

**Практические вопросы защиты ПДн.
Типовые технические решения.
Средства защиты сетей, средства защиты от
НСД. Средства защиты
от съема информации по каналам ПЭМИН.**

ООО «БухСофт-Екатеринбург»

Телефон: +7 (343) 384-2-86

E-mail: info@buhsoft-ekb.ru

Web: www.buhsoft-ekb.ru



Средства защиты информации, поставляемые для защиты персональных данных:



VipNet - широкий ряд сетевых продуктов, предназначенных для создания виртуальных защищенных сетей.



eToken - электронный ключ, персональное средство строгой аутентификации и безопасного хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и ЭЦП.



Secret Disk - система защиты конфиденциальной информации и персональных данных с возможностью шифрования системного раздела и двухфакторной аутентификацией пользователя до загрузки операционной системы.



ПАК «Соболь» - электронный замок, предназначен для обеспечения доверенной загрузки и предотвращения несанкционированного доступа к ресурсам защищаемого компьютера.



Страж NT - система для комплексной и многофункциональной защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах на базе персональных ЭВМ.



Dallas lock - программное средство защиты от несанкционированного доступа к информационным ресурсам компьютеров с возможностью подключения аппаратных идентификаторов.



Secret Net - система защиты информации на серверах и рабочих станциях от несанкционированного доступа;



ViPNet™ – программный комплекс для построения системы сетевой защиты корпоративных сетей на ОС Windows, Linux, Solaris.

Реализует:

- Формирование структуры защищенных сетей и централизованное управление конфигурацией, неограниченную масштабируемость;
- Шифрование информации на сетевом и прикладном уровнях (любой IP-трафик: видео-, аудиоконференции, файловый обмен, электронная почта);
- Разграничение доступа к информационным ресурсам (межсетевые и персональные сетевые экраны, виртуальные подсети, доверенный доступ к базам данных);
- Безопасный доступ к каналам общего пользования, включая Интернет.



ViPNet состоит из трех программных модулей

ViPNet[Клиент]

устанавливается на компьютер каждого VPN-пользователя, обеспечивает защищенное соединение по TCP/IP с другими пользователями и защиту самого компьютера от сетевых атак

ViPNet[Координатор]

VPN-сервер с интегрированным межсетевым экраном, защищенным почтовым сервером и туннельным сервером для защищенных соединений.

ViPNet[Администратор]

конфигурирование и создание VPN

ViPNet[Клиент]

Персональный сетевой экран

надежная защита рабочей станции/сервера от сетевых атак из LAN и Internet, включая такие возможности как:

- фильтрация IP-трафика по заданным параметрам ("белые" и "черные" списки по типу соединений, номерам портов и протоколов);
- безопасную работу VPN-пользователя с открытыми ресурсами (режим «невидимки»);
- обнаружение сетевых вторжений с помощью встроенной IDS;
- контроль сетевой активности приложений для обнаружения программ-«троянцев».

Шифратор TCP/IP-трафика

включает защиту (шифрование, аутентификацию) любого IP-трафика (сгенерированного приложением или операционной системой) проходящего между любыми VPN-объектами, такими как рабочие станции, серверы приложений, данных и др.

ViPNet[Координатор]

многофункциональное программное обеспечение, которое в зависимости от настроек может выполнять функции:

- VPN-сервера с набором служебных функций
- Туннелирующего сервера (защита связи типа LAN-LAN)
- Межсетевого экрана
- Сервера для безопасной работы с Internet
- Почтового сервера для работы встроенной в ViPNet[Клиент] защищенной почтовой службы

ViPNet[Администратор] состоит из двух

программ:

Центр Управления Сетью(ЦУС)

**Удостоверяющий
Ключевой
Центр(КУЦ)**



Центр Управления Сетью (ЦУС)

- Определяет узлы защищенной сети, пользователей и допустимые связи между ними, создает необходимые справочники и базу данных для работы Ключевого Удостоверяющего Центра;
- Определяет политику безопасности на каждом узле и формирует список прикладных задач, которые могут быть на этом узле запущены (шифрование трафика, ЭЦП, Деловая Почта и т.д.);
- Поддерживает сервис автоматической доставки (с квитиованием) до узлов сети разнообразной справочно-ключевой информации (справочников связей узлов, корневых и отозванных сертификатов, новых ключей шифрования, информации о связях с другими ViPNet-сетями и др.);
- Позволяет проводить автоматическое обновление ПО ViPNet на удаленных компьютерах;
- Поддерживает удаленный доступ к журналам событий на узлах защищенной сети.

Удостоверяющий Ключевой Центр(УКЦ)

- Ключевой Центр: формирует и обновляет все необходимые ключи (шифрования, авторизации) и пароли узлов/пользователей защищенной сети. Ключевая информация пользователя может быть сохранена на аппаратном носителе (дискета, Touch-memory, eToken, смарт-карта и т.п.);
- Удостоверяющий Центр: поддерживает все необходимые механизмы по работе с ЭЦП в формате X.509v3 для аутентификации различных сетевых объектов, включая внешних пользователей (издание секретного ключа, сертификация ЭЦП, формирование списка отозванных сертификатов, кроссертификация с другими УЦ и т.д.).

5 технических доводов «Почему ViPNet?»

- Технология ViPNet ориентирована на взаимодействие клиент-клиент, в то время как большинство VPN-решений обеспечивает только соединения уровня сервер-сервер или сервер-клиент. Это дает возможность реализовать любую необходимую политику безопасности в рамках всей защищенной сети.
- Большое внимание в ViPNet уделено решению проблемы функционирования системы через разнообразное сетевое оборудование (с NAT и NAT), что максимально облегчает процесс установки и настройки.
- В ViPNet используются отечественные алгоритмы шифрования с длиной ключа 256 бит. Ключевая система основана на комбинации симметричных и асимметричных процедур выработки ключевой информации.
- Каждый ViPNet модуль содержит встроенный сетевой экран и систему обнаружения вторжений, что позволяет получить надежную распределенную систему межсетевых и персональных сетевых экранов.
- Для разрешения возможных конфликтов IP-адресов в локальных сетях, включаемых в единую защищенную сеть, ViPNet предлагает развитую систему виртуальных адресов.

5 коммерческих доводов «Почему ViPNet?»

- По сравнению с классическими VPN-решениями ViPNet предоставляет целый ряд дополнительных возможностей по защищенному обмену информацией: встроенные службы обмена сообщениями, файлами, собственная защищенная почтовая служба с элементами автоматизации обмена письмами и поддержкой ЭЦП.
- Дополнительные сетевые возможности ViPNet, такие как контроль сетевой активности приложений, строгий контроль доступа к Интернет, механизмы аварийной перезагрузки и защиты от вторжений на этапе загрузки системы, позволяют защититься от большинства сетевых атак и минимизировать затраты на систему безопасности в целом.
- Наличие развитых интерфейсов пользователя делают ежедневную работу с ViPNet приложениями легкой и не требующей от пользователя специальной подготовки.
- Так как ViPNet является программным решением, то его развертывание на требует приобретения специализированного оборудования и может быть произведено на уже существующем компьютерном парке заказчика. В большинстве случаев также не требуется переконфигурации сетевого оборудования.
- Гибкое ценообразование позволяет сформировать оптимальное ценовое решение для каждого заказчика.

Персональное средство аутентификации и хранения данных, аппаратно поддерживающее работу с цифровыми сертификатами и электронной цифровой подписью.



- eToken поддерживает работу и интегрируется со всеми основными системами и приложениями, использующими технологии смарт-карт или PKI (Public Key Infrastructure).
- eToken может выступать в качестве единой корпоративной карты, служащей для визуальной идентификации сотрудника, для доступа в помещения, для входа в компьютер, в сеть, для доступа к защищенным данным, для защиты электронных документов (ЭЦП, шифрование), для установления защищенных соединений (VPN, SSL), для проведения финансовых транзакций

- **Двухфакторная аутентификация пользователей** при доступе к защищенным ресурсам - компьютерам, сетям, приложениям (*знать* – PIN-код, *иметь* – смарт-карту)
- **Аппаратное выполнение криптографических операций в доверенной среде** (в чипе смарт-карты: аппаратный датчик случайных чисел, генерация ключей шифрования, симметричное и асимметричное шифрование, вычисление хэш-функций, формирование ЭЦП)
- **Безопасное хранение** криптографических ключей, данных пользователей, настроек приложений и др.
 - Аутентификация в унаследованных (не PKI) приложениях
 - Решение проблемы «слабых» паролей
 - Мобильное хранение данных
- **Аутентификация по одноразовым паролям (OTP)**



- **Технология RFID**

- Ангстрем БИМ-002
- HID ISOProxII
- Mirfare
- EM-Marine
- и другие



- **Единое устройство**

- Физический доступ
- Логический доступ

- 1** Чип смарт-карты
- 2** Фото, Логотип
- 3** RFID-метка



- Назначение

- Шифрование конфиденциальных данных на компьютерах, ноутбуках, серверах, сменных носителях + контроль сетевого доступа

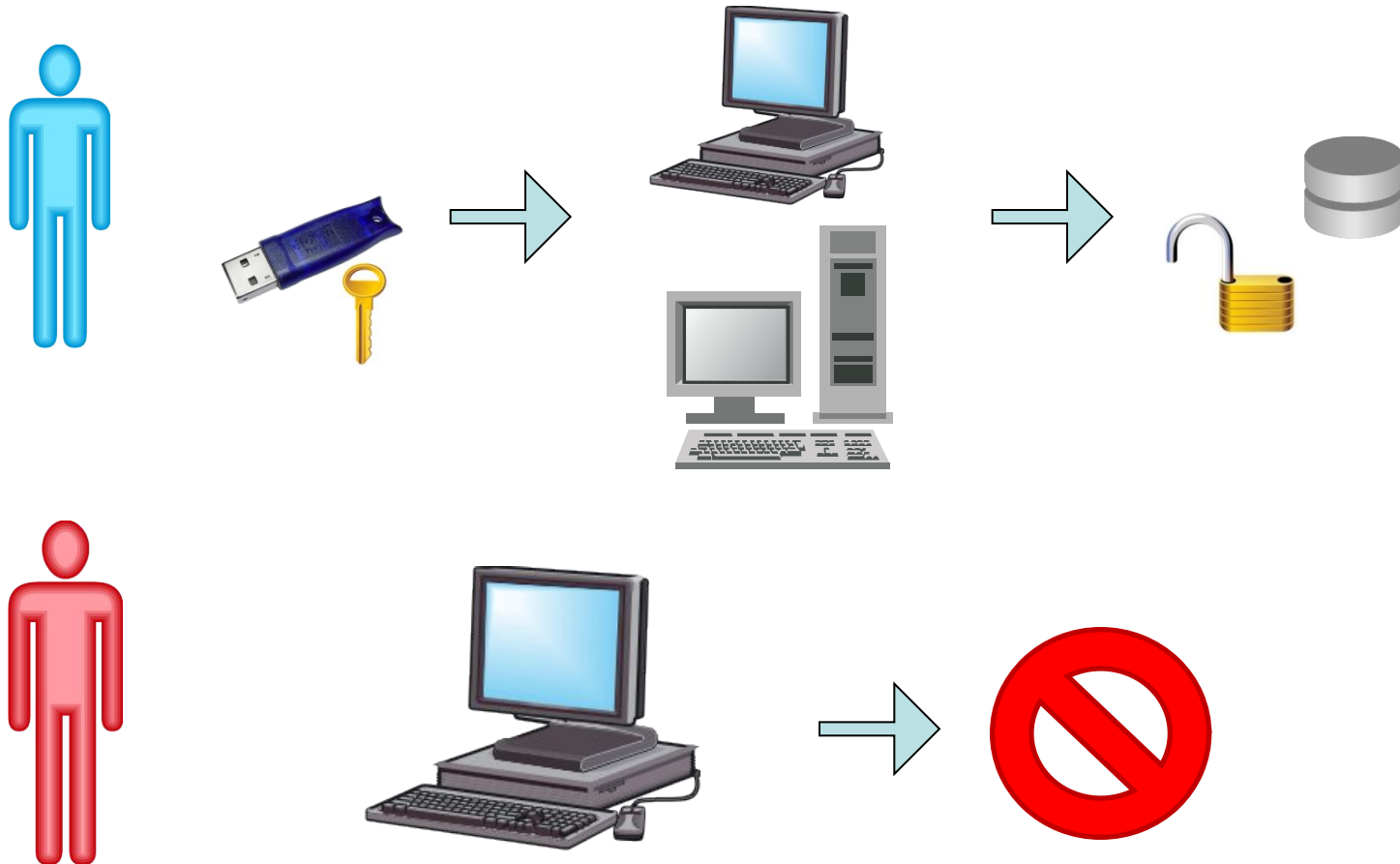
- Особенности

- Двухфакторная аутентификация (eToken + PIN)
- Поддержка российской криптографии
- Контроль сетевого доступа к данным

- Сертифицированная версия

- Сертификация производства во ФСТЭК РФ
- На соответствие ЗБ («Общие Критерии»)
- На отсутствие НДС (по 4 уровню контроля)
- Для защиты конфиденциальной информации в системах до 1Г





- *Доступ к зашифрованным данным может получить только авторизованный пользователь*

- ✓ Защита системного раздела и контроль начальной загрузки
- ✓ Многопользовательская работа
- ✓ Разделение прав работы с диском
- ✓ Поддержка нескольких ОС
- ✓ Расширенная безопасность
 - Поддержка ждущего и спящего режимов
 - Защита содержимого dump-файлов
 - Система восстановления



- ✓ Шифрование данных на HDD, RAID, SAN
- ✓ Контроль доступа к зашифрованным дискам по сети
- ✓ Аутентификация администраторов с использованием смарт-карт и USB-ключей eToken
- ✓ Гибкая система подачи сигнала «Тревога»
 - Красная кнопка
 - Радио-брелок
 - Охранная сигнализация
 - GSM-модуль
- ✓ Защита от сбоев и система восстановления



- Назначение

- Предотвращение доступа посторонних лиц к информации, хранящейся на ПЭВМ, и регистрации попыток доступа к ПЭВМ.

Особенности

- Осуществляет ведение системного журнала, записи которого хранятся в специальной энергонезависимой памяти

Сертифицированная версия

- Сертифицирован ФСБ и Гостехкомиссией РФ
- На отсутствие НДВ (по 3 уровню контроля)

Для защиты ащиты информации, составляющей государственную тайну, и конфиденциальной информации в системах до 1В



- ✓ Идентификация и аутентификация пользователей.
- ✓ Регистрация попыток доступа к ПЭВМ.
 - Факт входа пользователя;
 - Введение неправильного пароля;
 - Предъявление не зарегистрированного идентификатора пользователя;
 - Превышение числа попыток входа в систему;
 - Другие события.
- ✓ Запрет загрузки ОС со съемных носителей.
- ✓ Контроль целостности программной среды.



- Назначение

- Комплексная и многофункциональная защиты информационных ресурсов от несанкционированного доступа при работе в многопользовательских автоматизированных системах

- Особенности

- устанавливается как на автономных рабочих местах, так и на рабочих станциях и файл-серверах локальной вычислительной сети

- Сертифицированная версия

- Сертифицирован Гостехкомиссией РФ

- На отсутствие НДВ (по 2 уровню контроля)

- Для защиты информации, конфиденциальной информации в системах до 1Б



- ✓ идентификация и аутентификация пользователей;
- ✓ избирательное разграничение доступа пользователей к защищаемым ресурсам;
- ✓ разграничение доступа к информации различных уровней конфиденциальности;
- ✓ возможность изменения наименований меток конфиденциальности;
- ✓ управление и настройка механизмов защиты локально и удаленно;
- ✓ регистрация событий безопасности, ведение дополнительных журналов аудита;
- ✓ создание замкнутой среды пользователя;
- ✓ контроль целостности защищаемых ресурсов;
- ✓ гарантированная очистка содержимого файлов после их удаления;
- ✓ блокировка и разблокировка рабочей станции;
- ✓ автоматическое проставление учетных признаков в документах, выводимых на печать;
- ✓ ведение журнала документов, выданных на печать;
- ✓ создание и удаление пользователей;
- ✓ тестирование работоспособности СЗИ;
- ✓ учет отчуждаемых носителей информации;
- ✓ создание и применение шаблонов настроек программных средств.

- Назначение

- Защита информационных ресурсов от несанкционированного доступа

- Особенности

- встроенная возможность печати гриффов конфиденциальности на любых документах и возможность использования системы для защиты ресурсов мобильных (Notebook) и промышленных компьютеров.

- Сертифицированная версия

- Сертифицирован ФСТЭК и Гостехкомиссией РФ
На отсутствие НДВ (по 2 уровню контроля)
Для защиты информации, конфиденциальной информации в системах до 1Б



- ✓ Запрет загрузки компьютера посторонними лицам.
- ✓ Двухфакторная авторизация по паролю и аппаратным идентификаторам (USB eToken, Touch Memory) до загрузки ОС.
- ✓ Разграничение прав пользователей на доступ к локальным и сетевым ресурсам.
- ✓ Контроль работы пользователей со сменными накопителями.
- ✓ Мандатный и дискреционный принципы разграничения прав.
- ✓ Организация замкнутой программной среды.
- ✓ Аудит действий пользователей.
- ✓ Контроль целостности ресурсов компьютера.
- ✓ Очистка остаточной информации.
- ✓ Возможность автоматической печати штампов (меток конфиденциальности) на всех распечатываемых документах.
- ✓ Защита содержимого дисков путем прозрачного преобразования.
- ✓ Удаленное администрирование, выделенный центр управления, работа в составе домена безопасности.
- ✓ Возможна установка на портативные компьютеры (Notebook).
- ✓ Отсутствие обязательной аппаратной части.
- ✓ Удобные интерфейс, установка и настройка.

- Назначение

- Защита информации от несанкционированного доступа

- Особенности

- встроенная возможность печати грифов конфиденциальности на любых документах и возможность использования системы для защиты ресурсов мобильных (Notebook) и промышленных компьютеров.

- Сертифицированная версия

- Сертифицирован ФСТЭК и Гостехкомиссией РФ
На отсутствие НДВ (по 2 уровню контроля)
Для защиты информации, конфиденциальной информации в системах до 1Б



- ✓ Идентификация и аутентификация пользователей
- ✓ Защита от загрузки с внешних носителей
- ✓ Разграничение доступа к устройствам
- ✓ Полномочное управление доступом
- ✓ Контроль печати конфиденциальной информации
- ✓ Замкнутая программная среда
- ✓ Контроль целостности программ и данных
- ✓ Гарантированное уничтожение данных
- ✓ Контроль аппаратной конфигурации компьютера
- ✓ Функциональный самоконтроль подсистем
- ✓ Механизм отчетов
- ✓ Регистрация событий



Использование средств аппаратной поддержки:

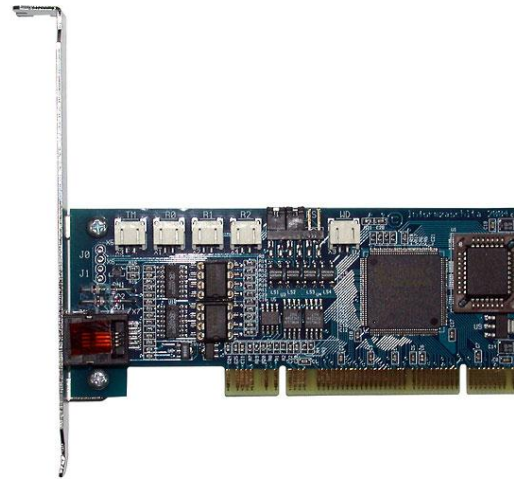
- ✓ программно-аппаратный комплекс «Соболь»;
- ✓ Secret Net Touch Memory Card.

Для идентификации могут быть использованы:

- ✓ iButton;
- ✓ eToken R2;
- ✓ eToken Pro.



- Режим входа в систему:
- ✓ мягкий
 - ✓ жёсткий



Защита от несанкционированной загрузки с внешних носителей

- ✓ Пространственное зашумление
- ✓ Блокираторы сотовых телефонов
- ✓ Защита телефонных линий
- ✓ Защита сети 220 В
- ✓ Акустическое и виброакустическое зашумление
- ✓ Подавление диктофонов
- ✓ Уничтожение информации





Устройство "Блокада" предназначено для защиты информации, обрабатываемой на объектах информатизации, включая вычислительную технику, от утечки за счёт побочных электромагнитных излучений и наводок от них на цепи электропитания, заземления и проводные слаботочные линии посредством создания маскирующих шумовых сигналов (типа «белый шум») в диапазоне частот от 0,01 до 2000 МГц и наведённых ими маскирующих помех на цепи электропитания, заземления и проводные слаботочные линии в диапазоне частот от 0,01 до 300 МГц.



Генератор шума предназначен для маскировки информативных побочных электромагнитных излучений и наводок (ПЭМИН) персональных компьютеров, рабочих станций на объектах вычислительной техники путем формирования и излучения в окружающее пространство электромагнитного поля шума (ЭПМШ) и наведения шумового сигнала в отходящие цепи и инженерные коммуникации в в диапазоне частот 0,1 - 2000 МГц.

На изделие имеется сертификат ФСТЭК No 1003, действительный до 04.04.2008, и сертификат СанПиН No H00399.



Переносной блокиратор SEL SP-162 "Батог" предназначен для подавления работы сотовых телефонов, работающих в стандартах CDMA-450, GSM-900, GSM-1800, UMTS (3G).

Блокиратор может быть использован для предотвращения утечки информации через работающие сотовые телефоны при проведении конфиденциальных переговоров, а также для поддержания порядка и тишины в учреждениях, где переговоры по сотовым телефонам не допускаются.

Отличительные особенности:

- Блокирование может осуществляться как одновременно, так и выборочно в вышеперечисленных поддиапазонах, что значительно расширяет возможности использования изделия.
- Уникальное конструктивное исполнение позволяет использовать данный аппарат практически в любых условиях применения: при проведении конфиденциальных переговоров в стационарных помещениях, театрах, библиотеках, в автомобиле, самолетах и т.п.
- Изделие исключительно простое в использовании.



"Молния" - это средство защиты от несанкционированного прослушивания переговоров как по телефону, так и в помещении с помощью устройств, работающих в проводных линиях или линиях электросети.

Принцип действия прибора основан на электрическом пробое радиоэлементов. При нажатии на кнопку "Пуск" в линию подается мощный короткий высоковольтный импульс, способный полностью разрушить или нарушить функциональную деятельность средств съема информации.



Устройство "Щит" служит для маскировки конфиденциальной речевой информации (речи), получаемой по телефонной сети и подобным каналам связи.

"Щит" включается между телефонной линией и телефонным аппаратом абонента, принимающего конфиденциальную информацию. Во время приёма речевого сообщения от удалённого абонента "Щит" генерирует и подает в телефонную линию мощный шумовой сигнал в полосе частот телефонного канала. Речь удаленного абонента смешивается с помехой и полностью маскируется на всём протяжении телефонной линии. В поступающей на вход устройства смеси речевого сигнала и шума "Щит" автоматически, в реальном масштабе времени, практически без задержки, компенсирует помеху, поскольку характеристики шумового сигнала маскиратору известны.



Предназначен для защиты радиоэлектронных устройств и средств вычислительной техники от утечки информации по цепям электропитания с напряжением 220 В.

Фильтр применяется для обеспечения электромагнитной развязки по цепям электропитания радиоэлектронных устройств, средств вычислительной техники и электросетей промышленных объектов и офисных помещений.

Отличительные особенности:

- защита средств оргтехники от воздействия внешних высокочастотных помех;
- повышение помехоустойчивости радиоэлектронной аппаратуры.

Имеет сертификат ФСТЭК № 148/2, продлённый до 01.04.2010.



Устройство защиты по сети электропитания МП-3 предназначено для исключения утечки информации в сеть питания при акустическом воздействии на изделие и пропадании сетевого напряжения. МП-3 может быть использовано для защиты от утечки информации любого изделия, которое потребляет от сети переменного тока напряжением 220 В не более 170 Вт.



Аудиоизлучатели АИ-3М являются специализированными электроакустическими преобразователями и предназначены для возбуждения акустического шума. Конструкция и размеры аудиоизлучателей АИ-65 и элементов их крепления оптимизированы для его установки:

- в надпотолочном пространстве;
- в вентиляционных каналах;
- дверных тамбурах.

Аудиоизлучатели АИ-3М являются элементами аппаратуры «Соната АВ» модели 3М и рассчитаны на подключение входящих в её состав генераторных блоков.



Виброизлучатели ПИ-3М являются специализированными электроакустическими преобразователями малой мощности и предназначены для возбуждения шумовых вибраций в остеклении окон (дверей, офисных перегородок и т.п.).

"Лёгкие" виброизлучатели ПИ-3М являются элементами аппаратуры «Соната АВ» модели 3М и рассчитаны на подключение входящих в её состав генераторных блоков.

ООО «БухСофт-Екатеринбург»

Телефон: +7 (343) 384-2-86

Факс: +7 (343) 384-82-86,

Адрес: 620028, г.Екатеринбург, ул. Кирова, д. 34,
оф. 212

E-mail: info@buhsoft-ekb.ru

Web: www.buhsoft-ekb.ru

