных и удаленных пользователей;
- Создание систем защиты информации от несанкционированного доступа и разграничения доступа к компьютеру.

Преимущества устройств серии КРИПТОН:

- Аппаратная реализация алгоритма криптографического преобразования гарантирует целостность алгоритма;
- Шифрование производится в самой плате, и ключи шифрования хранятся в ней же, а не в оперативной памяти компьютера;
- Аппаратный датчик случайных чисел;
- Загрузка ключей шифрования в устройство КРИПТОН со смарт-карт и идентификаторов Touch Memory (i-Button) производится напрямую, минуя ОЗУ и системную шину компьютера, что исключает возможность перехвата ключей;
- Возможность создания систем защиты информации от несанкционированного доступа и разграничения доступа к компьютеру на базе устройств КРИПТОН;
- Применение специализированного шифрпроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера;

Характеристики:

Наименование параметра	Характеристика
Алгоритм шифрования	ГОСТ 28147-89
Стандарт системной шины	PCI Local BUS Revision 2.0, 2.1, 2.2
Скорость шифрования, Мбайт/с	8
Размерность ключа шифрования, бит	256
Датчик случайных чисел (ДСЧ)	аппаратный
Поддерживаемые операционные системы	MS-DOS, Windows 2000/XP/2003 x32
Типы ключевых носителей	дискеты, смарт-карты
	Touch Memory
Потребляемая мощность, не более, Вт	4
Габариты модуля КРИПТОН-8/PCI, мм	190,3 x 122 x 22
Масса не более, г	100



КРИПТОН-8/PCI

Устройство криптографической защиты данных и ограничения доступа к компьютеру.

Комплект поставки

Наименование	Количество
Формуляр	1
Модуль КРИПТОН-8/PCI	1
Кабель RESET	1
Дистрибутив «Пакет программ Crypton API»	1
Дистрибутив «КРИПТОН-8/PCI Драйверы»	1
Руководство по эксплуатации изделия КРИПТОН-8/PCI	1
Упаковка	1

Характеристики:

Наименование параметра	Характеристика
Алгоритм шифрования	ГОСТ 28147-89
Стандарт системной шины	PCI Express x1
Скорость шифрования, Мбайт/с	14
Размерность ключа шифрования, бит	256
Число ключей хранящихся в ОЗУ шифратора	32
Датчик случайных чисел (ДСЧ)	аппаратный
Поддерживаемые операционные системы	MS-DOS, Windows 2000/XP/2003/2008, Windows 7 x32/64
Типы ключевых носителей	дискеты, смарт-карты
	Touch Memory
Потребляемая мощность, Вт, не более	4
Габариты модуля КРИПТОН-10, мм	132 x 120 x 22
Масса не более, г	100

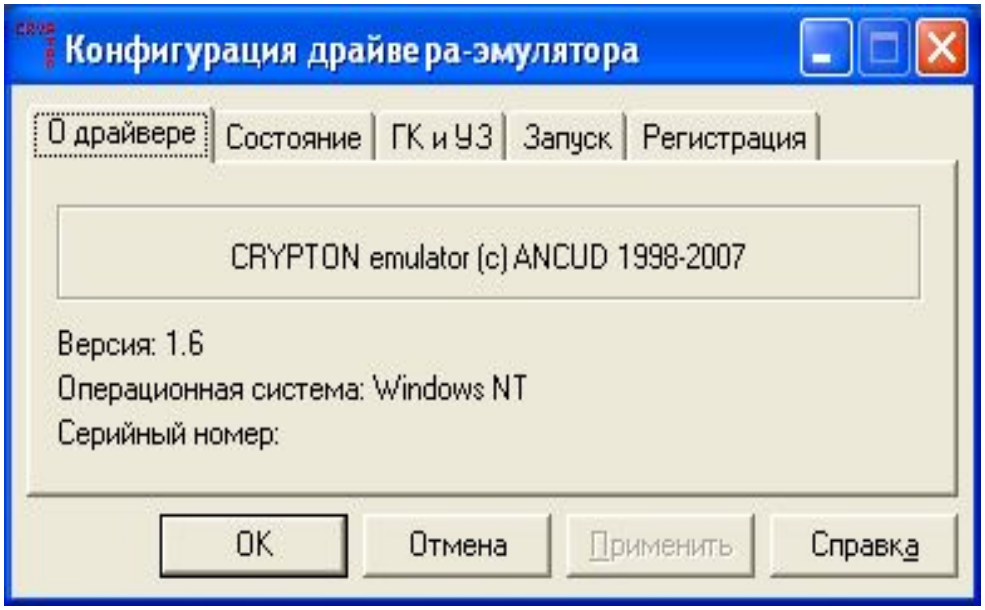
КРИПТОН-10/PCI-E
Устройство криптографической защиты данных и ограничения доступа к компьютеру

Комплект поставки

Наименование	Количество
Формуляр	1
Модуль КРИПТОН-10	1
Контактирующее устройство для ТМ	1
Руководство по эксплуатации	1
Дистрибутив «УКЗИ КРИПТОН-10. Программное обеспечение».	1
Дистрибутив «Пакет программ Crypton API»	1
Упаковка	1

В комплект поставки не входят носители ключевой информации (Touch Memory)

Crypton Emulator



Пакет программ Crypton Emulator (далее - "Эмулятор") обеспечивает программную эмуляцию функций шифрования УКЗД серии "Криптон" в следующих операционных системах:

- ОС Windows-95/98/Me/NT 4.0/2000/XP/2003/7 (x32);
- Solaris 2.x, 7, 8 (для архитектур x86, Sparc);
- Linux 2.2, 2.4, 2.6.

Эмулятор обеспечивает шифрование по алгоритму ГОСТ 28147-89, по функциям шифрования эмулятор полностью совместим с УКЗД серии "Криптон". Таким образом, возможна замена аппаратного УКЗД "Криптон" его программным эмулятором без какого-либо изменения программного обеспечения, использующего УКЗД "Криптон" или Crypton Emulator.

Шифраторы жестких дисков

Назначение:

Аппаратно-программные криптографические комплексы М-590 («КРИПТОН - ПШД/IDE), М-575 («КРИПТОН - ПШД/SATA») и М-623 («КРИПТОН - ИНТЕГРАЛ») предназначены для защиты информации (в том числе сведений, составляющих государственную тайну) на дисках компьютера и защиты от несанкционированного доступа (НСД) ресурсов компьютера. В состав комплексов входит модуль проходного аппаратного шифратора серии «КРИПТОН» и подсистема защиты от НСД на базе аппаратно-программного модуля доверенной загрузки «КРИПТОН-ЗАМОК».

Основные возможности:

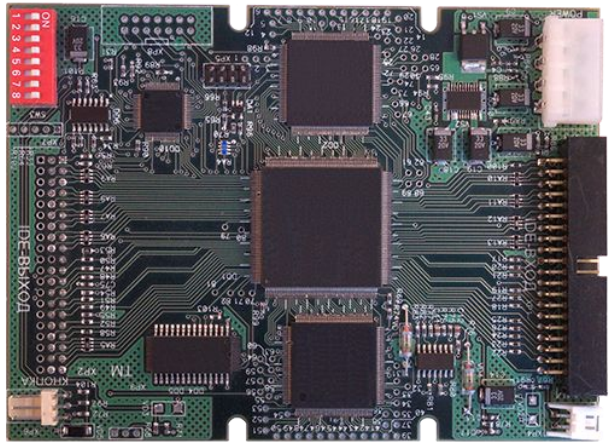
Прозрачное шифрование данных по ГОСТ 28147-89, передаваемых между хост-контроллером на системной плате компьютера и жестким диском или съемным USB носителем;

Основные преимущества:

- Аппаратная реализация алгоритма криптографического преобразования гарантирует целостность алгоритма;
- Шифрование производится в самой плате, и ключи шифрования хранятся в ней же, а не в оперативной памяти компьютера;
- Аппаратный датчик случайных чисел;
- Загрузка ключей шифрования в устройство КРИПТОН-ПШД со смарт-карт и идентификаторов Touch Memory (i-Button) производится напрямую, минуя ОЗУ и системную шину компьютера, что исключает возможность перехвата ключей;
- Возможность создания систем защиты информации от несанкционированного доступа и разграничения доступа к компьютеру на базе устройств КРИПТОН-ЗАМОК;
- Применение специализированного шифрпроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера;
- Широкий спектр поддерживаемых типов носителей;
- Независимость от ОС и файловой системы.

Характеристики:

Наименование параметра	Характеристика
Алгоритм шифрования	ГОСТ 28147-89
Интерфейс жесткого диска	Стандарт AT Attachment with Packet Interface – 6 (ATA/ATAPI – 6) для IDE устройств и ANSI x3.298-1997
Режимы работы	PIO 0-4, MWDMA 0-2, UltraDMA.
Скорость криптографического преобразования данных при записи и чтении с жесткого диска.	не менее 6 Мбайт/сек
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Носитель ключевой информации	Устройство памяти Touch Memory



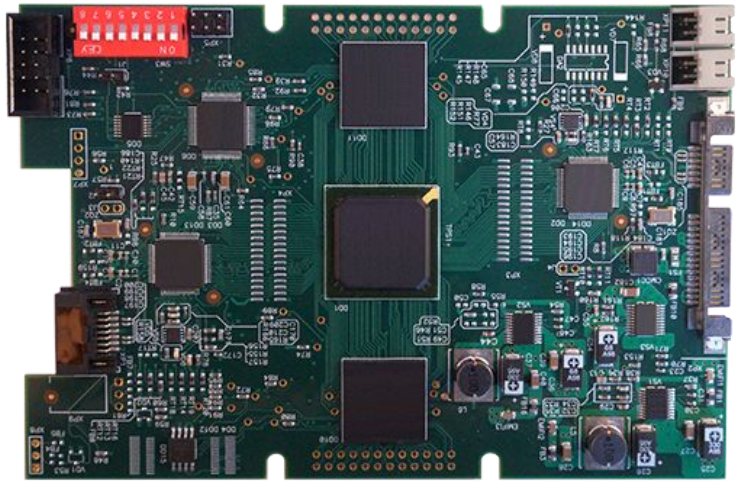
М-590 («КРИПТОН-ПШД/IDE»)
Сертификат ФСБ России 020-1556 от 4 октября 2010г.

Комплект поставки

Наименование	Количество
Формуляр	1
Модуль ПШД/IDE	1
Кабель межплатного интерфейса	1
Кабель UDMA	1
iButton 64Кбит – 2 шт.	1
Монтажный комплект	1
Руководство пользователя	1
Руководство администратора	1
Упаковка	1

Характеристики:

Наименование параметра	Характеристика
Алгоритм шифрования	ГОСТ 28147-89
Интерфейс связи с жестким диском и контроллером на системной плате компьютера	стандарт High Speed Serialized AT Attachment Revision 1.0a .
	Совместимость с SATA II
Режимы работы жесткого диска	PIO 0-4, MWDMA 0-2, UltraDMA.
Скорость криптографического преобразования данных при записи и чтении с жесткого диска.	до 30 Мбайт/сек.
Датчик случайных чисел (ДСЧ), тип	Аппаратный
Носитель ключевой	Устройство памяти Touch



М-575 («КРИПТОН-ПШД/SATA»)
Сертификат ФСБ России 020-1287 от 2 марта 2009г.

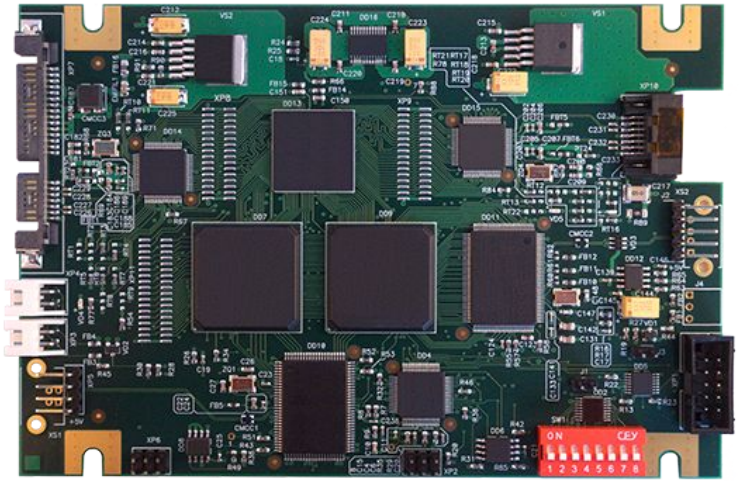
Комплект поставки

Наименование	Количество
Формуляр	1
Модуль ПШД/ SATA	1
Кабель межплатного интерфейса	1
iButton 64Кбит – 2 шт.	1
Кабель внутренний SATA	1
Дистрибутив «КРИПТОН-ПШД/SATA. Программное обеспечение»	1
Руководство пользователя	1
Руководство администратора	1
Упаковка	1

Технические средства защиты информации

Характеристики:

Наименование параметра	Характеристика
Алгоритм шифрования	ГОСТ 28147-89
Интерфейс связи с жестким диском и контроллером на системной плате компьютера	стандарт High Speed Serialized AT Attachment Revision 1.0a. или SATA II/SATA III.
Режимы работы жесткого диска	PIO 0-4, MWDMA 0-2, UltraDMA.
Скорость криптографического преобразования данных при записи и чтении с жесткого диска.	до 30 Мбайт/сек.
Скорость криптографического преобразования данных при записи и чтении с флеш-носителя стандарта USB 2.0.	- в полноскоростном режиме - не менее 2 Мбайт/с; - в высокоскоростном режиме не менее 10 Мбайт/с.
Носитель ключевой	Устройство памяти Touch



М-623 («КРИПТОН-ИНТЕГРАЛ»)

Сертификат ФСБ России 020-1562 от 4 октября 2010г.

Данное изделие предназначено для проходного шифрования данных на носителях как с интерфейсом SATA, так и с USB, а так же для безопасной записи информации со стационарного носителя на сменный, минуя системную шину и операционную систему.

Сетевые шифраторы

Изделия М-524Т, М-524Е, М-524СК, М-524К, М-525 (Сертифицированные аппаратно-программные комплексы «КРИПТОН AncNet Pro») предназначены для защищенной передачи данных в сети (в том числе и с высоким уровнем грифа секретности) и защиты компьютера сети от несанкционированного вмешательства посторонних лиц в его работу.

Основные возможности:

- Прием и передача кадров формата Ethernet II по протоколам семейства TCP/IP версия 4;
- Потоковое шифрование данных в соответствии с ГОСТ 28147-89.

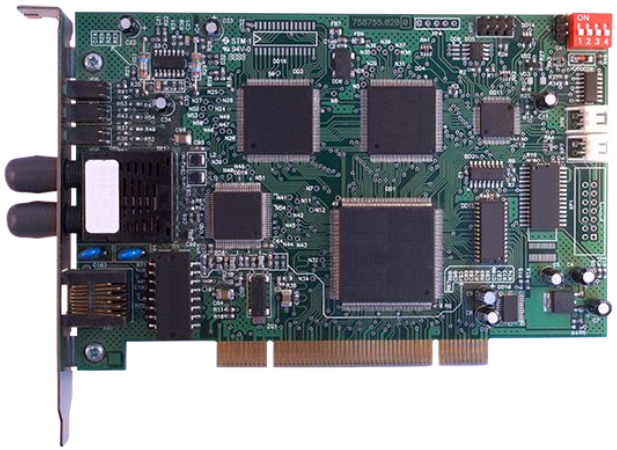
Преимущества:

- Аппаратная реализация алгоритма криптографического преобразования гарантирует целостность алгоритма;
- Шифрование производится в самой плате, и ключи шифрования хранятся в ней же, а не в оперативной памяти компьютера;
- Загрузка ключей шифрования в устройство КРИПТОН AncNet со смарт-карт и идентификаторов Touch Memory (i-Button) производится напрямую, минуя ОЗУ и системную шину компьютера, что исключает возможность перехвата ключей;
- Возможность создания систем защиты информации от несанкционированного доступа и разграничения доступа к компьютеру на базе устройств КРИПТОН AncNet;
- Применение специализированного шифрпроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера;
- Поддержка широкого спектра ОС.

Технические средства защиты информации

Характеристики:

Наименование параметра	Характеристика
Стандарты передачи данных	802.3, 2000 Edition (ISO/IEC 8802-3:2000) 802.3U, 802.3X
Сетевая среда	100 BASE – FX, 100 BASE – TX,
	10 BASE – T
Способ защиты	Прозрачное шифрование информационной части IP пакета
Стандарт шифрования данных	ГОСТ 28147-89
Пропускная способность передачи данных по сети	не менее 64 Мбит/с
Стандарт сетевого уровня	IPv4
Стандарт средств идентификации, аутентификации и контроля целостности загружаемой ОС	Требования ФСБ к АПМДЗ Класс защиты – 1Б
Операционная среда функционирования изделия	ОС Windows NT 4.0 SP 6, 2000/XP/7 x32/x64/2008 x64/ Linux
Стандарт интерфейса расширения компьютера	PCI Local BUS Revision 2.1, 2.2
Носитель ключевой информации	Устройство памяти Touch Memory
Носитель аутентифицирующей информации	Устройство памяти Touch Memory
Потребляемая мощность, не более	10 Вт
Габариты модуля КРИПТОН-8/PCI, мм	190,3 x 122 x 22
Масса КРИПТОН-8/PCI , не более, г	100



КРИПТОН AncNet Pro (M-524T)

Сертификат ФСБ России №020-1584 от 1 января 2011г.

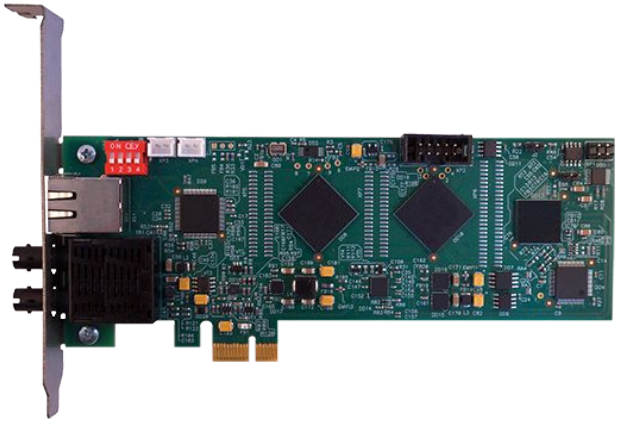
КРИПТОН AncNet Pro (М-524Т) имеет три различных исполнения. Комплект поставки необходимо уточнить при заказе.

В настоящее время специалистами ООО Фирма «АНКАД» разработаны устройства М-524Е и М-524К, поддерживающие шину PCI Express x1 и сетевую среду Gigabit Ethernet. Данные продукты имеют положительное заключение (М-524Е) и сертификат ФСБ России (М-524К).

ПРИМЕЧАНИЕ: Сетевые шифраторы КРИПТОН-AncNet не могут использоваться без АПМДЗ КРИПТОН-ЗАМОК.

Характеристики:

Наименование параметра	Характеристика
Стандарты передачи данных	802.3, 2000 Edition (ISO/IEC 8802-3:2000)
Сетевая среда	100BASE–FX, 100BASE-TX, 10BASE-T
Способ защиты данных	Прозрачное шифрование информационной части IP пакета, контроль не зашифрованной части заголовка пакета.
Стандарт шифрования данных	ГОСТ 28147-89
Скорость передачи данных по сети	Не менее 140 Мбит/с
Стандарт сетевого уровня	IP v.4
Стандарт средств идентификации, аутентификации и контроля целостности загружаемой ОС	Требования к АПМДЗ по классу 1Б
Стандарт интерфейса расширения компьютера	PCI Express x1 rev.1.0/1.0a/1.1 либо PCI Local BUS Revision 2.1, 2.2
Операционная среда функционирования изделия	ОС Windows NT 4.0 SP 6, 2000/XP/7 x32/x64/2008 x64/ Linux
Носитель ключевой информации , аутентифицирующий носитель пользователя	Устройство памяти типа Touch Memory
Потребляемая мощность изделия	не более 10 Вт
Габариты модуля КРИПТОН AncNet Express, мм	180 x 81 x 22
Масса	не более 100 г



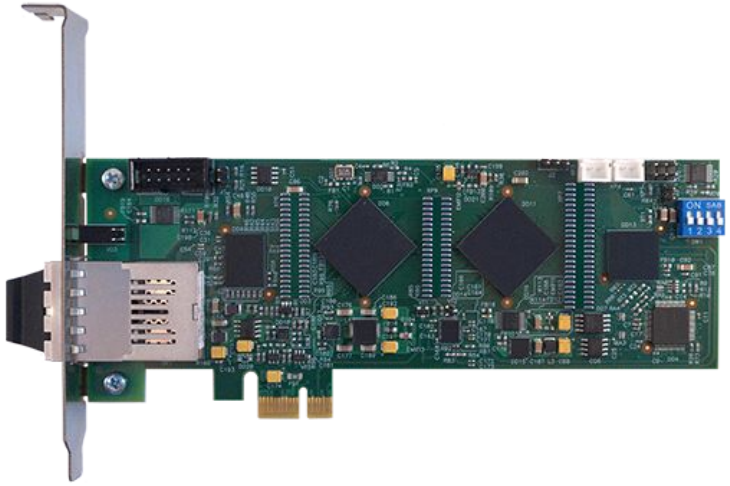
КРИПТОН AncNet Express (M-524E)

Заключение ФСБ России КРИПТОН AncNet Pro (M-524E) имеет два различных исполнения. Комплект поставки необходимо уточнить при заказе.

ПРИМЕЧАНИЕ: Сетевые шифраторы КРИПТОН-AncNet не могут использоваться без

Характеристики:

Наименование параметра	Характеристика
Стандарты передачи данных	802.3, 2000 Edition (ISO/IEC 8802-3:2000)
Сетевая среда	1000BASE-SX
Способ защиты данных	прозрачное шифрование информационной части IP пакета, контроль не зашифрованной части заголовка пакета.
Стандарт шифрования данных	ГОСТ 28147-89
Скорость передачи данных по сети	до 400 Мбит/с
Стандарт сетевого уровня	IP v.4
Стандарт средств идентификации, аутентификации и контроля целостности загружаемой ОС	требования к АПМДЗ по классу 1Б.
Операционная среда функционирования изделия	Windows XP/7 x32/x64/2008 x64/ Linux
Стандарт интерфейса расширения компьютера	PCI Express x1, rev.1.0/1.0a/1.1 либо PCI Local BUS Revision 2.1, 2.2
Носитель ключевой информации	Устройство памяти типа Touch Memory
Габариты, мм	180 x 81 x 22
Масса, не более, г	100



КРИПТОН AncNet 1000 (М-524К)

Сертификат ФСБ России №024-2447 от 17 июля 2014г.

Сетевые адаптеры

Назначение:

Сетевые адаптеры AncNet предназначены для передачи данных в компьютерных сетях. Они обеспечивают совместимость со всеми типами активного сетевого оборудования и сетевыми адаптерами зарубежных производителей. Специально разработаны драйверы сетевой платы, которые поддерживают работу в ОС DOS, Windows и Linux.

В современных условиях особое значение уделяется вопросу импортозамещения и доверенные средства отечественного производства вызывают все больший интерес российских потребителей. В этих условиях Фирма «АНКАД» представляет свои доверенные сетевые адаптеры AncNet.

Преимущества:

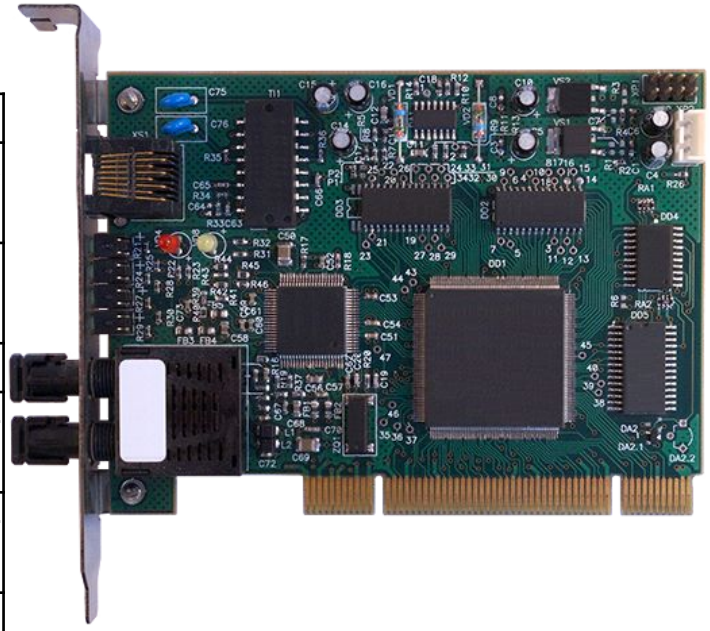
- Сетевые адаптеры семейства AncNet произведены полностью на отечественном производстве;
- Технологии производства и разработки устройств позволяют гарантировать доверенность и защищенность сетей, построенных на базе устройств AncNet;
- Современная элементная база позволяет гарантировать производство на протяжении всего срока эксплуатации системы, в которую будут внедрены изделия;
- Семейство сетевых адаптеров AncNet имеют возможность работать в различных средах передачи данных (FX,TX). При использовании в сетях, построенных на оптических средах передачи данных, есть возможность выбора не только вида подключения к сетевому оборудованию (SC,ST), но так же по типу оптического волокна (multi mode, single mode);
- Устройства семейства AncNet серии 1000 выполнены в формфакторе half-size PCI Express, что позволяет внедрять их в различные комплексы, где малый размер и высокая производительность необходимы для надежной и интенсивной работы.

Управление сетевыми адаптерами AncNet 1000 с помощью семейства устройств КРИПТОН-ЗАМОК обеспечивает построение сложных систем, в которых необходимо гарантированное управление доступом пользователей к сетевой среде.

Технические средства защиты информации

Характеристики:

Наименование параметра	Характеристика
Стандарты передачи данных	802.3, 2000 Edition (ISO/IEC 8802-3:2000), 802.3U , 802.3X
Сетевая среда	100 BASE – FX, 100Base – TX, 10Base-T
	тип разъема:
	- 100BASE– FX - ST(multi-mode);
	- 100BASE– FX - SC(multi-mode);
	- 100Base– TX – RJ45;
	- 10Base–T – RJ45.
Стандарт системной шины	PCI Local BUS Revision 2.1, 2.2
Параметры системной шины PCI	Разрядность - 32 бита;
ОС функционирования изделия	Windows 7, Windows 7 x64, Windows Server 2008 R2 x64
Средняя скорость выработки случайных чисел, Кбайт/с	100
Габариты модуля AncNet Pro, мм	121 x 90 x 22
Масса, не более, г	100



Сетевые адаптеры AncNet Pro

Изделие AncNet Pro имеет десять исполнений в зависимости от типа физической среды компьютерной сети, типа разъема подключения к сети и наличия или отсутствия ДСЧ. Цену, срок поставки и комплектацию уточняйте у наших специалистов.

Сетевой адаптер AncNet x2 позволяет осуществлять аппаратное разграничение доступа к двум различным компьютерным сетям с использованием только одной сетевой карты. Данное устройство имеет два раздельных сетевых выхода с возможность их аппаратного включения/отключения на ранних стадиях загрузки компьютера.

Сетевые адаптеры AncNet x2 - оригинальная разработка Фирмы «АНКАД», обеспечивающая совместимость со всеми типами активного сетевого оборудования и сетевыми адаптерами зарубежных производителей. Специально разработаны также драйверы сетевой платы, которые поддерживают работу под управлением ОС DOS, Windows и Linux.

Модуль AncNet Pro x2, имеет пять исполнений в зависимости от типа физической среды компьютерной сети и типа разъема подключения к сети. Цену, срок поставки и комплектацию уточняйте у наших специалистов.

Сетевые адаптеры AncNet x2

Характеристики: Технические средства защиты информации

Наименование параметра	Характеристика
Стандарты передачи данных	802.3, 2000 Edition (ISO/IEC 8802-3:2000), 802.3U, 802.3X
Сетевая среда	100BASE-FX, 100BASE-TX, 10BASE-T
	тип разъема:
	- 100BASE-FX - ST(multi-mode);
	- 100BASE-FX - SC(multi-mode);
	- 100BASE-TX - RJ45;
	- 10BASE-T - RJ45.
Стандарт системной шины	PCI Local BUS Revision 2.2
ОС функционирования изделия	Windows 2000 Professional SP4, Windows XP Professional SP3, Windows XP Professional x64 SP2, Windows Server 2003 R2 SP2, Windows Server 2003 R2 x64 SP2, Windows 7 Professional SP1 , Windows 7 Professional x64 SP1, Windows Server 2008 R2 x64 SP1.
Параметры системной шины PCI	Разрядность - 32 бита;
Потребляемая мощность, не более, Вт	5
Габариты печатной платы, мм	121 x 137 x 22
Масса, не более, кг	0,2

Характеристики:

Наименование параметра	Характеристика
Стандарты передачи данных	802.3, 2000 Edition (ISO/IEC 8802-3:2000)
Сетевая среда	1000BASE-SX, 1000BASE-T
Стандарт системной шины	PCI Express x1
Поддерживаемые операционные системы	Win7 x32, x64; Win8 x32, x64; Linux Ubuntu (версии 3.5); Debian/Linux 6.0.4 (ядро версии 2.6.32-5-amb64); Ubuntu 12.04.1 LTS (ядро версии 3.2.0-34)
Скорость передачи данных по сети, не менее Мбит/с	900
Потребляемая мощность, не более, Вт	5
Габариты модуля СИА-1G, мм	134 x 80,2 x 22
Масса, не более, г	100

Сетевые адаптеры AncNet Pro 1000

Модуль AncNet Pro 1000, имеет два исполнения в зависимости от типа физической среды компьютерной сети и типа разъема подключения к сети. Цену, срок поставки и комплектацию уточняйте у наших специалистов.

Средства разграничения доступа

Сертификат ФСБ России №СФ/022-1887 от 18 июля 2012г.

Сертификат ФСТЭК России №3130 от 08.04.2014г.

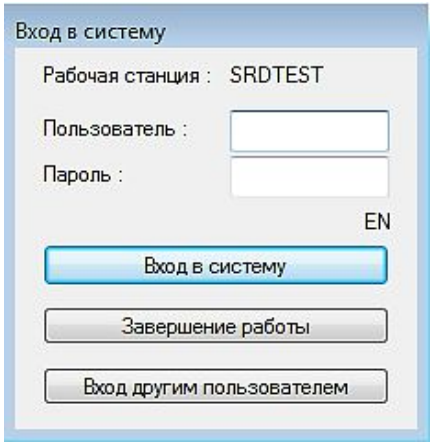
Система разграничения доступа «КРИПТОН-ЩИТ» представляет собой аппаратно-программный комплекс средств защиты информации, предназначенный для защиты от несанкционированного доступа к информации в 32 и 64-битных операционный системах Microsoft Windows. «КРИПТОН-ЩИТ» функционирует как на автономных персональных компьютерах, так и на средствах вычислительной техники, объединенных в локальную сеть.

Система «КРИПТОН-ЩИТ» соответствует всем требованиям руководящих документов Гостехкомиссии (ФСТЭК России) по уровню защиты гостайны – реализуя мандатный принцип разграничения доступа по набору иерархических и неиерархических категорий и используя полную матрицу доступа «пользователи-процессы-ресурсы».

Система «КРИПТОН-Щит» работает на уровне микроядра операционной системы (MS Windows NT, 2000, XP 32/64, 2003 32/64, Vista 32, 7 32/64), независимо от встроенных в ОС средств контроля доступа, и отличается низкими системными требованиями. «КРИПТОН-ЩИТ» не изменяет системный файлы Windows. В настоящее время СРД «КРИПТОН-ЩИТ» поставляется в двух вариантах:

СРД «КРИПТОН-ЩИТ» имеет Сертификат ФСБ России №СФ/022-1887 от 18 июля 2012г., работает в ОС (MS Windows NT, 2000, XP x32/64, 2003 x32/64, Vista 32, 7 x32/64)

СРД «КРИПТОН-ЩИТ 7» имеет сертификат ФСТЭК России №3130 от 08.04.2014г., работает в ОС (MS Windows NT, 2000, XP x32/64, 2003 x32/64, Vista 32, 7 x32/64). Основным отличием от СРД «КРИПТОН-ЩИТ» является возможность работы без аппаратной составляющей, с использованием в качестве электронного ключа Rutoken.



Основные возможности СРД «КРИПТОН-ЩИТ»:
Идентификация и аутентификация пользователей

- Реализована единая и одноразовая идентификация и аутентификация для пользователя, с формированием профиля прав доступа;
- Контроль доступа к ресурсам компьютера;
- Контроль целостности операционной среды методом контрольного суммирования;
- Мандатный и дискреционный принцип разграничения доступа к ресурсам ОС;
- Интегрированная настройка и описание пользователей, прав доступа пользователей к ресурсам;
- Автоматическая блокировка доступа к ресурсам персонального компьютера во время отсутствия пользователя (период неактивности пользователя, характеризующийся отсутствием работы с клавишами клавиатуры и мыши);
- Возможность трассировки обращений к ресурсам программного обеспечения в специальном отладочном режиме;
- Разграничение доступа к процедурам (программам);
- Обеспечение единого интерфейса пользователя для работы с процедурами (программами), одновременно выполняющего разграничение доступа к процедурам для каждой категории пользователя;
- Ролевая модель разграничения доступа к процедурам (программам);
- Поддержка многошаговых процедур с возможностью наследования полномочий и без него.

Интеграция с аппаратными средствами защиты

Система разграничения доступа «КРИПТОН-ЩИТ» интегрирована с изделиями семейства АПМДЗ «КРИПТОН-ЗАМОК», изделиями семейства «КРИПТОН-AncNet», шифраторами дисков семейств «КРИПТОН-ПШД», а также абонентскими шифраторами серии «КРИПТОН» , что позволяет существенно повышать уровень защиты за счет дополнительных криптографических возможностей.

Разграничение и контроль доступа к периферийным устройствам

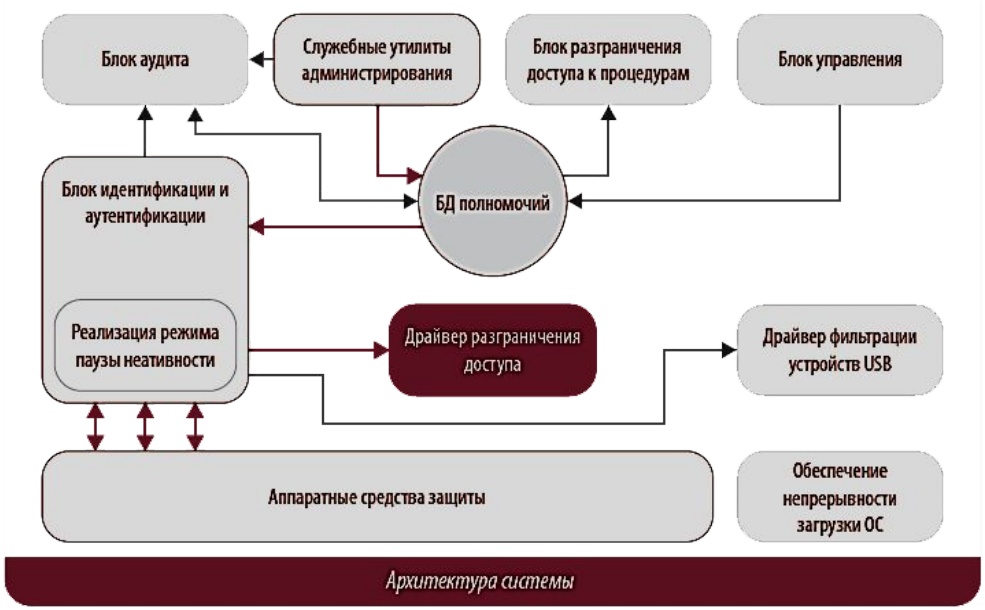
- Дополнительное разграничение доступа к USB-устройствам, регистрация данных при печати файлов на принтере
- Гибкая система протоколирования и аудит событий в системе защиты информации;
- Поддержка двух журналов аудита пользователя – учета событий и обращений к ресурсам. Кроме того, ведется журнал печати;
- Автоматизированные средства построения профилей (белый список);
- Контроль отладочных регистров;
- Динамический контроль целостности;
- Гарантированная очистка оперативной памяти.

Система защиты на базе «КРИПТОН-ЩИТ» должна строиться на основе комплексного подхода и включать организационные меры и технические средства. Под техническими средствами защиты понимается совокупность аппаратных и программных средств, реализующих в информационных системах функцию защиты информации от НСД.

Технические средства защиты информации

Компоненты, входящие в систему СРД «КРИПТОН-ЩИТ»:

- Подсистема контроля целостности эталонного программного обеспечения, интегрированная с аппаратными средствами (КРИПТОН-ЗАМОК/У);
- Подсистема идентификации и аутентификации пользователей, интегрированная с аппаратными средствами (КРИПТОН-ЗАМОК/У);
- Подсистема разграничения доступа к процедурам (диспетчер меню), реализующая ролевую модель, и рабочим станциям;
- Подсистема разграничения доступа к ресурсам операционной системы, реализующая дискреционный и мандатный принцип доступа;
- Подсистема управления, реализующая контроль исполнения процессов (процедур) в системе;
- Подсистема протоколирования работы пользователя и фиксации событий несанкционированного доступа в специальном журнале учета;
- Средства администратора защиты и программиста сопровождения по настройке прав доступа пользователей к процедурам и ресурсам системы и другие служебные утилиты;
- Средства получения справок о событиях и попытках НСД в системе;
- Программа реализации паузы неактивности, обеспечивающая блокировку персонального компьютера во время отсутствия пользователя.



Аппаратные средства защиты

- идентификация и аутентификация пользователя;
- проверка целостности файловой системы;
- предотвращение загрузки ОС с альтернативных носителей;
- контроль конфигурации компьютера.

Подсистема идентификации и аутентификации

- продолжение идентификации и аутентификации (определение статуса пользователя);
- формирование профиля прав доступа пользователя;
- подключение к ресурсам ОС;
- дополнительная аутентификация при выходе из сеанса.

Подсистема разграничения доступа к ресурсам ОС

- дискреционный принцип разграничения доступа;
- мандатный принцип разграничения доступа;
- наследование прав доступа;
- контроль доступа на уровне процессов ОС.

Блок разграничения доступа к USB-устройствам

- идентификация USB-устройств;
- разграничение доступа.

Диспетчер меню

- разграничение доступа к процессам (процедурам);
- создание для пользователя списка доступных процедур;
- управление работой пользователя в сеансе.

Подсистема аудита

- фиксация событий НСД;
- фиксация информационных событий;
- фиксация событий настройки полномочий;
- средства ведения и просмотра журнала;
- фиксация обращений к ресурсам ОС в зависимости от настройки.

Режим паузы неактивности

- блокировка компьютера и гашение экрана по истечении заданного интервала времени при отсутствии признаков активности пользователя;
- восстановление сеанса пользователя после введения пароля.

Блок регистрации печати

- регистрация документов, выдаваемых на принтер через спулер;
- фиксация реквизитов выдаваемый документов (размер, дата, время, пользователь и т. д.).

Служебные процедуры и вспомогательные утилиты

- настройка БД полномочий (заведение объектов и субъектов защиты, прав доступа и т.д.);
- настройка прав доступа для системных задач;
- разблокировка пользователей;
- генерация паролей пользователей в ОС;
- просмотр журнала обращений к ресурсам ОС в отладочном режиме;
- определение идентификационных данных подключаемых USB-устройств;
- просмотр текущего профиля пользователя во внутреннем формате;
- автоматическое формирование прав доступа к процессу при специальном запуске.

Управление сеансом пользователя

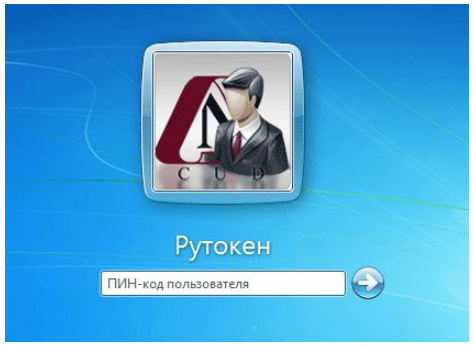
- контроль за запуском и завершением процессов в ОС;
- управление процессом загрузки и выгрузки сеанса пользователя(непрерывность загрузки);
- управление взаимодействием с АПМДЗ.

Продукция Crypton Lock
Сертификат ФСТЭК России №2600 от 21 марта 2012г.

Назначение:
Программное средство защиты информации Crypton Lock предназначено для обеспечения санкционированного доступа на сервер, либо на рабочую станцию под управлением Microsoft Windows и домена Windows. При использовании Crypton Lock стандартная аутентификация пользователя по логину-паролю заменяется строгой двухфакторной аутентификацией посредством USB-токена Рутокен.
Основные возможности:

- Позволяет ужесточить требования политики безопасности к пользовательским паролям;
- Минимизирует риск кражи паролей за счет снижения человеческого фактора;
- Делает процедуру авторизации пользователя более удобной, так как позволяет отказаться от ввода логина и пароля;
- Поддерживает механизмы доменной авторизации Windows;
- Позволяет авторизовать как доменных пользователей, так и локальных пользователей компьютера;
- Позволяет надежно блокировать рабочую станцию при временном прекращении работы.

Преимущества:



- Программная часть модуля Crypton Lock сертифицирована по 4 классу отсутствия недекларированных возможностей (НДВ) (Сертификат ФСТЭК №2600 от 21 марта 2012г.);
- Используется двухфакторная аутентификация пользователя, заменяя стандартные механизмы защиты ОС Windows;
- В качестве ключевого носителя применяется USB-токен РУТОКЕН, имеющий сертификат ФСТЭК России.

Типовой сценарий применения Crypton Lock

Модуль Crypton Lock совместим с ОС Microsoft Windows 2000/XP/2003/Vista/2008/7.

Для разворачивания Crypton Lock следует:

- Установить Crypton Lock на все защищаемые компьютеры;
- Провести регистрацию каждого пользователя на предназначенном ему USB-токене Рутокен;
- Раздать устройства пользователям (при этом сообщать пароль пользователям не требуется).

При работе Crypton Lock подменяет стандартный интерфейс входа в Windows и блокировки компьютера, при этом просит пользователя подключить Рутокен и ввести его PIN-код.

4.11.6. Защита компьютеров при транспортировке - Кейс «ТЕНЬ»

Кейс «ТЕНЬ» предназначен для транспортировки ноутбуков под охраной с возможностью автоматического уничтожения информации при попытке несанкционированного доступа. Имеет автономный источник питания, дистанционное управление. Монтируется в пыле-, влаго-, взрывозащищенный кейс (рис. 4.52).

Также может быть использован для транспортировки жестких дисков, дискет, аудио-, видео-, стримерных кассет. Профессиональная модель предназначается для уничтожения в любой момент информации с магнитных носителей при их транспортировке. Имеет повышенную защиту, собственное микропроцессорное управление, автономный источник резервного питания. Изготавливается только под заказ, на основании определенной клиентом комплектации. Рекомендуется как средство защиты информации (копии, дубликаты, Backup) при ее транспортировке к месту хранения. В базовой комплектации состоит.

Рис. 4.52. Кейс «ТЕНЬ»

из модуля уничтожения, модуля микро-процессорного управления, модуля резервного питания на 12 ч. Монтируется в стандартный чемодан типа «дипломат». Можно перевозить до 2-х накопителей, под которые рассчитан модуль уничтожения. Активация производится нажатием потайной кнопки, радиобрелка, при попытке несанкционированного вскрытия (защита всего периметра). Питание только от автономного источника питания. Управление и защита базовых моделей может быть усилена за счет комплектации дополнительными модулями защиты, управления и оповещения

Контроль эффективности защиты

Аттестация по требованиям безопасности информации предшествует разрешению на обработку подлежащей защите информации и официально подтверждает эффективность совокупности применяемых на конкретном объекте информатизации мер и средств защиты информации.

Комплекс специальных аттестационных мероприятий называется аттестационной проверкой и включает в себя контроль эффективности защиты – проверку соответствия качественных и количественных показателей эффективности мер технической защиты установленным требованиям или нормам эффективности защиты информации. Показатель эффективности защиты информации представляет собой меру или характеристику для ее оценки.

Нормы эффективности защиты информации соответствуют показателям, установленным нормативными документами.

Под методом контроля эффективности защиты информации понимают порядок и правила применения расчетных и измерительных операций при решении задач контроля эффективности защиты. Виды контроля эффективности защиты делятся на:

– организационный контроль – проверка соответствия мероприятий по технической защите информации требованиям руководящих документов;

– технический контроль – контроль эффективности технической защиты информации, проводимый с использованием технических средств контроля.

Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что утечка информации с объекта невозможна, т.е. на объекте отсутствуют технические каналы утечки информации. Технический контроль состояния защиты информации в системах управления производствами, транспортом, связью, энергетикой, передачи финансовой и другой информации осуществляется в соответствии со специально разрабатываемыми программами и методиками контроля, согласованными с ФСТЭК России, владельцем объекта и ведомством по подчиненности объекта контроля.

По способу проведения и содержанию технический контроль эффективности технической защиты информации относится к наиболее сложным видам контроля и может быть:

• комплексным, когда проверяется возможная утечка информации по всем опасным каналам контролируемого объекта;

• целевым, когда проводится проверка по одному из интересующих каналов возможной утечки информации;

• выборочным, когда из всего перечня технических средств на объекте для проверки выбираются только те, которые по результатам предварительной оценки с наибольшей вероятностью имеют опасные каналы утечки защищаемой информации.

В зависимости от вида выполняемых операций методы технического контроля делятся на:
• инструментальные, когда контролируемые показатели определяются непосредственно по результатам измерения контрольно-измерительной аппаратурой;
• инструментально-расчетные, при которых контролируемые показатели определяются частично расчетным путем и частично измерением значений некоторых параметров физических полей аппаратными средствами;
• расчетные, при которых контролируемые показатели рассчитываются по методикам, содержащимся в руководящей справочной литературе.
С целью исключения утечки информации не допускается физическое подключение технических средств контроля, а также формирование тестовых режимов, запуск тестовых программ на средствах и информационных системах, находящихся в процессе обработки информации.
Технический контроль состояния защиты информации в автоматизированных системах управления различного назначения осуществляется в полном соответствии со специально разработанными программами и методиками контроля, согласованными с ФСТЭК России, владельцем объекта и ведомством, которому подчиняется объект контроля.
Целью технического контроля является получение объективной и достоверной информации о состоянии защиты объектов контроля и подтверждение того, что на объекте отсутствуют технические каналы утечки информации.

Контроль состояния защиты информации заключается в проверке соответствия организации и эффективности защиты информации установленным требованиям и/или нормам в области защиты информации.

Организационный контроль эффективности защиты информации – проверка полноты и обоснованности мероприятий по защите информации требованиям нормативных документов по защите информации.

Технический контроль эффективности защиты информации – контроль эффективности защиты информации, проводимый с использованием технических и программных средств контроля.

Средство контроля эффективности защиты информации – техническое, программное средство, вещество и/или материал, используемые для контроля эффективности защиты информации.

Технический контроль определяет действенность и надежность принятых мер защиты объектов информатизации от воздействия технических средств разведки.

Технический контроль предназначен для:

- выявления возможных каналов утечки конфиденциальной информации;
- проверки соответствия и эффективности принятых мер защиты нормативным требованиям;
- разработки рекомендаций по совершенствованию принятых защитных мероприятий.

Технический контроль проводится по отдельным физическим полям, создаваемых объектами информатизации, и состоит из:

• сбора исходных данных, характеризующих уязвимости объекта информатизации по отношению к воздействиям технической разведки;

• определения возможных типов и средств технической разведки;

• предварительного расчета зон разведдоступности;

• определения состава и подготовки к работе контрольно-измерительной аппаратуры;

• измерения нормируемых технических параметров защищаемого объекта по отдельным физическим полям на границе контролируемой зоны;

• определения эффективности принятых мер защиты и в отдельных случаях разработки необходимых мер усиления защиты.

Для проведения технического контроля требуется наличие норм эффективности защиты, методик (методов) проведения контроля и соответствующей контрольно-измерительной аппаратуры.

Все контролируемые нормативные показатели разделяются на информационные и технические [5].

Информационные показатели относятся к вероятности обнаружения, распознавания и измерения технических характеристик объектов с заданной точностью.

Техническими показателями эффективности принятых мер защиты являются количественные показатели, характеризующие энергетические, временные, частотные и пространственные характеристики информационных физических полей объекта. Примерами таких характеристик могут быть напряженности электрического и магнитного полей ПЭМИ средств вычислительной техники, уровень сигналов наводок в силовых и слаботочных линиях за пределами контролируемой зоны, уровни акустических сигналов за пределами ограждающих конструкций и т.д. Нормой эффективности принятых мер защиты считается максимально допустимое значение контролируемых параметров на границе контролируемой зоны (в местах возможного нахождения технических средств разведки).

Инструментально-расчетные методы применяются тогда, когда комплект контрольно-измерительной аппаратуры не позволяет получить сразу конечный результат или не обладает достаточной чувствительностью.

Расчетные методы технического контроля применяются в случае отсутствия необходимой контрольно-измерительной аппаратуры, а также при необходимости быстрого получения предварительных ориентировочных результатов о зонах разведдоступности, например, перед инструментальными аттестациями рабочих мест.

При проведении технического контроля требуется контрольно-измерительная аппаратура, которая в большинстве случаев обеспечивает получение объективных характеристик контролируемых параметров или исходных данных для получения инструментально-расчетных характеристик. Контрольно-измерительная аппаратура по возможности должна быть портативной, что важно для аттестующих организаций, иметь достаточную чувствительность, соответствующую чувствительности аппаратуры разведки, быть надежной в эксплуатации.

Как правило, при проведении контроля расчетно-инструментальным методом проводится большое число измерений на дискретных интервалах и соответственно большое число сложных расчетов, что приводит к быстрой утомляемости испытателей. Поэтому современная тенденция развития контрольно-измерительной аппаратуры заключается в разработке для целей контроля программно-аппаратных комплексов, обеспечивающих полную автоматизацию измерения параметров физических полей и расчета нормируемых показателей защищенности объекта.

По результатам контроля состояния и эффективности защиты информации составляется заключение с приложением протоколов контроля.

6.2. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ

Типовой объект вычислительной техники (ВТ) – это средство вычислительной техники (СВТ) в типовой комплектации (например ПЭВМ в составе – системный блок, монитор, клавиатура, мышь, принтер), размещенное в отведенном для него помещении. Для проведения специальных исследований типового объекта ВТ на ПЭМИ необходимы следующие документальные данные по объекту:

- предписание на эксплуатацию СВТ из состава объекта ВТ;
- план-схема КЗ объекта;
- схема расположения объекта ВТ внутри контролируемой зоны (КЗ);
- схема расположения основных технических средств и систем (ОТСС) и вспомогательных средств и систем (ВТСС) на объекте;
- схема размещения технических средств защиты информации (ТСЗИ) от утечки за счет ПЭМИ (если они установлены на объекте);
- сертификаты соответствия ТСЗИ;
- акт категорирования объекта ВТ.

Из анализа исходных данных должно быть установлено:

• заявленная категория объекта ВТ;

• состав ОТСС объекта (например ПЭВМ в типовой комплектации);

• ближайшие к объекту ВТ места возможного размещения стационарных, возимых, носимых средств разведки ПЭМИН;

• измеренные на объекте расстояния от ОТСС объекта ВТ до мест возможного размещения средств разведки ПЭМИН (Rкз, м);

• величины предельных расстояний (R2) от ОТСС объекта ВТ до мест возможного размещения средств разведки (из предписания на эксплуатацию СВТ);

• опасные режимы работы СВТ (обработки защищаемой информации);

Настоящая методика определяет виды контроля защищенности от разведки побочных электромагнитных излучений и наводок (РПЭМИН), порядок и способы его проведения на объектах информатизации [51].

Контроль защищенности осуществляется с целью предупреждения возможности получения аппаратурой РПЭМИН информации, циркулирующей на защищаемом от РПЭМИН объекте, и оценки эффективности мероприятий по противодействию РПЭМИН.

Контроль защищенности объекта предполагает проверку всех основных технических средств, средств защиты и вспомогательных технических средств, содержащих в своем составе генераторы, способные создавать электромагнитные излучения с модуляцией информационным сигналом.

Основные и вспомогательные технические средства в дальнейшем для краткости будут именоваться как «технические средства». Устройство считается защищенным, если на границе КЗ отношение «информативный сигнал/помеха» не превышает предельно допустимого значения δ как для побочных излучений, так и для наводок в цепях питания, заземления, линиях связи и т. д.. Объект считается защищенным, если защищено каждое устройство объекта.

Различается два вида контроля защищенности объектов от РПЭМИН:

– аттестационный контроль,

– эксплуатационный контроль.

Аттестационный контроль проводится при вводе объекта в эксплуатацию и после его реконструкции или модернизации, а эксплуатационный – в процессе эксплуатации объекта.

При проведении контроля защищенности проверяются параметры, которые характеризуют защищенность технических средств или объекта в целом в соответствии с установленной категорией объекта защиты.

Оценка защитных мероприятий электронных средств обработки информации состоит в проверке следующих возможных технических каналов утечки:

• побочных электромагнитных излучений информативного сигнала от технических средств и линий передачи информации;

• наводок информативного сигнала, обрабатываемого техническими средствами, на посторонние провода и линии, на цепи заземления и электропитания, выходящие за пределы контролируемой зоны;

• модуляции тока потребления технических средств информативными сигналами;

• радиоизлучений или электрических сигналов от возможно внедренных закладочных устройств в технические средства и выделенные помещения.

Технический контроль выполнения норм защиты информации от утечки за счет ПЭМИН по каждому перечисленному каналу утечки проводится для всех электронных устройств объекта ВТ.

Аттестационный контроль

Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту.

В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, контрольную аппаратуру и тестовые средства, приводящие к минимальной погрешности результатов испытаний и позволяющие воспроизвести эти результаты.

Аттестационный контроль состоит из организационной и инструментальной частей. В организационной части аттестационного контроля необходимо [51]:

• изучить план-схему местности, границы контролируемой зоны объекта и места возможного ведения разведки ПЭМИН с указанием средств (носимых, возимых, стационарных);

• уточнить категорию объекта информатизации, особенности его расположения, характер циркулирующей на объекте информации, в том числе и речевой, время её обработки техническими средствами;

• зафиксировать фактический состав основных и вспомогательных технических средств и средств защиты на объекте и поэкземплярно указать в перечне технических средств;

• уточнить план реального размещения технических средств на объекте и указать на нем кратчайшие расстояния от каждого технического средства и средства защиты до мест возможного ведения РПЭМИН;
• проверить визуально в доступных местах с возможным привлечением к этой работе штатных сотрудников организации выполнение монтажа коммуникаций, устройство заземления и электропитания на объекте защиты на соответствие проекту и СТР;
• проверить выполнение требований эксплуатационной документации по размещению и установке на объекте каждого технического средства и средства защиты с учетом расстояний до мест возможного ведения РПЭМИН;
• проверить обоснованность применения средств активной защиты (САЗ) и выполнение рекомендаций по их размещению;
• проверить наличие приемо-сдаточных документов и в доступных местах проверить правильность монтажа экранирующих средств на соответствие требованиям эксплуатационной документации и СТР.

Проверке подлежат следующие исходные данные и документация [51]:
• техническое задание на объект информатизации или приказ о начале работ по защите информации;
• технический паспорт на объект информатизации;
• приемо-сдаточная документация на объект информатизации;
• акты категорирования технических средств и систем;
• акт классификации АС по требованиям защиты информации;

• состав технических и программных средств, входящих в АС;
• планы размещения основных и вспомогательных технических средств и систем;
• состав и схемы размещения средств защиты информации;
• план контролируемой зоны учреждения;
• схемы прокладки линий передачи данных;
• схемы и характеристики систем электропитания и заземления объекта информатизации;
• описание технологического процесса обработки информации в АС;
• технологические инструкции пользователям АС и администратору безопасности информации;
• инструкции по эксплуатации средств защиты информации;
• предписания на эксплуатацию технических средств и систем;
• протоколы специальных исследований технических средств и систем;
• акты или заключения о специальной проверке выделенных помещений и технических средств;
• сертификаты соответствия требованиям безопасности информации на средства и системы обработки и передачи информации, используемые средства защиты информации;
• данные по уровню подготовки кадров, обеспечивающих защиту информации;
• данные о техническом обеспечении средствами контроля эффективности защиты информации и их метрологической поверке;
• нормативная и методическая документация по защите информации и контролю ее эффективности.

В инструментальной части аттестационного контроля необходимо провести следующие работы:

• измерить или рассчитать для технических средств значения схемно-конструктивных параметров, характеризующих их защищенность от РПЭМИН (перечень этих параметров и методики их измерения указывается в эксплуатационной документации на эти технические средства);

• определить реальные размеры зоны R2 технических средств, установленных на объекте, по соответствующим методикам из сборника методик инструментального контроля в следующих случаях:

−для технических средств с неизвестными размерами зоны R2,

−для технических средств, эксплуатируемых на объектах, если размеры зоны R2 этих технических средств соизмеримы с расстоянием до мест возможного ведения РПЭМИ;

• проверить работоспособность всех средств защиты, включая САЗ, по методикам, приведенным в эксплуатационной документации на эти средства;

• определить эффективность применения САЗ для защиты АСУ и ЭВТ в соответствии с «Дополнением к Методике контроля защищенности объектов ЭВТ».

В случае положительных результатов предыдущих измерений формируются исходные данные для проведения эксплуатационного контроля защищенности от РПЭМИН технических средств АСУ и ЭВТ. С этой целью при отключенных средствах активной защиты измеряется уровень побочных электромагнитных излучений от технических средств АСУ и ЭВТ на двух-трех частотах с максимальным значением зоны R2 (реперные точки).

Частоты реперных точек, измеренные значения напряженности электрических и магнитных полей, типы и расположение антенн, а также другие условия проведения измерений фиксируются и используются при эксплуатационном контроле защищенности от РПЭМИН технических средств АСУ и ЭВТ.

По результатам аттестационного контроля для данного объекта оформляется Аттестат соответствия.

Технический контроль проводится путем запуска на ЭВМ специальной тестовой программы типа «Зебра», замера аппаратурой контроля излучаемых ЭВМ сигналов и последующим сравнением их с нормируемыми значениями.

Порядок инструментального контроля ПЭМИН:

• Измерение уровней ПЭМИ и наводок информативных сигналов:

– электрической составляющей;

– магнитной составляющей;

– индуктивной составляющей наводок в симметричных и несимметричных линиях как гальванически связанных, так и не связанных с проверяемым устройством, но имеющих выход за границы контролируемой зоны (если не выполняются требования предписания на эксплуатацию по зоне r1);

– измерение реального затухания в опасных направлениях на границе контролируемой зоны;

– измерение параметров применяемых средств защиты (фильтры в отходящих линиях, системы активного зашумления и т.д.).

• Расчет выполнения норм и оценка защищенности.

• Оформление протоколов по результатам проведенных проверок.

Контроль проводится для устройств, обрабатывающих или передающих информацию, представленную в последовательном коде. Измерения проводятся выборочно для частот, которые при специсследованиях дали максимальные значения зоны R2. Аналогично проводятся измерения эффективности систем активной защиты.

Если значения зоны R2 близки или превышают расстояние до границы контролируемой зоны (охраняемой территории), проводятся измерения реального затухания в опасном направлении, после чего производится расчет значений на границе контролируемой зоны. Измерения реального затухания проводится отдельно для каждого значения частоты сигнала. Реальное затухание исследуемой линии в опасном направлении определяется по приведенной ниже схеме (рис. 6.1).

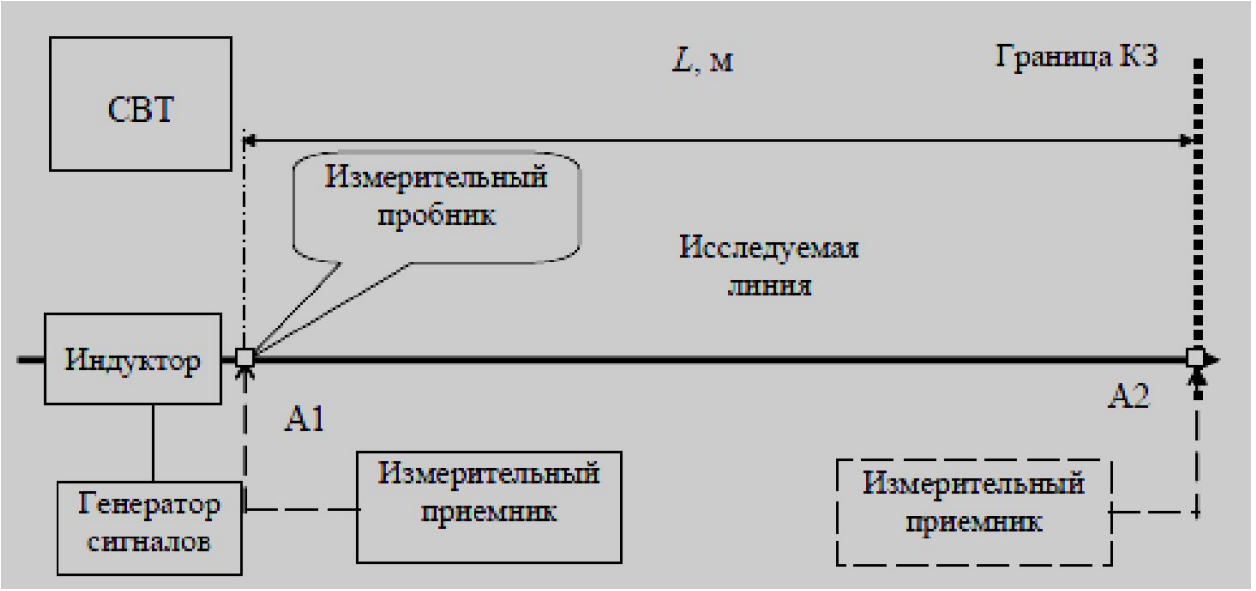


Рис. 6.1. Схема измерения реального затухания в линии

На каждой j-й частоте в исследуемую линию вблизи СВТ подают сигнал от вспомогательного источника и измеряют напряжение этого сигнала пробником напряжения в двух точках: вблизи СВТ в точке А1 (напряжение U_{1uj}) и на границе контролируемой зоны А2 (напряжение U2uj). Коэффициент затухания вычисляют по формуле:

$$K_{лj} = \frac{U_{1uj}}{U_{2uj}}$$

При помощи измерительного приемника можно получить данные для расчета реального коэффициента затухания по ПЭМИ.

Для распределенных систем (например, локальных вычислительных сетей) проводятся исследования характеристик линий, по которым передается информации, по специальной методике расчета контролируемой зоны от экранированных кабелей связи АСУ и ЭВМ.

Применение неэкранированных кабелей для связи ЭВМ не допускается.

Эксплуатационный контроль

Эксплуатационный контроль защищенности от РПЭМИН на объекте предназначен для проверки выполнения правил эксплуатации и технического состояния каждого технического средства и оценки соответствия текущего состояния защищенности объекта и зафиксированного при аттестационном контроле.

Эксплуатационный контроль состоит из двух частей: организационной и инструментальной

При выполнении организационной части эксплуатационного контроля необходимо [51]:

• проверить наличие Аттестата соответствия, журнала учета проведения эксплуатационного контроля, перечня и плана размещения технических средств на объекте;

• уточнить места возможного ведения РПЭМИ и при необходимости внести изменения в план-схему контролируемой зоны;

• проверить поэкземплярно соответствие реального состава технических средств и состава, указанного в перечне технических средств на объекте, а также регулярность проведения их эксплуатационного контроля по журналу учета проведения эксплуатационного контроля;

• сверить соответствие действительного расположения технических средств и средств защиты расположению, приведенному в плане размещения технических средств на объекте и в доступных местах выполнение требований по монтажу каждого технического средства и его коммуникаций, приведенных в эксплуатационной документации и СТР;

• проверить соответствие сведений о степени секретности обрабатываемой информации и установленной категории объекта совместно с представителем режимной службы предприятия.

В инструментальной части эксплуатационного контроля необходимо:

• для средств защиты и технических средств произвести измерения параметров защищенности от РПЭМИ, которые были определены на этапе аттестационного контроля;

• для технических средств АСУ и ЭВТ измерить напряженность электрических и магнитных полей в реперных точках и результаты измерений сравнить с результатами аттестационного контроля;

• проверить работоспособность средств активной защиты согласно указаниям в эксплуатационной документации на эти средства.

В случае положительных результатов эксплуатационный контроль объекта считается завершенным, о чем составляется Акт проведения эксплуатационного контроля на объекте. При выявлении недостатков последние устраняются и контроль повторяется.

При проведении эксплуатационного контроля на объекте допускается проведение работ выборочно относительно отдельных технических средств.

6.3. Методы испытаний

Общие положения [51]

1.1. Испытания ПЭВМ и периферийных устройств на соответствие нормам ПЭМИН проводят в соответствии с требованиями ГОСТ 51320-99.

1.2. ПЭВМ испытывают в составе базового комплекта (по ГОСТ 27201) и всех периферийных устройств, предусмотренных технической документацией на ПЭВМ.

Периферийное устройство испытывают совместно с базовым комплектом ПЭВМ, удовлетворяющим нормам ПЭМИН, установленным для ПЭВМ конкретного класса.

1.3. Если ПЭВМ или периферийное устройство, испытываемое совместно с базовым комплектом ПЭВМ, содержит идентичные технические средства или идентичные модули, то допускается проводить испытания при наличии хотя бы одного технического средства (модуля) каждого типа.

1.4. При испытаниях периферийных устройств (кроме сертификационных) допускается применение имитатора базового комплекта ПЭВМ при условии, что имитатор имеет электрические характеристики реального базового комплекта в части высокочастотных сигналов и импедансов и не влияет на параметры электромагнитной совместимости.

1.5. Значение напряжения (напряженности поля) посторонних радиопомех на каждой частоте измерений, полученное при выключенном испытуемом устройстве, должно быть не менее чем на 10 дБ ниже нормируемого значения на данной частоте. Допускается проводить измерения при более высоком уровне посторонних радиопомех, если суммарное значение полей, создаваемых испытуемым устройством, и посторонних радиопомех не превышает нормы.

1.6. При испытаниях расположение и электрическое соединение технических средств, входящих в состав испытуемого устройства, должны соответствовать условиям, приведенным в технической документации на ПЭВМ. Если расположение технических средств и соединительных кабелей не указано, то выбирают такое, которое соответствует типовому применению и при котором создаваемые испытуемым устройством ПЭМИН имеют максимальное значение.

1.7. При испытаниях должны использоваться соединительные кабели, требования к которым указаны в технической документации на ПЭВМ или периферийное устройство. Если допустимы различные длины кабелей, то выбирают такие, при которых создаваемые испытуемым устройством ПЭМИН имеют максимальное значение. При испытаниях допускается применять экранированные или специальные кабели для подавления ПЭМИН в тех случаях, когда это указано в технической документации на ПЭВМ или периферийное устройство.

1.8. Излишне длинные кабели сворачивают в виде плоских петель размером 30–40 см приблизительно в середине кабеля.

1.9. Если изменения режима работы ПЭВМ (периферийного устройства) оказывают влияние на уровень ПЭМИН, то испытания проводят при режиме, соответствующем максимальному уровню ПЭМИН.

1.10. Расположение технических средств испытуемого устройства и соединительных кабелей, а также режимы работы ПЭВМ должны быть указаны в протоколе испытаний.

Аппаратура и оборудование [51]

2.1. Измеритель ПЭМИН с квазипиковым детектором и детектором средних значений по ГОСТ Р-51319-99.

2.2. V – образный эквивалент сети по ГОСТ Р-51319-99, тип 5 – в полосе частот от 0,15 до 100 МГц.

2.3. Измерительные антенны – по ГОСТ Р-51319-99 . При измерении напряженности поля ПЭМИН в полосе частот от 30 до 1000 МГц используют линейный симметричный вибратор, в полосе частот от 0,15 до 30 МГц – штыревую антенну. Допускается использование биконических антенн.

2.4. Металлический лист для измерения напряжения ПЭМИН по ГОСТ 51320-99.

2.5. Набор металлических листов общей площадью, обеспечивающей размещение испытуемого комплекта ПЭВМ и измерительной аппаратуры для измерения напряженности поля ПЭМИН по п. 4.3. Допускается использовать перфорированные металлические листы или сетку с размером перфорации или ячеек не более 0,02×0,02 м.

2.6. Столы и поворотные платформы для размещения испытуемого устройства и измерительных приборов должны быть изготовлены из изоляционного материала.

*Измерения напряжения ПЭМИН [*51]

3.1. Размеры помещения для проведения измерений должны быть такими, чтобы расстояние от испытуемого устройства (включая все технические средства и соединительные кабели, входящие в состав испытуемого устройства) до остальных металлических предметов и токонесущих поверхностей (кроме металлического листа) было не менее 0,8 м.

3.2. Измерения проводят в экранированном помещении. Эффективность его экранирования и фильтрации сети электропитания в помещении должна быть такой, чтобы обеспечивать выполнение требований п. 1.5. При выполнении требований п. 1.5 допускается проведение испытаний в неэкранированном помещении. Расположение аппаратуры при измерении напряжений полей, создаваемых ПЭВМ показано на рис. 6.2.

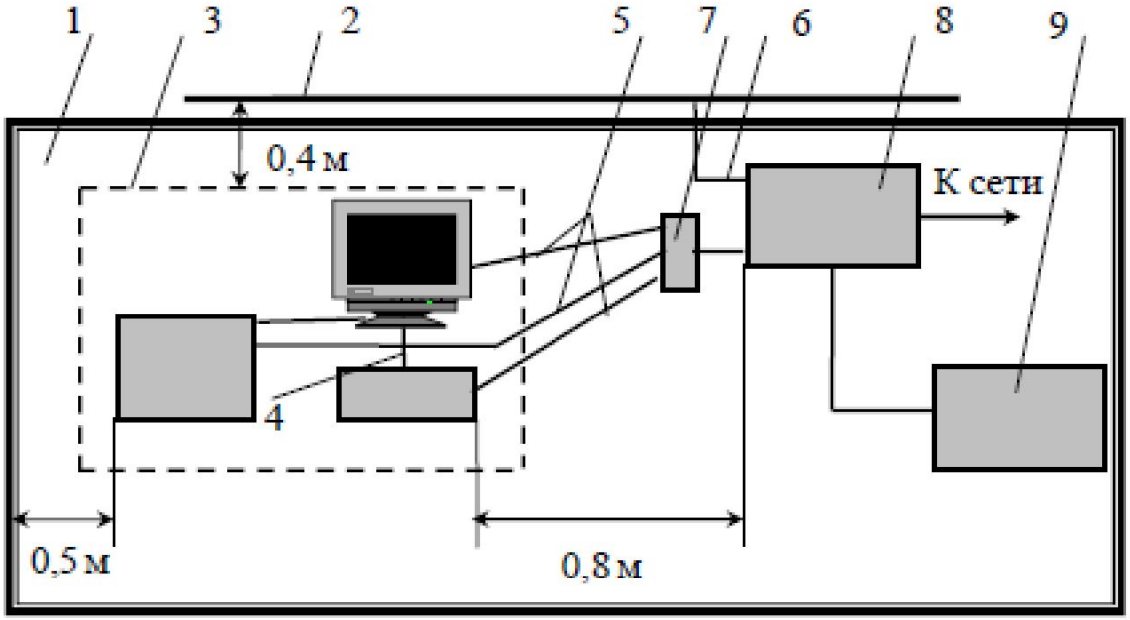


Рис. 6.2. Расположение аппаратуры при измерении напряжений полей, создаваемых ПЭВМ: 1 – стол; 2 – вертикально расположенный металлический лист;
3 – испытуемое устройство; 4 – межблочные соединения; 5 – сетевые кабели;
6 – шина заземления; 7 – штепсельная колодка; 8 – эквивалент сети;
9 – измеритель ПЭМИН

На столе, установленном у вертикально расположенной токопроводящей поверхности (металлического листа размером не менее 2×2 м или стены экранированного помещения), размещают ПЭВМ и эквивалент сети. Испытуемое устройство размещают на расстоянии 0,8 м от эквивалента сети и 0,4 м от металлического листа.

3.3. Эквивалент сети устанавливают непосредственно около токопроводящей поверхности и его корпус соединяют с этой поверхностью шиной шириной не менее 0,005 м и минимально возможной длиной, но не более 0,4 м.

3.4. Если ПЭВМ имеет единственный сетевой кабель, то он подключается к эквиваленту сети. Если ПЭВМ имеет более одного сетевого кабеля, то все они подключаются к штепсельной колодке, расположенной в непосредственной близости от эквивалента сети. Если длина сетевых кабелей превышает 1 м, то оставшиеся части кабелей сворачивают в соответствии с требованиями п. 1.8.

3.5. Расположение испытуемого устройства и измерительной аппаратуры при измерении напряжения ПЭМИН, создаваемых периферийным устройством, показано на рис. 6.3. Периферийное устройство размещают на расстоянии 0,8 м от эквивалента сети и 0,4 м от металлического листа. Сетевой кабель периферийного устройства подключают к эквиваленту сети. Сетевые кабели других технических средств, входящих в испытуемое устройство, подключают к сети электропитания.

3.6. Если по требованиям электробезопасности испытуемое устройство имеет специальные зажимы для подключения заземляющего провода, то заземляющий провод длиной 1 м прокладывают параллельно сетевому кабелю на расстоянии не более 0,1 м и подключают к зажиму заземления металлического листа.

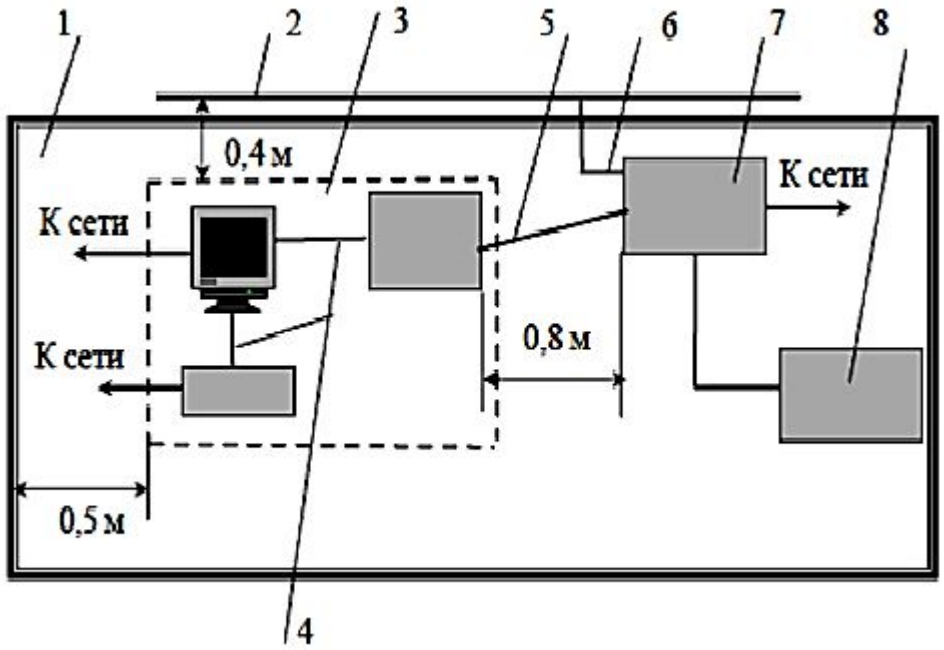


Рис. 6.3. Расположение аппаратуры при измерении напряжений полей, создаваемых периферийным устройством: 1 – стол; 2 – вертикально расположенный металлический лист; 3 – испытуемое устройство; 4 – межблочные соединения; 5 – сетевой кабель периферийного устройства; 6 – шина заземления; 7 – эквивалент сети; 8 – измеритель поля

3.7. При испытаниях проводят измерение квазипикового несимметричного напряжения ПЭМИН. За результат измерений на каждой частоте принимают наибольшее из значений, полученных для двух проводов.

3.8. Перед началом измерений, перестраивая измеритель ПЭМИН в пределах полосы нормирования, фиксируют частоты, на которых наблюдаются максимумы напряжения ПЭМИН. Измерения проводят на этих частотах. При большом числе таких частот допускается сократить их количество, но не менее чем до 10, выбрав те, на которых значения напряжения ПЭМИН наибольшие. Измерения напряженности поля [51]

4.1. Измерения напряженности поля, создаваемых ПЭВМ или периферийным устройством, проводят на измерительной площадке, соответствующей требованиям ГОСТ 51320-99. Испытуемое устройство размещают на поворотной платформе на высоте 0,8 м над металлическим листом (рис. 6.4).

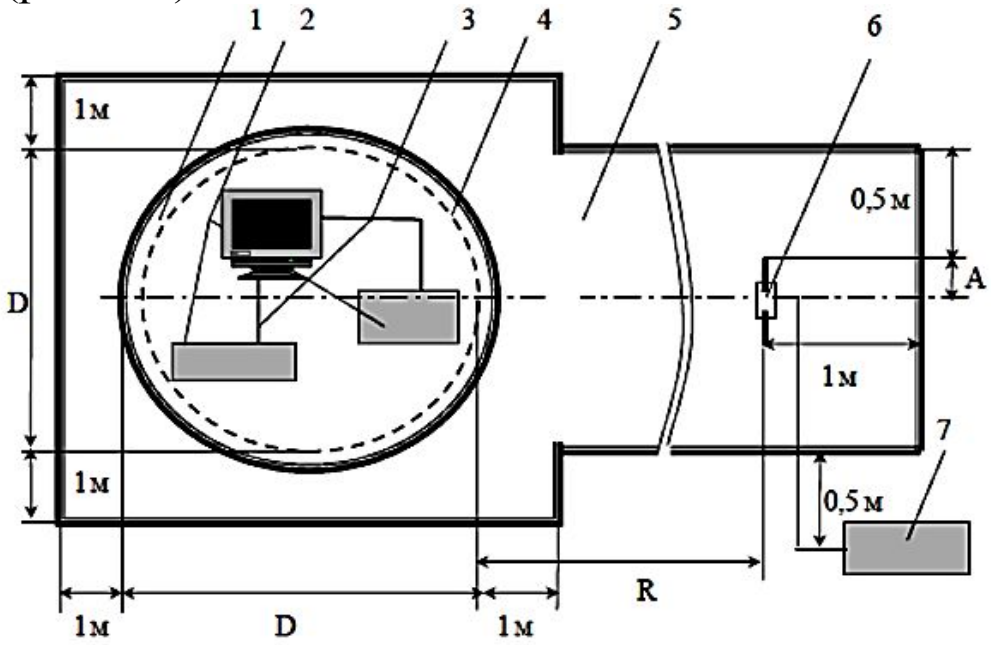


Рис. 6.4. Расположение аппаратуры при измерениях напряженности поля ПЭМИН, создаваемых испытуемым устройством: 1 – поворотная платформа; 2 – испытуемое устройство; 3 – межблочные соединения; 4 – граница испытуемого устройства; 5 – металлический лист; 6 – измерительная антенна; 7 – измеритель ПЭМИН; D – максимальный размер испытуемого устройства; R измерительное расстояние; A – максимальная длина антенны

4.2. Площадь под испытуемым устройством, между ним и измерительной антенной должна быть покрыта металлическими листами. Металлические листы должны выступать не менее чем на 1 м за границу испытуемого устройства с одного конца и не менее чем на 1 м за измерительную антенну с другого конца. Границу испытуемого устройства представляет воображаемая линия, описывающая простую геометрическую фигуру, заключающую в себе технические средства испытуемого устройства. Все соединительные кабели должны быть включены в пределы этой геометрической фигуры.

4.3. При измерении напряженности поля ПЭМИН в полосе частот от 30 до 100 МГц используют эквивалент сети. Сетевой кабель испытуемого устройства прокладывают кратчайшим путем вертикально вниз вдоль оси вращения поворотной платформы.

4.4. Расстояние R от проекции центра измерительной антенны на землю до границы испытуемого устройства должно соответствовать требованиям, указанным в Методике измерения побочных информативных сигналов, излучаемых техническими средствами АСУ и ЭВМ, но не менее 1 м.

4.5. При измерении напряженности поля ПЭМИН нижнюю точку штыревой антенны устанавливают на высоте 1 м, центр симметрии линейного симметричного вибратора – на высоте h, определяемой путем перемещения приемной антенны по вертикали вблизи исследуемого оборудования до положения, соответствующего максимуму принимаемого сигнала.

В полосе частот от 0,15 до 30 МГц определяют наибольшее квазипиковое значение вертикальной составляющей электрического поля ПЭМИН на частоте измерений при повороте платформы с испытуемым устройством. В полосе частот от 30 до 1000 МГц определяют наибольшие квазипиковые значения горизонтальной и вертикальной составляющих электрического поля ПЭМИН на частоте измерений при повороте платформы с испытуемым устройством. За результат измерений на каждой частоте принимают наибольшее из полученных значений.

6.4. Порядок проведения контроля защищенности АС от НСД

В информационных системах и в автоматизированных системах обработки информации проверяются [51]:

• наличие сведений, составляющих государственную или служебную тайну, циркулирующих в средствах обработки информации и помещениях в соответствии с принятой на объекте технологией обработки информации;

• правильность классификации автоматизированных систем в зависимости от степени секретности обрабатываемой информации;

• наличие сертификатов на средства защиты информации;

• организация и фактическое состояние доступа обслуживающего и эксплуатирующего персонала к защищаемым информационным ресурсам, наличие и качество организационно-распорядительных документов по допуску персонала к защищаемым ресурсам, организация учета, хранения и обращения с конфиденциальными носителями информации;

• состояние учета всех технических и программных средств отечественного и иностранного производства, участвующих в обработке защищаемой информации, наличие и правильность оформления документов по специальным исследованиям и проверкам технических средств информатизации, в том числе на наличие недекларированных возможностей программного обеспечения;

• обоснованность и полнота выполнения организационных и технических мер по защите информации;

• наличие, правильность установки и порядка эксплуатации средств защиты от несанкционированного доступа к информации;
• выполнение требований по технической защите информации при подключении автоматизированных систем к внешним информационным системам общего пользования.

В ходе проверки анализируется система информационного обеспечения объекта:
• используемые типы ЭВМ и операционных систем;
• виды и объемы баз данных;
• распределение закрытой и открытой информации по рабочим местам пользователей;
• порядок доступа к информации, количество уровней разграничения доступа;
• порядок поддержания целостности информации и резервного копирования.

Осуществляется проверка эффективности реально установленных механизмов защиты информации требованиям соответствующего класса защиты информации от НСД.

Структура систем защиты средств и систем информатизации от несанкционированного доступа должна включать в себя четыре подсистемы:

1. Подсистему управления доступом, которая осуществляет персонализацию действий в системе на основе идентификаторов и профилей пользователей (паспортов) отдельно для каждого уровня, а также разграничение доступа на их основе

2. Подсистему учета и контроля, накапливающую и в дальнейшем обрабатывающую в журнале учета статистические сведения о доступе пользователей к различным ресурсам сети и возможных попытках НСД.
3. Криптографическую подсистему (для информации с грифом «СС» и выше) для шифрования конфиденциальной информации, записываемой на магнитные носители и передаваемой по линиям связи. Вся информация, не подлежащая открытому распространению, шифруется непосредственно в ее источнике (рабочей станции, терминале, базе данных) и передается по открытым линиям связи в зашифрованном виде.
4. Подсистему обеспечения целостности, которая осуществляет контроль целостности средств операционных систем, прикладных программ и баз данных, а также средств защиты информации.

6.5. Методы контроля побочных электромагнитных излучений генераторов технических средств

Модуляция информационным речевым сигналом высокочастотных колебаний у генераторов технических средств может возникать из-за изменения индуктивностей и емкостей их задающих контуров под воздействием акустического поля. Перехват модулированных сигналов по каналу ПЭМИ с последующей демодуляцией приводит к утечке речевой информации.

Для исследования влияния акустического поля на техническое средство необходимо собрать установку по схеме рис. [52] и выполнить следующие действия.

• Установить измерительную антенну измерительного прибора на расстоянии d = 1м от исследуемого ВТСС на наиболее опасном с точки зрения перехвата сигнала направлении.

• Включить исследуемое ВТСС в штатный режим работы.

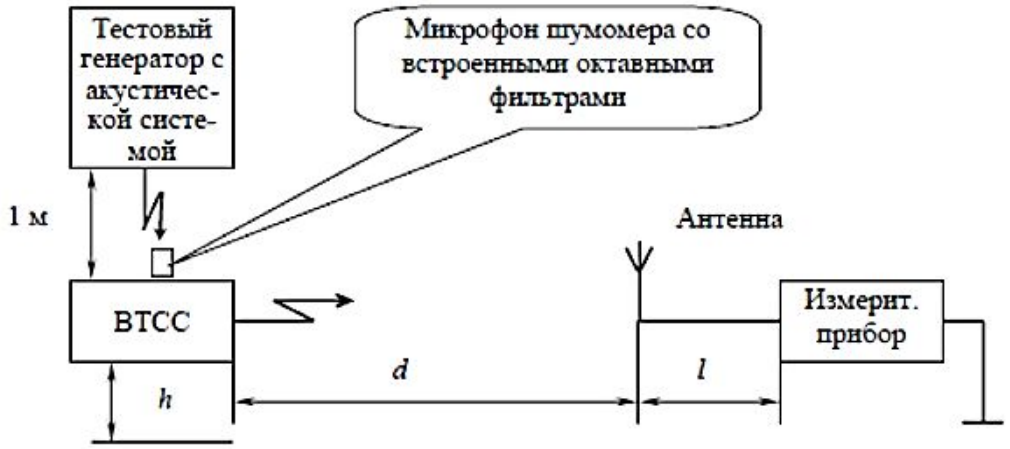


Рис. 6.5. Измерение побочных электромагнитных излучений ВТСС

• Перестройкой измерительного приемника в исследуемом диапазоне частот, обнаружить сигналы, создаваемые генератором ВТСС.

• Настроить измерительный приемник на частоту наиболее мощного обнаруженного сигнала, которая, как правило, совпадает с частотой генератора. Полоса пропускания измерительного приемника устанавливается максимально близкой к ширине спектра сигнала генератора ВТСС.

• Акустическую систему излучателя генератора тестовых акустических сигналов разместить на расстоянии 1 м от исследуемого технического средства и направить в его сторону.

• В месте размещения ВТСС на расстоянии 1 м от излучателя акустической системы установить измерительный микрофон шумомера со встроенными октавными фильтрами.

• Включить акустическую систему и настроить ее на частоту f1 = 1000 Гц. Установить необходимый уровень звукового давления: 80 дБ при наличии средств звукоусиления, 72 дБ – при их отсутствии.

Если акустоэлектрические преобразования обнаружены, то необходимо:

• Провести измерение уровней напряженности электрического (Еи) и магнитного (ρНи) полей, создаваемых генератором, и ширину спектра сигнала (ΔFc) на частоте генератора.

• На частоте генератора ВТСС произвести измерения уровней напряженностей помех Епj и ρНпj . Измерения проводятся без изменения режима работы приемника.

• Произвести расчет значений уровня информативного сигнала Ес и ρНс по формулам [52]:

$$E_c = \sqrt{(\xi_и E_и)^2 - (E_п/\xi_и)^2}, \text{ мкВ/м}, \qquad (6.1)$$

$$\rho H_c = \sqrt{(\xi_и \rho H_и)^2 - (\rho H_п/\xi_и)^2}, \text{ мкВ/м}, \qquad (6.2)$$

где Ес ,ρНс– уровни информативного сигнала, мкВ/м; ξа – погрешность входного преобразователя (погрешность коэффициента калибровки антенны), дБ;

$$\xi_и = 1 + \sqrt{(10^{0,05\xi_а} - 1)^2 + (10^{0,05\xi_{ип}} - 1)^2}$$

– относительная среднеквадратичная ошибка измерения (в разах); ξип – погрешность измерительного приемника, дБ; ρ=377 Ом – волновое сопротивление неограниченной среды (для вакуума ρ=120π =377Ом).

• Через волновое сопротивление измерения напряженности магнитного поля из мкА/м пересчитываются в соответствующую напряженность электрического поля, измеряемую в мкВ/м.

• Измерить расстояние r в метрах от ВТСС до ближайшего места возможного расположения средств технической разведки за пределами контролируемой зоны. Рассчитать значение коэффициента затухания Vr по следующим формулам.

Если частота обнаруженного сигнала генератора ниже частоты f ≤ 47,75МГц, то коэффициент затухания рассчитывается по формуле:

$$V_r = \begin{cases} r^3, \text{ если } r \le \dfrac{47{,}75}{f}; \\ \dfrac{47{,}75}{f}, \text{ если } r \le \dfrac{47{,}75}{f} < r \le \dfrac{1800}{f}; \\ \dfrac{8{,}59 \cdot 10^4 r}{f^2}, \text{ если } r > \dfrac{1800}{f}, \end{cases} \quad (6.3)$$

где f – частота измеренного сигнала, МГц.

Если частота обнаруженного сигнала генератора удовлетворяет условию 47,75 МГц < f ≤1800МГц, то коэффициент затухания определяется по формуле

$$V_r = \begin{cases} r^2, \text{ если } r \le \dfrac{1800}{f}; \\ \dfrac{1800r}{f}, \text{ если } r > \dfrac{1800}{f}. \end{cases} \quad (6.4)$$

Если частота обнаруженного сигнала генератора удовлетворяет условию f >1800МГц, то коэффициент затухания определяется по формуле:

$$V_r = r. \quad (6.5)$$

Рассчитать действующую высоту антенны h_a по формуле:

$$h_a = \frac{2}{10^{\frac{K_a^*}{20}}} \approx \frac{63 \cdot 10^{\frac{G_a^*}{20}}}{f}, \text{ м}, \qquad (6.6)$$

где K^*_a – антенный коэффициент (логарифмический), дБ относительно 1/м; f – частота сигнала, МГц; $G^*_a = 10 \lg Ga$, дБ – коэффициент усиления антенны в относительных единицах, определяемый через коэффициент усиления антенны Ga , эффективную площадь антенны Sa и длину волны сигнала λ как $G_a = 4\pi S_a / \lambda^2$.

• Рассчитать уровень шумов на входе радиоприемного устройства по формуле:

$$U_ш = \sqrt{\left(\frac{U_ш^{*2}}{\Delta F_п^* \cdot 10^{\frac{q^*}{10}}} + \frac{10^{\frac{E_a^* - K_a^*}{10}}}{\Delta F_a} \right) \Delta F_c} \qquad (6.7)$$

где $U^*_ш$ – чувствительность радиоприемного устройства, мкВ; ΔF*п– полоса пропускания тракта приемного устройства, при котором измерялась чувствительность, Гц; q*– отношение сигнал/шум, при котором измерялась чувствительность приемного устройства, дБ; E*a – чувствительность антенны, измеренная при q* = 1 и полосе пропускания приемника ΔF , дБ относительно мкВ/м; K*a – антенный коэффициент (логарифмический), дБ относительно 1/м; ΔFc – ширина спектра сигнала генератора, Гц; ΔFa – полоса пропускания, при которой производилось измерение чувствительности антенны.

Рассчитать отношение сигнал/шум на входе разведывательного приемника по формулам:

для электрического поля $$q_E = (E_c h_д)/(2V_r U_ш);$$

для магнитного поля $$q_H = (\rho H_c h_д)/(2V_r U_ш),$$

где Ес ,ρНс– уровни информативного сигнала, мкВ/м; Uш – напряжение шумов на входе разведывательного приемника, мкВ; hд – действующая длина антенны разведывательного приемника, м.

Рассчитать предельно допустимое значение сигнал/шум по формуле:

$$\delta = (3{,}2 + \Phi^{-1}(x)P_п)/(3{,}16 - \Phi^{-1}(x)P_п), \qquad (6.10)$$

где $$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} \exp(-\frac{t^2}{2})dt$$ – интеграл вероятности; Ф−1(х) – функция обратная Ф(х); Рп– предельно допустимое значение вероятности правильного обнаружения сигнала средствами разведки.

Сравнить рассчитанные значения сигнал/шум qE и qH с предельно допустимым δ . При выполнении условия q ≤ δ считается, что перехват ПЭМИ ВТСС на частотах работы высокочастотного генератора средствами разведки невозможен.

В случае, если это неравенство не выполняется, то необходимо определить реальный коэффициент затухания сигнала Vr∗ при его распространении от места проведения измерения до места возможного нахождения средств технической разведки на расстоянии r. Для этого необходимо [52]:

• вблизи ВТСС установить вспомогательный излучатель, состоящий из генератора синусоидального сигнала и излучающей электрической антенны, которую необходимо поместить вместо ВТСС;

• настроить генератор на частоту генерации ВТСС;

• установить измерительную антенну приемника на расстоянии d = 1 м от излучающей антенны вспомогательного излучателя, приемник настроить на частоту генератора, причем, полосы пропускания генератора и приемника должны быть приблизительно равны;

• измерить уровень напряженности электрического поля от вспомогательного излучателя;

• установить измерительную антенну в месте предполагаемого размещения средств разведки и измерить расстояние r;

• измерить уровень напряженности электрического поля $E^r_г$ в этой точке от вспомогательного излучателя;
• при выключенном генераторе измерить уровень помех $E^r_п$;

• определить реальное затухание как $V_r^* = E_т / E_т^r$;

• провести расчет отношения сигнал/шум на входе измерительного приемника по формуле $q_E^* = (q_E V_r)/V_r$

Далее по рассмотренной ранее методике определяются условия возможности или невозможности перехвата ПЭМИ ВТСС на частотах работы высокочастотного генератора.

Вопросы?