Компания «РНТ»

СДЕЛАНО В РОССИИ

Каталог продукции

О КОМПАНИИ

Компания «РНТ» (ЗАО «РНТ», с 1993 г.) специализируется на разработке сертифицированных средств защиты информации и оказании услуг в области проектирования, внедрения и обслуживания автоматизированных информационных и телекоммуникационных систем в защищенном исполнении. В «РНТ» имеется собственная производственная база, аккредитованная испытательная лаборатория и необходимые лицензии для разработки, изготовления и сертификации изделий защиты информации.

Высокий уровень качества устройств защиты информации, которые разрабатываются в «РНТ», подтверждает технологическое сотрудничество с лидерами российского и мирового рынка программного обеспечения и высокотехнологичного оборудования, а также внедрение системы менеджмента качества по требованиям ГОСТ ISO 9001:2011 на проектирование, разработку, производство, поставку технических средств, монтаж, обслуживание, исследование, испытание систем и другие виды деятельности.

Устройства защиты информации, представленные в каталоге, реализуются через сеть авторизованных партнеров, которые выполняют поставку и техническую поддержку в российских регионах.

Чтобы стать авторизованным партнером, обращайтесь в коммерческую службу «РНТ» по адресу: sales@rnt.ru или заполните форму регистрации на сайте: www.rnt.ru.

СОДЕРЖАНИЕ

СИСТЕМА ОБНАРУЖЕНИЯ АТАК «ФОРПОСТ» (СОА «ФОРПОСТ»)

Обеспечение защиты информации за счет автоматического выявления воздействий на автоматизированную информационную систему, которые могут быть классифицированы как компьютерные атаки или вторжения, и блокирования развития выявленных компьютерных атак.

Более 15 лет СОА «Форпост» устанавливается на объектах защиты государственного значения.

Основные функции

- Обнаружение атак на серверы телематических служб (WEB, FTP, E-mail, СУБД и пр.) и АРМ, размещенных в контролируемых сегментах АИС.
- Оповещение администратора ИБ об обнаруженных атаках.
- Блокировка источников атак с помощью отправки последовательности команд сетевому оборудованию.
- Удаленное управление сетевым оборудованием по защищенному каналу (КриптоПро CSP 3.6).
- Ведение системного журнала аудита и генерация отчетов на основе служебной информации от компонентов СОА, сетевого оборудования (SNMP и SYSLOG) и ПАКов сторонних производителей.
- Интеграция с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, создаваемой в соответствии с Указом Президента Российской Федерации N 31с от 15 января 2013 г., а также с внешними SIEM системами.
- Возможность централизованного обновления базы сигнатур компьютерных атак.

Сертификаты

- Сертификат ФСБ России № СФ/129-1753 от 01.12.2011 на соответствие требованиям ФСБ России, предъявляемым к СОА класса Б.
- Сертификат ФСТЭК №2845 от 18.03.2013 на соответствие требованиям к СОВ (ФСТЭК России, 2011) по 3 классу (оценочный уровень доверия по ГОСТ Р ИСО/МЭК 15408-03-ОУД 4, уровень контроля НДВ-3).

ПРОГРАММНЫЙ КОМПЛЕКС «ФОРПОСТ-МОНИТОРИНГ»

Оперативный контроль состояния и проактивный мониторинг доступности ресурсов АИС, качества услуг и ИТ-сервисов. Выявление проблем в функционировании АИС, определение характера и места сбоя, его оперативное устранение или локализация.

Возможности

- Сбор данных и оценка соответствия рабочих станций политикам безопасности.
- Предоставление доступа к сети после оценки систем и установления соответствия требованиям политики.
- Исправление политик безопасности рабочих станций, не соответствующих требованиям.
- Дополнительный мониторинг состояния соответствия через установленные администратором промежутки времени.
- Интегрированная консоль для мониторинга сетей, серверов. виртуальных устройств и приложений.
- Автономный мониторинг сети.
- Объединение всех существенных признаков функционирования сети.
- Мониторинг до 500 устройств/серверов или 10000 сетевых интерфейсов.

Состав

- *Узловые датчики (мониторинг состояния ОС и ПО на серверах и рабочих станциях АИС под управлением ОС MS Windows).*
- *Узловые датчики уровня сегмента сети (сбор информации с серверов и сетевого оборудования, на которых установлены ОС, отличные от MS Windows).*
- *Центр управления (используется для сбора и анализа информации от датчиков мониторинга, формирует отчеты и информирует администратора безопасности о состоянии устройств в сети).*

ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «ФОРПОСТ»

Сертифицированное решение для обнаружения компьютерных атак/вторжений «в одной коробке», реализованное на серверных платформах российской сборки ПК «Аквариус».

Достоинства

- Быстрый ввод в эксплуатацию.
- Возможность масштабирования системы.
- Интуитивно понятный интерфейс консоли управления.
- Обнаружение атак в режиме реального времени.
- Использование в системе собственной безопасности сертифицированных ФСБ России СКЗИ (КриптоПро CSP 3.6).

Применение

- В органах государственной власти Российской Федерации в АИС, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну (в соответствии с требованиями ФСБ России).
- В ИС, в которых обрабатывается информация, содержащая секретные сведения (в соответствии с требованиями ФСТЭК России - в АС до класса защищещнности 1В включительно, информационных системах персональных данных до 1 класса включительно).

Технические параметры

ПАК «ФОРПОСТ 200»

Параметр:	Значение:
Скорость обработки сетевого трафика	до 200 Мбит/с
Сетевой интерфейс для передачи данных	1 медный со скоростью 1 Гбит/с
Сетевой интерфейс для съема трафика	1 медный со скоростью 1 Гбит/с
Компактная бесшумная аппаратная платформа для монтажа в 19" стойку или настольной установки	

ПАК «ФОРПОСТ 2000»

Параметр:	Значение:
Скорость трафика в режиме Half Duplex	до 2000 Мбит/с
Скорость трафика в режиме Full Duplex	до 4000 Мбит/с
Сетевой интерфейс для передачи данных	1 медный со скоростью 1 Гбит/с
Сетевые интерфейсы для съема трафика «ФОРПОСТ 2400»	2 x SFP+ со скоростью 10 Гбит/с
Сетевые интерфейсы для съема трафика «ФОРПОСТ 2405»	2 медных со скоростью 10 Гбит/с
Промышленное исполнение с возможностью монтажа в 19" стойку	
Резервирование ключевых аппаратных компонентов (отказоустойчивый RAID-массив с использованием серверных жестких дисков, резервирование блока питания)	

Исполнения ПАК «ФОРПОСТ»

Серия 200

- Аппаратная платформа в компактном корпусе с возможностью настольной установки
- Низкий уровень шума
- Максимальный размер базы данных зафиксированных событий - до 4 ГБ

Простое исполнение
(решение для обнаружения вторжений «в одной коробке»)

ПАК «Форпост 200»

- До 200 Мбит/с
- 1 анализирующий интерфейс (медный, 1 Гбит/с)

Модульное исполнение
(отдельный центр управления, к которому подключаются сетевые датчики)

ПАК «Форпост 200МЦ»
Центр управления

ПАК «Форпост 200МД»
Сетевой датчик

- До 200 Мбит/с
- 1 анализирующий интерфейс (медный, 1 Гбит/с)

Серия 2000

- Промышленное исполнение с возможностью монтажа в стойку 19"
- Резервирование ключевых компонентов сервера: отказоустойчивый RAID-массив с использованием серверных жестких дисков, резервирование блока питания
- Высокая производительность сетевых датчиков и поддержка ими режима Full Duplex

Простое исполнение
(решение для обнаружения вторжений «в одной коробке»)

ПАК «Форпост 2000»

- До 1 Гбит/с в режиме Half Duplex
- До 2 Гбит/с в режиме Full Duplex
- 2 анализирующих интерфейса (медные, 1 Гбит/с)

ПАК «Форпост 2400»

- до 2 Гбит/с в режиме Half Duplex
- До 4 Гбит/с в режиме Full Duplex
- 2 анализирующих интерфейса (SFP+, 10 Гбит/с)

ПАК «Форпост 2405»

- до 2 Гбит/с в режиме Half Duplex
- До 4 Гбит/с в режиме Full Duplex
- 2 анализирующих интерфейса (медные, 10 Гбит/с)

Модульное исполнение
(отдельный центр управления, к которому подключаются сетевые датчики)

ПАК «Форпост 2000МЦ»
Центр управления

ПАК «Форпост 2000»

- До 1 Гбит/с в режиме Half Duplex
- До 2 Гбит/с в режиме Full Duplex
- 2 анализирующих интерфейса (медные, 1 Гбит/с)

ПАК «Форпост 2400»

- до 2 Гбит/с в режиме Half Duplex
- До 4 Гбит/с в режиме Full Duplex
- 2 анализирующих интерфейса (SFP+, 10 Гбит/с)

ПАК «Форпост 2405»

- до 2 Гбит/с в режиме Half Duplex
- До 4 Гбит/с в режиме Full Duplex
- 2 анализирующих интерфейса (медные, 10 Гбит/с)

ПРОГРАММНЫЙ КОМПЛЕКС «ФАНТОМ»

Сертифицированное программное средство защиты информации (СЗИ) «Фантом» предназначено для создания защищенного рабочего места на персональном компьютере с использованием технологии виртуализации.

Применение

«Фантом» устанавливается на персональный компьютер пользователя или переносной USB-диск и контролирует функционирование операционных систем MS Window или Linux, периферийных устройств, сетевого взаимодействия, а также прикладного окружения пользователя.

Работа пользователя на компьютере с «Фантом» обеспечивает попеременный доступ в защищённые сегменты сетей и в сети общего пользования путем настройки нескольких виртуальных рабочих мест. Переключение между ними осуществляется практически мгновенно (менее 1 сек) при помощи легко запоминаемой комбинации клавиш.

Преимущества

- Безопасная работа одновременно в двух и более сетях различной категории конфиденциальности.
- Значительные затруднения для несанкционированного доступа к информации даже в случае утери, кражи компьютера или переносного USB-диска с установленным СЗИ «Фантом».
- Полный контроль работы ОС и периферийных устройств компьютера, наличие средств повышения отказоустойчивости, аудита ИБ.

Существенным достоинством решения является возможность разворачивания СЗИ «Фантом» и виртуальных рабочих мест на переносном USB-диске. При загрузке персонального компьютера с этого диска работа пользователя никак не отличается от работы с внутренним диском компьютера. При этом внутренний диск полностью изолирован: вся информация хранится исключительно на внешнем диске пользователя, а внутренний диск полностью защищен на чтение и запись информации.

ПЕРСОНАЛЬНЫЕ ЭВМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ «ОБРУЧ»

Персональные ЭВМ в защищенном исполнении «ОБРУЧ» являются техническими средствами обработки информации и предназначены для защиты сведений, составляющих государственную тайну, служебной информации ограниченного распространения, конфиденциальной информации и персональных данных.

Преимущества

- Эксплуатация не требует специального обучения и квалификации в области защиты информации.
- Возможно использование как отдельной рабочей станции, так и в составе локальной сети или выделенном сегменте.
- Входной контроль комплектующих для ПЭВМ.
- Технология снижения информативных излучений пассивными методами.
- При использовании не требуется применение средств активной защиты.
- Гарантия максимального уровня защиты от перехвата.
- Возможность встраивания модулей доверенной загрузки и СКЗИ.

Поставка

В стандартный комплект поставки ПЭВМ «ОБРУЧ-2», «ОБРУЧ-3», «ОБРУЧ-Ф» входят системный блок, монитор, клавиатура, манипулятор «мышь», комплект интерфейсных кабелей и кабелей электропитания, комплект эксплуатационной документации и документы, регламентирующие порядок эксплуатации на режимных категорированных объектах.

По согласованию с Заказчиком в комплект поставки могут включаться защищённые принтер, флэш-накопитель USB, оптический привод, оптический выход для подключения к внешней вычислительной сети.

Сертификаты

- Гарантированная защита подтверждается сертификатами ФСТЭК России и ФСБ России («ОБРУЧ-Ф»). ПЭВМ «ОБРУЧ» могут использоваться в качестве объектов информатизации 2-й («ОБРУЧ-2»), 3-й («ОБРУЧ-3») категорий.
- ПЭВМ «ОБРУЧ-Ф» может использоваться в помещениях до 2-й категории включительно, в том числе в органах государственной власти Российской Федерации, на режимных объектах ФСО России и ФСБ России.
- Включены в Государственный реестр сертифицированных средств защиты информации.
- Обладают сертификатом Росстандарта.

НОВОЕ!

ПЭВМ «ОБРУЧ-2» и «ОБРУЧ-3» могут поставляться в компактном ***моноблочном исполнении*** *с улучшенными характеристиками по ПЭМИН, подтвержденными испытаниями.*

ЗАЩИЩЕННЫЙ АБОНЕНТСКИЙ ПУНКТ «ОБРУЧ-АП-2»

Абонентский пункт «ОБРУЧ-АП-2» специально предназначен для подключения к информационным ресурсам международной сети Интернет, обработки общедоступной информации и защиты государственной тайны, конфиденциальной информации и персональных данных.

Преимущества

- Соответствует требованиям ФСБ России к средствам вычислительной техники, предназначенным для использования в выделенных помещениях до 2-й категории включительно при осуществлении международного обмена по сетям общего пользования по классу ВАП-1.55.
- Сертификат соответствия ФСБ России в Системе сертификации № РОСС RU.001.030001.
- Обладает всеми преимуществами базовой ПЭВМ «ОБРУЧ».
- Дополнительно укомплектован программно-аппаратным комплексом защиты от несанкционированного доступа «Соболь» версии 3.0 класса 1Б (сертифицирован ФСБ России) и комплексом виброакустической защиты «Шлем ПК».

Выпускается с 2009 года в соответствии с Указом Президента Российской Федерации от 17.03.2008 №351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

УСТРОЙСТВО ЗАЩИТЫ ГРОМКОГОВОРИТЕЛЕЙ «УЗГ»

«УЗГ» предназначено для защиты циркулирующей в помещении речевой информации, содержащей сведения, составляющие государственную тайну, служебную информацию ограниченного распространения, конфиденциальной информации и персональных данных.

Преимущества

- Соответствует требованиям нормативного документа «Сборник норм защиты информации от утечки за счет побочных электромагнитных излучений и наводок «ПЭМИН)» (Гостехкомиссия России, 1998).
- Включено в Государственный реестр сертифицированных средств защиты информации.
- Обеспечивает разрыв линии оповещения или радиотрансляции при отсутствии сигнала.
- Применение не оказывает влияния на функциональные возможности громкоговорителей систем оповещения и трансляции.
- Простота использования («Включил и работай»). Эксплуатация не требует специального обучения и квалификации в области защиты информации.
- Не требует внешнего источника электропитания.

Сертификаты

Сертификат ФСТЭК подтверждает применение «УЗГ» на объектах информатизации до 1-й категории включительно.

МАСКИРАТОРЫ ПОБОЧНЫХ ИЗЛУЧЕНИЙ И НАВОДОК «МАИС-М»

Маскираторы серии «МАИС-М» предназначены для защиты информации, содержащей сведения, составляющие государственную тайну, служебную информацию ограниченного распространения, конфиденциальной информации и персональных данных от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН) на цепи электропитания, заземления и коммуникаций.

Преимущества

- Соответствуют требованиям нормативного документа «Сборник норм защиты информации от утечки за счет побочных электромагнитных излучений и наводок (ПЭМИН)» (Гостехкомиссия России, 1998).
- Включены в Государственный реестр сертифицированных средств защиты информации.
- Простота использования («Включил и работай»). Эксплуатация не требует специального обучения и квалификации в области защиты информации.
- Управление сводится к подключению к источнику питания перед включением основных технических средств (систем) и отключению после их включения.
- Световая и звуковая индикация работоспособности.
- Выполнены как обычный разветвитель или адаптер, миниатюрные и экономичные.

Сертификаты

Сертификаты соответствия ФСТЭК на «МАИС-М», «МАИС-М1», «МАИС-М2», которые могут применяться на объектах информатизации до 1-й категории включительно и устанавливаться в выделенных помещениях до 1-й категории включительно, в том числе оборудованных системами звукоусиления речи, без применения дополнительных мер защиты информации.

Технические параметры

«МАИС-М»

Постановка маскирующих помех со сплошным спектром в диапазоне частот от 10Гц до 10 ГГц.

«МАИС-М1» И «МАИС-М2»

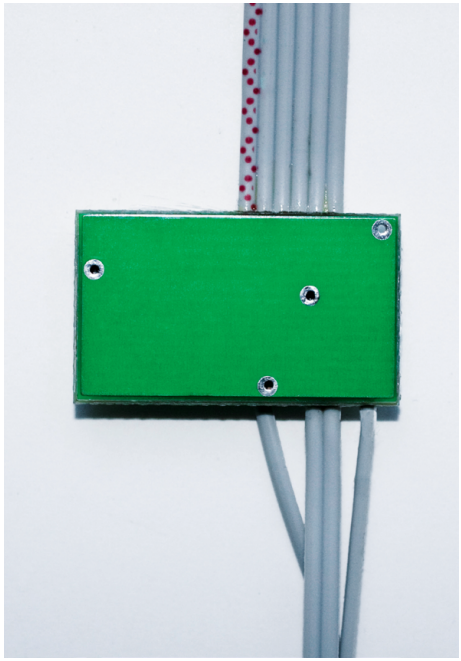
Излучение в окружающее пространство электромагнитного поля шума в диапазоне частот от 10кГц до 2ГГц и наведение маскирующего сигнала в цепи питания и заземления в диапазоне частот от 10КГц до 1ГГц.

Параметр:	***Значение:***
Коэффицеиент качества шума	*не менее 0,8*
Коэффициент межспектральных корреляционных связей	*не более 2,0*
Время непрерывной работы	*24 часа*
Ток нагрузки, подключаемой к розеткам изделия	*не более 5 А*
Габаритные размеры «МАИС-М», «МАИС-М1» в корпусе сетевого фильтра «Пилот L» (5 или 6 розеток)	*380х65х53 мм*
Габаритные размеры «МАИС-М2» в корпусе адаптера	*65х100х120 мм*

УСТРОЙСТВО БЛОКИРОВАНИЯ НЕСАНКЦИОНИРОВАННОГО ВКЛЮЧЕНИЯ МИКРОФОНОВ ЦИФРОВОГО ТЕЛЕФОННОГО АППАРАТА «УБМ-1»

Цифровые АТС предоставляют широкие возможности дистанционного программирования и управления цифровыми абонентскими аппаратами. Вследствие этого появляются дополнительные угрозы безопасности и речевой информации, циркулирующей в помещениях, предназаченных для проведения конфиденциальных переговоров через установленные в них абонентские аппараты путем использвоания объявленных и не объявленных производителями цифровых АТС возможностей или услуг (конференция и т.д.), приводящих к скрытному дистанционному включению имеющихся в телефонном аппарате микрофонов и спикерфона.

Для предотвращения этой возможности предназначено устройство блокирования несанкционированного включения микрофонов телефонного аппарата «УБМ-1». Устройство физически (аппаратно) разрывает электрические цепи микрофонов при однократном нажатии на клавишу.
При повторном нажатии электрические цепи цифрового телефонного аппарата восстанавливаются. Таким образом, применение данного устройства не оказывает влияния на функциональные возможности цифрового телефонного аппарата. Состояние микрофонов цифрового телефонного аппарата показывает светодиод этой клавиши.



- *«УБМ-1» устанавливается непосредственно в корпус цифрового телефонного аппарата (Siemens Openstage, Avaya, Cisco, Sony Ericsson, LG);*
- *не требует дополнительного источника питания;*
- *прост в использовании;*
- *надежен в работе.*

УСТРОЙСТВО ВИБРОАКУСТИЧЕСКОЙ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ «ВП23-5П-nK»

Устройство «ВП23-5П-nK» предназначено для защиты циркулирующей в помещении речевой информации, содержащей сведения, составляющие государственную тайну, служебную информацию ограниченного распространения, конфиденциальную информацию, персональные данные. Устройство надежно защищает от прямого прослушивания, а также от прослушивания с использованием различных микрофонов, стетоскопов и лазерных систем съема информации. Используется для защиты в выделенных помещениях до 1-й категории включительно.

Преимущества

- Соответствует требованиям нормативного документа «Сборник нормативно-методических документов по противодействию акустической речевой разведке» (Гостехкомиссия России, 2000).
- Сертификат соответствия ФСТЭК России в Системе сертификации средств защиты информации по требованиям защиты информации № РОСС RU.001.1БИ00.
- Включено в Государственный реестр сертифицированных средств защиты информации.
- Управление сводится к включению устройства перед проведением переговоров и выключению после их завершения, возможно автоматическое включение/выключение.

Состав:

- *блок управления (одно-, двух-, трехканальный) с блоком питания;*
- *вибрационный преобразователь (для оконных стекол);*
- *вибрационный преобразователь (для ограждающих и инженерных конструкций);*
- *акустомат;*
- *блок дистанционного управления.*

СИСТЕМА ВИБРОАКУСТИЧЕСКОЙ ЗАЩИТЫ «ВВ 301»

Система «ВВ 301» предназначена для защиты циркулирующей в помещении речевой информации, содержащей сведения, составляющие государственную тайну, служебную информацию ограниченного распространения, конфиденциальную информацию, персональные данные. Применяется в выделенных помещениях до 1-й категории включительно.

Преимущества

- Соответствует требованиям нормативного документа «Сборник нормативно-методических документов по противодействию акустической речевой разведке» (Гостехкомиссия России, 2000).
- Сертификат соответствия ФСТЭК России в Системе сертификации средств защиты информации по требованиям защиты информации № РОСС RU.001.1БИ00.
- Включена в Государственный реестр сертифицированных средств защиты информации.
- Управление сводится к включению системы перед проведением переговоров и выключению после их завершения, возможно автоматическое включение/выключение.
- Различная комплектация в зависимости от особенностей защищаемого помещения.

Состав:

- *основной блок двухканальный;*
- *блок электропитания (поддерживает работу трех основных блоков с полной нагрузкой);*
- *блок дистанционного управления с пультом;*
- *дополнительный акустомат;*
- *вибропреобразователи для зашумления строительных конструкций, инженерных коммуникаций, для оконных конструкций;*
- *акустические преобразователи для зашумления дверных проемов и технологических ниш;*
- *установочные и крепежные элементы (по требованию).*

КОМПЛЕКС ВИБРОАКУСТИЧЕСКОЙ ЗАЩИТЫ «ШЕЛЕСТ-4К»

Комплекс «ШЕЛЕСТ-4К» предназначен для защиты циркулирующей в помещении речевой информации, содержащей сведения, составляющие государственную тайну, служебную информацию ограниченного распространения, конфиденциальную информацию, персональные данные. Устройство надежно защищает от прямого прослушивания, а также от прослушивания с использованием различных микрофонов, стетоскопов и лазерных систем съема информации. Используется для защиты в выделенных помещениях до 1-й категории включительно. Для защиты больших площадей применяется совместно с системой виброакустической защиты (аппаратурой виброакустической защиты помещений) «ВВ 301».

Преимущества

- Соответствует требованиям нормативного документа «Сборник нормативно-методических документов по противодействию акустической речевой разведке (Гостехкомиссия России, 2000).
- Сертификат соответствия ФСТЭК России в Системе сертификации средств защиты информации по требованиям защиты информации № РОСС RU.001.1БИ00.
- Включен в Государственный реестр сертифицированных средств защиты информации.
- Управление сводится к включению комплекса (отдельного канала) перед проведением переговоров и выключению после их завершения, возможно автоматическое включение/выключение.

Состав:

- *блок управления;*
- *вибрационный преобразователь (для оконных стекол);*
- *вибрационный преобразователь (для ограждающих и инженерных конструкций);*
- *датчик уровня сигнала;*
- *акустический преобразователь;*
- *блок дистанционного управления;*
- *пульт управления;*
- *модуль индикации.*

Контакты:

Компания «РНТ» (ЗАО «РНТ»)
129515, Москва
Ул. 2-я Останкинская, д. 6
Тел.: +7 (495) 777-75-77
Факс: +7 (495) 777-75-76
Отдел продаж: sales@rnt.ru
Техническая поддержка: support@rnt.ru
Пресс-служба: pr@rnt.ru
Сайт: www.rnt.ru