

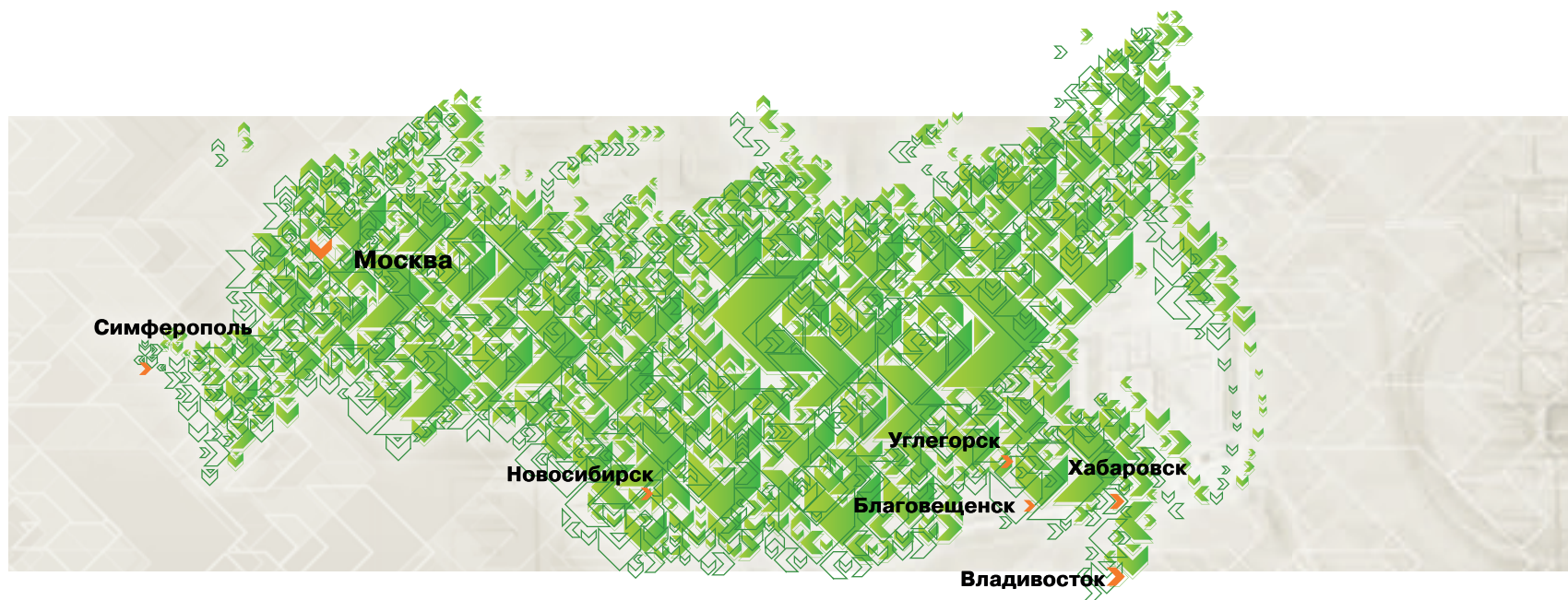


**Комплексный подход  
к безопасности**





- О Группе компаний
- Услуги и Решения
- Технологии



**Год основания:** ➤ 1991 год

**Страна:** ➤ Россия

**Отрасль:** ➤ Безопасность и защита информации

**Направление деятельности:** ➤ Разработка, поставка и внедрение интегрированных комплексных систем безопасности и защищенных сетей связи и передачи данных.  
Строительство специальных объектов

**Цель деятельности:** ➤ Удовлетворение актуальных потребностей государства и бизнеса в комплексном обеспечении безопасности с применением перспективных технологий и в полном соответствии с требованиями законодательства



**О КОМПАНИИ**



**Группа компаний МАСКОМ** – российский разработчик и интегратор комплексных решений в сфере безопасности и защиты информации. Являясь одним из лидеров рынка, ГК МАСКОМ вот уже четверть века развивает отрасль, разрабатывая и внедряя новые технологии, обеспечивая безопасность государственных организаций и коммерческих предприятий. Успех деятельности ГК МАСКОМ заключается в трех главных источниках и трех неотъемлемых составляющих:

#### ИСТОЧНИКИ

- »» Высоккоквалифицированные специалисты
- »» Инновационные подходы
- »» Территориальное распределение потенциала

#### СОСТАВЛЯЮЩИЕ

- »» Разработка и внедрение технологий
- »» Реализация комплексных решений
- »» Оперативность реагирования на изменения рынка

**ГК МАСКОМ** – это 11 предприятий, работающих в Центральном, Сибирском, Дальневосточном и Крымском федеральных округах. Головное предприятие Группы компаний МАСКОМ располагается в Москве. Все разработки и решения Группы компаний МАСКОМ сертифицированы, сопровождаются технической поддержкой и обучением специалистов в собственном учебном центре.

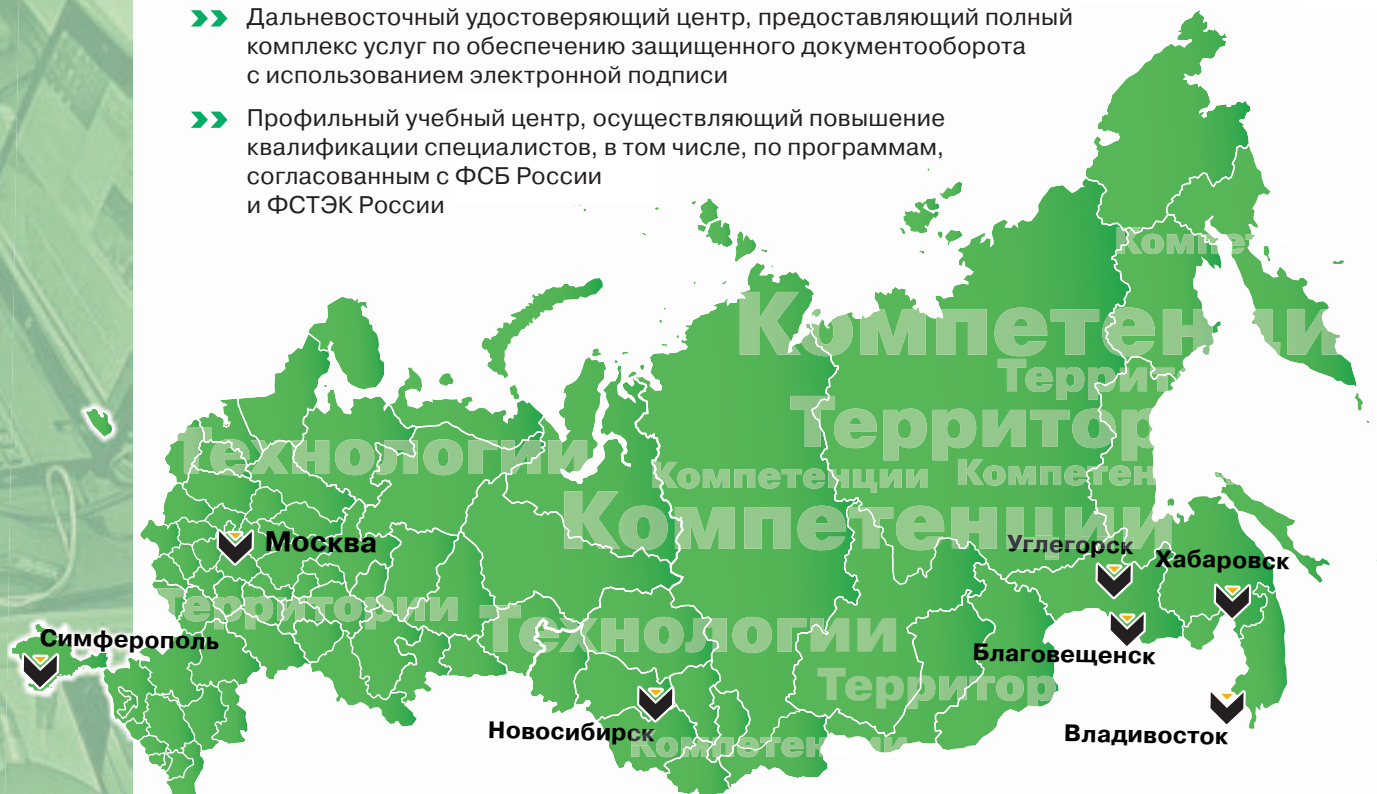
## РЕСУРСЫ:

### ПРОИЗВОДСТВЕННЫЙ ПОТЕНЦИАЛ ГРУППЫ КОМПАНИЙ МАСКОМ:

- »» Подразделения, оказывающие услуги по обеспечению радиотехнической и информационной безопасности, а также по созданию сетей связи и передачи данных, в том числе, в защищенном исполнении
- »» Подразделения по защите объектов инженерно-техническими средствами охраны и комплексными системами безопасности
- »» Подразделения, осуществляющие капитальное строительство специальных зданий и защищенных объектов
- »» Собственное производство средств и систем защиты информации, включая автоматизированные комплексы инструментального контроля защищенности
- »» Единый специализированный центр разработки программного обеспечения

### НАУЧНО-ТЕХНИЧЕСКИЙ ПОТЕНЦИАЛ ГРУППЫ КОМПАНИЙ МАСКОМ:

- »» Научно-технический центр и конструкторское бюро, ведущие научно-техническую и опытно-конструкторскую работу
- »» Испытательные лаборатории, выполняющие сертификационные испытания продукции на соответствие требованиям сертификации ФСБ России и ФСТЭК России
- »» Дальневосточный удостоверяющий центр, предоставляющий полный комплекс услуг по обеспечению защищенного документооборота с использованием электронной подписи
- »» Профильный учебный центр, осуществляющий повышение квалификации специалистов, в том числе, по программам, согласованным с ФСБ России и ФСТЭК России



▼ **Калинин Сергей Владимирович** › Генеральный директор

«... Наша история насчитывает уже четверть века. За это время МАСКОМ из производителя устройств по защите телефонных линий вырос в Группу компаний, чей научно-технический и технологический потенциал позволяет разрабатывать и внедрять комплексные системы безопасности любого уровня сложности. Нашу главную задачу мы видим в том, чтобы предложить рынку технологии, открывающие путь к развитию не только Группы компаний МАСКОМ, но и отрасли безопасности в целом.»»



▼ **Панин Александр Евгеньевич** › Технический директор

«... Необходимо отметить несколько ключевых тенденций, нашедших свое отражение в новых решениях ГК МАСКОМ. Речь идет о взаимной диффузии технологий и технологических решений между отраслями, об интеграции технологий защиты информации в базовые технологии до уровня «невидимости» для пользователя, о крайне высоком значении технологий миниатюризации, о значимости доступности и целостности информационных ресурсов и о важности фактора вовлеченности пользователей в процесс обеспечения информационной безопасности. Поэтому новыми направлениями деятельности ГК МАСКОМ являются как обеспечение безопасности внедрения и эксплуатации АСУ ТП и использования систем связи (в т.ч. беспроводной), так и разработка и внедрение комплексных распределенных систем обеспечения безопасности промышленных объектов. Как и прежде, продолжается развитие «исторических» для ГК МАСКОМ направлений в области технической защиты информации и ПД ИТР.»»



▼ **Клянчин Олег Станиславович** › Заместитель генерального директора

**Курирует Департамент, специализирующийся на создании и внедрении уникальных высококачественных решений и технологий по обеспечению радиотехнической безопасности**

«... В интересах Заказчика мы ставим перед собой не только задачи защиты информации от утечки по техническим каналам, но и недопущение существенных ограничений эксплуатации защищаемых ресурсов, обеспечение выполнения санитарных и экологических норм, эффективность вложения Заказчиком денежных средств. Такой непростой баланс достигается как разработкой принципиально новых средств защиты, так и эффективным использованием новейших строительных материалов.»»



▼ **Шатохин Василий Степанович** › Заместитель генерального директора по управлению персоналом и административным вопросам

«... Мы считаем основной своей ценностью работающих у нас специалистов – настоящих профессионалов, людей, увлеченных своим делом. Хорошие специалисты в технической компании сегодня – товар дефицитный. Для них, прежде всего, мы создаем все условия для карьерного, профессионального и личностного роста, стремимся дать людям не только достойную заработную плату, но и весомые социальные гарантии. Особую ценность представляет благоприятная психологическая атмосфера в нашем коллективе, которую мы культивируем, ибо данный фактор напрямую влияет на эффективность сотрудников.»»





▼ **Ефисько Александр Олегович** ▶ Руководитель центра комплексных систем безопасности

«... Направление комплексной безопасности в Группе компаний МАСКОМ последние годы активно развивается. Выполнены сложные проекты в различных отраслях, как в интересах государственных заказчиков, так и для крупнейших коммерческих структур. Сейчас мы работаем над созданием комплексной системы безопасности космодрома «Восточный». На очереди ряд проектов по обеспечению комплексной безопасности нескольких крупных объектов. Главным преимуществом центра является большой опыт специалистов, работающих в нашей команде.»»



▼ **Фалин Андрей Сергеевич** ▶ Директор департамента информационных технологий

«... Ключевым фактором успеха наших работ является непрерывное совершенствование применяемых нами технических решений, чаще всего эксклюзивных, нетиповых и очень современных. Накопленный опыт и специализированные знания в области информационной безопасности позволяют формировать предложения под требования каждого заказчика. Наши заказчики всегда могут быть уверены в том, что разработанное для них решение является технологически передовым и надежно обеспечивает максимальный уровень защиты информации. Высокий профессионализм, нацеленность на результат, ответственность и опыт – вот за что нас ценят клиенты.»»



▼ **Поярков Андрей Юрьевич** ▶ Генеральный директор МАСКОМ Восток

«Холдинг МАСКОМ Восток многопрофильное объединение 8 компаний, расположенных на Дальнем Востоке и в Сибири. Четыре Центра компетенций: «ДСЦБИ «МАСКОМ» - обеспечения безопасности информации и защиты государственной тайны; «МАСКОМ-Инстрой» - проектирования и капитального строительства специальных зданий и защищенных объектов, создания комплексных систем технической и физической безопасности; «МАСКОМ-Техлайн» - системной интеграции, построения ИТКС, закрытых и открытых систем и объектов связи, защищенного электронного документооборота с использованием квалифицированной электронной подписи, через собственный Удостоверяющий центр; «Стандарт Телеком» - проектирования, создания, эксплуатации и техобслуживания информационно-навигационных систем (ГЛОНАСС/GPS). А также три территориальные компании: «МАСКОМ-Приморье», «МАСКОМ-АМУР», «МАСКОМ-Сибирь.»»»



▼ **Лобанов Максим Иосифович** ▶ Директор УЦ МАСКОМ

«... Учебный центр продолжает наращивать свой учебный потенциал, сохраняя, безусловно, главное, присущее ему, сочетание: традиционно высокий уровень обучения и его практическую ориентированность. Уже намечены и будут еще появляться новые направления обучения как внутри сектора информационной безопасности, так и в смежных с ним направлениях. Сейчас главная наша работа — переоснащение центра, освоение новых учебных форм и современных образовательных технологий, соответствующих статусу отраслевого образовательного учреждения, а также активное развитие филиалов на Дальнем Востоке и в Крыму.»»



▼ **Пименов Артем Михайлович** ▶ Генеральный директор М Софт

«... Разработка специализированного программного обеспечения – перспективное направление деятельности ГК МАСКОМ. Накопленный многолетний опыт и компетенции позволяют разрабатывать и внедрять собственные продукты, так и осуществлять отдельные проектные работы любого уровня сложности. Проектная деятельность и методология разработки регламентируется внутренними стандартами компании, которые основаны на лучших практиках отрасли, благодаря чему гарантировано строгое соблюдение сроков и высокое качество выполненных работ. Наше преимущество – стратегический актив высококвалифицированных специалистов в области системного и бизнес-анализа, прикладных разработчиков и тестировщиков.»»



## УСЛУГИ И РЕШЕНИЯ



## ЭКСПЕРТИЗЫ

### СПЕЦИАЛЬНЫЕ ЭКСПЕРТИЗЫ

Аттестационный центр проведения специальных экспертиз Группы компаний МАСКОМ наделен правом осуществления комплекса мероприятий по подготовке организаций к получению лицензий ФСТЭК России и ФСБ России.

Необходимость проведения специальных экспертиз в рамках лицензирования на осуществление деятельности предприятий и организаций в области защиты информации определена постановлением Правительства РФ №333 от 15.04.1995.

#### Аттестационный центр специальных экспертиз ГК МАСКОМ осуществляет:

- »» Проведение специальных экспертиз для соискателей лицензий ФСТЭК России и ФСБ России
- »» Консалтинг в сфере подготовки организаций к осуществлению лицензируемых видов деятельности в области защиты конфиденциальной информации

**Проведение специальных экспертиз** является финальной составляющей комплекса мероприятий по подготовке организаций к осуществлению деятельности в области технической защиты информации, содержащей государственную тайну, и получению соответствующих лицензий ФСБ России и ФСТЭК России. Специальные экспертизы также необходимы при продлении данных лицензий.

**Консалтинг** лицензируемых ФСТЭК России и ФСБ России видов деятельности в области защиты конфиденциальной информации предоставляется в рамках подготовки организаций к осуществлению данной деятельности.



## СЕРТИФИКАЦИЯ

### СЕРТИФИКАЦИОННЫЕ ИСПЫТАНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ И ЗАЩИЩЕННЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Проведение сертификационных испытаний необходимо для подтверждения соответствия функциональных и специальных свойств средств защиты информации, а также информационных систем и бизнес-приложений требованиям действующих нормативных документов и стандартов.

#### Услуга актуальна для Вас, если:

- » необходимо подтвердить уровень защиты, обеспечиваемый применяемыми средствами;
- » необходимо применять средства защиты, сертифицированные по требованиям безопасности информации;
- » необходимо обеспечить продление действующего сертификата с истекающим сроком действия;
- » Вы являетесь производителем средств защиты информации.

#### При проведении работ мы руководствуемся следующими принципами:

- » Объективность результатов
- » Строгое и полное соответствие требованиям действующих документов
- » Проведение работ в минимальные сроки
- » Минимизация затрат

#### Ценность сертификации:

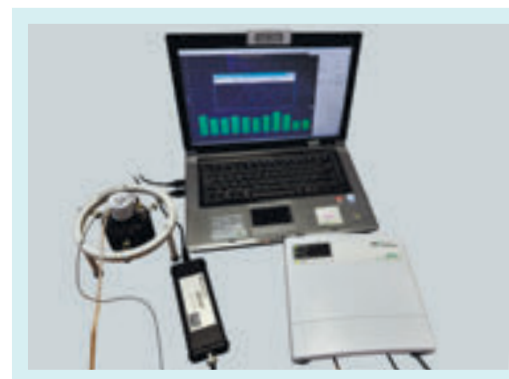
- » Расширение возможностей сбыта Вашего продукта
- » Возможность применения сертифицированных продуктов для защиты информации ограниченного доступа (в соответствии с действующим законодательством)

#### Наши преимущества:

- » Полное техническое и документальное сопровождение процесса подготовки к испытаниям
- » Обеспечение непрерывности бизнеса (предоставляем замену сертифицируемого изделия на период испытаний; возможно проведение работ на Вашей территории)
- » Разработка рекомендаций (по итогам испытаний) по доработке продукта, с целью повышения его конкурентоспособности
- » Консультационная поддержка, сопровождение эксплуатации
- » Подготовка Ваших специалистов в Учебном Центре МАСКОМ по согласованным с регуляторами программам

#### Варианты испытаний:

- » Сертификационные испытания в соответствии с системами сертификации ФСТЭК России и ФСБ России
- » Анализ защищенности информационных систем и бизнес-приложений
- » Испытания на устойчивость к взлому средств защиты, а также тестов на проникновение объектов IT-инфраструктуры



## КОНСАЛТИНГ

### КОНСАЛТИНГ И АУДИТ

ГК МАСКОМ осуществляет консалтинг и аудит в сфере информационной безопасности, охватывающие вопросы безопасности автоматизированных систем, сетей связи и передачи данных, ЦОДов, ситуационных центров и др.

### Консалтинг в области информационной безопасности

- »» что защищаем?
- »» где защищаем?
- »» как защищаем?



Ответы на эти вопросы соискатели лицензий ФСБ России и ФСТЭК России могут получить в рамках консультаций по информационной безопасности, включая вопросы обеспечения информационной безопасности ЛВС, АРМ, ЦОД и облачных вычислений.

Консультации проводят специалисты ГК МАСКОМ, имеющие высокую профессиональную квалификацию в области информационной безопасности.

### При проведении консультаций мы руководствуемся следующими принципами:

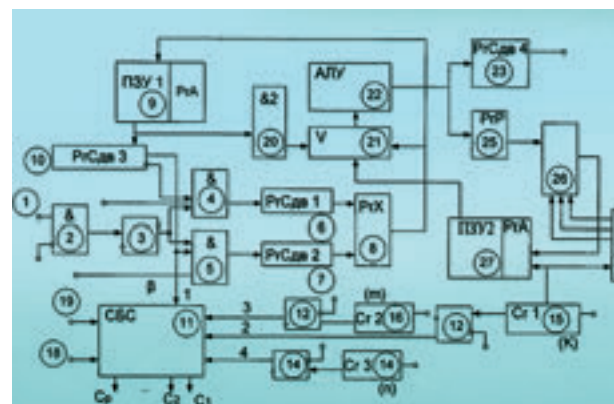
- »» Нацеленность на конечный результат с безусловным учетом интересов Заказчика
- »» Профессионализм и достоверность
- »» Неукоснительное следование требованиям руководящих документов регуляторов в области защиты информации

### В результате проведения консультаций Вы получаете:

- »» Проекты нормативно-распорядительной документации предприятия (политики безопасности, различных руководств и инструкций, стандартов предприятия) в области информационной безопасности
- »» Проекты требуемой регуляторами документации
- »» Проекты документации Заявителя для проведения аттестации объектов информатизации
- »» Техническое задание на создание защищенной информационной системы

### Перечень работ:

- »» Разработка (консультирование по разработке) проектов нормативно-распорядительной документации предприятия в области информационной безопасности
- »» Разработка (консультирование по разработке) проектов рабочей и конструкторской, а также программной документации средств защиты информации или защищенных программных продуктов для их успешной сертификации на соответствие требованиям безопасности информации
- »» Разработка (консультирование по разработке) проектов документов Заявителя для успешной аттестации автоматизированной системы на соответствие требованиям безопасности информации
- »» Разработка (консультирование по разработке) проектов документации, регламентирующей эксплуатацию информационных систем
- »» Разработка Технических заданий на создание системы защиты, защищенных информационных систем или средств защиты информации



### Наши преимущества:

- »» Доскональное знание правовой базы и нормативно-методических документов регуляторов
- »» Высокий профессионализм и многолетний опыт сотрудников
- »» Нацеленность на конечный результат с безусловным учетом интересов Заказчика

### Аудит информационной безопасности

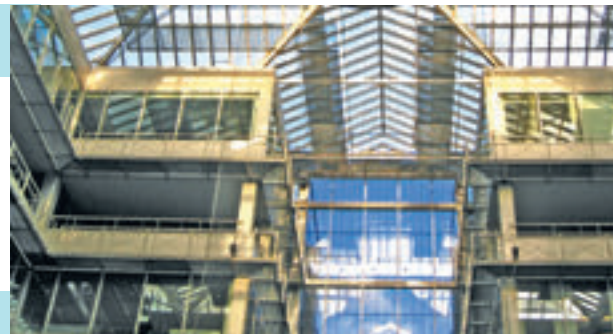
Аудит информационной безопасности от ГК МАСКОМ – многоуровневый анализ защищенности объектов ИТ-инфраструктуры – дает возможность получить полную и объективную оценку защищенности Ваших объектов

### Перечень работ

- »» Оценка реального состояния объектов ИТ-инфраструктуры, проверка достаточности принятых технических и организационных мер защиты обрабатываемой информации на основе действующей нормативно-правовой базы, российских и международных стандартов
- »» Анализ и оценка рисков, связанных с угрозами безопасности информационных ресурсов
- »» Разработка рекомендаций по внедрению дополнительных, а также повышению эффективности существующих организационных и технических мер обеспечения требуемого уровня безопасности информации
- »» Разработка рекомендаций по модернизации самих объектов ИТ-инфраструктуры (при необходимости)
- »» Тест на проникновение (по желанию Заказчика)

### В результате проведения аудита Вы получаете:

- » Объективное представление об уровне защищенности Ваших объектов IT-инфраструктуры
- » «Руководство к действию» по развитию имеющейся системы защиты
- » Повышение капитализации бизнеса



### Наши преимущества:

- » Выполнение аудита по российским и/или международным стандартам
- » Возможность разработки уникальной методики, адаптированной к особенностям конкретных бизнес-процессов
- » Практические рекомендации по итогам аудита для повышения уровня безопасности
- » Возможность выполнения всего спектра работ по приведению объекта IT-инфраструктуры заданным требованиям (по результатам аудита)
- » Обучение Ваших IT-специалистов в Учебном центре МАСКОМ



### Варианты аудита:

- » ISO 27001 (ГОСТ Р ИСО/МЭК 27001)
- » Стандарт безопасности платежных карт PCI DSS
- » Стандарты Банка России СТО БР ИББС
- » Аудит промышленных систем (АСУ ТП, SCADA)
- » Анализ защищенности по индивидуальной программе, согласованной с Заказчиком





## КОМПЛЕКСНЫЕ СИСТЕМЫ БЕЗОПАСНОСТИ

ГК **МАСКОМ** предоставляет полный спектр услуг по созданию комплексных систем безопасности для защиты объектов, включая разработку концепций безопасности, объединяющих все элементы системы защиты для достижения наибольшей эффективности её функционирования, а также материалы, содержащие анализ уязвимости объектов и оценку эффективности существующих систем защиты.

### Основные особенности решений

Для объектов защиты любой категории важности и сложности создаются интегрированные комплексы инженерно-технических средств охраны, объединяющих структурно, конструктивно, функционально и информационно связанные системы и средства обеспечения безопасности в единую систему с общими каналами связи, программным обеспечением и базами данных.

### Перечень работ, которые реализуются:

- »» Разработка концептуальных материалов, инжиниринговые услуги, разработка проектной документации;
- »» Поставка оборудования, строительно-монтажные и пусконаладочные услуги, гарантийное и сервисное обслуживание;
- »» Выполнение ОКР, разработка конструкторской и эксплуатационной документации;
- »» Разработка и производство оборудования, консультационные услуги

### Преимущества решений

- »» Системный подход к выработке решений, позволяющий получить наиболее целостное описание системы безопасности объекта защиты и выбрать наиболее эффективное
- »» Безусловное соответствие созданных решений заданной категории, степени сложности и конфигурации объекта защиты







## РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

### СПЕЦИАЛИЗИРОВАННЫЙ ЦЕНТР РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Компания М Софт создана в 2014 году как специализированный центр разработки программного обеспечения в составе Группы компаний МАСКОМ.

#### Компетенции М Софт:

- »» Интеграционное программное обеспечение систем физической безопасности и систем технической защиты информации
- »» Системы автоматизации, диспетчеризации и мониторинга процессов в реальном времени (SCADA, OPC).
- »» Программное обеспечение для встраиваемых систем
- »» Системы автоматизации бизнес-процессов предприятий (CRM, ERP), в том числе, в защищённом исполнении
- »» Многопользовательские базы данных и системы электронного документооборота многозвенной архитектуры, в том числе в защищённом исполнении
- »» Программное обеспечение для мобильных платформ в защищённом исполнении
- »» Веб-приложения, веб-сервисы различного назначения



#### Преимущества М Софт:

- »» Отлаженный единый процесс разработки для всех программных проектов, основанный на гибкой итеративной методологии (SCRUM)
- »» Опытная команда специалистов, включающая аналитиков, архитекторов ПО, программистов, инженеров по тестированию
- »» Опыт разработки программного обеспечения по требованиям ФСТЭК России и ФСБ России в сфере защиты информации

#### Используемые технологии:

- »» Платформы: .Net, Java, Mono, Microsoft Windows, Linux (Debian, Ubuntu, Astra Linux, openSUSE), Web, MacOS, Android, iOS, Windows Phone.
- »» Языки программирования: C#, Java, C, C++, JavaScript, ActionScript 3, SQL/T-SQL, Objective-C.
- »» Библиотеки и фреймворки: Asp .Net MVC, Spring, NHibernate/Hibernate, EntityFramework, WCF, LinqToSql, MS Unity, Autofac, less, Sass, jQuery, AngularJS, Backbone и др
- »» Базы данных (СУБД): MS SQL Server 2008, PostgreSQL, Oracle, MySQL, SQLite, Firebird, MS Access.
- »» Среды разработки: Microsoft Visual Studio 2013, Xamarin Studio, Adobe Flex, Qt Creator, NetBeans, IDEA, Eclipse.

Программные продукты М Софт	
Решения для Госсектора	
Интеграционная платформа для систем безопасности АССОИ	Программное обеспечение автоматизированной системы сбора и обработки информации, предназначенное для организации в единый информационный и управленческо-логический комплекс систем технической защиты информации (ТЗИ), инженерно-технических средств охраны (ИТСО), систем контроля управления доступом (СКУД), систем видеонаблюдения и функциональных инженерных систем
СПО «Система поддержки принятия решений»	Многокритериальная аналитическая система помощи при принятии решений в сложной информационной среде.
СПО «СЭДО РСО»	Система электронного документооборота для автоматизации работы режимно-секретного отдела, обрабатывающего информацию с уровнем секретности данных до «совершенно секретно» включительно.
СПО «СЭДО СП ТС»	Система электронного документооборота для автоматизации процесса проведения специальных проверок технических средств в соответствии с ОСТ ФСБ России.
АПК «Защищенный мобильный офис»	Аппаратно-программный комплекс, включающий в себя специальное ПО, построенное на базе ОС Android, с функциями усиленной аутентификации, контроля целостности и шифрования, позволяющими осуществлять связь с абонентом по зашифрованному каналу.
АПК «Свиток»	Система криптографической аутентификации пространственно-распределённых IP-источников, обеспечивающая защиту информации в системах видеонаблюдения, технологического телевидения, АСУ ТП, диагностики и мониторинга состояния объектов.
СПО «Система контроля за пользователями информационных систем»	Специальное ПО, обеспечивающее независимую регистрацию обращений пользователей к информационным ресурсам различного назначения, придающее результатам регистрации юридическую значимость в соответствии с ГОСТ 6.10.4-84.
СПО «Реестр внутреннего документооборота»	Автоматизированная система, предназначенная для учета нормативно-правовых актов (НПА), нормативно-правовых документов (НТД) и любых внутренних документов организации с возможностью их оперативной инвентаризации.
Решения для Бизнеса	
СПО «Учет судебных дел»	Система автоматизации работы юридических подразделений, обеспечивающая возможность ведения системного учета и анализа судебных дел, исполнительного производства и претензионной работы с функцией формирования отчетности и вывода документов по произвольным шаблонам.
СПО «Реестр внутреннего документооборота»	Комплексная система работы с внутренними документами компании, обеспечивающая возможность полного перехода на электронный документооборот.
СПО CRM «Клиент + Call-центр»	Реестр действующих и потенциальных клиентов со сведениями о каждом взаимодействии, в том числе запись звонков и регистрация электронных писем.
СПО «Взыскание»	Система учета юридических и физических лиц, имеющих задолженность перед партнерами, банками или страховыми компаниями, обеспечивающая автоматический поиск информации о данных должников в сети ИНТЕРНЕТ, а также их оповещение в автоматическом режиме по разным каналам связи с возможностью дальнейшего анализа результатов.
СПО ERP «Автоматизация предприятия»	Распределенная система комплексной автоматизации производства продукции от заказа до отгрузки, позволяющая предприятию сократить накладные расходы на всех этапах производства за счет систематизации и автоматизации всех процессов производственного цикла и сопровождения изделий.

## ИНТЕГРАЦИОННАЯ ПЛАТФОРМА ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ АССОИ

**АССОИ** – автоматизированная система сбора и обработки информации, предназначенная для организации в единый информационный и управленческо-логический комплекс систем технической защиты информации (ТЗИ), инженерно-технических средств охраны (ИТСО), систем контроля управления доступом (СКУД), систем видеонаблюдения и функциональных инженерных систем.

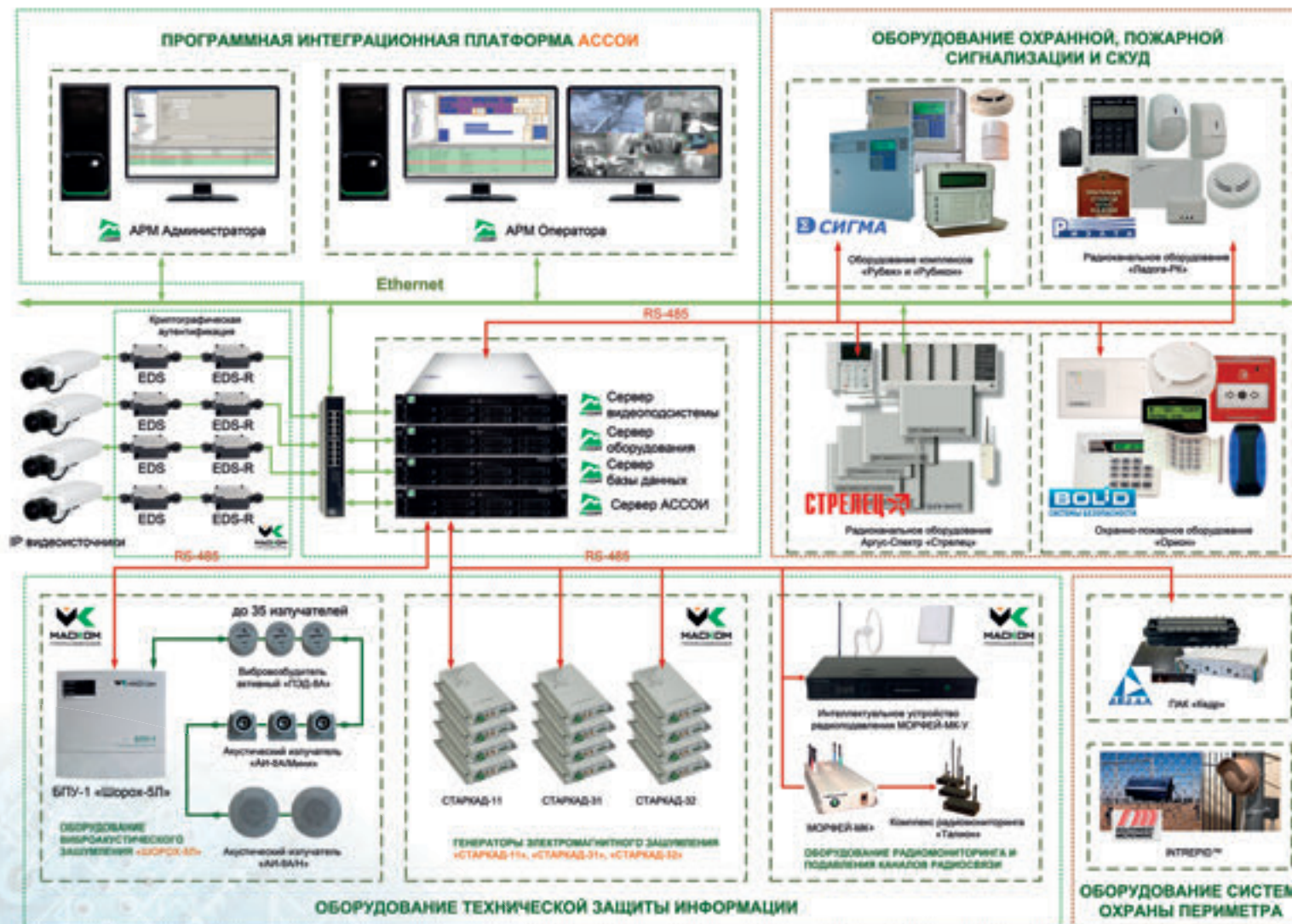
Задача АССОИ – формирование единого информационного пространства для различных систем безопасности и логическое их взаимодействие.

### Основные особенности АССОИ:

- »» **Масштабируемость.** Система обеспечивает возможность неограниченного расширения как по объёму используемых в ней данных, так и по числу активных узлов системы и пользователей за счёт иерархической секторной архитектуры. Возможность быстрой интеграции в систему новых программных модулей, оборудования и протоколов.
- »» **Защищённость.** Доступ к функциям и данным системы смогут получать только авторизованные пользователи. Действия авторизованных пользователей протоколируются. Полномочия пользователей по конфигурированию системы, управлению объектами системы, доступу к данным системы могут гибко настраиваться.
- »» **Программируемость.** Система поддерживает встроенные средства, позволяющие автоматизировать протекающие в ней процессы на уровне конфигурации системы (без внесения изменений в программный код).
- »» **Надёжность.** Устойчивость к программным сбоям и минимизация их последствий.
- »» **Отказоустойчивость.** Обеспечение «горячего» резервирования важных элементов системы.
- »» **Диагностируемость.** Система способна выдавать диагностическую информацию, позволяющую оценивать её работоспособность, прогнозировать возможные сбои в будущем и выявлять причины произошедших сбоев в работе.
- »» **Локализуемость.** Пользовательский интерфейс системы поддерживает возможность локализации.

### На данный момент в АССОИ уже интегрированы следующие оборудование и системы:

- »» Оборудование производства ГК МАСКОМ:
  - » система защиты информации от утечки по каналу АВАК «Шорох-5Л»;
  - » генераторы электромагнитного зашумления «Старкад-32», «Старкад-31» и «Старкад-11»;
  - » система радиомониторинга «Талион»;
  - » блокиратор средств беспроводной связи «Морфей-МК-У»;
  - » Система криптографической аутентификации «Свиток» производства ГК МАСКОМ;
- »» Оборудование СКУД, охранной, тревожно-вызывной и пожарной сигнализации комплексов «Рубеж» и «Рубикон» производства ГК СИГМА;
- »» Оборудование системы охраны периметра INTREPID компании Southwest Microwave;
- »» IP-видеоисточники, в том числе, поддерживающие стандарт Onvif;
- »» Внутриобъектовая радиосистема охранно-пожарной и адресно-аналоговой пожарной сигнализации и оповещения «СТРЕЛЕЦ» производства компании «Аргус-Спектр»;
- »» Система беспроводной охранной и пожарной сигнализации «Ладога-РК» производства компании «Риэлта»;
- »» Комплексные технические средства физической защиты ОАО НПК «Дедал»;
- »» Охранное и пожарное оборудование системы «Орион» производства компании BOLID.



## СИСТЕМЫ РАДИОТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ

### РАДИОЭЛЕКТРОННОЕ ПОДАВЛЕНИЕ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ (РЭП БСС)

Промышленный шпионаж в последнее время набирает обороты и приводит к нерадостной статистике: убытки компаний от промышленного шпионажа достигают десятков миллионов долларов. Одним из наиболее простых и дешевых методов получения конфиденциальной информации, которым широко пользуются современные злоумышленники, является использование беспроводных каналов утечки информации.

#### Наши принципы:

- » Системы подавления создаются эффективными и оптимальными
- » Внедрение систем подавления осуществляется в соответствии с требованиями ГКРЧ и операторов беспроводных систем связи
- » Системы подавления должны быть безопасны для здоровья человека

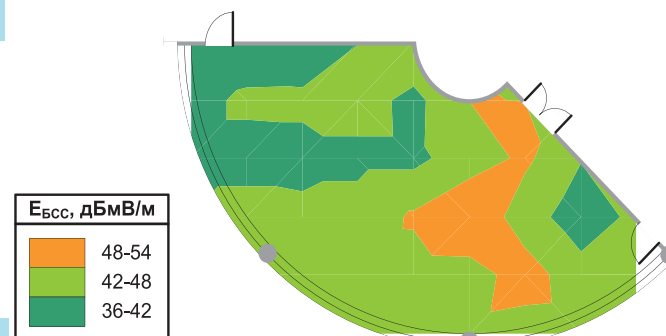
### Построение систем РЭП БСС

#### При построении систем РЭП БСС учитываются:

- » Архитектурно-строительные, инженерные и дизайнерские особенности помещения
- » Диапазоны подавления
- » Электромагнитная обстановка на объекте
- » Электромагнитная совместимость с другими системами объекта

#### Результат:

- » Защищённое по каналу БСС помещение, в котором вы можете проводить конфиденциальные мероприятия, не опасаясь утечки информации



Карта распределения значений E<sub>БСС</sub> в диапазоне частот 1805–1880 МГц



### Преимущества нашего подхода:

- » Учитываем требования ГКРЧ и Роспотребнадзора (СанПиН)
- » Имеем многолетний опыт в решении задач любой сложности в условиях сложной электромагнитной обстановки
- » Используем запатентованную методику проведения исследований радиообстановки
- » Применение комбинации пассивных (электромагнитное экранирование) и активных (технические средства защиты) решений для защиты каналов БСС

### Перечень работ:

- » Предварительное обследование (оценка объектовой электромагнитной обстановки)
- » Подбор оптимального и эффективного решения РЭП (ТЭО)
- » Проектно-изыскательские работы
- » Внедрение и контроль эффективности
- » Гарантийное и техническое обслуживание

**Проекты РЭП БСС уже реализованы нами в ряде крупных корпораций, силовых структурах, государственных учреждениях**



## СИСТЕМЫ РАДИОТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ

### ЗАЩИТА ПОМЕЩЕНИЙ

Подавляющее большинство подразделений безопасности в своей практике сталкиваются с задачей обеспечения комплекса мероприятий по защите информации на своих ремонтируемых, реконструируемых или строящихся объектах.

#### Два возможных варианта организации защиты помещений:

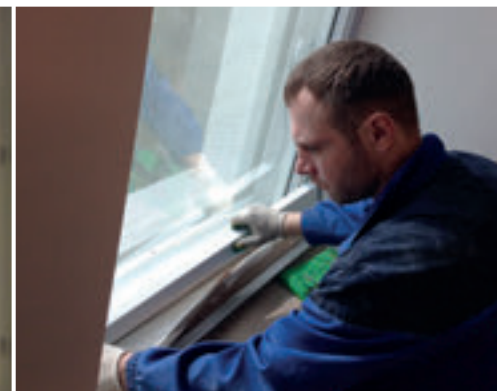
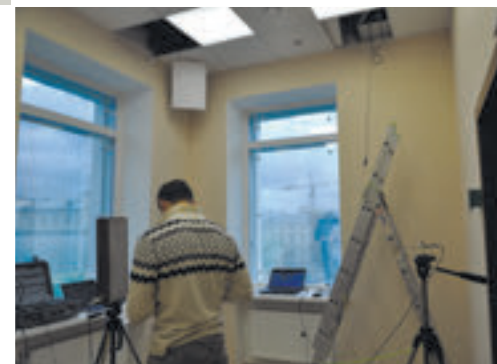
- »» Организация выполнения комплекса мероприятий по защите информации по завершению строительных работ и сдачи объекта в эксплуатацию
- »» Выполнение данных работ в рамках капитального строительства

Мы рекомендуем осуществлять защиту помещений на этапе капитального строительства или капитального ремонта.

### ОРГАНИЗАЦИЯ ЗАЩИТЫ ПОМЕЩЕНИЙ В РАМКАХ КАПИТАЛЬНОГО СТРОИТЕЛЬСТВА

#### Ключевые особенности:

- » Решение, где предусмотрены преимущественно пассивные меры защиты, в соответствии с требованиями СанПиН и ГКРЧ.
  - ▶ **Результат** – экологичное эффективное решение (без паразитных шумов и навесного монтажа)
- » Проведение специальных проверок и специальных исследований оборудования, устанавливаемого в помещении, до его инсталляции, исключающих необходимость демонтажа ранее установленного оборудования для последующих проверок.
  - ▶ **Результат** – существенная экономия времени и сохранение гарантии на устанавливаемое оборудование

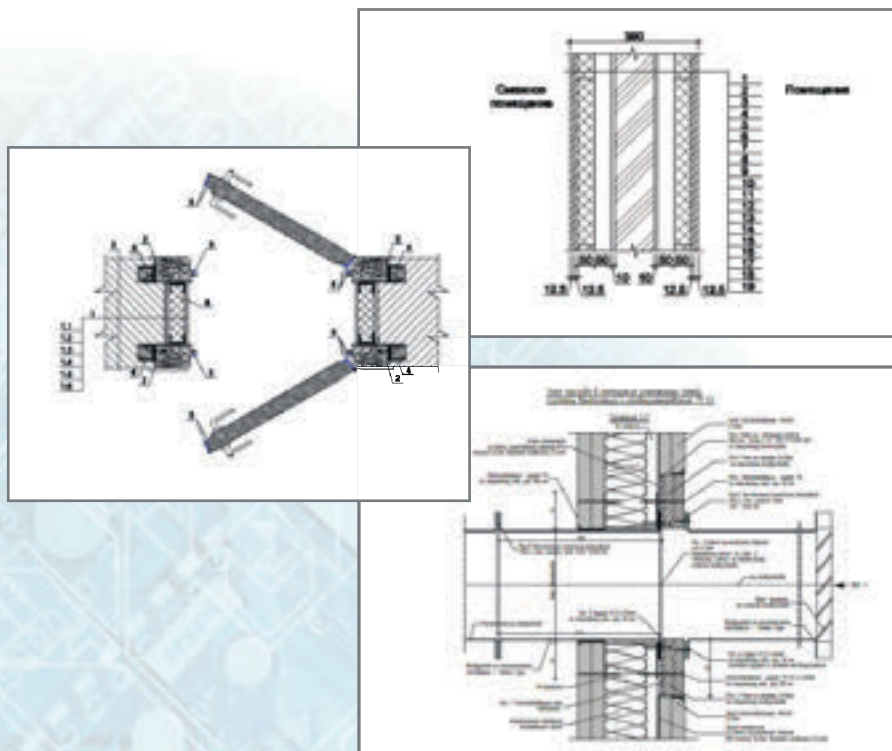
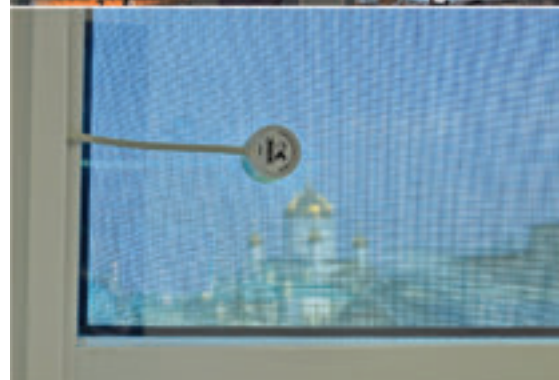




- Возможность выявить все каналы утечки информации, спланировать установку активного оборудования, строительные мероприятия по звукоизоляции, виброизоляции на этапе строительства
  - ▶ **Результат** – экономия средств при сохранении качества защиты
- Учёт индивидуальных особенностей объекта и пожеланий Заказчика на этапе формирования ТЗ и выполнения проектно-изыскательских работ
  - ▶ **Результат** – удобство эксплуатации, вписанность средств защиты в дизайн и архитектуру помещения
- Работы выполняются по титулу капитального строительства, а не из бюджета подразделения
  - ▶ **Результат** – эффективное управление денежными средствами, защищенный объект введен в эксплуатацию, готов к работе, а не является подготовленным объектом в общестроительном плане

#### Выполненные работы:

- За 25 лет компанией реализовано более 300 проектов в интересах таких крупных Заказчиков, как МО РФ, ФСБ России, ФСО России, МВД России, ФНС России, Минпромторг, АТЦ СНГ, Росатом, ФСК ЕЭС, РусГидро, Газпром и др.



## Экранированные сооружения

Группа компаний МАСКОМ проектирует, создает и модернизирует экранированные сооружения (ЭС) – экранированные (ЭК) и безэховые камеры (БЭК) различного назначения и с различными тактико-техническими характеристиками:

- » защитные и испытательные ЭС в области технической защиты информации и противодействия иностранным техническим разведкам;
- » защитные и испытательные ЭС в области электромагнитной совместимости и экологической безопасности;
- » комбинированные камеры с электромагнитной защитой, звуко- и виброизоляцией.

**Классы экранирования:** 1-й, 2-й, 3-й классы по ГОСТ

**Диапазоны:** 10 кГц – 40 ГГц с затуханием до 120 дБ

### Наши преимущества:

- » ГК МАСКОМ выполняет полный цикл работ по созданию ЭС: от формирования технического задания и разработки рабоче-конструкторской документации до ввода объекта в эксплуатацию с его последующей аттестацией, гарантийным техническим и сервисным обслуживанием.
- » Наличие собственных технологических и производственных мощностей позволяет реализовывать нестандартные проекты по требованиям Заказчика.

### Выполненные работы:

- » ГК МАСКОМ построено и модернизировано более 50 экранированных и безэховых камер для различного целевого назначения: от испытательных полигонов до защищённых центров обработки данных – в интересах различных министерств, ведомств, служб и промышленных предприятий, в числе которых Минобороны России, ФСБ России, ФСИН России, Министерство промышленности и торговли России, НИИСУ и др.
- » Все камеры созданы на базе инженерно-технических и аппаратно-программных решений собственного производства.



## Выпускаемая продукция для экранированных сооружений

### Дверные системы



#### Экранированные двери/ворота

##### Технические характеристики:

Класс экранирования – 2

Затухание до 80 дБ в диапазоне частот 10 кГц – 37,5 ГГц

#### Двери в звукоизоляционном исполнении

##### Технические характеристики:

Затухание по акустическому шуму – до 60 дБ

#### Двери с элементами электромагнитной защиты

##### Технические характеристики:

Затухание 30 дБ в диапазоне 450 МГц – 2,7 ГГц

Затухание по акустическому шуму – до 50 дБ

### Радиопоглощающие материалы



#### «ЭРИДАН МР-530»

##### Технические характеристики:

Внешние размеры – 525×175×530 мм (Д×Ш×В);

Диапазон частот 40 МГц – 40 ГГц;

Крепление – сборная конструкция, блоками с размером 525×525 мм (Д×Ш);

Коэффициент отражения по мощности при падении электромагнитной волны по нормали к изделию:

- |                       |                              |
|-----------------------|------------------------------|
| а) 40 МГц – «–15 дБ»  | д) 300 МГц – «–40 дБ»        |
| б) 60 МГц – «–15 дБ»  | е) 600 МГц – «–40 дБ»        |
| в) 100 МГц – «–22 дБ» | ж) 1,5 ГГц – «–40 дБ»        |
| г) 150 МГц – «–30 дБ» | з) 3 ГГц – 40 ГГц – «–50 дБ» |

Условия эксплуатации:

- |  |
|--|
| а) Температура окружающей среды – от +5 до +60°C |
| б) Относительная влажность – не более 80%        |

Горючесть – самозатухающий материал

### Помехоподавляющие фильтры



#### Водопроводные фильтры

##### Технические характеристики:

Диапазон: 150 кГц – 2 ГГц.

Затухание: не менее 80 дБ

Расход жидкости: 150 куб. м/час

Давление: рабочее – 6 атм. максимальное – 8 атм.

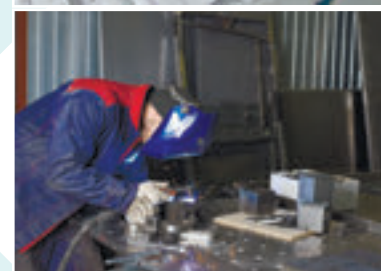


#### Электрические фильтры серии «Фазан»

##### Технические характеристики:

Диапазон: 0,02 – 1000 МГц

Затухание: не менее 60 дБ



## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ

### СОЗДАНИЕ СЕТЕЙ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ

ГК МАСКОМ предоставляет полный спектр услуг по созданию сетей связи и передачи данных.

#### В рамках выполнения работ производится:

- »» Проектирование систем и объектов связи
- »» Проектирование центров обработки и хранения данных
- »» Проектирование локально-вычислительных сетей, структурированных кабельных сетей телефонной связи, видеоконференцсвязи
- »» Строительно-монтажные и пусконаладочные работы любой сложности
- »» Техническое обслуживание поставляемого оборудования

#### Преимущества нашего подхода, к созданию сетей связи и передачи данных:

- »» Выполнение работ собственными силами (собственное проектное бюро и строительно-монтажные подразделения)
- »» Реализация проектов с бюджетом до 3 млрд. рублей по одному договору (наличие соответствующего свидетельства СРО)
- »» Большой опыт выполнения работ в соответствии со специальными требованиями МО РФ, ФСО России и иных регуляторов
- »» Все работы выполняются в соответствии с требованиями производителей и стандартами EIA/TIA-568-C/0, ISO/IEC IS11801, ГОСТ

#### Результат:

- »» Гарантия положительного заключения любой экспертной организации
- »» Надёжное современное решение в области обеспечения связи и передачи данных



## ЗАЩИЩЁННЫЕ АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ

ГК МАСКОМ создает защищенные (защищает существующие) автоматизированные системы:

- » Информационные системы персональных данных
- » Государственные информационные системы
- » Информационные системы, обрабатывающие информацию, составляющую государственную тайну
- » Информационные системы, обрабатывающие информацию, составляющую коммерческую тайну

### Принципы, которые мы неукоснительно соблюдаем:

- » Минимизация влияния системы защиты на основные функции АС
- » Комплексность и целесообразность системы защиты (нейтрализация актуальных угроз)
- » Правомочность (соответствие требованиям) и эффективность системы защиты

### В рамках выполнения работ производится:

- » Предварительное обследование
- » Подбор оптимального и эффективного решения (ТЭО)
- » Проектирование
- » Внедрение и контроль эффективности

### Преимущества нашего подхода к построению защищенных АС:

- » Наши решения эффективны и сбалансированы по цене
- » Мы имеем многолетний опыт по защите автоматизированных систем любой сложности
- » Рассчитываем и учитываем риски

### Результат:

- » Защищенная АС, нейтрализующая актуальные угрозы безопасности информации и соответствующая требованиям руководящих документов
- » Гарантия и уверенность в безопасности информации, спокойствие за сохранение конфиденциальности, доверие партнеров, комфорт и качество выполненных работ

Защищённые автоматизированные системы уже построены нами в ряде крупных корпораций, силовых структурах, государственных учреждениях



- .....» Доступ в сеть «Интернет»
- - - -» Защищенный терминальный доступ
- ==== Криптографически защищенное соединение удалённых сегментов

## ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ

### ЗАЩИЩЕННЫЕ СТРУКТУРИРОВАННЫЕ КАБЕЛЬНЫЕ СЕТИ

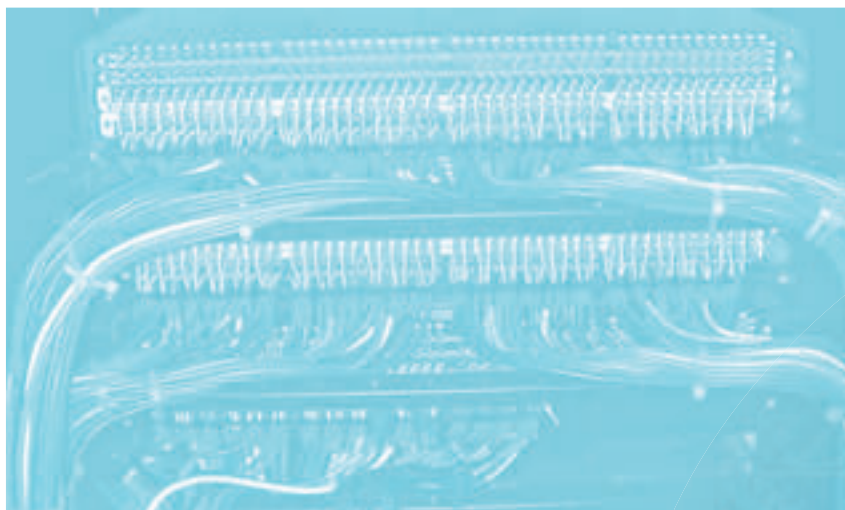
ГК МАСКОМ предоставляет весь комплекс услуг по проектированию и монтажу защищённых структурированных кабельных систем (СКС).

#### Принципы, которые мы неукоснительно соблюдаем:

- » Учет требований заказчика и перспектив развития его информационной системы
- » Соблюдение оптимального соотношения «стоимость-эффективность»
- » Своевременность, точность и полнота выполнения нами своих обязательств

#### В рамках выполнения работ производится:

- » Консультирование, проведение технического обследования объекта
- » Согласование топологии будущей защищённой структурированной кабельной системы
- » Подготовка коммерческого предложения с указанием материалов, оборудования, работ, цены и общей стоимости
- » Разработка проекта, включающего в себя документы, чертежи и схемы, необходимые для выполнения работ



- » Проведение монтажных работ, включая подготовительные, в том числе, монтаж трассы, прокладка кабеля, сборка монтажных шкафов и другие работы в рамках проекта
- » Тестирование всех кабельных трасс с помощью специализированного оборудования

#### Преимущества нашего подхода к проектированию и построению защищённой структурированной кабельной системы:

- » Исполняем требования производителей, специальные требования и стандарты ГОСТ, TIA или ISO
- » Готовим качественную проектную документацию и полное документирование построенных сетей
- » Располагаем квалифицированным персоналом
- » Обладаем успешным опытом реализации проектов в ряде крупных корпораций, в государственных учреждениях, на объектах силовых структур
- » Берем на себя полную ответственность за ведение проекта любой сложности, тщательно планируем каждый его этап, обеспечиваем качественные результаты в установленные сроки

#### Результат:

- » Единая среда передачи сигналов для всего действующего и перспективного оборудования различного класса
- » Высокое качество и надежность всех элементов защищённых СКС
- » Системная гарантия не менее 15 лет на систему и не менее 20 лет на компоненты



## СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

ГК МАСКОМ предоставляет полный комплекс услуг по созданию системы защиты персональных данных. Информационные системы персональных данных должны быть надежно защищены и соответствовать требованиям Федерального закона «О персональных данных» (№ 152 от 27.07.2006 г.)

### Принципы, которые мы неукоснительно соблюдаем:

- »» Строим индивидуальную систему защиты персональных данных для каждого клиента, каждый проект прорабатываем индивидуально
- »» Создаем систему защиты персональных данных с возможностью дальнейшей модернизации и масштабирования
- »» Проектируем системы защиты персональных данных с учетом оптимального соотношения «стоимость-эффективность»
- »» Используем отечественные сертифицированные средства защиты информации и лицензионное программное обеспечение
- »» Следуем правилам профессиональной этики и гарантируем полную конфиденциальность сведений, полученных в процессе сотрудничества



### В рамках выполнения работ производится:

- »» Обследование информационных систем персональных данных
- »» Разработка концепции защиты персональных данных и выработка рекомендаций по оптимизации процессов обработки и защиты информации
- »» Идентификация и классификация информационных систем персональных данных
- »» Разработка модели угроз безопасности персональных данных и модели нарушителя
- »» Разработка Технического задания на создание системы защиты персональных данных
- »» Проектирование системы защиты персональных данных
- »» Разработка комплекта организационно-распорядительной документации
- »» Поставка средств защиты информации
- »» Установка и настройка средств защиты информации
- »» Оценка эффективности принимаемых мер по обеспечению безопасности персональных данных





### Преимущества нашего подхода к созданию системы защиты персональных данных:

- » Высокий профессионализм специалистов и успешный опыт реализации крупных проектов являются залогом качественного выполнения поставленных задач по обеспечению безопасности данных в информационных системах
- » Мы берем на себя полную ответственность за ведение проекта любой сложности и всегда тщательно планируем каждый этап реализации проекта, обеспечивая достижение качественных результатов в установленные сроки
- » Документация, разработанная нами, соответствует требованиям законодательных актов, методик руководящих документов ФСТЭК России и ФСБ России, а также требованиям ГОСТ
- » У нас есть типовые решения по созданию систем защиты персональных данных.

### Результат:

- » Созданная система защиты персональных данных соответствует требованиям законодательства, как в части технических средств защиты, так и в части организационных процедур
- » Информационная система персональных данных надежно защищена и обеспечена техническим обслуживанием в течение гарантийного срока



Роскомнадзор



ФСБ России



ФСТЭК России

## СИСТЕМЫ ВИРТУАЛИЗАЦИИ И ЦОД

ГК МАСКОМ выполняет весь спектр работ по проектированию, созданию и поддержке ЦОД, виртуальных систем, супер-вычислительных комплексов и высокопроизводительных кластерных платформ любых масштабов. Также в сферу нашей компетенции входит создание IT-инфраструктуры ЦОД специального назначения.

### Принципы, которые мы неукоснительно соблюдаем:

- »» Комплексный подход. Мы используем как собственные наработки, так и лучшие отраслевые практики
- »» Сотрудничество с ведущими мировыми производителями оборудования и ПО. Мы делаем упор на наиболее технологичные продукты таких вендоров, как IBM, HP, EMC, Cisco и др.
- »» Защищенное исполнение. Особенность наших ЦОД заключается в возможности реализации любых требований по информационной безопасности и отказоустойчивости

### Преимущества нашего подхода к построению защищенных систем виртуализации и ЦОД:

- »» Сбалансированность по цене
- »» Наш многолетний опыт по защите автоматизированных систем любой сложности
- »» Выполнение работ собственными силами по всем разделам проекта

### В рамках выполнения работ производится:

- »» Обследование и анализ бизнес-процессов
- »» Нагрузочное тестирование приложений Заказчика
- »» Формализация требований Заказчика и регуляторов
- »» Разработка решений и регламентов эксплуатации и обслуживания
- »» Подготовка/строительство зданий/сооружений
- »» Оборудование инженерными системами и проводными сетями различного назначения
- »» Поставка и развертывание компонентов ЦОД
- »» Выполнение комплекса мероприятий по защите информации
- »» Сертификация

### Результат:

- »» Снижение рисков нарушения целостности, доступности и конфиденциальности информации
- »» Обеспечение непрерывности бизнес-процессов
- »» Повышение уровня эффективности использования вычислительных ресурсов
- »» Снижение издержек на управление и дальнейшее развитие IT-инфраструктуры
- »» Возможности диверсифицировать бизнес, оказывать клиентам новые виды услуг



## ЗАЩИЩЕННЫЕ СИСТЕМЫ ВКС И СИТУАЦИОННЫЕ ЦЕНТРЫ

Ситуационные центры в последнее время стали одним из важнейших инструментов государственного и корпоративного управления в штатных и кризисных ситуациях, обеспечивая руководителей исполнительных органов государственной власти, силовых ведомств, корпораций оперативной информацией. Подобные объекты, как правило, оснащаются системами видеоконференцсвязи (ВКС) в защищенном исполнении для организации передачи конфиденциальной и секретной информации по обычным каналам связи.

### Принципы, которые мы неукоснительно соблюдаем:

- »» Необходимость и достаточность
- »» Эффективность системы
- »» Соответствие руководящим документам регуляторов в области защиты информации
- »» Удобство Заказчика

### Ценность защищенных ВКС и ситуационных центров:

- »» Нейтрализация угроз утечки информации при ежедневных коммуникациях с удаленными собеседниками, защищенность от конкурентной разведки
- »» Обеспечение штатного функционирования системы и сведения неблагоприятных последствий к минимуму в режиме нештатной ситуации
- »» Экономия средств на командировки
- »» Повышение имиджа в деловой среде

### Преимущества нашего подхода:

- »» Мы имеем многолетний опыт в решении задач любой сложности
- »» Учитываем требования руководящих документов ФСТЭК России и ФСБ России
- »» Рассчитываем и учитываем риски

### В рамках выполнения работ производится:

- »» Предпроектное обследование
- »» Подбор оптимального и эффективного решения
- »» Проектирование
- »» Поставка оборудования
- »» Монтажные и пусконаладочные работы
- »» Испытания эффективности применяемых средств защиты

### Результат:

- »» ВКС – защищенное соединение с удаленными собеседниками, гарантирующее полную конфиденциальность переговорам во время сеанса
- »» Возможность одновременно довести распоряжения до большого числа филиалов (и/или подчиненных сотрудников)
- »» Ситуационный центр – удобный инструмент проведения оперативных совещаний
- »» Центр мониторинга и анализа текущих событий, информации, антикризисный центр управления



## СИСТЕМА ОБЕСПЕЧЕНИЯ ЖИЗНЕДЕЯТЕЛЬНОСТИ I-CITY

Концепция I-City – кардинально новое направление развития современного города за счет создания единого информационного пространства и интеграции аналитических систем, отвечающих за безопасность жизнедеятельности города.

### Концепция I-City предусматривает:

- »» Внедрение инновационных решений в области энергосбережения, ЖКХ, транспорта, образования, здравоохранения, экологии, информационных технологий
- »» Системный подход к организации единого интеллектуального пространства города
- »» Обеспечение и управление информационной безопасностью
- »» Использование мирового опыта

### Результат и перспективы внедрения:

В результате внедрения инновационных решений I-City город превращается в интеллектуальное пространство с принципиально новыми возможностями централизованного управления его процессами

- »» Обеспечение комфорта и безопасность жителей и гостей современных городов
- »» Повышение экономической эффективности коммунальной сферы, транспортной инфраструктуры
- »» Улучшение экологической обстановки

## ПРАКТИЧЕСКАЯ РЕАЛИЗАЦИЯ КОНЦЕПЦИИ I-CITY

Построение единой информационной сети на примере региона РФ



ЦЕНТРЫ УПРАВЛЕНИЯ ГУБЕРНАТОРА КРАЯ,  
ВКЛЮЧАЯ СИСТЕМУ ВИДЕОКОНФЕРЕНЦСВЯЗИ (ВКС)

ДЕЖУРНО-ДИСПЕТЧЕРСКИЕ ЦЕНТРЫ ЕДИНОЙ ДЕЖУРНО-  
ДИСПЕТЧЕРСКОЙ СЛУЖБЫ (ЕДДС). ВКЛЮЧАЯ ЦЕНТР УПРАВЛЕНИЯ  
КРИЗИСНЫМИ СИТУАЦИЯМИ (ЦУКС)

«СИСТЕМА-112» И ЕЕ ИНТЕГРАЦИЯ В ЕДДС

СИСТЕМА ОПОВЕЩЕНИЯ  
И ИНФОРМИРОВАНИЯ

СИСТЕМА «БЕЗОПАСНЫЙ ГОРОД»

По итогам внедрения Группа компаний МАСКОМ была отмечена благодарностью Губернатора Хабаровского края и признана лучшей компанией 2010 года, работающей на территории края.

В настоящее время работы по внедрению системы ведутся в Амурской области.

## I-City это:

- » «I-City центр» – Ситуационные центры и центры управления
- » «I-City 112» – Оперативное Управление городскими службами
- » «I-City Эко» – Экологическая безопасность
- » «I-City Безопасный город» – Система «Безопасный город»
- » «I-City ЖКХ» – Автоматизация и управление ЖКХ. Системы энергоэффективности
- » «I-City ИНФО» – Служба оповещения и информации
- » «I-City Диспетчер» – Единая дежурно-диспетчерская служба
- » «I-City Справка» – Информационно-справочные службы 112
- » «I-City Дороги» – Управление безопасностью дорожного движения



### СОВРЕМЕННЫЙ ГОРОД-ИНТЕЛЛЕКТУАЛЬНОЕ ПРОСТРАНСТВО

Основная стратегическая задача:

### УСТОЙЧИВОЕ РАЗВИТИЕ ГОРОДА



Общественная безопасность



Транспорт



Здравоохранение



Энергоснабжение



ДЕЯТЕЛЬНОСТЬ ГОРОДА



Водоснабжение



Экоустойчивость



Администрирование города



Образование



Жилищно-коммунальное хозяйство



Экономическое развитие



Строительство





**НАУКА**

## НАУКА

С самого момента рождения компании в ГК МАСКОМ ведется серьёзная научно-исследовательская и опытно-конструкторская работа. В научную деятельность инвестируется значительная часть интеллектуального и материального потенциала предприятия. Современный уровень научной деятельности обеспечен следующими факторами:

- »» Высоким профессиональным уровнем исполнителей, отдавших много лет своей трудовой биографии научно-исследовательской работе
- »» Накопленным опытом применения действующих методик и решений
- »» Высоким уровнем технического обеспечения (наличие экранированной камеры большого объёма и площади, отдельного помещения для акустических измерений, современные высокоточные средства измерений и исследований)

Мы активно участвуем в исполнении федеральных целевых программ, выполняем исследования в области защиты информации, которые можно отнести и к фундаментальным, и к прикладным областям. Нашими научными специалистами проводятся:

- »» Исследования в сфере разработки основополагающих методических материалов в областях акустики и вибраций, акустоэлектрических преобразований
- »» Разработки корректировок действующих документов
- »» Проектные и технические решения конкретных задач защиты
- »» Исследования и разработки в области защиты от утечки речевой информации, где накоплен особенно значительный опыт

Результаты наших научных работ:

- »» Проекты методических материалов
- »» Предложения по внесению изменений в уже действующие нормативно-методические материалы
- »» Новые методики
- »» Схемотехнические решения, как устройств защиты информации, так и аппаратуры контроля технических каналов утечки информации
- »» Проекты объектов, выполненные с учётом комплексной защиты информации по всем направлениям (каналам), включающие применение инновационных решений



Практическим подтверждением научного потенциала и опыта сотрудников МАСКОМ являются:

- » Более 50 НИОКР, 20 из которых выполнены за последние 3 года
- » Девять патентов на разработанные технические решения и подходы, примененные при создании технических средств и систем обеспечения безопасности.
- » Линейка современных автоматизированных систем, которые позволяют измерять параметры и контролировать все типовые технические каналы утечки информации.

**Ряд разработанных решений** стал, де факто, стандартом в своей области. Так, система оценки защищенности выделенных помещений по виброакустическому каналу «Шепот» и система оценки защищенности технических средств от утечки информации по каналу ПЭМИН «Сигурд» используются службами контроля ФСТЭК России.

**Многие системы** обладают уникальными параметрами не только в России, но и в мире. Например, система «Талис-НЧ», разработанная специалистами МАСКОМ, способна измерять сигналы в 15-20 наноВольт в неэкранированных линиях. Входное сопротивление при этом составляет десятки МегаОм.

**Наличие Аттестатов аккредитации** испытательной лаборатории в различных системах сертификации, позволяет нам выполнять работы по сертификации практически любых средств технической защиты информации.

**Нашими заказчиками в этой области** являются ФСТЭК России, силовые структуры федерального уровня (МО России, ФСБ России, ФСО России), ведущие (федеральные) агентства и ведомства оборонного комплекса и крупнейшие коммерческие фирмы страны.





УЧЕБНЫЙ ЦЕНТР



УЧЕБНЫЙ  
ЦЕНТР



**Учебный центр МАСКОМ создан в 1998 году** для повышения квалификации руководителей и специалистов, работающих в области обеспечения безопасности информации предприятий, организаций и учреждений.

Образовательная деятельность Центра осуществляется на основании Лицензии Департамента образования города Москвы.

Обучение проводится по программам, согласованным с ФСТЭК России и ФСБ России.

**В 2004 году Учебный центр МАСКОМ** получил статус некоммерческого образовательного учреждения. С 2005 года УЦ начинает проводить выездные курсы в регионах России.

**УЦ МАСКОМ** является одним из ведущих в Российской Федерации специализированных учебных заведений, осуществляющих образовательную деятельность в области защиты информации.

К настоящему времени в Учебном центре повысили квалификацию или приобрели новые знания по вопросам технической защиты информации более **10 000 человек**.

**Учебный центр МАСКОМ** включен Межведомственной комиссией по защите государственной тайны в список образовательных учреждений, документ об окончании которых дает право руководителям, ответственным за защиту сведений, составляющих государственную тайну, считаться прошедшими государственную (итоговую) аттестацию. (Указ Президента РФ от 06.10.2004 N 1286)

## НАПРАВЛЕНИЯ ОБУЧЕНИЯ



### Общие и специальные вопросы защиты государственной тайны и конфиденциальной информации

На курсах по данному направлению Вы получите не только знания по вопросам комплексной защиты конфиденциальной информации и сведений, составляющих государственную тайну в организации, но и практически закрепите полученный материал.

В процессе обучения Вы получите знания и навыки по разработке комплекта организационно-распорядительной документации по защите информации, а также опыт применения средств защиты и контроля защищенности информации.

**В рамках этого направления Учебный центр МАСКОМ предлагает пять курсов продолжительностью от 18 до 72 часов.**

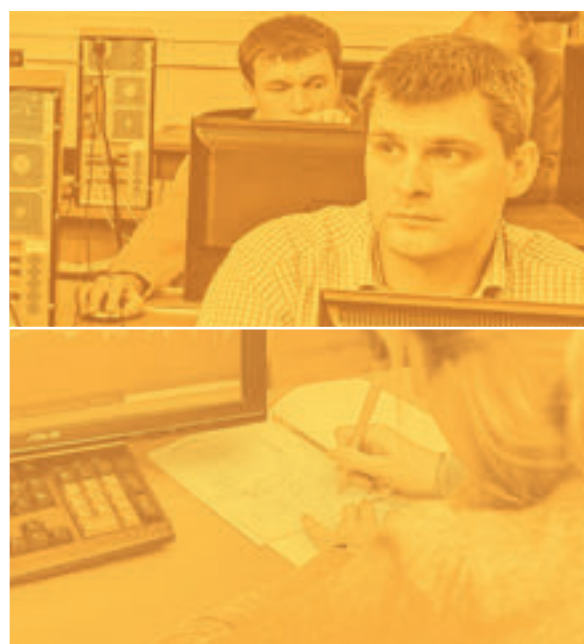
### Техническая защита информации

Направление технической защиты информации содержит ряд развернутых курсов и практических занятий, главной целью которых является повышение квалификации специалистов по вопросам защиты информации от утечки по техническим каналам и несанкционированного доступа.

В рамках курса Вы рассмотрите вопросы, связанные с проведением поисковых мероприятий, специальных обследований, специальных проверок, специальных исследований, контролю защищенности информации от несанкционированного доступа в соответствии с действующими нормативными документами.

Практические части курсов данной тематики составляют, как правило, более 70% от основного времени курса. При проведении практических занятий используется широкий спектр средств защиты и контроля защищенности информации, рекомендуемый лицензиатам ФСТЭК России и ФСБ России.

**Всего по технической защите информации в программе УЦ МАСКОМ 16 курсов продолжительностью от 8 до 72 часов.**



### Безопасность информационных технологий

Данное направление посвящено изучению угроз безопасности информации при ее обработке в автоматизированных и информационных системах, методах и средствах обеспечения защиты этой информации и средств ее обработки. Особое внимание в целом ряде курсов уделено изучению вопросов защиты персональных данных. Отдельный учебный курс посвящен безопасности информации ГИС.

На курсах по данному направлению Вы изучите вопросы обеспечения информационной безопасности вычислительных систем и корпоративных сетей от внешних и внутренних атак, включая принципы работы и использование систем обнаружения и предотвращения вторжений, средства анализа защищённости, организацию антивирусной защиты, настройку политик безопасности компьютеров и сетей и другие технические вопросы безопасности информации, а также правовые, организационные и практические вопросы расследования компьютерных инцидентов.

По данной теме в программе Учебного центра МАСКОМ 3 развернутых курса продолжительностью 16, 26 и 76 часов.

Подробности смотрите на сайте [www.mascom-uc.ru](http://www.mascom-uc.ru) в разделе «Курсы»



## ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ УЦ МАСКОМ

Занятия проводятся в комфортабельных классах, оборудованных всем необходимым для учебного процесса. Их оснащённость современными техническими средствами контроля и защиты информации, многие из которых разрабатываются и производятся Группой компаний МАСКОМ, позволяют Учебному центру готовить специалистов, владеющих новейшими информационными технологиями и умеющими применять в своей профессиональной деятельности знания и навыки, полученные в процессе обучения.

Классы специализированы. В каждом из них укомплектованы учебные стенды, включающие измерительную технику, имитаторы различных сигналов, образцы исследуемых технических средств.

8 УЧЕБНЫХ КЛАССОВ ➤ 400 КВ.М. УЧЕБНЫХ ПЛОЩАДЕЙ

### КЛАСС РАДИОМОНИТОРИНГА

Предназначен для отработки действий по выявлению закладочных устройств

#### Аппаратура:

- »» Комплекс радиоприемной аппаратуры «Кассандра-K21»
- »» Анализатор спектра «OSCOR»
- »» Анализатор стандарта беспроводной связи Wi-Fi типа «AirMagnet»
- »» Аппаратура обнаружения источника сигнала сотовой связи — комплекс «Поиск — GSM»
- »» Индикаторы поля
- »» Портативные частотомеры
- »» Сканирующие приемники
- »» Имитаторы сигналов



## ➤ КЛАСС ПРОВОДНОЙ ЛОКАЦИИ

Предназначен для отработки действий по выявлению закладочных устройств

### Аппаратура:

- Программно-аппаратный комплекс «Сириус»
- Анализатор проводных линий «Talan»
- НЧ усилитель типа СМА-100
- Генераторы ВЧ-сигналов



## ➤ КЛАСС НЕЛИНЕЙНОЙ ЛОКАЦИИ

Предназначен для отработки действий по выявлению закладочных устройств

### Аппаратура:

- Нелинейные радиолокаторы
- Зеркала
- Фонари
- Металлоискатели
- Эндоскопы



## » КОМПЬЮТЕРНЫЕ КЛАССЫ

- »» Компьютерный класс универсального назначения  
Оснащен современными компьютерами с процессорами Intel Core i3 3250, 8 Гб RAM, материнскими платами ASUS P8H77-V LE, и обеспечивает поддержку новейшего ПО.
- »» Специализированный компьютерный класс  
Специально подготовленные компьютеры со съемными аппаратно-программными комплексами Secret Net.



## » КЛАССЫ СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЙ

### Аппаратура:

- »» Система оценки защищенности «ШЕПОТ»
- »» Автоматизированная система «ТАЛИС-НЧ»
- »» Автоматизированная система «ТАЛИС-ВЧ»
- »» Система оценки защищенности «СИГУРД-М5»



## » КЛАССЫ ПО ПРОВЕДЕНИЮ ПОИСКОВЫХ МЕРОПРИЯТИЙ

Специализированные классы оборудованы местами установки имитаторов закладных устройств



## » ВЫДЕЛЕННЫЕ ПОМЕЩЕНИЯ

Пассивная и активная защита от утечки информации.  
Возможность проведения занятий и совещаний

- »» 3 класса
- »» 160 кв. м

Профессиональная переподготовка	
ПМ 1.0	Профессиональная переподготовка по направлению «Информационная безопасность»
Безопасность информационных технологий	
М 9.1	Информационная безопасность сетевого периметра
М 9.2	Расследование компьютерных инцидентов
М 9.3	Системы обнаружения и предотвращения вторжения
Курсы по технической защите информации	
М 1.7	Комплексная защита информации в организации
М 2.0	Защита информации от утечки по техническим каналам. Защита информации от несанкционированного доступа. Курс секретный
М 3.0	Техническая защита конфиденциальной информации (защита персональных данных)
М 3.1	Защита информации, не составляющей государственную тайну, в государственных информационных системах**
М 4.0	Аттестация объектов информатизации. Защита информации от несанкционированного доступа (техническая защита персональных данных)
М 5.0	Защита информации. Организационно-методические основы проведения специальных обследований и проверок. Курс секретный
М ГТ	Защита государственной тайны. Курс секретный
ТМ 2.1	Специальные исследования. Оценка защищенности объектов информатизации от утечки информации по каналам ПЭМИН. Система «СИ-ГУРД» Курс секретный/не секретный
ТМ 2.2	Специальные исследования. Оценка защищенности выделенных помещений от утечки информации по акустическому и виброакустическому каналам. Система «ШЕПОТ». Курс секретный/не секретный
ТМ 2.3	Специальные исследования. Оценка защищенности технических средств от утечки информации по каналу низкочастотного акустоэлектрического преобразования Система «Талис-НЧ-Лайт». Курс секретный/не секретный
ТМ 3.3	Защита персональных данных
М 10.0	Секретное делопроизводство
ТМ 5.1	Углубленное практическое изучение многофункционального поискового комплекса OSCOR-Green
ТМ 5.2	Углубленное практическое изучение современных индикаторов поля и универсальных приборов ST 006, ST 007, ST 031 ПИРАНЬЯ, ST 032
ТМ 5.3	Углубленное практическое изучение нелинейных локаторов серии NR -900, NR-mu, Orion
ТМ 5.5	Проведение поисковых мероприятий по выявлению закладочных устройств
ТМ 5.6	Углубленное практическое изучение аппаратно-программного комплекса «Крокус-КЦП»
ТМ 4.1	Администрирование системы защиты информации, составляющей гос. тайну, от НСД. Курс секретный
ТМ 4.2	Администрирование информационной безопасности компьютерных систем. Курс секретный
М 8.1	Специальные обследования. методика проведения мероприятий. Курс секретный
М 8.2	Специальные проверки. Методика проведения мероприятий. Курс секретный
М 8.3	Специальные исследования. Методика проведения мероприятий. Курс секретный
М 7.0	Криптографическая защита информации в организации
Курсы для инженеров-сметчиков	
МС 0.1	Составление смет по АСУ ТП, пуско-наладочным работам и слаботочным системам (занятия проходят в выходные дни)
МС 0.2	Составление смет по АСУ ТП, пуско-наладочным работам и слаботочным системам (занятия проходят в вечернее время)
Курсы для руководителей компаний	
МС 0.3	Информационная безопасность для бизнеса в период кризиса
** Курс М 3.1 проводится в 2-х вариантах: очно-заочный формат курса осуществляется в соответствии с датами, указанными в расписании: 1-4-ый день – (теоретическая часть) дистанционное обучение с окончанием модуля в виде вебинара; 5-8-ой день – (практическая подготовка) очное обучение. Заочный формат курса – сроки обучения не привязываются к расписанию: оба модуля проводятся дистанционно, по окончании курса проходит вебинар.	





**ЛАБОРАТОРИИ**

## СОЗДАНИЕ И ОСНАЩЕНИЕ СПЕЦИАЛИЗИРОВАННЫХ ЛАБОРАТОРИЙ

Начиная с 2005 года, одним из важных направлений деятельности **Группы компаний МАСКОМ** является разработка комплексных решений по созданию, оснащению и модернизации специальных лабораторий.

### Наши решения оптимальны и предназначены:

- »» для соискателей лицензий ФСТЭК России на деятельность в области технической защиты информации
- »» для соискателей лицензий ФСБ России на проведение специальных проверок и обследований, а также специальных исследований
- »» для ВУЗов, осуществляющих подготовку специалистов в области защиты информации

Обратившись к нам, Вы, как соискатель лицензии, получаете полный перечень работ по созданию и оснащению необходимых Вам лабораторий.

### Специалисты ГК МАСКОМ совместно с Вами:

- »» проведут анализ задач, которые необходимо решать и подберут перечень оборудования, полностью соответствующий требованиям нормативно-методических документов
- »» оптимизируют состав оборудования по цене и параметрам
- »» сформируют необходимый набор документального обеспечения деятельности
- »» подготовят технико-экономическое обоснование на создание специализированных лабораторий
- »» выполнят необходимые проектно-изыскательные, строительные-монтажные и пуско-наладочные работы
- »» проведут обучение персонала и специальную экспертизу для получения необходимой лицензии

### Примечание:

- »» Подбор средств измерений ведется по многим параметрам с учетом требований ФСТЭК России и ФСБ России
- »» Индивидуальный подбор оборудования и вспомогательных устройств позволяет обеспечить выполнение любых специальных работ, как лабораторных (стендовых), так и на объектах



## ИЗМЕРИТЕЛЬНАЯ ЛАБОРАТОРИЯ ФСТЭК

Лаборатория предназначена для осуществления мероприятий и оказания услуг в области защиты государственной тайны (конфиденциальной информации) в части технической защиты информации, включая проведение специальных исследований и аттестацию объектов информатизации.

### Алгоритм создания специализированной лаборатории:

- »» Разработка технико-экономического предложения
- »» Предпроектное обследование помещений, выделенных под лабораторию
- »» Разработка проектной документации на создание измерительной площадки
- »» Паспортизация измерительной площадки
- »» Подбор, согласование и поставка оборудования и программного обеспечения
- »» Обучение персонала
- »» Монтаж и настройка лабораторных и измерительных стендов
- »» Ввод в эксплуатацию оборудования лаборатории на объекте Заказчика
- »» Методическая поддержка соискателей лицензий
- »» Подготовка к спецэкспертизе на право получения лицензии



### Дополнительно мы осуществляем:

- »» Проектирование и создание безэховой экранированной камеры (мобильной и/или стационарной)
- »» Проектирование и создание измерительной площадки
- »» Экономический расчет окупаемости лаборатории

## ЛАБОРАТОРИЯ ДЛЯ ПРОВЕДЕНИЯ СПЕЦРАБОТ ФСБ

Лаборатория предназначена для проведения работ по выявлению электронных устройств негласного получения информации в помещениях и технических средствах, а также проведения специальных исследований на ПЭМИН технических средств.

### Алгоритм создания специализированной лаборатории:

- »» Предпроектное обследование помещений выделенных под лабораторию
- »» Разработка проектной документации на размещение рентгеновской установки
- »» Подготовка документации по монтажу вентиляции
- »» Подбор, согласование и поставка оборудования
- »» Обучение персонала
- »» Монтаж и настройка лабораторных и измерительных стендов
- »» Ввод в эксплуатацию оборудования лаборатории на объекте Заказчика
- »» Методическая поддержка соискателей лицензий
- »» Подготовка к спецэкспертизе на право получения лицензии



### Дополнительно мы осуществляем:

- »» Проектирование и создание экранированной камеры (мобильной и/или стационарной)
- »» Проектирование и создание измерительной площадки
- »» Экономический расчет окупаемости лаборатории

## МОБИЛЬНЫЕ ЛАБОРАТОРНЫЕ КОМПЛЕКСЫ

Мобильные лабораторные комплексы (подвижные лаборатории) предназначены для оценки эффективности защиты информации и проведения объектовых исследований, а также для организации работ по выявлению устройств негласного получения информации и для проведения анализа радиотехнической обстановки и локализации источников радиоизлучений.

### Преимущества:

- »» Оснащение подвижных лабораторий обеспечивает проведение специальных работ по выявлению и оценке технических каналов утечки информации
- »» Подвижные лаборатории обеспечивают возможность проведения спецработ (СП, СИ, СО) в полевых условиях
- »» Подвижные лаборатории обеспечивают проведение выездных работ по радиомониторингу, ЭМС и подавлению источников излучения
- »» Мобильные лабораторные комплексы комплектуются на основании требований нормативно-методических документов в зависимости от решаемых задач



## СПЕЦИАЛЬНЫЕ ИЗМЕРИТЕЛЬНЫЕ ЛАБОРАТОРИИ

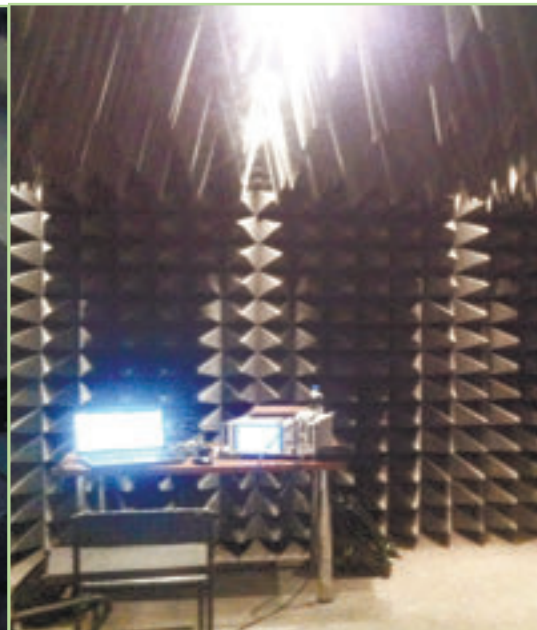
Специальные измерительные лаборатории предназначены для проведения измерений, испытаний и различных исследований в области электромагнитной совместимости, радиотехнических измерений и технической защиты информации.

### Основные типы лабораторий, создаваемых ГК МАСКОМ:

- »» Испытательные лаборатории технических средств по требованиям ЭМС
- »» Испытательные лаборатории для проведения сертификационных/специальных испытаний по требованиям ФСБ и ФСТЭК России
- »» Испытательные лаборатории в области радиотехнической безопасности и противодействия иностранным техническим разведкам
- »» Альтернативные измерительные площадки для проведения специальных лабораторных исследований
- »» Комбинированные звуко-вибро экранированные измерительные камеры
- »» Помещения под размещение в нем рентгено-досмотрового оборудования



В рамках создания измерительных лабораторий мы осуществляем полный цикл работ от подготовки технического задания и разработки рабоче-конструкторской документации до ввода лаборатории в эксплуатацию, включая комплексное оснащение лаборатории современными средствами измерений (в том числе собственной разработки), средствами автоматизации процесса измерений и решение сложных задач.



## УЧЕБНЫЕ ЛАБОРАТОРИИ И КЛАССЫ

На сегодняшний день подготовкой специалистов в области защиты информации занимается более 50-ти ВУЗов по всей России от Калининграда до Владивостока, и их количество ежегодно увеличивается.

Программа подготовки специалистов по защите информации требует как углубленного изучения базовых общематематических и естественно-научных дисциплин, так и досконального изучения современных технических и программных решений, принципов их функционирования и методик работы с ними в различных условиях эксплуатации. Указанные требования учебного процесса приводят к необходимости наличия в ВУЗе современной материально-технической базы, предназначенной для изучения практических навыков использования современных технических средств.

Если в Вашем ВУЗе проводится обучение будущих специалистов по защите информации, то мы разработаем для Вас учебный лабораторный комплекс или создадим



отдельные лаборатории.

### Работы по оснащению учебных лабораторий и классов:

- »» Моделирование необходимой структуры учебной лаборатории исходя из фонда помещений и организации учебного процесса
- »» Разработка проектной документации
- »» Архитектурная и инженерно-техническая подготовка помещений
- »» Создание и монтаж специализированных учебных стендов
- »» Оснащение оборудованием
- Обучение преподавательского состава

### Оборудование для оснащения учебных лабораторий и классов:

- »» Средства защиты информации
- »» Средства оценки защищенности информации
- »» Имитаторы каналов утечки информации
- »» Поисковое оборудование
- »» Вспомогательное оборудование для организации учебного процесса

### Учебные и методические материалы для лабораторных занятий:

- »» Демонстрационные плакаты и стенды
- »» Учебно-методические пособия для проведения лабораторных и практических работ
- »» Специализированная учебно-справочная литература



## СОЗДАННЫЕ ЛАБОРАТОРИИ

### Специализированная лаборатория «Защита информации от утечки за счет НСД»

Назначение лаборатории:

Обеспечение возможности получения слушателями теоретических знаний и практических навыков по следующим направлениям:

- »» физические основы, причины и схемы образования канала утечки информации от несанкционированного доступа (НСД) в локальных вычислительных сетях (демонстрация реальных примеров с использованием оборудования лаборатории);
- »» причины появления и способы реализации недеklarированных возможностей (НДВ) программного обеспечения. Существующие методы выявления и контроля НДВ, а также оборудование и средства для их реализации;
- »» анализ построения, технических параметров и применимости существующих современных решений по обеспечению защиты информации от утечки за счет НСД в локальных вычислительных сетях на основе изучения сертифицированных ФСТЭК России/ФСБ России программных и программно – аппаратных средств защиты информации (СЗИ);
- »» организация и проведение контроля защищенности информации от утечки за счет НСД в локально-вычислительных сетях (ЛВС) в соответствии с нормативной базой ФСТЭК России с использованием современных сертифицированных ФСТЭК России автоматизированных систем контроля защищенности;
- »» современные подходы при проектировании и создании комплексной системы защиты информации от утечки за счет НСД (от предварительного анализа существующей ЛВС и формирования модели угроз до практической реализации и контроля защищенности); организация и проведение испытаний функциональных свойств и контроля НДВ прикладного программного обеспечения, предназначенного для использования в составе защищенных ЛВС, в соответствии с действующей нормативной базой ФСТЭК России.



### Специализированная лаборатория «Защита информации от утечки за счет ПЭМИН»

Назначение лаборатории:

Обеспечение возможности получения слушателями теоретических знаний и практических навыков по следующим направлениям:

- »» физические основы, причины и схемы образования технических каналов утечки информации при ее обработке средствами вычислительной техники, включая примеры организации типовых локально-вычислительных сетей. Закрепление знаний на основе изучения типовых примеров организации технических каналов утечки информации с использованием измерительных стендов и оборудования входящего в состав лаборатории;
- »» проведение предварительного анализа объекта защиты, анализ технических характеристик и параметров объектов защиты;





- » проектирование и создание комплексной системы защиты информации на объекте, включая выбор сертифицированных ФСТЭК России средств защиты информации от утечки, оптимизация средств для конкретного объекта, особенности монтажа и настройки для защиты информации, обрабатываемой в ЛВС, за счет ПЭМИН;
- » создание комплекса организационно-технических мероприятий в рамках создания и сопровождения комплексной системы защиты информации на объекте;
- » проведение количественного контроля эффективности и достаточности выбранных мер защиты информации с использованием сертифицированных ФСТЭК России систем оценки защищенности технических средств, обрабатывающих защищаемую информацию, за счет ПЭМИН;
- » проведение периодического инструментального контроля эффективности мер защиты информации, контроля работоспособности отдельных элементов комплексной системы защиты информации.

### Специализированная лаборатория «Защита информации от утечки за счет АВАК»

Назначение лаборатории:

Обеспечение возможности получения слушателями теоретических знаний и практических навыков по следующим направлениям:

- » физические основы, причины и основные принципы образования технических каналов утечки речевой информации из защищаемых помещений, включая изучение типовых примеров возникновения технических каналов утечки информации, с использованием измерительных стендов и оборудования, входящего в состав лаборатории, по следующим видам каналов;
- » проведение предварительного анализа объекта защиты, анализ технических характеристик и параметров объектов защиты:
  - » помещений, в которых циркулирует защищаемая информация;
  - » средств вычислительной техники и построенных на их базе локальных вычислительных сетей, в которых производится обработка защищаемой информации;
- » использование современной контрольно-измерительной аппаратуры для определения количественных показателей защищенности (в соответствии с действующей нормативной базой ФСТЭК России), планирование и проведение специальных исследований с целью оценки защищенности:
  - » речевой информации от утечки за счет недостаточной звуко- и виброизоляции помещений;
  - » речевой информации помещений от утечки за счет акустоэлектрических преобразований в технических средствах и системах, расположенных в помещениях;
- » проектирование и создание комплексной системы защиты информации на объекте, включая выбор сертифицированных ФСТЭК России средств защиты информации от утечки, оптимизация средств для конкретного объекта, особенности монтажа и настройки;



- »» создание комплекса организационно-технических мероприятий в рамках создания и сопровождения комплексной системы защиты информации на объекте;
- »» проведение количественного контроля эффективности и достаточности выбранных мер защиты информации с использованием сертифицированных ФСТЭК России систем;
- »» проведение периодического инструментального контроля эффективности мер защиты информации, контроля работоспособности отдельных элементов комплексной системы защиты информации.

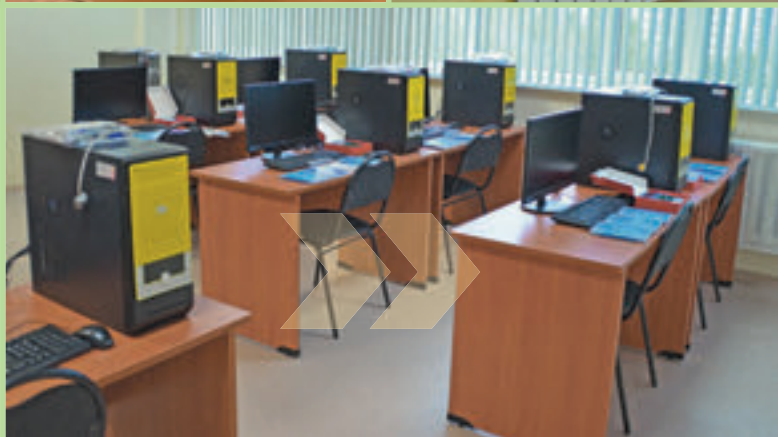
### Специализированная лаборатория «Поиск и выявление демаскирующих признаков ЭУНПИ»

Назначение лаборатории:

Обеспечивает возможности получения слушателями теоретических знаний и практических навыков по следующим направлениям:

- »» физические основы, структурная модель и общая характеристика основных видов электронных защитных устройств (ЗУ);
- »» организация работ по обследованию помещений;
- »» основные этапы проведения поисковых мероприятий и их особенности;
- »» проведение поисковых мероприятий в учебных классах «Радиомониторинга», «Проводной локации» и «Нелинейной локации»;
- »» с использованием технических средств радиомониторинга по выявлению радиоизлучающих ЗУ и ЗУ, использующих для передачи информации ИК-канал;
- »» с использованием средств контроля проводных коммуникаций по выявлению ЗУ, использующих для передачи информации проводные коммуникации;
- »» с использованием нелинейного локатора по выявлению ЗУ, в составе которых есть элементы, обладающие нелинейной вольтамперной характеристикой;
- »» выявление посторонних внедрений во внутренние структуры ограждающих конструкций и предметов интерьера помещений, указывающих на наличие ЗУ;
- »» особенности выявления металлических включений, указывающих на наличие ЗУ;
- »» визуально-оптический контроль с использованием средств визуального контроля;
- »» анализ выявленных по результатам поиска демаскирующих признаков ЗУ;
- »» создание комплекса организационно-технических мероприятий в рамках создания и сопровождения комплексной системы защиты информации на объекте;
- »» проведение периодического инструментального контроля эффективности мер защиты информации, контроля работоспособности отдельных элементов комплексной системы защиты информации.







## ОБЪЕКТЫ



## СОЗДАНИЕ ОБЪЕКТОВ СИСТЕМЫ БЕЗОПАСНОСТИ КОСМОДРОМА «ВОСТОЧНЫЙ» В РАМКАХ РЕАЛИЗАЦИИ ФЦП «РАЗВИТИЕ РОССИЙСКИХ КОСМОДРОМОВ НА 2006-2015 ГГ.»

**Цели проекта:** Проведение комплекса работ по созданию на территории позиционного района космодрома единой территориально распределенной комплексной системы безопасности с формированием единой базы пользователей, Центрального бюро пропусков, общекосмодромного и локальных центров управления и мониторинга безопасности

### Выполненные работы:

- »» Разработка концептуальных материалов по анализу уязвимости объектов НКИ космодрома
- »» Проведение 2-стадийного проектирования (стадия «П» и «Р»)
- »» Создание охранных периметров площадок, внутренних локальных зон и оборудование их средствами охраны
- »» Оборудование контрольно-пропускных пунктов средствами досмотра и антитеррористической защиты
- »» Оборудование внутриплощадочных зданий и сооружений средствами охранной сигнализации, контроля доступа и телевизионного наблюдения
- »» Создание внутриплощадочных сетей связи и СКС
- »» Проведение комплекса работ по созданию защищенной резервированной межплощадочной телекоммуникационной сети
- »» Проведение организационно-технических мероприятий по обеспечению защиты информации
- »» Поставка, монтаж и пуско-наладка стационарного оборудования ССОИ
- »» Производство и поставка технических средств КСБ



### Ключевые особенности:

Проведение строительно-монтажных работ по созданию КСБ объектов НКИ космодрома осуществляется в сложных климатических условиях в сжатые сроки.

В проекте применены передовые, инновационные и высоко-эффективные технологии в индустрии безопасности, инженерных систем, систем автоматизации, IT-сфере.

В рамках реализации проекта выполняются функции генерального подрядчика, внедрены и широко применяются методы и технологии проектного управления.

**Проект реализуется для ФКА России**

## СОЗДАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ ФГБУ «НИИ ЦПК ИМ. Ю. А. ГАГАРИНА»

**Цель проекта:** Повысить уровень безопасности объекта посредством применения технических и организационных мер в рамках создания комплексной системы безопасности

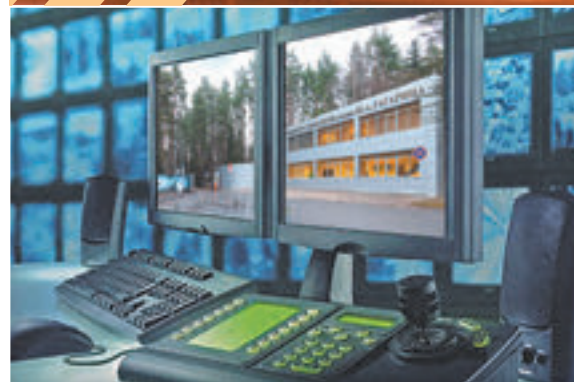
### Выполненные работы:

- »» Реализация проекта по созданию комплексной системы безопасности, отражающего концепцию обеспечения безопасности объекта в целом и включающую в себя:
  - »» систему телевизионного наблюдения (СТН)
  - »» систему охранного освещения (СОО)
  - »» систему контроля и управления доступом (СКУД)
  - »» систему физической защиты периметра (СФЗ)
- »» Работы по созданию комплексной системы безопасности объекта, включающей в себя следующие системы:
  - »» автоматическую пожарную сигнализацию (АПС)
  - »» систему оповещения и управления эвакуацией (СОУЭ)
  - »» систему охранной сигнализации (СОС)
- »» ПИР по оснащению объектов ФГБУ «НИИ ЦПК им. Ю. А. Гагарина»
  - »» автоматической пожарной сигнализацией (АПС)
  - »» системой оповещения и управления эвакуацией (СОУЭ)
  - »» системой охранной сигнализации (СОС)
- »» Расширение комплексной системы безопасности объекта
- »» Техническое обслуживание созданной комплексной системы безопасности

### Ключевые особенности:

Работы производились в условиях эксплуатируемого в круглосуточном режиме объекта с обеспечением непрерывности производственных циклов.

**Проект реализован для ФКА России**



## ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО СПЕЦИАЛИЗИРОВАННОГО ЗДАНИЯ ЦЕНТРА АСУ С ЦЕНТРОМ БОЕВОГО УПРАВЛЕНИЯ И ПОЛНЫМ ТЕХНИЧЕСКИМ ОСНАЩЕНИЕМ

**Цели проекта:** Выполнить весь комплекс работ и сдать в эксплуатацию объект, полностью соответствующий требованиям Заказчика

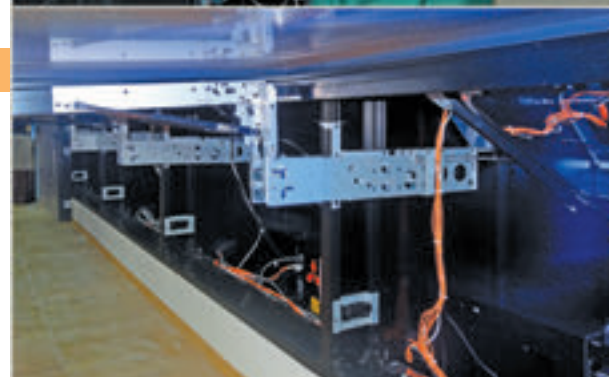
### Выполненные работы:

- »» Проектирование административного здания с полным оснащением, экспертиза, авторский надзор за строительством
- »» Строительство 5-этажного административного здания с подключением всех коммуникаций, оснащением и благоустройством территории
- »» Оборудование здания системами вентиляции и кондиционирования
- »» Прокладка внешних волоконных-оптических линий передачи данных
- »» Создание СКС, ИТСО, системы пожарной автоматики
- »» Создание закрытого и открытого сегмента локально-вычислительной сети
- »» Создание закрытой видеоконференцсвязи ЦБУ
- »» Создание системы бесперебойного электропитания
- »» Строительство контуров заземления
- »» Специальные работы по защите информации

### Ключевые особенности:

Строительство выполнялось на территории действующей войсковой части в сжатые сроки.

**Проект реализован для восточного регионального командования внутренних войск МВД России**



## РЕКОНСТРУКЦИЯ ОБЪЕКТА СПЕЦИАЛЬНОЙ СВЯЗИ

**Цель проекта:** Провести все работы по реконструкции объекта без переселения персонала и остановки производственных циклов

### Выполненные работы:

- » Капитальный ремонт здания
- » Оборудование здания системами вентиляции и кондиционирования
- » Прокладка внешних волоконно-оптических линий передачи
- » Создание СКС, ИТСО, системы пожарной автоматики
- » Производство специальных экранированных шкафов
- » Реконструкция системы электропитания
- » Поставка, монтаж и пуско-наладка ИБП и дизель-генераторной установки
- » Строительство контуров заземления
- » Специальные работы по защите информации

### Ключевые особенности:

Реконструкция производилась в условиях эксплуатируемого в круглосуточном режиме объекта с обеспечением непрерывности производственных циклов. В рамках проекта осуществлена разработка индивидуальных единичных расценок на специальные разделы проектов и согласование их в Федеральном центре ценообразования. В проекте применены технологии пассивной акустической и электромагнитной защиты помещений и серверных.

**Проект реализован для МВД России**





## ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ, ВИБРАЦИОННОМУ, ОПТИКО-ЭЛЕКТРОННОМУ КАНАЛУ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ

**Цель проекта:** Провести аттестацию выделенных помещений по требованиям ФСТЭК России и обеспечить гарантированное подавление беспроводных систем связи в помещениях во время проведения закрытых мероприятий

### Выполненные работы:

- »» Создание системы защиты речевой информации на эксплуатируемом объекте
- »» Исполнение требований регулятора

### Ключевые особенности:

Оснащение объекта системами подавления беспроводной связи осуществлялось на эксплуатируемом объекте в условиях плотной застройки центра Москвы.

**Проект реализован для ЦИК России**



## РЕКОНСТРУКЦИЯ ОБЪЕКТА СПЕЦИАЛЬНОЙ СВЯЗИ

**Цель проекта:** Провести работы по реконструкции объекта в условиях частичного перемещения персонала

### Выполненные работы:

- »» Капитальный ремонт здания
- »» Оборудование здания системами вентиляции и кондиционирования
- »» Прокладка внешних волоконно-оптических линий передачи
- »» Создание СКС, ИТСО, системы пожарной автоматики
- »» Производство специальных экранированных шкафов
- »» Создание локально-вычислительной сети
- »» Реконструкция системы электропитания
- »» Поставка, монтаж и пуско-наладка ИБП и дизель-генераторной установки
- »» Строительство контуров заземления
- »» Специальные работы по защите информации

### Ключевые особенности:

Реконструкция объекта осуществлена с обеспечением переноса производственных циклов и частичным перемещением подразделений, произведена разработка индивидуальных единичных расценок на специальные разделы проектов и согласование их в Федеральном центре ценообразования.

**Проект реализован для ФТС России**



## ПРОЕКТИРОВАНИЕ И СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ, ВИБРО-АКУСТИЧЕСКОМУ И ОПТИКО-ВОЛОКОННОМУ КАНАЛАМ В ВЫДЕЛЕННЫХ И ОСОБО ВАЖНЫХ ПОМЕЩЕНИЯХ НА ЭТАПЕ КАПИТАЛЬНОГО СТРОИТЕЛЬСТВА

**Цель проекта:** Создать защиту речевой информации от утечки по акустическому, вибро-акустическому и оптико-электронному каналам в выделенных и особо важных помещениях

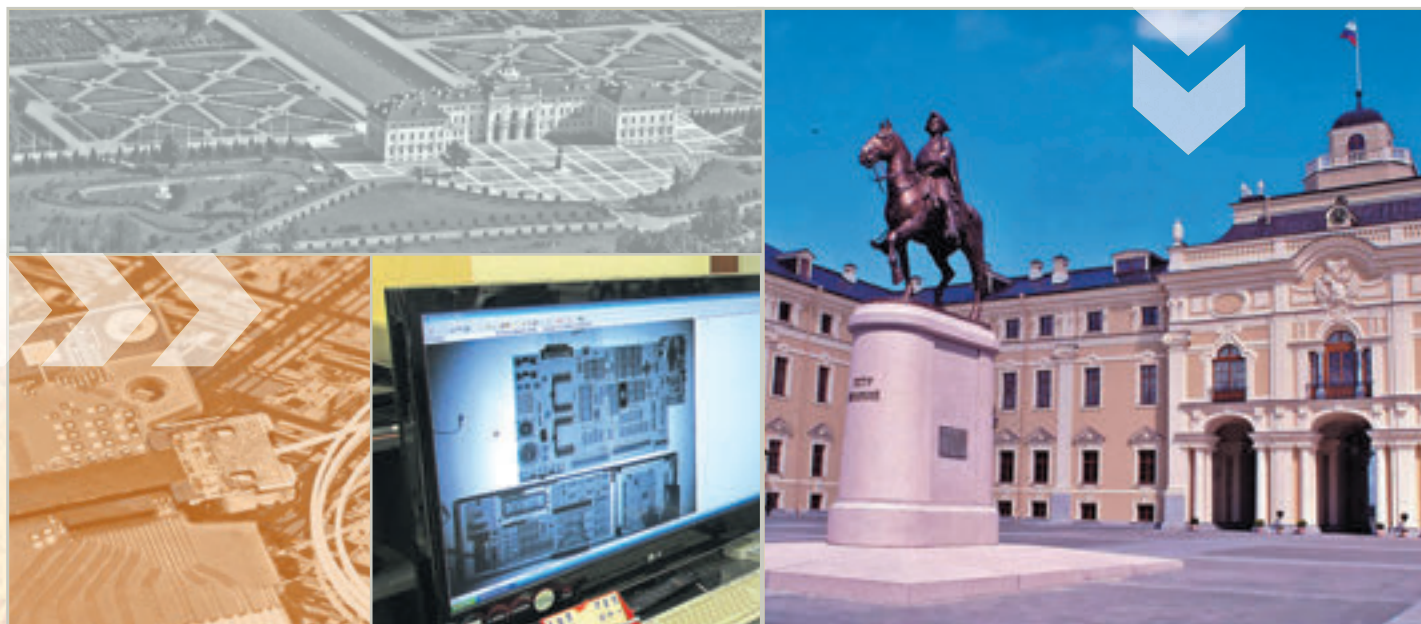
### Выполненные работы:

- »» Разработка специальных архитектурно-планировочных и инженерных решений, направленных на обеспечение необходимой звуко- и виброизоляции, с использованием методов строительной акустики
- »» Проведение натурных инструментальных испытаний макетов архитектурно-планировочных и инженерных решений на предмет их эффективности
- »» Разработка проектной документации на системы активной защиты
- »» Поставка оборудования, монтаж, настройка, инструментальная оценка эффективности

### Ключевые особенности:

За счет использования методов строительной акустики по большинству направлений удалось либо минимизировать паразитный акустический шум от работы системы активной защиты, либо вообще не использовать систему активной защиты, обеспечив достаточный уровень ослабления акустического сигнала.

**Проект реализован в государственном Комплексе «Дворец Конгрессов» (Стрельна)**



## РАЗРАБОТКА И МОНТАЖ ЗВУКО-ВИБРО-ЭКРАНИРУЮЩЕГО КОМПЛЕКСА, ВКЛЮЧАЮЩЕГО ЭКРАНИРОВАННУЮ КАМЕРУ

**Цель проекта:** Создать звуко-вибро-экранирующий комплекс в соответствии с техническим заданием

### Выполненные работы:

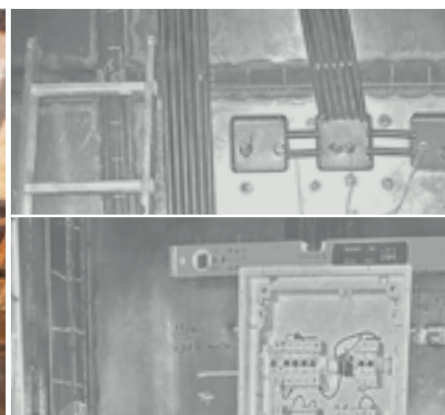
- »» Разработка рабочей конструкторской и эксплуатационной документации на комплекс
- »» Разработка рабочей конструкторской документации для изготовления и монтажа экранированной камеры
- »» Изготовление и монтаж экранированной камеры
- »» Монтаж звуко-вибро-экранирующего комплекса
- »» Специальные исследования на эффективность экранирования
- »» Специальные исследования на звуко-вибро-защищенность комплекса
- »» Проведение специальной проверки оборудования, устанавливаемого в комплексе.



### Ключевые особенности:

Монтаж экранированной камеры весом 6,5 т производился на 6 этаже здания и включал в себя монтаж специальных распределяющих нагрузки металлоконструкций. Работа шла в стесненных условиях, без отселения персонала из соседних помещений.

**Проект реализован для силовых ведомств**



## РЕКОНСТРУКЦИЯ УЧЕБНОГО КЛАССА ПРЕЗИДЕНТСКОГО ПОЛКА ФСО РФ

**Цель проекта:** Реализовать дооснащение системы поддержки заседаний в учебном классе

### Выполненные работы:

- »» Модернизация имеющегося звукотехнического оборудования (поставка, монтаж и пусконаладка)
- »» Проведение специальных проверок и специальных исследований поставляемого оборудования
- »» Проведение предварительных специальных исследований учебного класса по вибро-акустическому каналу с выдачей рекомендаций по дальнейшему дооснащению помещения как пассивными, так и активными средствами
- »» Проведение специальных исследований учебного класса по оценке защищенности помещения от утечки информации по вибро-акустическому каналу с настройкой средств активной защиты
- »» Аттестационные испытания системы на соответствие требованиям РД ФСТЭК России

### Ключевые особенности:

Выполнение работ произведено в удобном для Заказчика графике, с учетом непрекращающихся крупных мероприятий в учебном классе. Объектовая часть специальных исследований проведена на закрытой от транспорта окружающей территории (Красная площадь и т.д.) с привлечением специального транспорта и оборудования без демаскирующих признаков.

**Проект реализован для ФСО России**



## СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА СТРОЯЩЕМСЯ ОБЪЕКТЕ

**Цель проекта:** Создать систему защиты информации в категорированных помещениях с учетом архитектурно-строительных и дизайнерских особенностей проекта

### Выполненные работы:

- »» Проектирование с последующей реализацией комплексной системы защиты информации, включающей в себя:
  - » Систему защиты информации от утечки по техническим каналам в соответствии с требованиями руководящих документов ФСБ России и ФСТЭК России
  - » Систему защиты аудио-визуальной информации от утечки по техническим каналам беспроводных сетей и систем связи
- »» Производство комплекса специальных работ: специальная проверка технических средств, специальные исследования технических средств, инструментальные исследования электромагнитной совместимости сопряженных радиоволновых систем.

### Ключевые особенности:

- »» Проектирование и создание комплексной системы защиты информации осуществлялись на строящемся объекте с учётом архитектурно-строительных и дизайнерских особенностей защищаемых площадей в составе объекта.

Разработка технических решений велась с учетом взаимного влияния на смежные инженерно-технические системы, развиваемые на объекте. Создание комплексной системы защиты информации производилось с учетом локализации зон воздействия системы. При этом инженерно-строительные решения рассматривались в процессе разработки, проектирования и реализации как пассивные элементы комплексной системы защиты информации.

**Проект реализован для ОАО «ФСК ЕЭС» России**



## ЗАЩИТА И АТТЕСТАЦИЯ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

**Цель проекта:** Создать защиту и аттестацию объектов информатизации (автоматизированных рабочих мест, локальных вычислительных сетей, выделенных помещений) согласно требованиям безопасности информации

### Выполненные работы:

- » Установка, настройка и пусконаладка систем защиты информации от ее утечки по техническим каналам
- » Модернизация имеющихся систем защиты информации
- » Проведение специальных проверок и специальных исследований технических средств и систем объектов информатизации
- » Проведение предварительных специальных исследований объектов информатизации с выдачей рекомендаций по дальнейшему дооснащению объектов как пассивными, так и активными средствами защиты
- » Проведение специальных исследований объектов информатизации по оценке их защищенности от утечки информации по техническим каналам с настройкой средств активной защиты
- » Аттестационные испытания системы на соответствие требованиям РД ФСТЭК России

### Ключевые особенности:

Выполнение работ производилось в удобном для Заказчиков графике, с учетом необходимости оперативных выездов на объекты для проведения работ. Подбор технических решений по защите осуществлялся с учетом сложившейся на объектах практике (для сохранения единообразия). В проекты входило большое количество объектов, подлежащих аттестации и защите.

**Проекты реализованы в ОАО «Газпром», Банке России, Министерстве промышленности и торговли Российской Федерации**



## ВНЕДРЕНИЕ КОМПЛЕКСНОЙ ОБЪЕКТОВОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

**Цель проекта:** Обеспечение защиты информации от утечки по техническим каналам для средств информатизации, размещенных на территориально распределенном объекте при соблюдении требований ГКРЧ

### Выполненные работы:

- »» Разработка и согласование проекта размещения оборудования с учетом интерьерных решений и минимального влияния на экстерьер здания
- »» Изготовление и поставка оборудования
- »» Создание специализированной СКС
- »» Пусконаладочные работы
- »» Специальные работы по защите информации
- »» Проведение обучения обслуживающего персонала

### Ключевые особенности:

- »» Круглосуточный непрерывный контроль параметров всех элементов, включая несанкционированный доступ к элементам системы
- »» Контроль работоспособности оконечных устройств в реальном режиме времени
- »» Наличие удаленного ситуационного центра — поста мониторинга состояния и управления системой
- »» Возможность «горячей» замены и автоматического восстановления настроек оконечных устройств
- »» Возможность адаптации активных средств защиты к реальной электромагнитной обстановке
- »» Внедрение производилось в условиях эксплуатируемого в круглосуточном режиме объекта с обеспечением непрерывности производственных циклов.

**Проект выполнен для Министерства обороны Российской Федерации**



## СОЗДАНИЕ ЗАЩИЩЕННЫХ СИСТЕМ СВЯЗИ И ПЕРЕДАЧИ ДАННЫХ

**Цель проекта:** Модернизировать существующие и оборудовать новые объекты системами связи и передачи данных в защищенном исполнении в рамках реконструкции и капитального строительства

### Выполненные работы:

- » Разработка и внедрение технических решений по созданию распределительных сетей телефонной связи, СКС локальных вычислительных сетей в защищенном исполнении
- » Разработка и внедрение технических решений по созданию объектов автоматизации и связи в защищенном исполнении
- » Разработка и внедрение технических решений по созданию локальных вычислительных сетей открытого, закрытого и интернет сегментов, в том числе решений по защите каналов связи
- » Проведение строительно-монтажных и пусконаладочных работ в рамках реализации разработанных проектных решений

### Ключевые особенности:

Проекты выполнены в сжатые сроки. На части объектов работы производились в режиме их круглосуточной эксплуатации. Часть выделенных объектов оборудована спецсвязью ФСО. В процессе реализации проектов были реконструированы внутривозвездные сети связи.

**Проекты выполнены для Министерства обороны Российской Федерации**





## СОЗДАНИЕ ЗАЩИЩЕННОЙ ИТ-ИНФРАСТРУКТУРЫ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

**Цель проекта:** Провести аудит защищенности, разработать и реализовать технические решения по созданию защищенной ИТ-инфраструктуры центра обработки данных

### Выполненные работы:

- »» Проектно-изыскательские работы
- »» Разработка технических решений по созданию безопасной ИТ-инфраструктуры Центра обработки данных
- »» Поставка, сертификация по требованиям безопасности информации, монтаж и пуско-наладка коммутационного оборудования
- »» Поставка, монтаж и пуско-наладка средств защиты информации
- »» Аттестация по требованиям безопасности информации

### Ключевые особенности:

В рамках проекта был проведен аудит информационных систем на соответствие требования стандарта PCI DSS. Решение было разработано на базе новейшего оборудования ведущих вендоров рынка. Сертификация поставляемых СЗИ осуществлялась в собственной лаборатории.



## СОЗДАНИЕ ЗАЩИЩЕННОЙ ИТ-ИНФРАСТРУКТУРЫ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

**Цель проекта:** Создать защиту и провести аттестацию информационных систем, обрабатывающих персональные данные

### Выполненные работы:

- »» Проектно-изыскательские работы
- »» Поставка, монтаж и пуско-наладка средств защиты информации
- »» Сертификация средств защиты информации, имеющихся у Заказчика
- »» Аттестация ИСПДн по требованиям безопасности информации

**Проекты реализованы для ОАО «Аэрофлот»**



## СОЗДАНИЕ СУПЕРВЫЧИСЛИТЕЛЬНОГО КОМПЛЕКСА ОБЕСПЕЧЕНИЯ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ

**Цель проекта:** Обеспечить Заказчика супервычислительным комплексом в защищенном исполнении

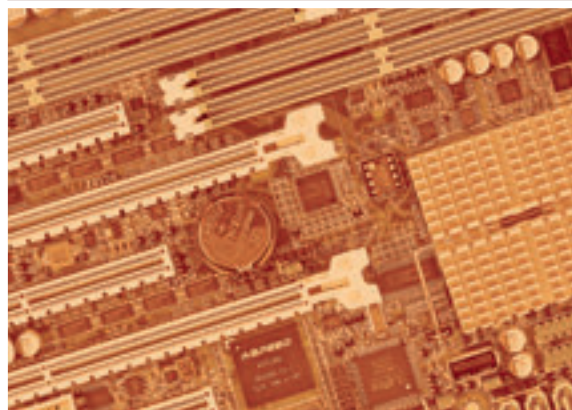
### Выполненные работы:

- »» Проектно-изыскательские работы
- »» Поставка, монтаж и пуско-наладка оборудования локальной вычислительной сети
- »» Поставка, монтаж и пуско-наладка оборудования супервычислительного комплекса
- »» Поставка, монтаж и пуско-наладка средств защиты информации
- »» Специальные работы по защите информации
- »» Аттестация по требованиям безопасности информации

### Ключевые особенности:

В рамках проекта потребовалось оборудовать объект инженерными системами (кондиционирование, вентиляция, система газового пожаротушения и др.). Найдено и внедрено решение нестандартной задачи по организации защиты информации от утечки по ТКUI.

**Проект выполнен для НИЦ «Курчатовский институт»**



### З ДОМ МО РФ

Специальная проверка (СП) и специальные исследования (СИ) высокотехнологичной системы отображения информации и видеоконмутации (СОИВ) Атриума

**Цель проекта:** Провести специальную проверку и специальные исследования технически сложного мультимедийного оборудования в сжатые сроки

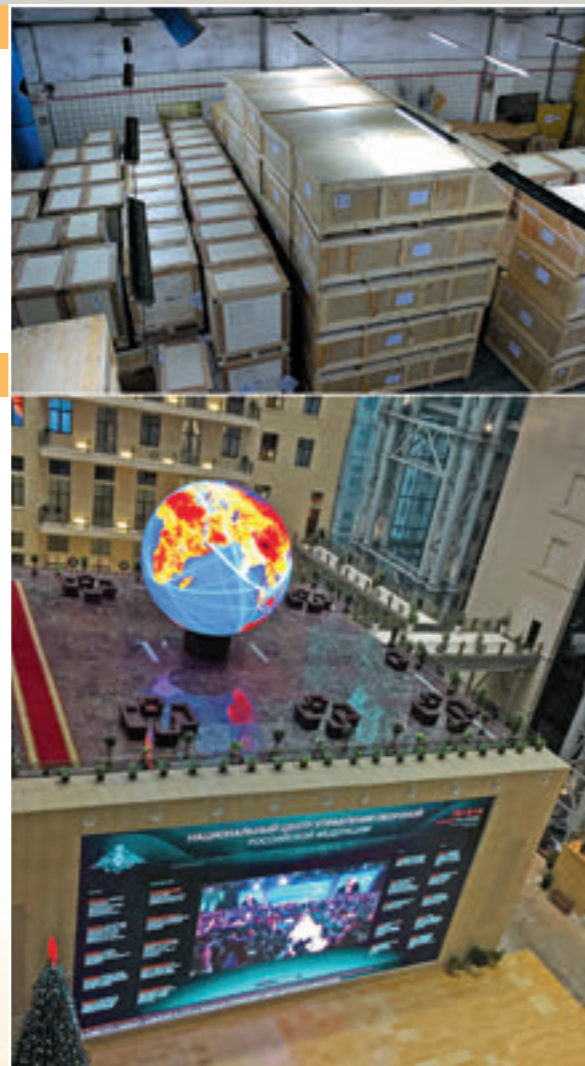
#### Задачи:

- »» Оперативное развертывание специальных лабораторий на нескольких площадках
- »» Организация приема и хранения крупногабаритного и дорогостоящего оборудования
- »» Оперативный входной и выходной контроль оборудования
- »» Оптимизация технологических процессов СП и СИ потоковым методом

#### Ключевые особенности:

Проведение специальных работ высокотехнологичного мультимедийного оборудования, не имеющего аналогов, в сжатые сроки с учетом неравномерного графика поставок технических средств. Применение конвейерного цикла проведения работ для частей сложного мультимедийного оборудования. Организация круглосуточного режима работы лабораторий с посменным графиком проведения работ. Применение новых технических решений для оптимизации времени проведения работ.

**Проект реализован для Министерства обороны Российской Федерации**



## ОБЕСПЕЧЕНИЕ ОЛИМПИЙСКИХ ОБЪЕКТОВ МОБИЛЬНЫМИ ИНСПЕКЦИОННО-ДОСМОТРОВЫМИ КОМПЛЕКСАМИ

**Цель проекта:** Поставка и ввод в эксплуатацию мобильных инспекционно-досмотровых комплексов (МИДК), обучение персонала с выдачей сертификатов на право эксплуатации. Разработка методики эксплуатации. Дооснащение МИДК системами автоматического обнаружения радиоактивных материалов

### Выполненные работы:

- » Разработка и реализация логистической схемы по доставке оборудования из Великобритании в г. Сочи
- » Адаптация и доработка МИДК Rapiscan EAGLE M60 к российским условиям эксплуатации и требованиям Заказчика
- » Инженерная подготовка, обустройство и аттестация площадок для эксплуатации МИДК
- » Ввод трех МИДК в эксплуатацию
- » Выполнение монтажа систем автоматического обнаружения радиоактивных материалов RadNuke на МИДК Smiths Heinmann
- » Обучение более 50 специалистов Заказчика эксплуатации МИДК с выдачей официального сертификата производителя
- » Организация технического сопровождения МИДК в режиме 24x7 и планового технического обслуживания



### Ключевые особенности:

Были спроектированы и реализованы схемы применения МИДК с учетом требований круглосуточного бесперебойного снабжения возводимых объектов строительными материалами. МИДК были адаптированы для эксплуатации в условиях высокогорья и резко континентального климата. Наряду с разработкой, проектированием и реализацией обеспечивающей инфраструктуры была проведена доработка МИДК, которая позволила использовать досмотровые комплексы от источника внешнего электропитания без запуска двигателя внутреннего сгорания. Для обеспечения минимального времени реакции на обращения была оптимизирована схема работы сервисной службы.

### Технологические инновации:

За счет комплексного подхода к проектированию схемы использования МИДК удалось оптимизировать затраты на реализацию механизма досмотра автотранспорта. Что, в конечном итоге, привело к повышению общего качества выполнения работ. Адаптация МИДК к экстремальным условиям эксплуатации и оптимально организованные процессы технической поддержки позволили минимизировать время технологических простоев.

Была разработана, впервые в РФ, программа обучения экипажей МИДК. С помощью этой программы удалось добиться получения глубоких знаний и устойчивых навыков у специалистов. При этом время отрыва от производства было минимальным. Компания партнер: Rapiscan System (UK).

**Проект выполнен для ГК «Олимпстрой»**



**МАСКОМ**  
ГРУППА КОМПАНИЙ

# КАТАЛОГ ОБОРУДОВАНИЯ

## Телефон-В >>>>>

### Защищённый сотовый телефонный аппарат

Телефонный аппарат стандарта GSM в защищённом исполнении Телефон-В оснащен средствами защиты, предназначенными для предотвращения возможной утечки акустической и визуальной информации, а также разведки побочных электромагнитных излучений и наводок (ПЭМИН) за счёт встроенных FM-приемника и модуля беспроводного средства доступа (Bluetooth).

Телефон-В предназначен для вноса в выделенные помещения до второй категории включительно. «Телефон-В» может использоваться в помещениях федеральных органов безопасности Российской Федерации, а также в помещениях органов государственной власти Российской Федерации.

#### Комплектация

Телефонный аппарат стандарта GSM в защищенном исполнении «Телефон-В»	1 шт.
Зарядное устройство	1 шт.
Комплект документации	1 к-т

#### Технические характеристики

Параметр и характеристика	Значение
Стандарт	GSM 900/1800
Тип корпуса	раскладной
Тип SIM-карты	обычная
Тип экрана	цветной
Диагональ экрана	не менее 1,4 дюймов
Размер изображения	не менее 128x128 px
Объем встроенной памяти	не менее 3 Мб
Тип аккумулятора	Li-Ion
Емкость аккумулятора	не менее 300 мАч
Размеры (ШxВxТ)	не более 80x140x22 мм
Вес	не более 200 г

## Технические средства в защищённом исполнении



Сертификат ФСБ России  
Сертификат ФСТЭК России  
Гарантия 12 месяцев

## Вектор >>>>>

### Защищённый сотовый телефонный аппарат

Защищенный сотовый телефонный аппарат «Вектор» – первое изделие, разработанное на базе аппаратной мобильной платформы Группы компаний МАСКОМ. Защищенный сотовый телефонный аппарат «Вектор» оснащен встроенной системой защиты, предотвращающей утечку акустической речевой и визуальной информации, циркулирующей в выделенных помещениях, по техническим каналам, а также за счет недекларируемых возможностей. Изделие предназначено для ведения открытых переговоров и может использоваться в выделенных помещениях. Телефонный аппарат «Вектор» имеет значительный потенциал - для модернизации и расширения функционала. Поставляемый в качестве опции комплект встроенного программного обеспечения собственной разработки позволяет повысить безопасность передаваемых данных и голоса, а также данных, обрабатываемых и хранимых с использованием телефонного аппарата.

#### Комплектация

Защищенный сотовый телефонный аппарат «Вектор»	1 шт.
Кабель интерфейсный	1 шт.
Зарядное устройство	1 шт.
Комплект документации	1 к-т

#### Технические характеристики

Параметр и характеристика	Значение
Стандарт	GSM (2G) – 900/1800 МГц
Рабочий диапазон частот	UMTS (3G) – 900/2100 МГц
Процессор	тактовая частота 1,2 ГГц
Тип процессора	четырёхъядерный
Количество слотов для SIM-карт	один
Оперативная память	1 ГБ
Объём встроенной памяти	16 Гб
Сенсорный экран	5" (разрешение: 1280×720)
Камеры: фронтальная	2 МП
тыловая	5 МП, автофокус
Связь	Wi-Fi / Bluetooth / GPS
Емкость АКБ	2500 мАч
Операционная система	Android

## Технические средства в защищённом исполнении



#### Дополнительные опции

- »» Модифицированная операционная система Android – блокирование возможности несанкционированной модификации ОС, предустановленный ограниченный набор прикладных программ без возможности несанкционированной модификации.
- »» Программный модуль криптографической защиты конфиденциальной информации – возможность шифрования обрабатываемых и хранимых данных с использованием сертифицированного ФСБ России криптопровайдера.
- »» Аппаратно-программный комплекс обеспечения криптографической защиты конфиденциальной информации – возможность шифрования голосовых переговоров и сообщений, обеспечение защищённого доступа к «внутренним» корпоративным информационным ресурсам с использованием сертифицированных ФСБ России криптосредств.

Оформляется сертификат ФСБ России  
Гарантия 12 месяцев

## Феликс-П207 >>>>>

## Технические средства в защищённом исполнении

### Защищённый факсимильный аппарат

Защищённый факсимильный аппарат «Феликс-П207» предназначен для передачи данных и ведения открытых переговоров, в том числе в выделенных помещениях до второй категории включительно; может использоваться в помещениях федеральных органов безопасности Российской Федерации, а также в помещениях органов государственной власти Российской Федерации.

«Феликс-П207» построен на базе факсимильного аппарата Panasonic KX-FP207 и оснащен средствами защиты, предназначенными для предотвращения возможной утечки защищаемой акустической речевой информации.

**Внимание!** Изделие не предназначено для ведения закрытых переговоров, а также передачи закрытой информации.



### Комплектация

Защищённый факсимильный аппарат «Феликс-П207»	1 шт.
Комплект документации	1 к-т

### Технические характеристики

Параметр и характеристика	Значение
Тип факса	факс/копир с печатью на листах
Диапазон частот шумового сигнала	90 11300 Гц
Коэффициент качества шумового сигнала	не хуже 0,9
Скорость модема	9,6 Кбит/с
Максимальный размер документа	216×600 мм
Ёмкость устройства автоподачи	10 листов
Ёмкость лотка для бумаги	20 листов
Дисплей	2 строки
Записная книжка	50 номеров
Память для приема факсов	28 листов
Масса	не более 2,7 кг
Габариты корпуса	не более 356×106×200 мм

Гарантия 12 месяцев



## Мобильный защищённый терминал >>>>

**Мобильный защищённый терминал (МЗТ)** представляет собой специальный планшетный компьютер, оборудованный средствами защиты с установленными, аппаратно отключаемыми радиомодулями, выделенным процессором для реализации криптографических алгоритмов и несъемными блоком твердотельной памяти. Мобильный защищенный терминал (МЗТ) предназначен для доступа к защищаемым сетям связи.

МЗТ поддерживает два режима функционирования:

- >> Открытый – обычный планшетный компьютер.
- >> Закрытый – на аппаратном уровне отключены радиомодули для доступа к открытым сетям связи и включен модуль служебной беспроводной радиосвязи

**Особенностью МЗТ** является реализация в его конструкции действующих требований, предъявляемых к абонентским пунктам для доступа к сети Интернет и защищенным сотовым телефонам, что позволяет использовать данное устройство в выделенных помещениях до второй категории включительно на объектах.

### Комплектация

Изделие «МЗТ»	1 шт.
Интерфейсный кабель USB	1 шт.
Зарядное устройство	1 шт.
Комплект документации	1 к-т

## Технические средства в защищённом исполнении



### Технические характеристики

Параметр и характеристика	Значение	Параметр и характеристика	Значение
Операционная система	Android	Wi-Fi	+
Частота процессора	1200 МГц	3G (опционально 4G)	+
Оперативная память	1,5 Гб	Bluetooth	+
Встроенная память	8 Гб	Тыловая камера	3 млн пикс
Поддержка карт памяти microSDHC	до 32 Гб	Фронтальная камера есть	1.3 млн пикс
Диагональ и разрешение экрана	7", 1280×800	GPS	+
Емкость аккумулятора	4000 мАч	ГЛОНАСС	+

## ЗИТА >>>>>

### Модуль защиты

Модуль защиты «ЗИТА» предназначен для встраивания в стационарные средства телефонии, оконечные устройства видеоконференцсвязи и т. д. с целью обеспечения защиты акустической речевой информации от утечки за счёт недеклалируемых возможностей данных технических средств.

Модуль защиты «ЗИТА» изготавливается в двух модификациях в зависимости от типа защищаемого ТС:

- >> «ЗИТА-А» – для защиты аналоговых ТС
- >> «ЗИТА-Ц» – для защиты цифровых ТС

### Комплектация

Модуль защиты «ЗИТА»	1 шт.
Комплект эксплуатационной документации	1 к-т

### Технические характеристики

Параметр и характеристика	Значение
Диапазон частот шумового сигнала	90 – 11300 Гц
Коэффициент качества шумового сигнала	не хуже 0,9
Возможность регулировки выходного уровня помехи	Да
Наличие функции самодиагностики состояния	Да
Возможность использования вибро-возбудителей	Да (для «Зита-Ц»)
Возможность использования внешнего индикатора состояния	Да
Напряжение питания	5-12 В
Габариты	не более 45×30×7 мм

## Технические средства в защищённом исполнении



Гарантия 12 месяцев

**Защищённый цифровой телефонный аппарат**

Защищённый цифровой телефонный аппарат «Синтез» (ЗЦТА «Синтез») предназначен для ведения открытых переговоров, в том числе в выделенных помещениях до второй категории включительно; может использоваться в помещениях федеральных органов безопасности Российской Федерации, а также в помещениях органов государственной власти Российской Федерации, без применения дополнительных средств защиты.

ЗЦТА «Синтез» оснащен средствами защиты, предназначенными для предотвращения возможной утечки защищаемой акустической речевой информации.

**Внимание!** Изделие не предназначено для ведения закрытых переговоров.

ЗЦТА «Синтез» изготавливается в трёх модификациях в зависимости от модели базового телефонного аппарата:

- >> Синтез-1 на базе Panasonic KX-DT333
- >> Синтез-2 на базе Panasonic KX-DT343
- >> Синтез-3 на базе Panasonic KX-DT346



**Комплектация**

Защищённый цифровой телефонный аппарат «Синтез»	1 шт.
Комплект документации	1 к-т

**Технические характеристики**

Параметр и характеристика	Значение	Параметр и характеристика	Значение
Тип телефона	Цифровой	Тип дисплея	ЖК
Диапазон частот шумового сигнала	90 – 11300 Гц	Размер дисплея: Синтез-1,2 Синтез-3	3 строки 6 строк
Коэффициент качества шумового сигнала	не хуже 0,9	Подсветка дисплея	Есть (кроме «Синтез-1»)
Система диагностики функции защиты	Есть	Регулировка угла наклона аппарата и дисплея	Есть
Система индикации состояния функции защиты	Есть, световая	Мелодии звонка: Синтез-1 Синтез-2,3	10 20
Спикерфон	Есть	Масса	не более 1,5 кг
Количество программируемых кнопок линий/функций	24	Габариты корпуса	не более 320×220×100 мм

## Шорох-3 >>>>>

### Система постановки виброакустических и акустических помех

Система Шорох-3 предназначена для защиты речевой информации в выделенных помещениях до 1-й категории включительно от утечки по акустическим и вибрационным каналам путём создания помех для достижения соотношений сигнал/шум, обеспечивающих невозможность утечки речевой информации. >>>>>

#### Система Шорох-3 обеспечивает:

>> Защиту выделенных помещений от утечки речевой информации по любым акустическим и вибрационным каналам

>> Автоматическое «отслеживание» возникновения и исчезновения речевого сигнала в защищаемом помещении

>> Контроль работоспособности преобразователей и их соединительных (проводных) линий

## Средства защиты информации



### Элементы системы

Название	Описание
ГШВА-2	блок генератора электрического шума (2 канала генерирования и формирования электрических помеховых сигналов)
ТАИС-ИПЗ	блок питания генератора электрического шума ГШВА-2 (возможно подключение не более 3 блоков ГШВА-2)
ПЭД-5	электродинамический вибровозбудитель (для защиты ограничивающих и инженерных конструкций)
ПЭД-6	электродинамический вибровозбудитель (для защиты остекления окон)
OMS-2000	малогабаритный акустический излучатель (для защиты дверных проемов, вентиляционных каналов и т. д.)
АСМик-1	акустический излучатель с регулировкой уровня громкости (для защиты дверных проемов, вентиляционных каналов и т. д.)

Технические характеристики

Параметр и характеристика	Значение
Количество независимых каналов	2
Рабочий диапазон частот	от 175 до 11200 Гц
Вид сигнала-помехи	Белый шум
Наличие эквалайзера (частотной регулировки по октавам)	Да
Нормализованный коэффициент качества шумового сигнала	0,9 ± 10 %
Индикация работоспособности системы	Да
Диапазон рабочих температур	10–35°С
Напряжение сети электропитания системы	220 В ± 20%
Частота сети электропитания системы	50 Гц ± 2%
Потребляемая мощность от сети напряжением 220 В 50 Гц	50 Вт



Сертификат ФСБ России  
 Санитарно-эпидемиологическое заключение  
 Решение о соответствии требованиям пожарной безопасности  
 Гарантия 12 месяцев

## Шорох-5Л >>>>>

### Система постановки виброакустических и акустических помех

Система «Шорох-5Л» предназначена для защиты акустической речевой информации, циркулирующей в выделенных помещениях до 1-й категории включительно от утечки по акустическому и вибрационному каналам.

Система «Шорох-5Л» построена по принципу единого блока питания и активных оконечных преобразователей, что позволяет производить настройку каждого оконечного преобразователя индивидуально.

#### Система «Шорох-5Л» обеспечивает:

>>> Защиту выделенных помещений от утечки речевой информации по акустическому и вибрационному каналам

>>> Питание и управление излучателями помехи по двухпроводной линии

>>> Регулировку спектра помехи каждого из излучателей в 7-октавных полосах, а также регулировку общего уровня помехи, что позволяет обеспечить оптимальную настройку системы с минимумом побочных паразитных акустических шумов

>>> Расширенный контроль работоспособности каждого излучателя: режим работы, потребляемый ток, работоспособность механического блока

>>> Контроль параметров соединительных (проводных) линий

>>> Удаленное управление и удаленную индикацию режима работы системы с возможностью выдачи тревожных сообщений

>>> Возможность дистанционного включения и выключение системы

>>> Настройку по интерфейсу USB посредством специализированного программного обеспечения (СПО)

## Средства защиты информации

Система «Шорох-5Л»



Акустический излучатель «АИ-8А/Мини»



Акустический излучатель «АИ-8А/Н»



Вибропреобразователь «ПЭД-8А»

>>> Возможность управления включением произвольной нагрузки, подключенной к блоку питания и управления

>>> Возможность работы от внешнего источника питания 12 Вольт

>>> Учёт времени наработки системы

**Элементы системы**

Название	Описание
БПУ-1	Блок питания и управления
ПЭД-8А	Универсальный вибропреобразователь для окон, стен, перекрытий и инженерных коммуникаций
АИ-8А/Н	Акустический излучатель для настенного крепления
АИ-8А/Мини	Малогабаритный акустический излучатель для установки в межрамное пространство, вентиляционные каналы и т.п.
ПО «Шорох-ДУ»	Для настройки оконечных излучателей

**Технические характеристики**

Параметр и характеристика	Значение
Диапазон рабочих частот	не менее (не хуже) значения, установленного в НМД ФСТЭК «Требования к средствам активной акустической и вибрационной защиты акустической речевой информации»
Энтропийный коэффициент качества шума	
Диапазон регулировки уровня шумового сигнала в полосе октавных фильтров >> 0,125; 8 кГц >> 0,25; 0,5; 1; 2; 4 кГц	не менее 18 дБ
Диапазон регулировки общего уровня шумового сигнала	не менее 30 дБ
Напряжение электропитания системы	220 В (+10 % – 15 %)
Напряжение электропитания излучателя	12 В
Ток потребления излучателя	не более 0,2 А
Потребляемая мощность при полной нагрузке	не более 130 ВА
Диапазон рабочих температур	от 5 до 40 °С (для АИ-8А/У: от минус 40 до +45 °С)
Максимальное количество излучателей, подключаемых к «БПУ-1»	35 шт.

## Старкад >>>>>

**Генераторы шума для защиты информации от утечки за счет побочных электромагнитных излучений и наводок для построения распределённой объектовой системы активной защиты**

**Генераторы шума «Старкад»** предназначены для защиты информации от утечки по техническим каналам за счёт побочных электромагнитных излучений (Старкад-32) и наводок (Старкад-11) путём пространственного электромагнитного зашумления и являются техническими средствами защиты информации, обрабатываемой на объектах информатизации до первой категории включительно от утечки по техническим каналам за счёт ПЭМИН.

**В генераторах шума «Старкад»** заложена функциональная возможность объединения в единую сеть для формирования распределенной системы защиты информации от утечки по каналам ПЭМИН объекта любой сложности, в том числе распределенного территориально. >>>>

### Отличительные возможности:

- >>> Наличие отдельных регулировок выходного уровня по диапазонам позволяет оптимальным образом сформировать защитную помеху, снижая уровни паразитных электромагнитных излучений (соблюдение норм ГКРЧ, СанПиН, требований по ЭМС)
- >>> Возможность управления по сети Ethernet позволяет объединять генераторы в единую сеть для формирования распределенной системы защиты информации от утечки по каналам ПЭМИН любого объекта с возможностью мониторинга и управления системой с одного операторского места посредством специализированного программного обеспечения
- >>> Электропитание генераторов по технологии PoE (Power over Ethernet) позволяет существенно упростить процесс объединения отдельных устройств в распределенную систему с возможностью осуществления централизованного электропитания оконечных устройств
- >>> Объединение генераторов в единую систему защиты информации от утечки по каналам ПЭМИН объекта возможно на любом этапе эксплуатации, задействовав для этого в качестве транспортной среды существующую локальную вычислительную сеть объекта

## Технические средства

Старкад-11



Старкад-32



- >>> Наличие расширенной системы сигнализации позволяет получать информацию о функционировании изделия в режиме реального времени; в случае объединения ГШ в единую систему защиты информации от утечки по каналам ПЭМИН, вся информация о тревожных событиях по каждому из устройств регистрируется в журнале событий на месте оператора

- >>> В генераторах предусмотрено сохранение рабочих настроек в энергонезависимой памяти на случай пропадания электропитания и нарушения связи, после устранения аварийной ситуации повторная настройка изделия не требуется

- >>> Для всех модификаций генераторов шума «Старкад» разработаны излучающие системы (антенные системы/индукторы), а также рекомендации по монтажу, которые позволяют оптимальным образом провести установку и настройку



### Комплектация Старкад-11

Генератор шума Старкад-11	1 шт.
Индуктор (10 кГц до 10 МГц)	1 шт.
Индуктор (10 МГц до 400 МГц)	1 шт.
Комплект монтажных частей	1 шт.
Комплект документации	1 к-т

### Комплектация Старкад-32

Генератор шума Старкад-32	1 шт.
Антенна дипольная плоская (140–1800 МГц)	1 шт.
Комплект монтажных частей	1 к-т
Комплект документации	1 к-т

### Технические характеристики

Параметр и характеристика	Значение
Диапазон частот: Старкад-11 Старкад-32	Старкад-11: 0,01 – 400 МГц Старкад-32: 0,01 – 1800 МГц
Энтропийный коэффициент качества шума	не менее 0,9
Регулировка уровня сигнала, подводимого к излучающим системам	есть
Поддиапазоны частот регулировок	Старкад-11: 0,01–1 МГц; 1МГц–10 МГц; 10–100 МГц; 100–400 МГц Старкад-32: 0,01–30 МГц; 30–140 МГц; 140–400 МГц; 400–800 МГц; 800–1500 МГц; 1500–1800 МГц
Глубина регулировки в каждом из поддиапазонов	25 дБ
Интерфейс управления	проводной типа Ethernet 10/100 Мбит
Наличие сигнализации (виды обрабатываемых тревог и аварий)	световая и звуковая (контроль выходных параметров; перегрев; вскрытие/перемещение)
Электропитание	от интерфейса LAN (по технологии PoE) или от электросети переменного тока (220 В, 50 Гц) через сетевой адаптер
Режим работы	непрерывный круглосуточный
Максимальная потребляемая мощность	12,95 Вт
Габаритные размеры	210×140×36 мм
Масса	0,8 кг

## Старкад-Мини >>>>>

### Генераторы шума

Генераторы шума «Старкад-Мини» предназначены для защиты информации по каналам ПЭМИН на объектах информатизации до 1-й категории включительно.

#### Комплектация

Генератор шума «Старкад-Мини»	1 шт.
Адаптер питания	1 шт.
Кабель USB	1 шт.
ПО «Старкад-Мини»	1 шт.
Комплект документации	1 к-т

#### Дополнительно рекомендуем

Универсальное крепление на ЖК-монитор (позволяет закрепить изделие на задней панели монитора; перед заказом уточните применимость под Вашу конкретную модель монитора).

## Средства защиты информации



#### Технические характеристики

Параметр и характеристика	Значение
Диапазон частот шумового сигнала	0,01 – 1800 МГц
Энтропийный коэффициент качества шума	не менее 0,9
Наличие возможности регулировки общего уровня помехи	Да
Системы индикации контроля работоспособности изделия	Да (световая, звуковая)
Интерфейс управления изделием	USB
Возможность удаленного мониторинга за состоянием изделия	опционально (RS-485)
Напряжение электропитания	220±22 В
Частота переменного напряжения электропитания	50±1 Гц
Потребляемая мощность	не более 20 ВА
Время непрерывной работы	не менее 8 часов

Гарантия 12 месяцев

## Ковер-Н >>>>>

### Средство защиты информации от утечки по каналу ВЧ-облучения

«Ковер-Н» предназначено для предотвращения утечки речевой информации по каналу ВЧ-облучения за счет формирования защитной мультипликативной помехи путем хаотичного переотражения падающих на него электромагнитных волн и может эксплуатироваться в выделенных помещениях до 2-ой категории включительно.

#### Преимущества:

- >>> Полное соответствие параметров изделия последним требованиям НМД
- >>> Простота монтажа и эксплуатации изделия
- >>> Отсутствие необходимости проведения настройки перед эксплуатацией
- >>> Возможность дистанционного управления неограниченным количеством изделий из единого пункта управления
- >>> Круглосуточный непрерывный режим работы

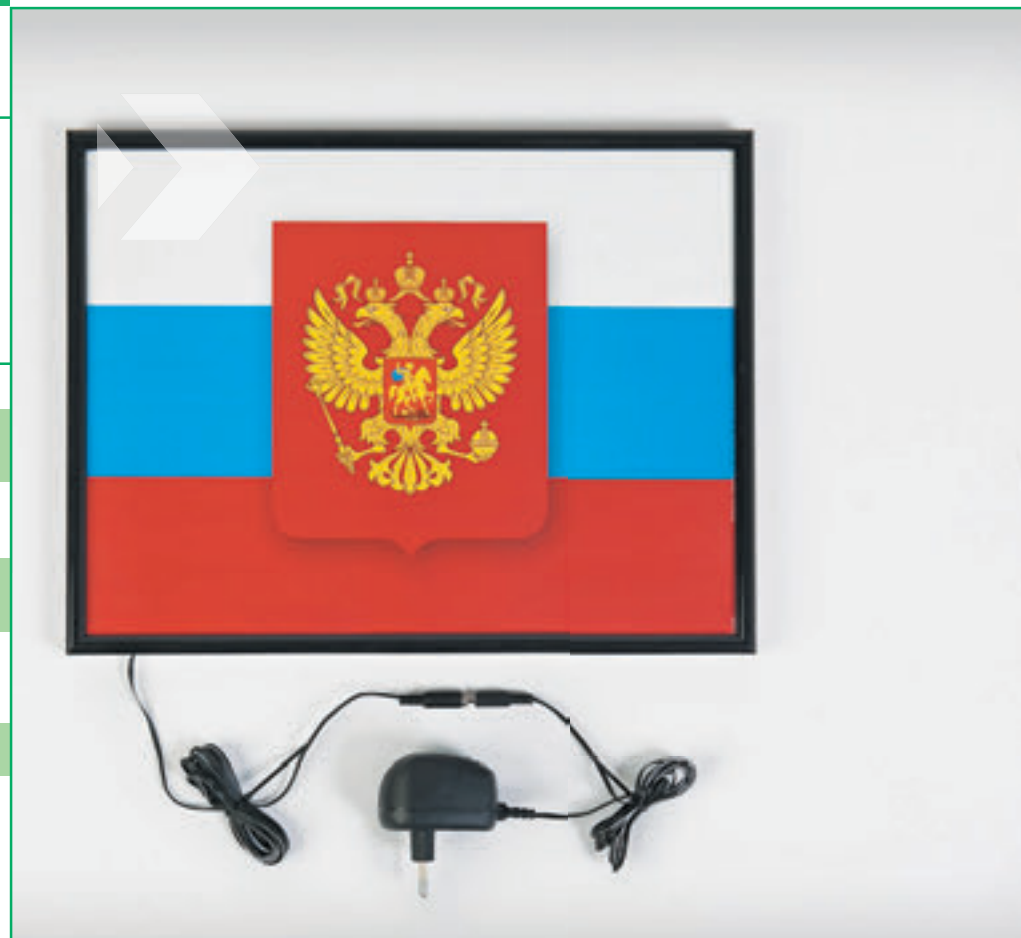
Средство защиты информации «Ковёр-Н» изготавливается в двух модификациях в зависимости от варианта исполнения:

- >>> Багет – в виде багета для фотографии;
- >>> Подставка – в виде подставки под техническое средство

#### Комплектация

Изделие «Ковёр-Н»	1 шт.
Сетевой блок питания	1 шт.
Комплект документации	1 к-т

## Средства защиты информации



#### Технические характеристики

Параметр и характеристика	Значение
Напряжение сети электропитания	220 В, 50 Гц
Потребляемая изделием мощность	не более 6 Вт

## Ключ-ВП >>>>>

### Управляемый размыкатель линий

Управляемые размыкатели линий «Ключ-ВП» предназначены для защиты информации от утечки в проводных коммуникациях, отходящих от технических средств, смонтированных на объекте защиты, за счет акустоэлектрических преобразований и воздействия методом ВЧ-навязывания.

Использование управляемых размыкателей линий «Ключ-ВП» совместно с системой «Шорох-5Л» позволяет при активации режима защиты автоматически размыкать защищаемые линии технических средств.

Принцип действия «Ключ-ВП» основан на размыкании защищаемой линии, отходящей от технического средства, по команде оператора или от системы защиты информации (на-пример, «Шорох-5Л»). >>>>>

Размыкатели линий представлены в нескольких модификациях:

- >> «Ключ-ВП (220)» — применяется в сетях питания 220В;
- >> «Ключ-ВП (СЛ)» — применяется в слаботочных линиях;
- >> «Ключ-ВП (ИТ)» — применяется в линиях компьютерных сетей и телефонии

#### Комплектация

Изделие «Ключ-ВП»	1 шт.
Комплект документации	1 к-т

#### Технические характеристики

Параметр и характеристика	Значение
Количество проводов линии (в зависимости от модификации)	3; 4; 8
Дистанционное управление	Да
Индикация состояния	Да
Время непрерывной работы	не менее 8 часов

## Средства защиты информации



Ключ-ВП (ИТ)



Ключ-ВП (220)

Гарантия 12 месяцев

Капсула >>>>>>>>>

Средства защиты информации

Акустический сейф

Акустический сейф «Капсула» предназначен для защиты закрытой акустической речевой информации, циркулирующей вблизи абонентских устройства сотовой связи, от утечки за счёт недекларируемых функций данных устройств.

>> Акустический сейф «Капсула» обеспечивает защиту речевой информации путем постановки акустической помехи во внутреннем объеме изделия.

>> Акустический сейф «Капсула» обладает возможностью индикации о поступлении входящих вызовов/сообщений на размещаемые внутри абонентские устройства сотовой связи.

Возможно изготовление акустического сейфа «Капсула» под конкретные габаритные размеры с учётом пожеланий по материалам внутренней и внешней отделки.

Комплектация

Акустический сейф «Капсула»	1 шт.
Комплект документации	1 к-т



Технические характеристики

Параметр и характеристика	Значение	Параметр и характеристика	Значение
Диапазон частот акустических шумовых сигналов	не менее 90 – 11300 Гц	Напряжение электропитания	220±22 В
Максимальный уровень звукового давления шумового сигнала в октавных полосах внутри защищаемого объема	не менее 100 дБ	Частота переменного напряжения электропитания	50±1 Гц
Система контроля работоспособности изделия	Да	Время непрерывной работы	не менее 8 часов
Возможность индикации о поступлении входящих вызовов/сообщений на размещаемые внутри абонентских устройства сотовой связи	Да (световая/звуковая)	Габариты изделия	Определяются конкретной модификацией

## Ларец-Авто»»»»»

Изделие «Ларец-Авто» предназначено для защиты закрытой акустической информации, циркулирующей на подвижном объекте (в салоне автомобиля), от утечки через абонентские устройства открытой спутниковой и сотовой связи за счет недекларируемых функций данных устройств.

»» «Ларец-Авто» обеспечивает защиту речевой информации путем постановки акустической помехи во внутреннем объеме изделия.

»» «Ларец-Авто» обладает возможностью индикации поступления входящих вызовов на размещаемые внутри него абонентские устройства спутниковой или сотовой связи.

»» «Ларец-Авто» позволяет блокировать возможность эксплуатации средств закрытой связи (далее ЗАС), размещенных на объекте (при их наличии), если защита информации от утечки по открытым каналам не обеспечивается.

»» «Ларец-Авто» устанавливается на заднем сиденье автомобиля и крепится с помощью штатного ремня безопасности и (или) посредством системы крепления Isofix.

»» Ларец-АВТО» может быть адаптирован под работу с любыми абонентскими устройствами связи Заказчика.

## Средства защиты информации



Комплектация

Изделие «Ларец-Авто»	1 шт.
ПО «Защита-Авто»	1 шт.
Комплект соединительных интерфейсных кабелей	1 к-т
Комплект документации	1 к-т

### Технические характеристики

Параметр и характеристика	Значение
Диапазон частот детектируемых передатчиков	100 – 2700 МГц
Диапазон частот акустических шумовых сигналов	не менее 80 – 11300 Гц
Количество октавных полос шумового сигнала	7
Возможность регулировки шумового сигнала по октавным полосам и общего уровня	Да
Максимальный уровень звукового давления шумового сигнала в октавных полосах внутри защищаемого объема	не менее 60 дБ
Система контроля работоспособности изделия	Да
Возможность индикации о поступлении входящих вызовов/сообщений на размещаемые внутри абонентских устройства спутниковой (сотовой) связи	Да (световая/звуковая)
Напряжение электропитания	10-18 В
Масса	не более 5,8 кг
Габариты корпуса	не более 465×285×330 мм

Гарантия 12 месяцев

## Ключ-Авто-2 >>>>>

### Модуль защиты

Модуль защиты «Ключ-Авто-2» предназначен для предотвращения утечки акустической речевой информации за счёт недеklarированных возможностей мультимедийных систем, а также иных потенциально «опасных» систем, установленных на подвижном объекте (в салоне автомобиля) и имеющих в своём составе акустоэлектрические и электроакустические преобразователи.

#### Комплектация

Модуль защиты «Ключ-Авто-2»	1 шт.
Предохранитель 15 А	1 шт.
Комплект разъёмов и соединителей	1 к-т
Комплект документации	1 к-т

#### Технические характеристики

Параметр и характеристика	Значение
Количество коммутируемых цепей	5 шт.
Коммутируемый	не более 15 А
Сопротивление замкнутых контактов	0,1 Ом
Напряжение питания	8–30 В
Ток потребления	30 – 500 мА
Масса	не более 0,35 кг
Габариты корпуса	не более 95×53×40 мм

## Средства защиты информации



Гарантия 12 месяцев

## Морфей-МК-У >>>>>

### Подавитель сотовой связи

Подавитель сотовой связи «Морфей-МК-У» предназначен для блокирования возможности организации связи между базовыми станциями и оконечными устройствами беспроводной связи.

Блокиратор «Морфей-МК-У» является интеллектуальной системой подавления, принцип работы которого основан на анализе спектра сигнала базовой станции и последующем излучении помехового сигнала, специальной формы. Благодаря этому достигается высокая эффективность блокирования любого количества абонентских терминалов беспроводных систем связи при меньшей мощности излучения. >>>>>

### Комплектация

Блок подавителя	1 шт.
Блок излучающих антенн	1 шт.
Приемная антенна	1 шт.
Программное обеспечение	1 шт.
Комплект документации	1 к-т

## Средства защиты информации



### Технические характеристики

Параметр и характеристика	Значение
Блокируемые стандарты	CDMA 450 EGSM, GSM 900, UMTS 900 (3G) GSM(DCS) 1800 UMTS 2100 (3G) LTE и LTE800 (4G) DECT Bluetooth (IEEE 802.15.1) Wi-Fi (IEEE 802.11 b/g/n)
Напряжение электропитания	220±22 В
Потребляемая мощность при полной нагрузке	80 ВА
Масса	5 кг
Габаритные размеры	485×220×70 мм

Санитарно-эпидемиологическое заключение  
Решение о соответствии требованиям пожарной безопасности  
Гарантия 12 месяцев



**Фазан** >>>>>

**Средства защиты информации**

**Помехоподавляющие сетевые фильтры**

Фильтры серии «Фазан» предназначены для защиты средств вычислительной техники и иных технических средств от утечки информации за счёт наводок информативных сигналов в однофазных (трёхфазных) сетях электропитания с максимальным рабочим током до 200 А, а также для подавления напряжений радиопомех в диапазоне частот 0,02 – 1000 МГц в двухпроводных (четырёхпроводных) сетях электропитания с глухозаземлённой или изолированной нейтралью.

Фильтры серии «Фазан» изготавливаются в следующих модификациях в зависимости от типа сети и максимального рабочего тока:

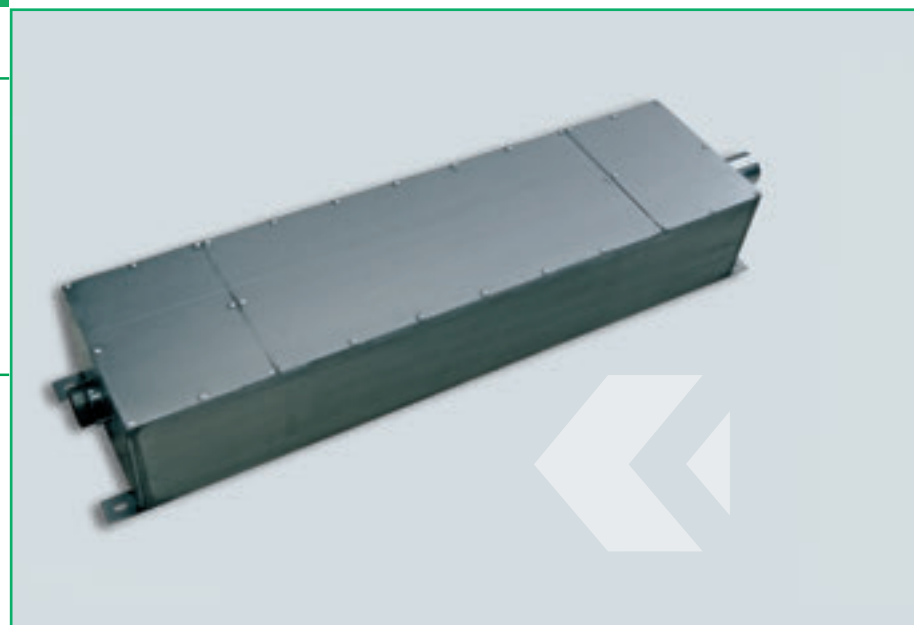
- >> «Фазан-1Ф-20» для однофазной сети до 20 А;
- >> «Фазан-1Ф-40» для однофазной сети до 40 А;
- >> «Фазан-1Ф-100» для однофазной сети до 100 А;
- >> «Фазан-3Ф-200» для трёхфазной сети до 200 А

**Комплектация**

Фильтр серии «Фазан»	1 шт.
Комплект документации	1 к-т

**Технические характеристики**

Параметр и характеристика	Значение	Параметр и характеристика	Значение
Диапазон частот подавления электромагнитного поля	0,02–1000 МГц	Частота питающей сети	(50±1,25) Гц
Вносимое затухание в диапазоне частот подавления электромагнитного поля	не менее 60 дБ	Максимальный рабочий ток для фильтра «Фазан-1Ф-20»; для фильтра «Фазан-1Ф-40»; для фильтра «Фазан-1Ф-100»; для фильтра «Фазан-3Ф-200»	20 А 40 А 100 А 200 А
Величина падения напряжения на каждой шине фильтра при номинальном рабочем токе на частоте 50 Гц от значения напряжения сети	не более 2 %	Масса	не более 24 кг
Общий уровень воздушного шума, создаваемого изделием	не более 35 дБА	Габаритные размеры (с патрубком)	не более 1020×220×100 мм не более 1020×220×150 мм
Напряжение питающей сети для фильтров «Фазан-1Ф-20», «Фазан-1Ф-40», «Фазан-1Ф-100» для фильтра «Фазан-3Ф-200»	220 В (+10 % –15 %) 380 В (+10 % –15 %)	для фильтров «Фазан-1Ф-20», «Фазан-1Ф-40», «Фазан-1Ф-100» для фильтра «Фазан-3Ф-200»	



## АПК «СВИТОК»

## Средства защиты информации

### Аппаратно-программный комплекс «Свиток»

Предназначен для защиты распределённых информационных систем.

Основные возможности:

- » Криптографическая аутентификация удаленных IP-источников информации методом электронной подписи (ЭЦП).
- » Обеспечение целостности информации методом имитозащиты.
- » Обеспечение конфиденциальности информации методом шифрования.
- » Сигнализация оператору защищаемой информационной системы о наступлении событий безопасности, например, обнаружение факта подмены источника.
- » Обеспечение юридической значимости результатов обработки путем формирования электронных документов, подписанных ЭЦП ответственного лица (оператора).



#### Основные технические характеристики

Вычисление и проверка электронной подписи	ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012.
Вычисление и проверка имитоприставки	ГОСТ 28147-89.
Пропускная способность EDS	до 1 Гбит/с
Пропускная способность EDSR	от 1 Гбит/с до 10 Гб/с
СПО мониторинга функционирует	Под операционными системами семейства Windows
Электропитание АМ	5 В, 12 В постоянного тока
Потребляемая мощность АМ	5 Вт

#### Основные технические характеристики

	Подпись	Имитозащита / Шифрование
<b>Задержка</b>	Не влияет на передачу трафика	0,3 мс
<b>Объем служебного трафика</b>	64 байта ~ каждую секунду	16 байт на каждый IP-пакет

Кожух видеокамеры  
Свиток



Распределительная  
коробка Свиток



Пыле- и влагозащищенный  
корпус Свиток



#### Комплектация

Аппаратные модули – абонентские Свиток-EDS и центральные Свиток-EDSR, обеспечивающие криптографическую аутентификацию IP-источников, а также имитозащиту или шифрование трафика между ними

СПО мониторинга и оповещения о событиях безопасности

СПО работы с ключевой информацией и конфигурирования аппаратных модулей

#### Аппаратные модули поставляются в модификациях:

##### »» Абонентский модуль Свиток-EDS:

- ▶ в отдельном пыле- и влагозащищённом корпусе;
- ▶ интегрированным в защитный кожух или корпус видеокамеры;
- ▶ интегрированным в распределительную коробку.

##### »» Центральный модуль Свиток-EDSR:

- ▶ в отдельном пыле- и влагозащищённом корпусе (поддерживает трафик до 1 Гбит/с);
- ▶ в серверном корпусе 1U (поддерживает трафик до 10 Гбит/с).

#### АПК «Свиток» может применяться для решения следующих задач:

- »» Защита от подмены информации, обрабатываемой в информационных системах технологического телевидения, видеонаблюдения, контроля выполнения правил дорожного движения и др.
- »» Защита от подмены видеоинформации, транслируемой на экраны общего пользования.
- »» Защита от подмены управляющей информации в АСУ ТП, в том числе в АСУ ТП пространственно распределенных критически важных объектов.
- »» Обеспечение целостности и контроль модификации информации, хранящейся в видео- и аудиоархивах, архивах электронных документов, архивах биллинга, архивах показаний приборов и датчиков измерительных систем и систем управления производством, медицинских архивах, архивах произведений искусства и т. д.
- »» Обеспечение целостности и контроль модификации информации в системах диагностики и мониторинга состояния объектов, таких как медицинские информационные системы, специализированные информационные системы контроля за перемещением объектов (транспорта) и т. д.
- »» Интеграция систем регистрации в создающуюся (созданную) систему электронного документооборота ведомства и в межведомственный электронный документооборот.

## Сигурд >>>>>

**Система оценки защищённости технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН)**

Система «Сигурд» предназначена для измерений параметров электромагнитных излучений и наводок при проведении специальных исследований технических средств.

**Система «Сигурд» обеспечивает:**

» Автоматизированное исследование технического средства на наличие информативных сигналов ПЭМИН в полном соответствии с действующими нормативно-методическими документами

» Автоматический и ручной поиск сигналов ПЭМИН исследуемого технического средства на фоне постоянно присутствующих радиосигналов по электрической и по магнитной составляющим электромагнитного поля, а также в отходящих линиях

» Автоматическое и ручное распознавание информативных сигналов ПЭМИН

» Расчет показателей защищённости технических средств от утечки информации по каналу ПЭМИН в соответствии с действующими нормативными документами, с выводом результатов по выбору оператора в файл стандарта HTML или MS Word (DOC)

» Автоматизированное исследование систем активного зашумления (САЗ) и расчет показателей их эффективности

» Дистанционное автоматическое управление измерительным приёмником (анализатором спектра) при поиске сигналов ПЭМИН, а при использовании опции «Сигурд-ИК» – и дистанционное автоматическое управление состоянием исследуемого технического средства при поиске его сигналов ПЭМИН

» Автоматическую передачу исходных данных в расчет показателей защищённости технического средства и эффективности САЗ



## Системы оценки защищённости



Основные модификации системы «Сигурд»:

- » M5 (Rohde&Schwarz FSH4)
- » M6 (Rohde&Schwarz FSH8)
- » M7 (Rohde&Schwarz ESRP)
- » M8 (Rohde&Schwarz FSV)
- » M19 (Rohde&Schwarz FSC3)

Сертификат ФСТЭК России  
Сертификат ФСТЭК России на СПО  
Свидетельство об утверждении типа средств измерений  
Гарантия 12 месяцев

- »» Возможность создания и пополнения базы данных по постоянно присутствующим радиосигналам в выбранном диапазоне частот
- »» Возможность визуализации в процессе исследования радиосигналов, представляющих интерес
- »» Формирование сообщений о неверных действиях оператора с указанием характера ошибки
- »» Расчет минимально допустимых расстояний R2 от технического средства до границы контролируемой зоны
- »» Расчет минимально допустимых расстояний r1 от технического средства до сосредоточенных случайных антенн
- »» Расчет минимально допустимых расстояний r1' от технического средства до распределенных случайных антенн
- »» Расчет отношения «сигнал/шум» на границе контролируемой зоны
- »» Расчет отношения «сигнал/шум» на границе контролируемой зоны с учетом применения систем активного зашумления
- »» Расчет отношения «сигнал/шум» в отходящих линиях
- »» Расчет отношения «сигнал/шум» в отходящих линиях с учетом применения систем активного зашумления

**Поддерживаемые СПО «Сигурд» анализаторы спектра:**

Rohde&Schwarz серия FSH	Rohde&Schwarz серия FSV	Rohde&Schwarz серия FSC
Rohde&Schwarz серия ESRP	Rohde&Schwarz серия ESPI	Rohde&Schwarz серия FSP
Rohde&Schwarz серия FSL;	Agilent Technologies E4402B/E4405B/E4407B	Aeroflex IFR 2394/2394A/2395A/2399/2399C

**Технические характеристики**

Параметр и характеристика	Значение
Границы диапазона частот при измерении системой напряженности электрического поля	9 кГц–2000 МГц
Границы диапазона частот при измерении системой напряженности магнитного поля	9 кГц–30 МГц
Границы диапазона частот при измерении системой силы тока и напряжения переменного тока, наведенного электромагнитным полем	9 кГц–300 МГц
Динамический диапазон измерений напряженности электромагнитного поля, силы тока и напряжения переменного тока, наведенного электромагнитным полем	не менее 75 дБ
Устанавливаемые полосы пропускания	не менее 0,1; 0,3; 1; 3; 10; 30; 100; 300 кГц
Продолжительность поиска при выполнении тестового задания «Сигурд-Тест» (без учета времени ввода условий исследования)	не более 300 с
Точность расчета показателей R2, r1 и r1' для объектов 1-й, 2-й и 3-й категории и для стационарных, возимых и носимых средств разведки	не хуже предельных значений, заданных в нормативных документах

## Шепот-М1 >>>>>

### Система оценки защищённости выделенных помещений по виброакустическому каналу

**Система «Шепот-М1»** предназначена для проведения специальных акустических и вибрационных измерений в помещениях с целью оценки их защищённости от утечки речевой информации по акустическому и вибрационному каналам.

**Система «Шепот-М1» обеспечивает:**

>>> Автоматическое измерение уровня звукового давления тестового сигнала вблизи и на удалении от его источника, а также уровня наведенного им виброускорения в 7-октавных полосах

>>> Автоматические измерения уровня звукового давления тестового сигнала вблизи и на удалении от его источника в 19 третьоктавных полосах с центральными частотами

>>> Автоматические измерения уровня звукового давления тестового сигнала вблизи от его источника и уровня наведенного им виброускорения в 19 третьоктавных полосах с центральными частотами

>>> Использование данных измерений по 5-ти, 6-ти либо 7-октавным полосам для расчёта показателей защищённости выделенных помещений по виброакустическому каналу утечки речевой информации

>>> Формирование и ведение базы данных о результатах выполненных измерений, включающей информацию о месте проведения измерений (объект, помещение, контрольная точка) и о результатах измерений и расчетов в каждой контрольной точке

>>> Составление отчета по результатам измерений в форме, отвечающей требованиям нормативных документов

## Системы оценки защищённости



>>> Автоматический и/или ручной режим ввода данных для расчёта показателей защищённости выделенных помещений по виброакустическому каналу

>>> Возможность перехода на ручное управление аппаратурой системы

>>> Установку параметров проведения измерений для каждого измерительного цикла

>>> Ввод калибровочных значений измерительных микрофонов и акселерометра, их сохранение и корректировку

>>> Формирование акустических сигналов различных видов при использовании звуковой карты ПЭВМ в качестве генератора шумового сигнала

Оформляется сертификат ФСТЭК России

Оформляется свидетельство об утверждении типа средств измерений

Гарантия 12 месяцев

### Комплектация

Измерительный блок (шумомер)	2 шт.
ICP микрофон	2 шт.
ICP-акселерометр	1 шт.
Источник калиброванного звукового давления	1 шт.
Управляющая ПЭВМ ноутбук	1 шт.
Комплект специального программного обеспечения	1 к-т
Колонка акустическая активная	1 шт.
Штатив для громкоговорителя и микрофонов	3 шт.
Полужесткая транспортная укладка	1 шт.
Комплект документации	1 к-т

### Технические характеристики

Параметр и характеристика	Значение
Диапазон рабочих частот	80 – 11300 Гц
Диапазон измерений звукового давления	24 – 132 дБ (20 мкПа)
Диапазон измерений виброускорения	$2 \cdot 10^{-3} - 200 \text{ м} \cdot \text{с}^{-2}$
Погрешность измерений уровня звукового давления и виброускорения	±0,7 дБ
Неравномерность частотной характеристики при измерении звукового давления	Соответствует шумомерам 1-го класса точности по ГОСТ Р 53188.1-2008
Максимальное звуковое давление тест-сигнала на расстоянии 1 м от излучателя (интегральное, в полосе частот 80–11300 Гц)	106 дБ
Нестабильность излучателя тест-сигнала (при измерении в 7-октавных полосах с центральными частотами 250, 500, 1000, 2000 и 4000 Гц) за 10 мин	±1 дБ
Неравномерность АЧХ излучателя тест-сигнала в полосе частот 80 – 11300 Гц (при измерении в 7 октавных полосах с центральными частотами 125, 250, 500, 1000, 2000, 4000 и 8000 Гц)	не более ±12 дБ

## Талис-М1 >>>>>

**Автоматизированная система исследования эффекта акустоэлектрических преобразований в технических средствах и отходящих от них линиях**

**Система «Талис-М1»** предназначена для проведения исследований характеристик технических средств с целью оценки наличия акустоэлектрических преобразований, возникающих в них и отходящих от них линиях при воздействии акустическим сигналом. Система обеспечивает автоматизированное исследование технического средства на наличие эффекта ВЧ АЭП в паразитных излучениях в соответствии с действующими нормативно-методическими документами. >>>>>

**Система «Талис-М1» обеспечивает:**

>>> Автоматизированное исследование технического средства на наличие эффекта ВЧ АЭП в паразитных излучениях в соответствии с действующими нормативно-методическими документами

>>> Проведение расчетов показателей защищенности технических средств от утечки информации по каналу ВЧ АЭП в соответствии с действующими нормативными документами, с выводом результатов в файл стандарта HTML или DOC (по выбору оператора)

>>> Автоматическую передачу в расчет показателей защищенности технического средства по каналу ВЧ АЭП результатов измерений сигналов, отнесенных системой «Талис-М1» и/или ее оператором к опасным сигналам, и характеристик использованного для измерений оборудования, в том числе и амплитудно-частотных характеристик антенно-фидерных устройств

>>> Предоставление оператору системы «Талис-М1» пользовательского интерфейса, позволяющего установить все необходимые параметры для работы системы как в режиме автоматического выполнения задания, так и в режиме ручного исследования сигналов

## Системы оценки защищенности



>>> Возможность создания и пополнения базы данных по постоянно присутствующим радиосигналам в зоне расположения исследуемого технического средства с целью уменьшения количества срабатываний системы «Талис-М1» на такие сигналы

>>> Возможность визуализации в процессе исследования радиосигналов, представляющих интерес

>>> Автоматический поиск и измерение параметров сигналов исследуемого технического средства в соответствии с подготовленным заданием

>>> Возможность прослушивания демодулированного сигнала

Оформляется свидетельство об утверждении типа средств измерений  
Гарантия 12 месяцев



**Комплектация**

Анализатор спектра	1 шт.
Модуль цифровой обработки	1 шт.
Комплект измерительных антенн	1 к-т
Пробник напряжения	1 шт.
Измерительный блок (шумомер)	1 шт.
ICP микрофон	1 шт.
Комплект формирования тестового акустического сигнала	1 к-т
Устройство управления исследуемым техническим средством	1 шт.
Управляющая ПЭВМ ноутбук	1 шт.
Комплект программного обеспечения	1 к-т

**Технические характеристики**

Параметр и характеристика	Значение
Диапазон частот при измерении системой «Талис-М1» напряженности электрического поля	0,9 – 2000 МГц
Диапазон частот при измерении системой «Талис-М1» напряженности магнитного поля	0,9-30 МГц
Диапазон частот при измерении системой «Талис-М1» силы тока и напряжения переменного тока, наведенного электромагнитным полем	0,9-300 МГц
Динамический диапазон измерений напряженности электромагнитного поля, силы тока и напряжения переменного тока, наведенного электромагнитным полем	не менее 75 дБ
Минимальный измеряемый уровень напряженности электрического поля	15 дБ (мкВ/м)
Минимальный измеряемый уровень напряженности магнитного поля	20 дБ (нА/м)
Минимальный измеряемый уровень силы тока, наведенного электромагнитным полем	38 дБ (мкА)
Минимальный измеряемый уровень напряжения переменного тока	26 дБ (мкВ)
Диапазон частот измерения звукового давления	не менее 80 – 11300 Гц
Диапазон измерений звукового давления	не менее 24 – 132 дБ (20 мкПа)
Погрешность измерений уровня звукового давления и виброускорения	не более $\pm 0,7$ дБ
Диапазон частот формирования акустического тест-сигнала	не менее 80 – 11300 Гц
Максимальное звуковое давление тест-сигнала на расстоянии 1 м от излучателя (интегральное, в полосе частот 80–11300 Гц)	не менее 106 дБ
Минимальный измеряемый коэффициент (индекс) модуляции	не хуже $1 \cdot 10^3$
Погрешность измерения коэффициента (индекса) модуляции	не хуже 10%

## Талис-НЧ-Лайт >>>>>

**Автоматизированная система исследования эффекта АЭП в ТС и отходящих от них линиях в речевом диапазоне частот**

**Система «Талис-НЧ-Лайт»** предназначена для проведения селективных измерений сверхмалых величин уровня электрического напряжения переменного тока (при его изменении в рабочем диапазоне частот) и разработана для применения при исследованиях технических средств и отходящих от них линий с целью оценки наличия в них акустоэлектрических преобразований, возникающих при воздействии акустическим сигналом, и решения практических измерительных задач. Система «Талис-НЧ-Лайт» является электронным селективным вольтметром (нано-вольтметром), предназначенным для измерений уровня напряжения переменного тока в слаботочных линиях и линиях электропитания напряжением 220 В с частотой 50 Гц. >>>>>

**Отличительные возможности системы:**

- >> Использование методов цифровой обработки для фильтрации сигналов помех и выделения на их фоне информативного сигнала
- >> Управляемая адаптивная фильтрация 1-ой и 3-ей гармоник сети питания 220 В
- >> Возможность прямых измерений в линиях электропитания 220В без их обесточивания при помощи пробника Талис-НЧ-ПЭС
- >> Отсутствие влияния на работу элементов системы (включая пробники и кабели) паразитного воздействия акустического тест-сигнала и/или электромагнитных полей

## Системы оценки защищенности



Свидетельство об утверждении типа средств измерений  
Гарантия 12 месяцев

### Комплектация

Блок преобразований	1 шт.
Входной НЧ фильтр-усилитель	1 шт.
Пробник для промышленной электросети	1 шт.
Управляющая ПЭВМ	1 шт.
Программный модуль управления системой	1 шт.
Комплект измерительных кабелей и устройств	1 шт.
Комплект соединительных кабелей и вспомогательных устройств	1 к-т
Транспортная укладка	1 шт.
Комплект документации	1 к-т

### Дополнительно рекомендуем

ПО Талис-НЧ-Дельта (программный модуль расчета показателей защищенности информации от утечки по каналу АЭП в ТС и отходящих от них линиях в речевом диапазоне частот)
УЭК (колонка акустическая экранированная со штативом и укладкой для транспортировки)

### Технические характеристики

Параметр и характеристика	Значение
Диапазон измеряемых частот напряжения переменного тока в линии	от 100 до 10 000 Гц
Диапазон измерений напряжения в слаботочных линиях	от $5 \cdot 10^8$ до 0,3 В
Диапазон измерений напряжения в линиях электропитания	от $3 \cdot 10^7$ до 1,0 В
Напряжение сети электропитания системы	220
Частота сети электропитания системы	50

## Талис-НЧ-М1»»»»»

**Автоматизированная система исследования эффекта акустоэлектрических преобразований в технических средствах и отходящих от них линиях в речевом диапазоне частот** »»

Система «Талис-НЧ-М1» предназначена для измерения электрических сигналов, возникающих за счет акустоэлектрических преобразований в технических средствах и отходящих от них линиях в речевом диапазоне частот и оценки защищенности технических средств от утечки речевой информации.

Система «Талис-НЧ-М1» базируется на элементах собственной разработки и предназначена для исследования слаботочных линий и линий электропитания напряжением 220 В с частотой 50 Гц.

### Отличительные возможности системы:

- »» Автоматизация процесса поиска, выявления и измерения сигналов акустоэлектрических преобразований, включая оценку помеховой обстановки и корректности измерений
- »» Проведение измерений в произвольных «слаботочных» линиях и в линиях электропитания, находящихся под напряжением 220 В/50 Гц
- »» Адаптивное глубокое подавление частоты промышленной электросети и её гармоник
- »» Автоматизированный и ручной режим проведения исследований
- »» Экранированный тракт формирования тестового акустического сигнала практически не вносит погрешности в измерения

## Системы оценки защищенности



Свидетельство об утверждении типа средств измерений  
Гарантия 12 месяцев

### Комплектация

Блок преобразований	2 шт.
Входной НЧ фильтр-усилитель	1 шт.
Пробник для промышленной электросети	1 шт.
Устройство развязывающее для слаботочных линий	1 шт.
Преполяризованный ИСР конденсаторный микрофон	1 шт.
Генератор-усилитель тестового акустического сигнала	1 шт.
Колонка акустическая экранированная со штативом и укладкой для транспортировки	1 шт.
Управляющая ПЭВМ	1 шт.
Программный модуль управления системой	1 шт.
Программный модуль управления цифровым анализатором спектра	1 шт.
Комплект измерительных кабелей и устройств	1 шт.
Комплект соединительных кабелей и вспомогательных устройств	1 шт.
Транспортная укладка	1 шт.
Комплект документации	1 к-т

### Дополнительно рекомендуем

ПО Талис-НЧ-Дельта (программный модуль расчета показателей защищённости информации от утечки по каналу АЭП в ТС и отходящих от них линиях в речевом диапазоне частот)

### Технические характеристики

Параметр и характеристика	Значение
Диапазон измеряемых частот напряжения переменного тока в линии	от 100 до 10000 Гц
Диапазон измерений напряжения в слаботочных линиях	от $5 \cdot 10^8$ до 0,3 В
Диапазон измерений напряжения в линиях электропитания	от $3 \cdot 10^7$ до 1,0 В
Диапазон рабочих частот при измерении звукового давления	от 12,5 до 12500 Гц
Диапазон измерения уровня звукового давления	от 25 до 128 дБ
Диапазон частот акустического тестового сигнала	от 88 до 11200 Гц
Напряжение сети электропитания системы	220
Частота сети электропитания системы	50

## Лазурит >>>>>

### Автоматизированная система измерения параметров волоконно-оптических систем передачи и оценки защищённости оптических линий связи

Система «Лазурит» предназначена для измерения параметров волоконно-оптических систем передачи и оценки защищённости оптических линий связи.

В системе «Лазурит» заложены возможности оптического тестера и рефлектометра, в том числе: измерение мощности оптического излучения, измерение затухания в оптических волокнах и их соединениях, определение длин волоконно-оптических линий, локализация неоднородностей и соединений волокон, включая те, которые вызваны поломкой кабеля, визуальное определение мест повреждения волокна, генерация стабилизированного оптического излучения.

#### Система «Лазурит» обеспечивает:

- >> Автоматизированный расчёт заданных показателей защищённости ВОСП от утечки информации по оптическому каналу на основе исходных параметров и характеристик и данных, полученных от специализированных средств измерений для ВОЛС
- >> Оценку соответствия ВОСП установленной категории защищённости от утечки информации по оптическому каналу
- >> Вывод результатов расчета показателей защищённости в файл стандарта HTML или DOC (по выбору оператора) и составление технического паспорта исследуемой ВОСП
- >> Защиту от несанкционированного использования при помощи технологии электронных идентификационных ключей

## Системы оценки защищённости



Сертификат ФСТЭК России на расчетную часть СПО  
Гарантия 12 месяцев

### Комплектация

Многофункциональный оптический измерительный прибор	1 шт.
Оптический тестер	2 шт.
Управляющая ПЭВМ	1 шт.
Комплект СПО	1 к-т
Комплект кабелей и вспомогательных устройств для подключения к ВОЛС	1 к-т
Укладка для транспортировки	1 шт.
Комплект документации	1 к-т

### Технические характеристики

Наименование характеристики	Значение
Диапазон длин волн	850 нм 1300 нм (Многомодовый режим)
	1310 нм 1550 нм (Одномодовый режим)
Динамический диапазон: 850 нм 1300 нм 1310 нм 1550 нм	27 дБ 29 дБ 36 дБ 34 дБ
Диапазон измерения мощности оптического излучения: 850 нм 1310 нм, 1550 нм	от минус 70 до +7 (от 100 пВт до 5 нВт) дБм
Диапазон измеряемых расстояний	2, 5, 10, 20, 40, 80, 120, 160, 240 км



## ИКАР >>>>>

## Инженерно-технические средства охраны

### Интегрированный комплекс

**Интегрированный комплекс «Икар»** объединяет программно-аппаратные и инженерно-технические средства и системы и предназначен для создания многофункциональных систем охраны объектов различных категорий, степени сложности и конфигурации.

#### Основные функции:

- >>> Обнаружение и локализация попыток несанкционированного проникновения, проноса (провоза) запрещённых веществ и предметов;
- >>> Обеспечение непрерывного круглосуточного управления и контроля доступа персонала и транспортных средств на территорию и в помещения охраняемого объекта, а также ведение учёта личного состава, находящегося на территории охраняемого объекта;
- >>> Обеспечение непрерывного круглосуточного наблюдения за доступом персонала и транспортных средств на территорию и в помещения охраняемого объекта;
- >>> Отображение видеoinформации о состоянии участков наблюдения на мониторе рабочего места оператора;
- >>> Обеспечение необходимой видеoinформацией и информацией журналов событий на АРМ для принятия своевременного решения по прекращению несанкционированного проникновения;



- >>> Осуществление архивирования поступающей видеoinформации и информации журналов событий;
- >>> Обеспечение непрерывного круглосуточного контроля работоспособности технических средств, входящих в состав комплекса



### Комплектация

<b>Интегрированный комплекс «Икар» включает следующие основные функциональные системы:</b>
Сигнально-заградительная система охранной сигнализации «Икар СОС»
Система телевизионного наблюдения «Икар СОТ»
Система управления доступом и охранной сигнализации «Икар СУДОС»
Система сетевого компьютерного управления «Икар ССКУ»
Вспомогательные средства и системы

Сигнально-заградительная система охранной сигнализации в зависимости от категории охраняемого объекта, назначения локальных зон и зданий (сооружений) включает:

- »» Сигнализационные и инженерные заграждения;
- »» Периметровые средства обнаружения;
- »» Средства сбора и обработки информации;
- »» Вспомогательные средства.

### Основные технические характеристики

Время готовности	не более 90 с
Время восстановления дежурного режима	не более 30 с
Вероятность обнаружения при преодолении сигнализационного заграждения без использования подручных средств при доверительной вероятности	0,95
Гарантийный срок	12 мес.

## СПДУ-1 >>>>>

### Стол поворотный диэлектрический управляемый

СПДУ-1 предназначен для автоматизации проведения специальных исследований технических средств на наличие ПЭМИН.

СПДУ-1 разработан с учётом требований «Сборника методических документов по контролю защищённости информации, обрабатываемой средствами вычислительной техники, от утечки за счёт побочных электромагнитных излучений и наводок».

Наиболее эффективно использовать СПДУ-1 в составе специализированных автоматизированных систем, например, таких как система оценки защищённости технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок «Сигурд».



#### СПДУ-1 обеспечивает:

>>> Ручной и автоматизированный режимы поиска в горизонтальной плоскости направления распространения сигналов ПЭМИН исследуемого технического средства.

>>> В автоматизированном режиме предоставление оператору СПДУ-1 необходимого пользовательского интерфейса, позволяющего установить все требуемые для работы параметры.

>>> Вращение столешницы в любую сторону на 360°.

>>> Ручной поворот столешницы при отключенном электроприводе

>>> Управление столом осуществляется от пульта дистанционного управления по каналу ИК-связи.

## Дополнительное оборудование



Гарантия 12 месяцев

**Комплектация**

Поворотный стол	1 шт.
Пульт дистанционного управления	1 шт.
Элемент питания	2 шт.
Кабель оптический	1 шт.
Комплект документации	1 к-т

**Примечания:**

Имеется возможность съёма столешницы для обеспечения удобства транспортировки стола.

Параметр и характеристика	Значение
Высота от пола до поверхности столешницы	800 мм
Диаметр столешницы	1300 мм
Максимальная допустимая нагрузка на столешницу	80 кг
Скорость вращения столешницы	12 – 15 град/с
Диапазон вращения столешницы по углу поворота	0 – 360 град
Длина оптического соединительного кабеля	10 м
Время непрерывной работы изделия без ухудшения рабочих характеристик	не менее 8 час.
Напряжение сети электропитания изделия	220 ± 20 В
Частота сети электропитания изделия	50 ± 2 Гц
Максимальная допустимая мощность, потребляемая испытуемой аппаратуры	1000 Вт



## Модуль ЦОС «МК-14» >>>>>

### Модуль цифровой обработки сигналов

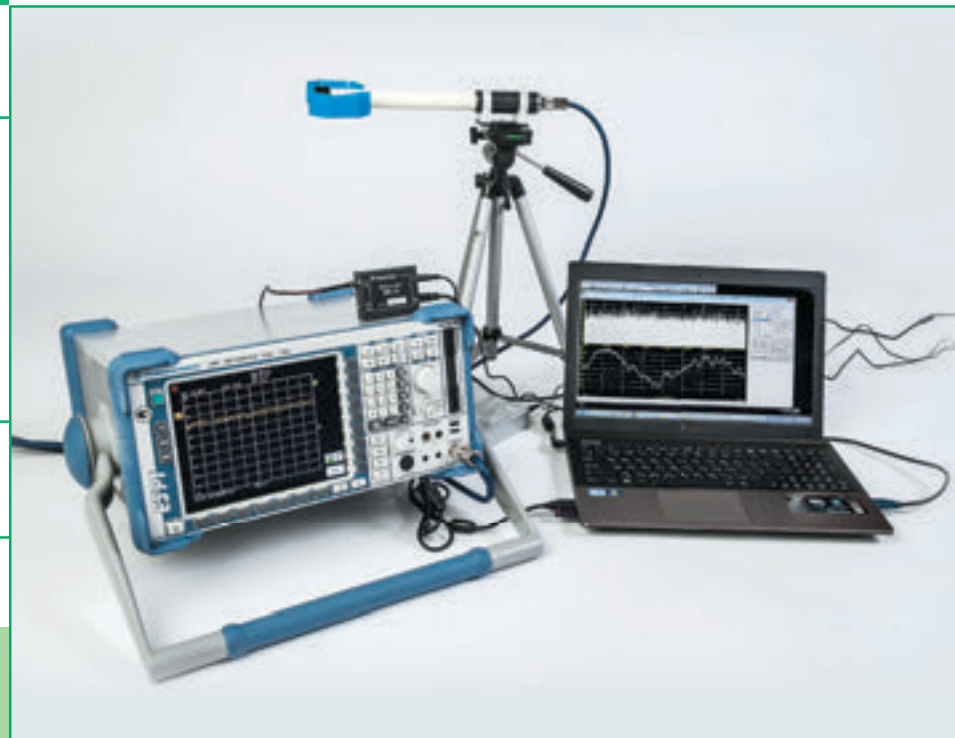
Модуль цифровой обработки сигналов «МК-14» предназначен для приёма и последующего многофункционального анализа электрических сигналов в заданном диапазоне частот. Является дополнительной опцией автоматизированной системы оценки защищённости технических средств от утечки информации по каналу ПЭМИН «Сигурд» и обеспечивает расширение возможностей моделей анализаторов спектра или измерительных приёмников.

Модуль ЦОС «МК-14» может использоваться как составная часть и в других, кроме «Сигурд», измерительных и исследовательских системах. >>>>

#### Модуль ЦОС «МК-14» позволяет:

- >>> Сократить время поиска сигналов при высоком разрешении по частоте до 50 раз (быстрее, чем это можно сделать средствами анализатора)
- >>> Повысить чувствительность системы от 10 до 100%
- >>> Производить поиск и анализ сигналов с высоким разрешением по частоте, что, в свою очередь, даёт более детальное представление о сигнале (особенно заметно, при масштабировании графиков)
- >>> Проводить коррекцию и верификацию сигналов прямо в цикле поиска (сканирования)

## Дополнительное оборудование



Гарантия 12 месяцев

**Отличительные возможности:**

- Отображение амплитудного спектра сигнала в логарифмическом и линейном масштабе облегчает восприятие спектров оператором
- Просмотр амплитудной и фазовой модуляции, а также амплитудной и частотной комплексного сигнала в полярных координатах
- Включение и отключение полосового и видео-фильтров для исследуемой частоты, просмотр графика амплитуды без постоянной составляющей, просмотр графика частоты без постоянной составляющей
- Исследование выходного сигнала модуля ЦОС в декартовых координатах (действительная и мнимая часть комплексного сигнала)

**Комплектация**

Модуль ЦОС	1 шт.
Комплект кабелей	1 к-т
Комплект документации	1 к-т
Адаптер питания	1 шт.
Мини-кейс для переноски	1 шт.



## Пункт телевизионного наблюдения МСШЕ.425358.003 >

Конструктивно и функционально законченное устройство, входящее в состав системы охранного телевидения наблюдения «Контур СОТ».

**Пункт телевизионного наблюдения** обеспечивает дистанционное наблюдение за подступами к охраняемым зонам, участкам периметров, зон доступа и другими областями пространства, а также охраняемыми помещениями и критически важными точками объекта с целью оценки текущей обстановки, наблюдения за действиями и продвижением нарушителей, координации действий персонала службы безопасности. >>>

### Основные функции:

- >> Обеспечение круглосуточной работы
- >> Обеспечение целостности передаваемой информации
- >> Передача информации на устройство сбора информации
- >> Автоматическое управление фокусным расстоянием объектива и диафрагмой
- >> Компенсация прямых засветок объектива и засветок цели сзади
- >> Автоматический контроль работоспособности и линии передачи сигнала
- >> Всепогодная эксплуатация с защитой оборудования от неблагоприятных воздействий окружающей среды

## Дополнительное оборудование

ПТН №3. Внешний вид на опоре



### Отличительные особенности:

- >> Оснащен устройством предварительного подогрева
- >> Многоступенчатая автоматическая система обогрева
- >> Непосредственный нагрев стекла по периметру
- >> Металлическая распределительная коробка
- >> Металлические кабельные вводы и металлорукав
- >> Соответствует климатическим характеристикам военной техники
- >> Возможность подключения модуля грозозащиты линии Ethernet без использования специального инструмента

Оформляется сертификат соответствия в Системе сертификации ГОСТ Р  
Гарантия 3 года

### Технические характеристики

Параметр и характеристика	Значение
Напряжение питания	220 В переменного тока
Класс защиты	IP 66
Температурный режим	-40°С +40° С
Матрица	1/3"–КМОП
Разрешение камеры	2 Мегапикселя
Количество потоков	не менее 2-х
Частота кадров	До 25 к/сек (1920×1080)
Формат сжатия видео	H264 и MJPEG
Интерфейс	Сетевой 100 Base-TX
Фокусное расстояние объектива	(2,8–9) мм
Угол обзора	От 87° (2,8 мм) до 32° (9 мм)

### Комплектация

Пункт телевизионного наблюдения с двухрежимной IP-камерой «день/ночь», вариофокальным объективом для мегапиксельных камер «день-ночь» в термокожухе с распределительной коробкой, тороидальным трансформатором 100 ВА, устройством грозозащиты линии Ethernet и линии электропитания, кабельные гермовводы	1 шт.
Формуляр	1 шт.
Руководство по эксплуатации	1 шт.
ИК-прожектор уличный с кронштейном (опция)	1 шт.
Комплект монтажных частей для установки на мачту, стену здания (опция)	1 к-т

### Дополнительно рекомендуем

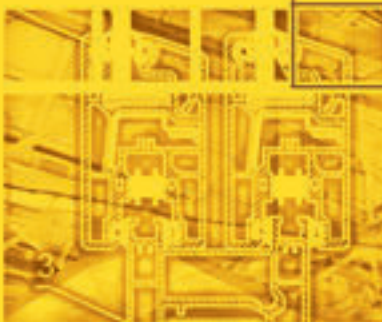
Применение средства криптографической защиты информации «Свиток»
--

### Область применения

Использование в тяжелых климатических условиях
Использование в местах с высоким риском актов вандализма
С ИК-прожектором – в условиях отсутствия или недостаточной освещённости объектов
Для организации скрытого наблюдения



**СЕРТИФИКАТЫ  
И ЛИЦЕНЗИИ**





## СЕРТИФИКАТЫ И ЛИЦЕНЗИИ

### Лицензии ФСБ России:

- »» Лицензия Управления ФСБ России по г.Москве и Московской области № 26360 от 28.05.2015 г. на проведение работ, связанных с использованием сведений, составляющих государственную тайну.
- »» Лицензия Управления ФСБ России по г.Москве и Московской области № 26946 от 09.09.2015 г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 552 Т от 28.04.2014 г. на осуществление разработки, производства, реализации и приобретения в целях продажи специальных технических средств, предназначенных для негласного получения информации.
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 15105 С от 04.05.2016 г. на создание средств защиты информации, содержащей сведения, составляющие государственную тайну.
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 15106 М от 04.05.2016 г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 15107 М от 04.05.2016 г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 15108 М от 04.05.2016 г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 15109 В от 06.05.2016 г. на осуществление выявления электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 15120 Н от 06.05.2016 г. на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнения работ, оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).
- »» Лицензия Центра по лицензированию, сертификации и защите государственной тайны ФСБ России № 15121 К от 06.05.2016 г. на осуществление разработки и производства средств защиты конфиденциальной информации.

### Лицензии ФСТЭК России:

- »» Лицензия Федеральной службы по техническому и экспортному контролю № 1373 от 26.11.2011 г. на проведение работ, связанных с созданием средств защиты информации.
- »» Лицензия Федеральной службы по техническому и экспортному контролю № 1051 от 26.11.2011 г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части противодействия иностранным техническим разведкам).
- »» Лицензия Федеральной службы по техническому и экспортному контролю № 94 от 26.11.2011 г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации).
- »» Лицензия Федеральной службы по техническому и экспортному контролю № 0010 от 26.09.2002 г. на деятельность по разработке и производству средств защиты конфиденциальной информации.
- »» Лицензия Федеральной службы по техническому и экспортному контролю № 0010 от 26.09.2002 г. на деятельность по технической защите конфиденциальной информации.
- »» Лицензия Федеральной службы по техническому и экспортному контролю № 2003 от 14.04.2008 г. на осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.

### Аттестаты аккредитации ФСБ России:

- »» Аттестат аккредитации ФСБ России в качестве испытательной лаборатории № СЗИ.RU.ЛИ0098 от 15.10.2015 г.
- »» Аттестат аккредитации испытательной лаборатории при ФСБ России № АФ-187 от 15.10.2015 г.

#### Аттестаты аккредитации ФСТЭК России:

- »» Аттестат аккредитации органа по аттестации при ФСТЭК России № **СЗИ RU.094.B011.022** от 26.11.2003 г.
- »» Аттестат аккредитации испытательной лаборатории при ФСТЭК России № **СЗИ RU.094.Б025.058** от 26.11.2003 г.

#### Лицензии Минобороны России:

- »» Лицензия Минобороны России № **1078** от 02.07.2014 г. на деятельность в области создания средств защиты информации.

#### Свидетельства СРО:

- »» Свидетельство Саморегулируемой организации, основанной на членстве лиц, осуществляющих строительство Ассоциации «Саморегулируемая организация «Объединений подрядных организаций» о допуске к определенному виду или видам работ, которые оказывают влияние на безопасность объектов капитального строительства № **0124.08-2016-7729098893-С-185** от 21.04.2016 г.
- »» Свидетельство Саморегулируемой организации, основанной на членстве лиц, осуществляющих подготовку проектной документации некоммерческое партнерство «Межрегиональное объединение организаций в области проектирования «Ярд» о допуске к определенному виду или видам работ, которые оказывают влияние на безопасность объектов капитального строительства № **П-116-1027739738817-2010-061.6** от 23.04.2016 г.

#### Лицензии Роспотребнадзор:

- »» Лицензия Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека № **77.99.15.002.Л.000238.01.07** от 29.01.2007 г. на осуществление деятельности в области использования источников ионизирующего излучения.

#### Лицензии и свидетельства Ростехнадзор:

- »» Свидетельство Федеральной службы по экологическому, технологическому и атомному надзору № **6139** от 30.10.2015 г. о регистрации электролаборатории.
- »» Лицензия Федеральной службы по экологическому, технологическому и атомному надзору № **ЦО-03-101-6209** от 05.08.2011 г. на эксплуатацию блоков атомных станций (АС), в части выполнения работ и оказания услуг эксплуатирующей организации при ремонте, реконструкции и модернизации АС.
- »» Лицензия Федеральной службы по экологическому, технологическому и атомному надзору № **ЦО-02-101-6210** от 05.08.2011 г. на сооружение блоков атомных станций (АС), в части выполнения работ и оказания услуг эксплуатирующей организации при строительстве АС.

#### Сертификаты соответствия:

- »» Сертификат соответствия Системы добровольной сертификации Газпромсерт № **ГО00.RU.1233.P00268** на следующие услуги (работы): монтаж, пусконаладочные работы, ремонт и техническое обслуживание инженерно-технических средств охраны.
- »» Сертификат соответствия Системы сертификации Euro-Standard № **РОСС RU.OC/07.СМК.14-0297** от 07.08.2014 г., удостоверяющий, что система менеджмента качества соответствует требованиям ISO 9001:2008 (ГОСТ ISO 9001-2011).
- »» Сертификат соответствия Органа по сертификации систем менеджмента качества Закрытого акционерного общества «Каскад-Телеком» № **ВР 34.1.8331-2014**, удостоверяющий, что система менеджмента качества соответствует требованиям ГОСТ ISO 9001-2011 и ГОСТ РВ 0015-002-2012



**КОНТАКТЫ**

 **ГРУППА КОМПАНИЙ МАСКОМ**

 <p><b>ЦБИ МАСКОМ</b> 119421, г. Москва, ул. Новаторов, д. 40, к.1 +7 (495) 740-43-40 www.mascom.ru</p>	 <p><b>НОУ ДПО УЦБИ МАСКОМ</b> 119421, г. Москва, ул. Новаторов, д. 40, к.1 +7 (495) 740-43-40, доб. 13-10 www.mascom-uz.ru</p>
 <p><b>МСОФТ</b> 117630, г. Москва, ул. Академика Челомея, д. 3, к. 2 +7 (495) 660-06-08 www.mascomsoft.ru</p>	 <p><b>МК-СПЕЦМОНТАЖ</b> 117630, г. Москва, ул. Академика Челомея, д. 3, к.2 +7(495) 660-06-08</p>
<p><b>Холдинг МАСКОМ Восток</b></p>	
 <p><b>ООО «МАСКОМ Восток»</b> 680038, г. Хабаровск, ул. Яшина, д.40 +7 (4212) 45-46-32; +7 (4212) 76-48-78 (факс) info@mascom-vostok.ru, www.mascom-vostok.ru</p>	 <p><b>ООО «ДСЦБИ «МАСКОМ»</b> 680038, г. Хабаровск, ул. Яшина, д.40 +7 (4212) 45-46-33; +7 (4212) 76-48-78 (факс) www.mascom-dv.ru info@mascomdv.ru</p>
 <p><b>ООО «МАСКОМ-ТЕХЛАЙН»</b> 680038, г. Хабаровск, ул. Яшина, д.40 +7 (4212) 45-46-32; +7 (4212) 76-48-78 (факс) www.mascom-it.ru, info@mascom-it.ru</p>	 <p><b>ООО «МАСКОМ-ИНСТРОЙ»</b> 680038, г. Хабаровск, ул. Яшина, д.40 +7 (4212) 45-46-31; +7 (4212) 76-48-78 (факс) www.mascom-instroy.ru, info@mascom-instroy.ru</p>
 <p><b>ООО «СТАНДАРТ ТЕЛЕКОМ»</b> 680038, г. Хабаровск, ул. Яшина, д.40 +7 (4212) 46-08-10; +7(4212) 76-48-78(факс) www.stnt.ru, info@stnt.ru</p>	 <p><b>ООО «МАСКОМ-ПРИМОРЬЕ»</b> 690001, г. Владивосток, ул., Светланская, д. 165, +7 (423) 230-23-30; +7 (423) 224-04-40(факс) www.mascomvl.ru, info@mascomvl.ru</p>
 <p><b>ООО «МАСКОМ-АМУР»</b> 675000, г. Благовещенск, ул. Калинина, д.126 +7 (4162) 22-28-43; +7 (4162) 222-839 (факс: доб. 103) www.mascom-amur.ru amur@mascom-amur.ru</p>	 <p><b>ООО «МАСКОМ-Сибирь»</b> 690001, г. Новосибирск, Фрунзе ул., д. 5, оф.325, (383) 218-87-18; +7(383) 221-12-41(факс) info@mascom-sib.ru</p>

