ГРУППА КОМПАНИЙ

МАСКОМ

Комплексный подход к безопасности

ГРУППА КОМПАНИЙ

- 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

- Высококвалифицированные специалисты
- Инновационные подходы
- Территориальное распределение потенциала

СОСТАВЛЯЮЩИЕ

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

ГК МАСКОМ – это предприятия, работающие в Центральном, Сибирском, Дальневосточном, Краснодарском 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.

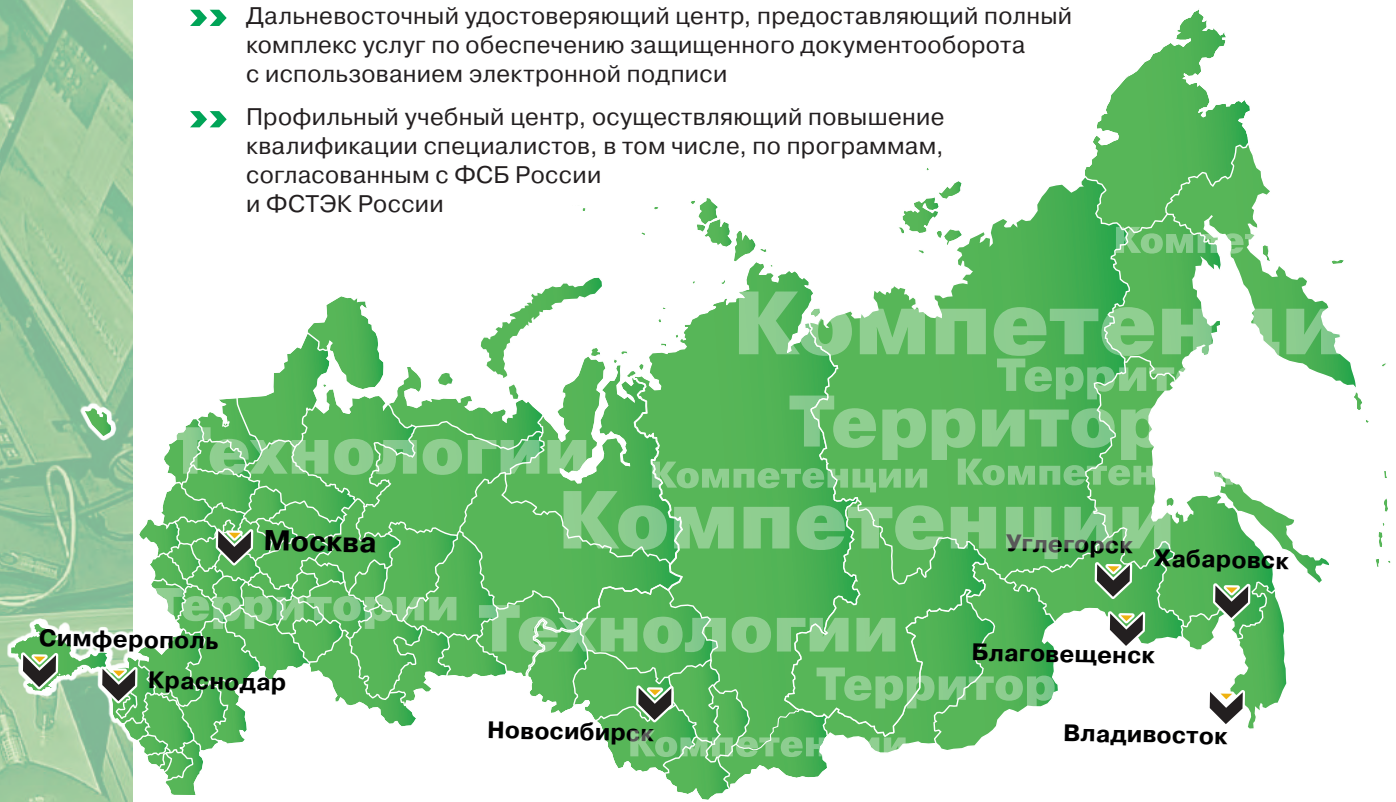
РЕСУРСЫ:

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.»

Арчаков Александр Витальевич › **Директор департамента оборудования**

«... 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 › **Директор департамента по работе с ключевыми заказчиками**

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.»

Черников Дмитрий Вячеславович › **Директор департамента реализации проектов**

«... Департамент реализации проектов решает сложные задачи в сфере стратегического развития ИТ-ресурсов организации и повышения эффективности процессов, а также оказывает услуги в области создания систем управления, проектирования и построения ИТ-инфраструктуры, управления данными и аналитики, системной интеграции и уникальных заказных решений, информационной безопасности и аутсорсинга.

Фактор нашего успеха – постоянное совершенство. Опыт, накопленный временем, и знания, специализированные в области информационной безопасности, позволяют формировать предложения под требования каждого Заказчика. Высокий профессионализм, нацеленность на результат, ответственность и опыт – вот за что нас ценят клиенты.

Мы – надёжный и ответственный партнёр, выстраивающий свою работу на основе доверия и взаимного уважения. Мы умеем слушать наших клиентов и предлагаем им оптимальные решения информационной безопасности. Мы не только работаем с проверенными решениями, но и открываем для российского рынка новые продукты, обеспечивая их непрерывное сопровождение на всей стадии жизненного цикла.»

Поярков Андрей Юрьевич › **Генеральный директор МАСКОМ Восток**

«... Холдинг МАСКОМ Восток сосредоточил под единым управлением основные производственные мощности как системообразующего предприятия холдинга – ООО «ДСЦБИ «МАСКОМ» (г. Хабаровск), так и дочерних обществ – ООО «МАСКОМ-Приморье» (г. Владивосток), ООО «Стандарт Телеком» (научно-технический центр, г. Хабаровск), ООО «МАСКОМ АМУР» (г. Благовещенск) и трех строительных организаций, которые оптимизированы под самостоятельное выполнение на территории Дальнего Востока и Сибири всего комплекса работ по ключевым направлениям деятельности холдинга. Мы не работаем ради краткосрочного результата. Наша цель – долгосрочное развитие и обеспечение стратегического успеха деятельности сотрудников холдинга, партнеров, Заказчиков. »

Лобанов Максим Иосифович › **Директор УЦ МАСКОМ**

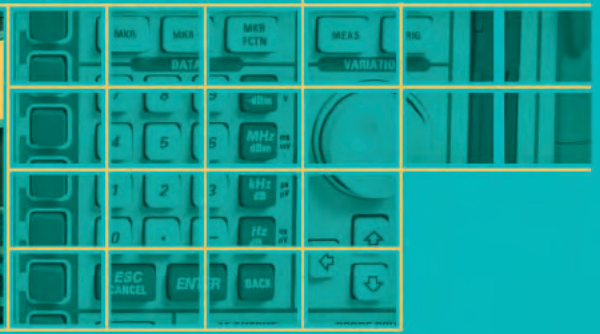
«... Учебный центр продолжает наращивать свой учебный потенциал, сохраняя, безусловно, главное, присущее ему, сочетание: традиционно высокий уровень обучения и его практическую ориентированность. Уже намечены и будут еще появляться новые направления обучения как внутри сектора информационной безопасности, 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 позволяюткак 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

МАСКОМ
ГРУППА КОМПАНИЙ



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.

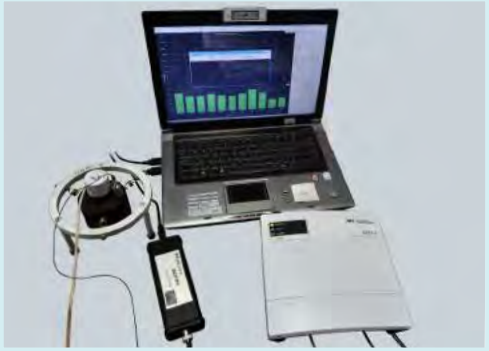
СЕРТИФИКАЦИЯ

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:

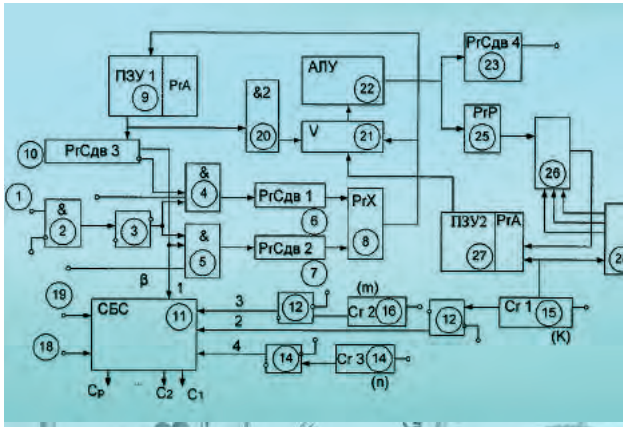
- Проекты нормативно-распорядительной документации предприятия (политики безопасности, различных руководств и инструкций, стандартов предприятия) в области информационной безопасности
- Проекты требуемой регуляторами документации
- Проекты документации Заявителя для проведения аттестации объектов информатизации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

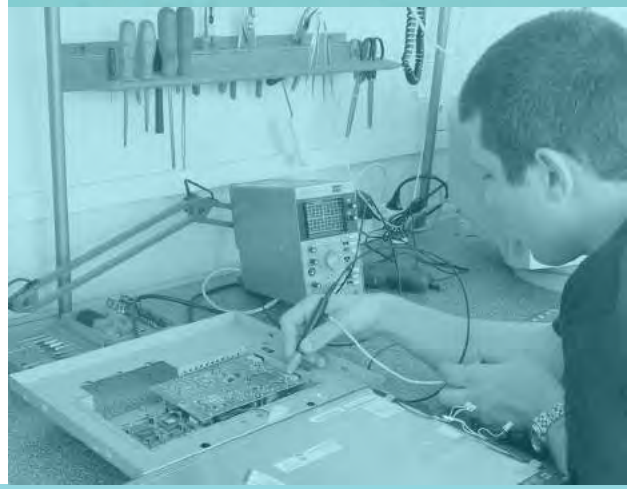
Перечень работ:

- 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 IT-инфраструктуры – дает возможность получить полную и объективную оценку защищенности Ваших объектов

Перечень работ

- Оценка реального состояния объектов IT-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 IT-инфраструктуры (при необходимости)
- Тест на проникновение (по желанию Заказчика)

В результате проведения аудита Вы получаете:

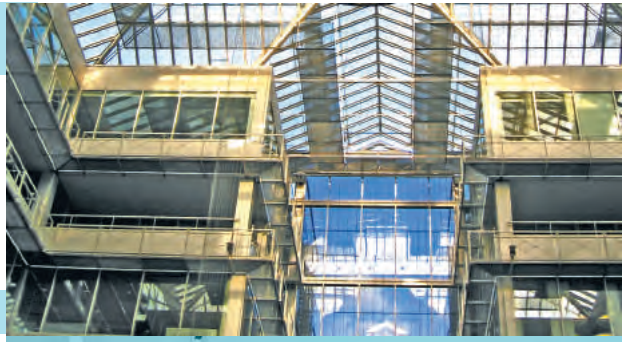
- Объективное представление об уровне защищенности Ваших объектов IT-инфраструктуры
- «Руководство к действию» по развитию имеющейся системы защиты
- Повышение капитализации бизнеса

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




ГРУППА КОМПАНИЙ
МАСКОМ
Комплексный
подход
к безопасности
КОСМОДРОМ
ВОСТОЧНЫЙ
ПОДНИМИ
ГОЛОВУ!!

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


9805

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, Линтер Бастион .
- Среды разработки: Microsoft Visual Studio 2019, 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.
САСД «Канцелярия 31»	Система электронного документооборота, предназначенная для организации электронного учёта документов и др. В режимно-секретных отделах предприятий. САСД «Канцелярия 31» позволяет автоматизиро-вать все процессы, связанные с учётом, инвентаризацией и т.д. документов, содержащих сведения, составляющих государственную тайну, предусмотренные действующим законодательством.
СПО «СЭДО СП ТС»	Система электронного документооборота для автоматизации процесса проведения специальных проверок технических средств в соответствии с ОСТ ФСБ России.
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	
ППО «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. **www.casecontrol.ru**
СПО «Реестр внутреннего документооборота»	Комплексная система работы с внутренними документами компании, обеспечивающая возможность полного перехода на электронный документооборот.
СПО CRM «Клиент»	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.
Облачная система «LiteFlow»	Система для автоматизации процесса подачи заявок, управления задачами и согласования документов. Автоматизация происходит при помощи гибкой настройки бизнес процессов Вашей компании. **www.liteflow.ru**
Youtell - агрегатор мессенджеров	Youtell - Поддерживает популярные мессенджеры и социальные сети, такие как Telegram, Facebook, ВКонтакте, Viber, Skype и т.д. Клиент сам сможет выбрать удобный для него канал общения, а вы получите агрегатор всех каналов связи с единым интерфейсом. **www.youtell.online.ru**

ИНТЕГРАЦИОННАЯ ПЛАТФОРМА ДЛЯ СИСТЕМ БЕЗОПАСНОСТИ АССОИ

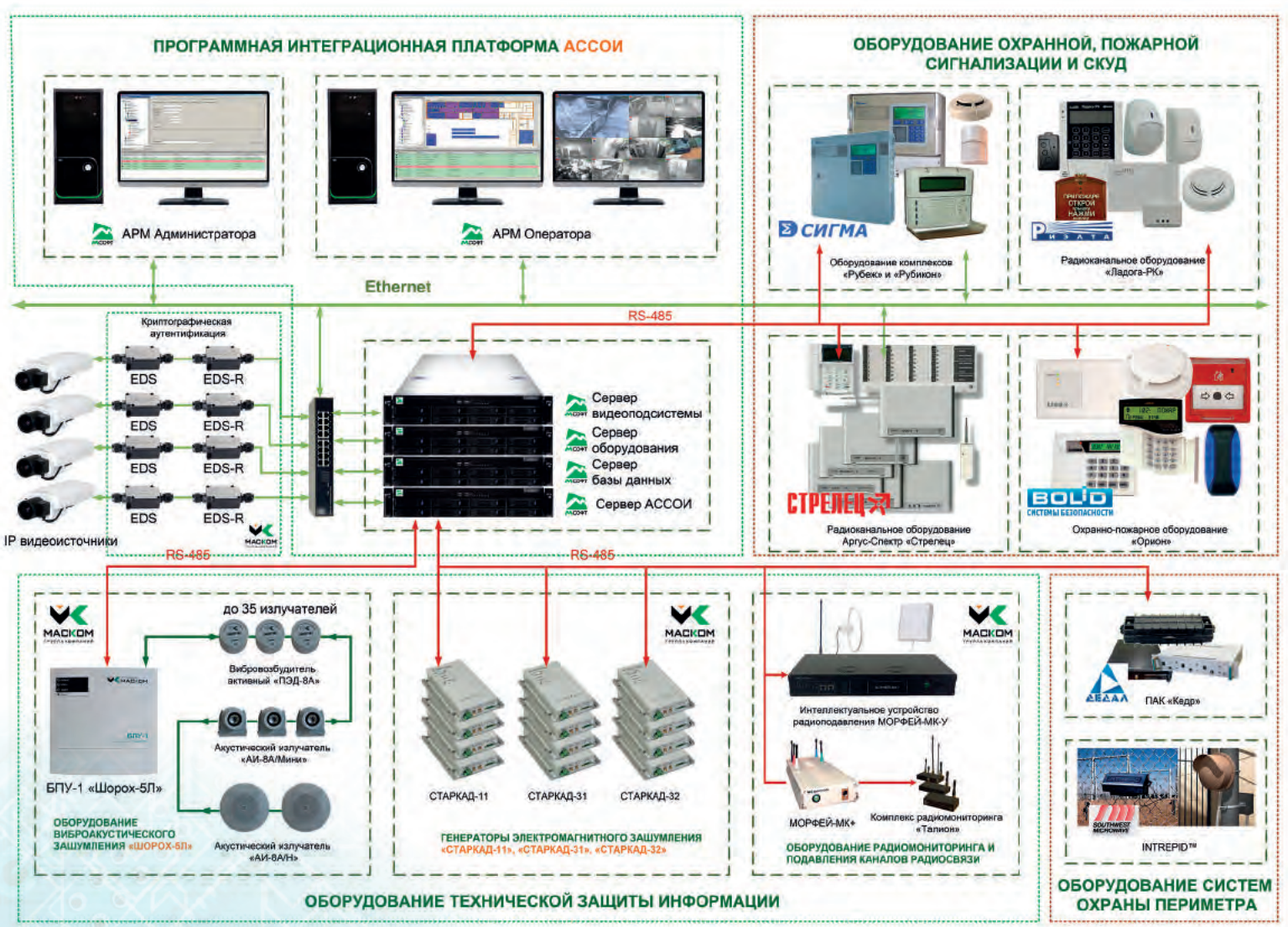
АССОИ - автоматизированная система сбора и обработки информации, предназначенная для организации в единый информационный и управленческо-логический комплекс систем технической защиты информации (ТЗИ), инженерно-технических средств охраны (ИТСО), систем контроля управления доступом (СКУД), систем видеонаблюдения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


ПРОГРАММНАЯ ИНТЕГРАЦИОННАЯ ПЛАТФОРМА АССОИ
АРМ Администратора
АРМ Оператора
Ethernet
RS-485
Криптографическая аутентификация
EDS
EDS-R
IP видеоисточники
Сервер видеоподсистемы
Сервер оборудования
Сервер базы данных
Сервер АССОИ
ОБОРУДОВАНИЕ ОХРАННОЙ, ПОЖАРНОЙ СИГНАЛИЗАЦИИ И СКУД
СИГМА
Оборудование комплексов «Рубеж» и «Рубикон»
Радиоканальное оборудование «Ладога-РК»
СТРЕЛЕЦ
Радиоканальное оборудование Аргус-Спектр «Стрелец»
BOLID
Охранно-пожарное оборудование «Орион»
до 35 излучателей
Виброизлучатель активный «ПЭД-8А»
Акустический излучатель «АИ-8А/Мини»
Акустический излучатель «АИ-8А/Н»
БПУ-1 «Шорох-5П»
ОБОРУДОВАНИЕ ВИБРОАКУСТИЧЕСКОГО ЗАШУМЛЕНИЯ «ШОРОХ-5П»
СТАРКАД-11
СТАРКАД-31
СТАРКАД-32
ГЕНЕРАТОРЫ ЭЛЕКТРОМАГНИТНОГО ЗАШУМЛЕНИЯ «СТАРКАД-11», «СТАРКАД-31», «СТАРКАД-32»
Интеллектуальное устройство радиоподавления МОРФЕЙ-МК-У
МОРФЕЙ-МК+
Комплекс радиомониторинга «Талион»
ОБОРУДОВАНИЕ РАДИОМОНИТОРИНГА И ПОДАВЛЕНИЯ КАНАЛОВ РАДИОСВЯЗИ
ОБОРУДОВАНИЕ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ
ПАК «Кедр»
INTREPID™
ОБОРУДОВАНИЕ СИСТЕМ ОХРАНЫ ПЕРИМЕТРА

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:

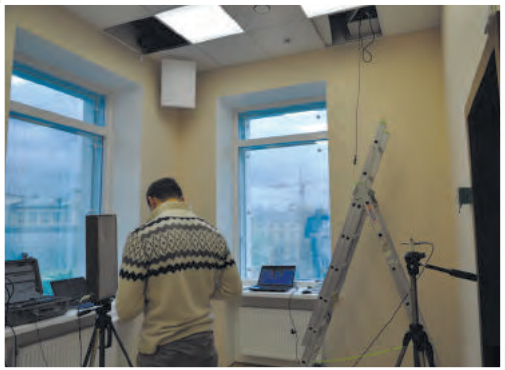
- Организация выполнения комплекса мероприятий по защите информации по завершению строительных работ и сдачи объекта в эксплуатацию
- Выполнение данных работ в рамках капитального строительства

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

ОРГАНИЗАЦИЯ ЗАЩИТЫ ПОМЕЩЕНИЙ В РАМКАХ КАПИТАЛЬНОГО СТРОИТЕЛЬСТВА

Ключевые особенности:

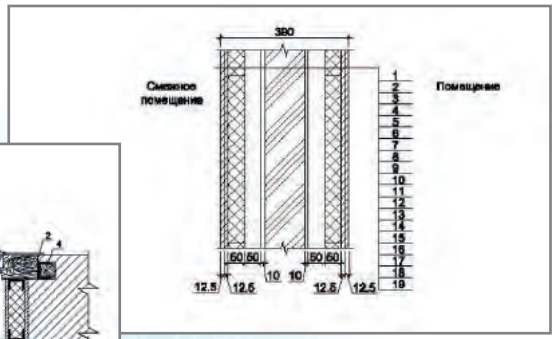
- Решение, где предусмотрены преимущественно пассивные меры защиты, в соответствии с требованиями СанПиН и ГКРЧ.
  - **Результат** – экологичное эффективное решение (без паразитных шумов и навесного монтажа)
- Проведение специальных проверок и специальных исследований оборудования, устанавливаемого в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

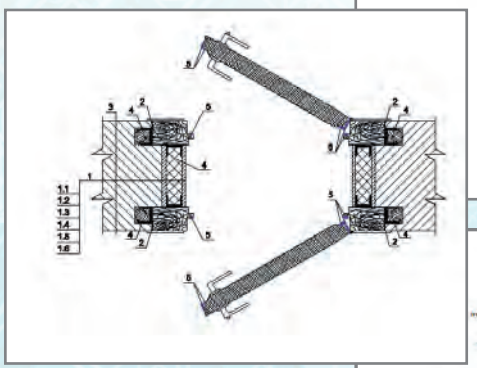


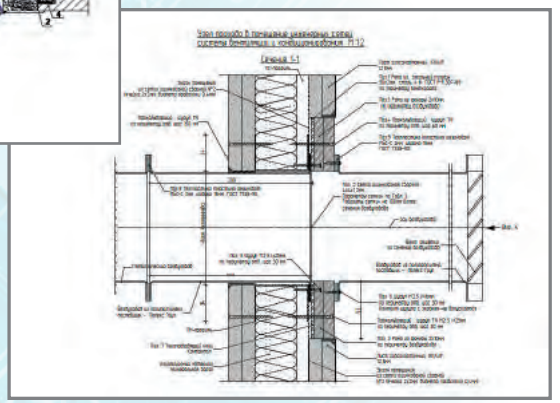
- Возможность выявить все каналы утечки информации, спланировать установку активного оборудования, строительные мероприятия по звукоизоляции, виброизоляции на этапе строительства.
  - **Результат** – экономия средств при сохранении качества защиты
- Учёт индивидуальных особенностей объекта и пожеланий 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 годы работы компанией реализовано более 300 проектов в интересах таких крупных Заказчиков, как МО России, ФСБ России, МВД России, ФНС России, Минпромторг, АТЦ СНГ, Росатом, ФСК ЕЭС, РусГидро, Газпром и др.







Безэховые камеры

Безэховые камеры (БЭК) применяются в различных отраслях промышленности для выполнения научно-исследовательских работ, а также проведения контроля на соответствие требованиям различных отраслевых стандартов.

ГК МАСКОМ выполняет полный цикл работ по созданию БЭК в соответствии с военными и гражданскими ГОСТами по ЭМС: от формирования технического задания и разработки рабочей конструкторской документации до ввода объекта в эксплуатацию с его последующей аттестацией, гарантийным техническим и сервисным обслуживанием.

Возможно комплексное оснащение лабораторий современными средствами измерений (в том числе собственной разработки), программно-аппаратными средствами автоматизации процесса измерений.

В соответствии с ГОСТ Р 50414-92 камеры обеспечивают эффективность экранирования, соответствующую 1 классу, в диапазоне частот от 0,01 МГц до 18 ГГц:

- магнитного поля: от 60 до 100 дБ в диапазоне частот от 10 кГц до 1 МГц;
- магнитного поля: не менее 100 дБ в диапазоне частот от 1 до 30 МГц;
- электрического поля: не менее 100 дБ в диапазоне частот от 30 до 500 МГц;
- плоской волны: не менее 100 дБ в диапазоне частот от 100 МГц до 18 ГГц.

ВАРИАНТЫ ИСПОЛНЕНИЯ

- Модульного цельносварного типа
- Сборно-разборного типа

ОСОБЕННОСТИ

- Инженерная подготовка помещения
- Обеспечение температурно-влажностного режима для любых условий
- «Чистые» БЭК

Габаритные размеры экранированной камеры зависят от требований заказчика либо от ее предназначения.

Экранированные камеры по требованиям ПД ИТР

ТИПЫ ЭКРАНИРОВАННЫХ КАМЕР, СОЗДАВАЕМЫХ В ГК МАСКОМ

- Защитные и испытательные экранированные камеры в области технической защиты информации и противодействия иностранным техническим разведкам.
- Комбинированные камеры с электромагнитной защитой (до 2-го класса экранирования включительно) и вибро/звукоизоляцией (60 дБ в речевом диапазоне частот).

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ ЭК

- В соответствии с ГОСТ Р 50414-92 камеры обеспечивают эффективность экранирования, соответствующую экранированной камере 1 класса, в диапазоне частот от 0,01 МГц до 18 ГГц:
- Магнитного поля: от 60 до 100 дБ в диапазоне частот от 10 кГц до 1 МГц;
- Магнитного поля: не менее 100 дБ в диапазоне частот от 1 до 30 МГц;
- Электрического поля: не менее 100 дБ в диапазоне частот от 30 до 500 МГц;
- Плоской волны: не менее 100 дБ в диапазоне частот от 100 МГц до 18 ГГц.
- Габаритные размеры экранированной камеры зависят от требований заказчика либо от ее предназначения.

Экранированные ворота и двери

ГК МАСКОМ разрабатывает и поставляет экранированные двери и ворота собственного производства **любых размеров и классов в соответствии с требованиями заказчика.**

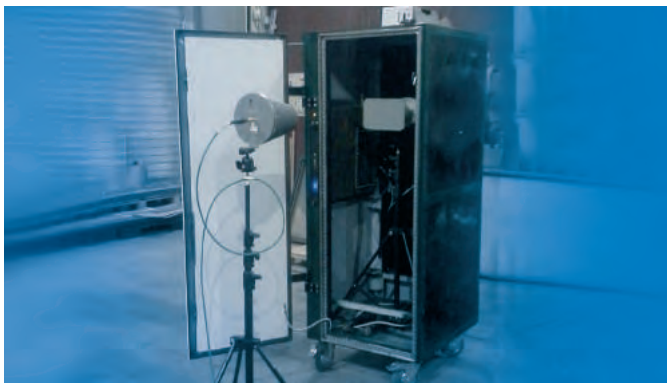
ТИПЫ ДВЕРЕЙ

- навесные двери (одностворчатые/двустворчатые)
- раздвижные двери/ворота

ХАРАКТЕРИСТИКИ

Эффективность экранирования в соответствии с ГОСТ до 100 дБ в диапазоне частот 0,01 МГц до 18 ГГц

Экранированные шкафы по требованиям ПД ИТР



ЭШ рассчитаны на диапазон 0,05-8 ГГц

Коэффициент экранирования составляет не менее 40 дБ во всем диапазоне

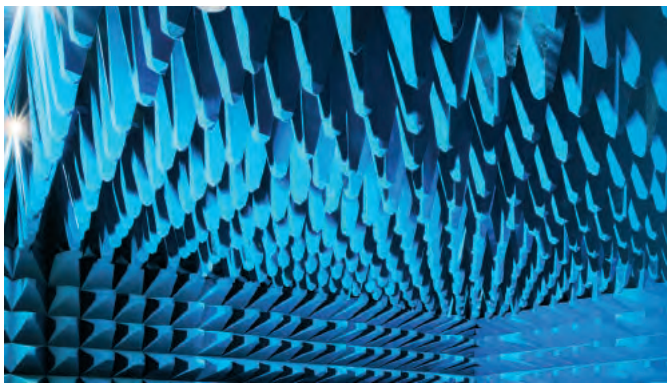
Стандартные габаритные размеры ЭШ
750х950х1977 мм (ШхГхВ)

Мы осуществляем производство экранированных шкафов любых размеров, в соответствии с требованиями заказчика.

Масса ЭШ при стандартных габаритных размерах 250 кг

Электропитание ЭШ 220 В, 50 Гц

Радиопоглащающие материалы



РПМ СЕРИИ «ЭРИДАН»

Внешние размеры
525х175х530 (Д х Ш х В)

Диапазон частот 40 МГц – 40 ГГц

Крепление сборная конструкция, блоками с размером 525х525 мм (Д х Ш)

УСЛОВИЯ ЭКСПЛУАТАЦИИ

Температура окружающей среды
от +5 до +60°С

Относительная влажность
не более 80%

Горючесть самозатухающий материал

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

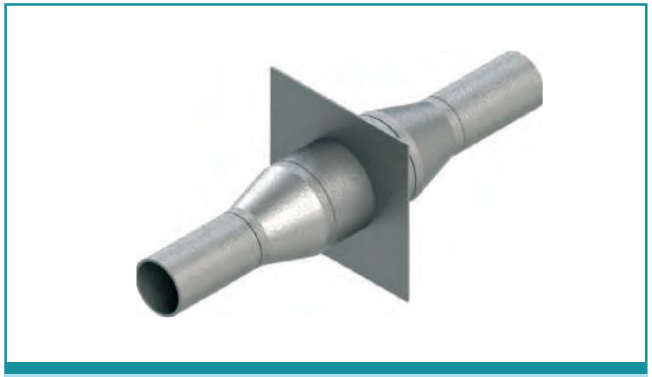
100 МГц	-15 дБ
150 МГц	-20 дБ
300 МГц	-30 дБ
600 МГц	-35 дБ
1,5 ГГц	-40 дБ
3 ГГц – 40 ГГц	-50 дБ

ФИЛЬТРЫ ОПТИЧЕСКИЕ СЕРИИ «КВАРТЕТ-С»

Диапазон частот
10 кГц- 40 ГГц

Затухание по магнитной составляющей
не менее 80 дБ

Затухание по электрической составляющей
не менее 80 дБ



ФИЛЬТРЫ ТРУБОПРОВОДНЫЕ СЕРИИ «КВАРТЕТ-Н»

Диапазон частот
10 кГц- 40 ГГц

Затухание по магнитной составляющей
не менее 80 дБ

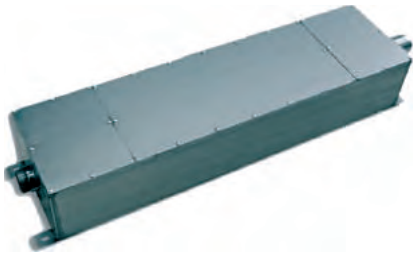
Затухание по электрической составляющей
не менее 80 дБ

ФИЛЬТРЫ ВОЗДУШНЫЕ СЕРИИ «КВАРТЕТ-О»

Диапазон частот:
10 кГц- 40 ГГц

Затухание по магнитной составляющей
не менее 80 дБ

Затухание по электрической составляющей
не менее 80 дБ



ФИЛЬТРЫ ПОМЕХОПОДАВЛЯЮЩИЕ СЕРИИ «КВАРТЕТ-Е»

Диапазон частот
150 кГц- 40 ГГц

Затухание по магнитной составляющей
не менее 60 дБ

Затухание по электрической составляющей
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:

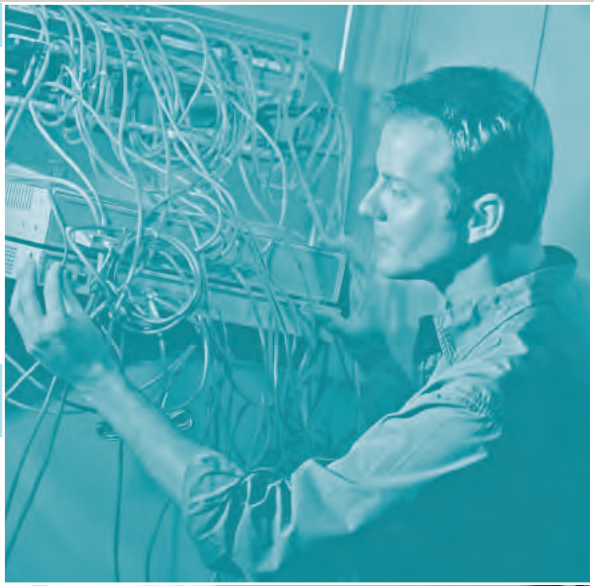
- Проектирование систем и объектов связи
- Проектирование центров обработки и хранения данных
- Проектирование локально-вычислительных сетей, структурированных кабельных сетей телефонной связи, видеоконференцсвязи
- Строительно-монтажные и пусконаладочные работы любой сложности
- Техническое обслуживание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

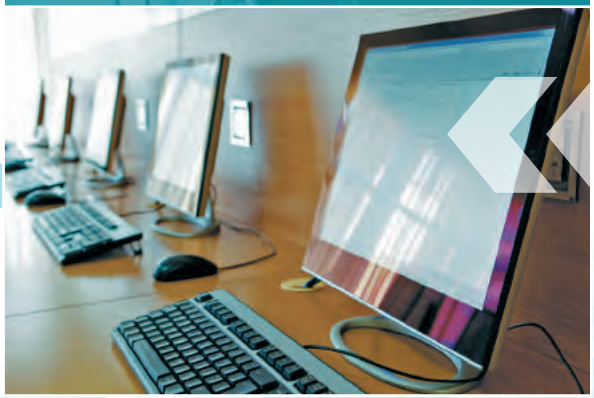
Преимущества нашего подхода, к созданию сетей связи и передачи данных:

- 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

ЗАЩИЩЁННЫЕ СТРУКТУРИРОВАННЫЕ КАБЕЛЬНЫЕ СЕТИ

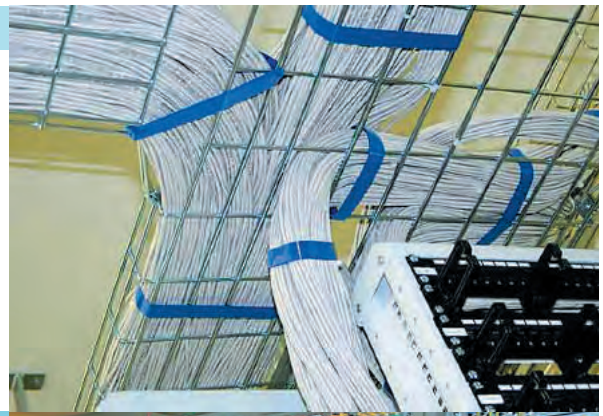
ГК МАСКОМ предоставляет весь комплекс услуг по проектированию и монтажу защищённых структурированных кабельных систем (СКС).

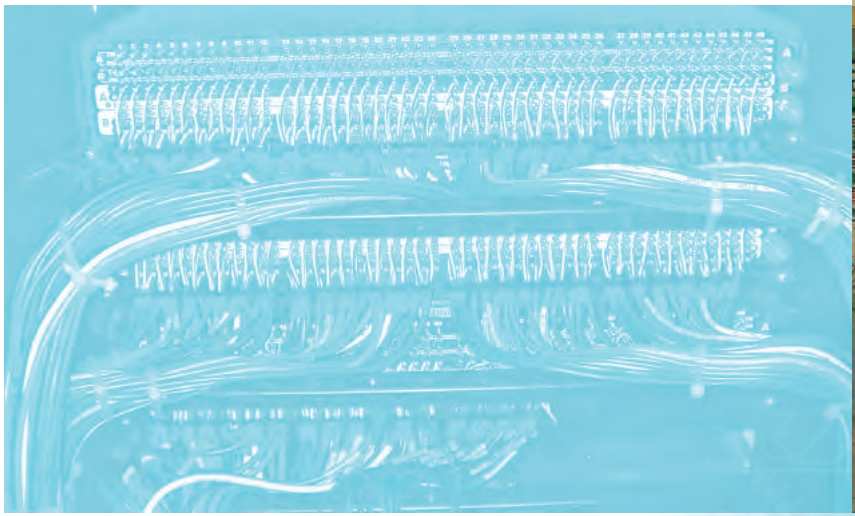
Принципы, которые мы неукоснительно соблюдаем:

- 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 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

Архитектура ЦОД

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

ВКС в защищенном исполнении уже внедрены нами в ряде крупных корпораций, в силовых структурах, в государственных учреждениях.

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 потенциала предприятия. Современный уровень научной деятельности обеспечен следующими факторами:

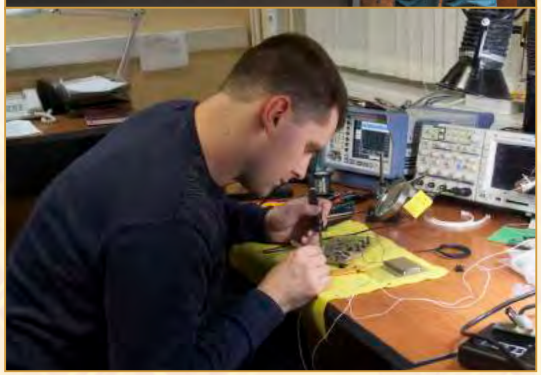
- Высоким профессиональным уровнем исполнителей, отдавших много лет своей трудовой биографии научно-исследовательской работе
- Накопленным опытом применения действующих методик и решений
- Высоким уровнем технического обеспечения (наличие экранированной камеры большого объёма и площади, отдельного помещения 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

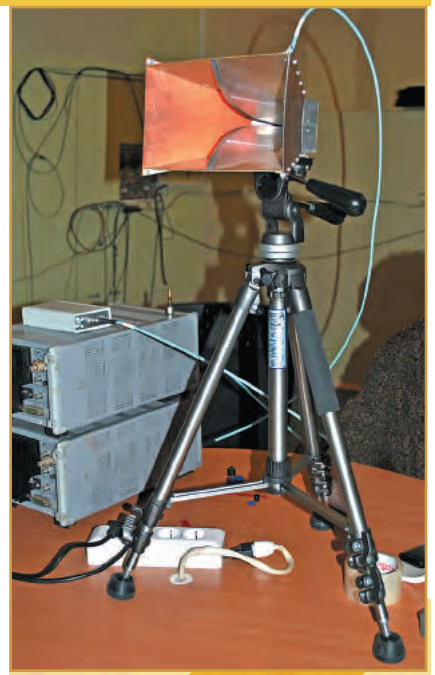
Результаты наших научных работ:

- 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.

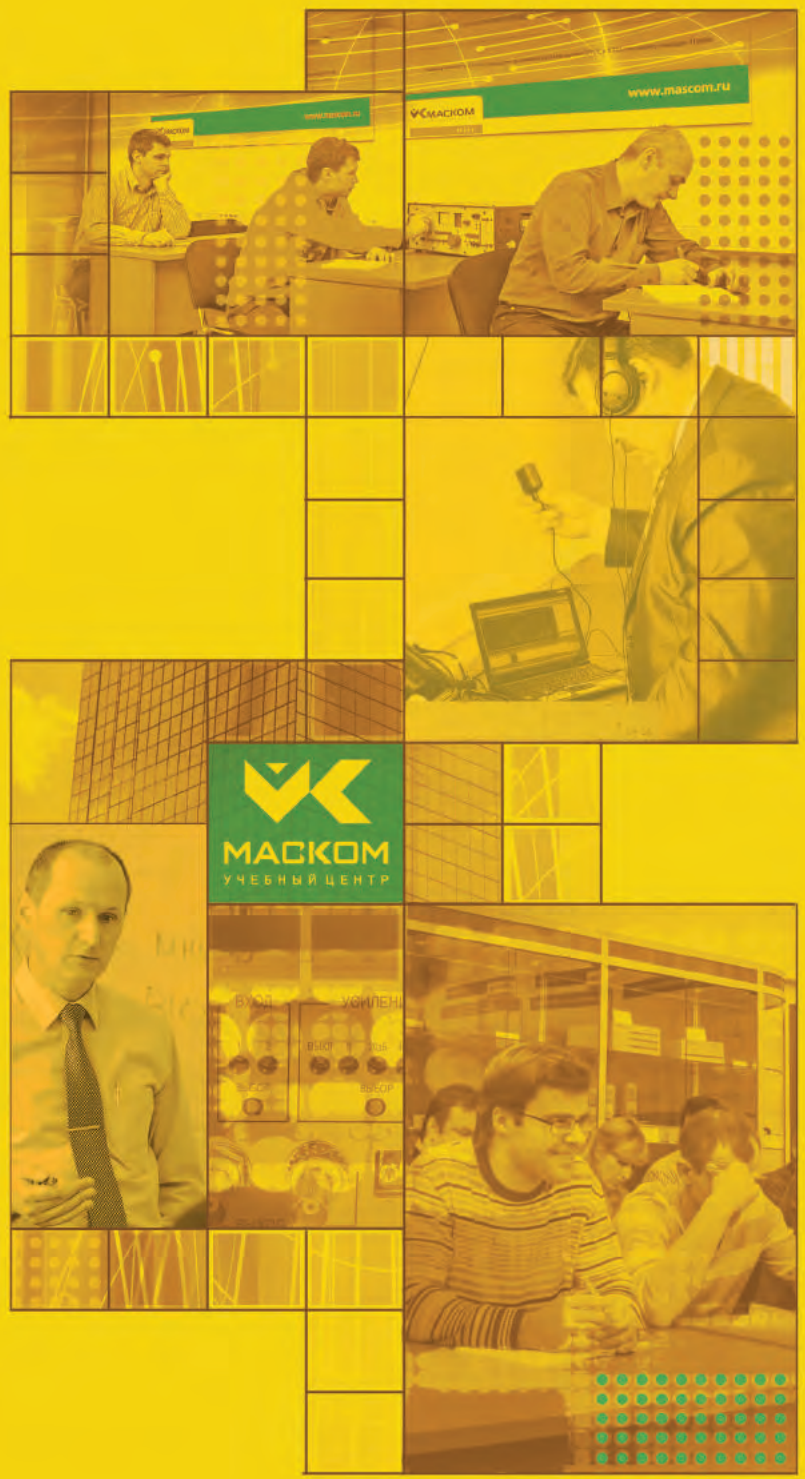


Ряд разработанных решений стал, де факто, стандартом в своей области. Так, система оценки защищенности выделенных помещений по виброакустическому каналу «Шепот» и система оценки защищенности технических средств от утечки информации по каналу ПЭМИН «Сигурд» используются службами контроля ФСТЭК России.

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

MACKOM
УЧЕБНЫЙ ЦЕНТР

Учебный центр MACKOM 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 MACKOM получил статус некоммерческого образовательного учреждения. С 2005 года УЦ начинает проводить выездные курсы в регионах России.
УЦ MACKOM 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 MACKOM 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 конфеденциальной 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 4 курса 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 21 курс продолжительностью от 8 до 144 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 в разделе «Курсы»

Профессиональная переподготовка

В процессе обучения по программе курса «Информационная безопасность» Вы получите знания в области требований нормативно-методических и руководящих документов, регламентирующих отношения в сфере деятельности по защите конфиденциальной информации. Также приобретете практические навыки защиты информации на современных предприятиях как с использованием шифровальных (криптографических) средств, так и с использованием иных технических и программных средств защиты конфиденциальной информации.
Программа «Техническая защита информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну» направлена на изучение общих требований, предъявляемых к технической защите конфиденциальной информации, а также способы и средства ТЗКИ. Отдельный раздел курса посвящен изучению нормативно-правовой базы, действующей в области информационной безопасности. В рамках курса профессиональной подготовки предусмотрен обширный практикум.

В рамках этого направления Учебный центр МАСКОМ предлагает 2 курса продолжительностью 512 часов.

Школа управленческих технологий

Карьера. Отрасли. Мир. Все меняется. Школа управленческих технологий дает возможность идти не только в ногу с этими изменениями, но и управлять ими. Деловое образование может стать ценным вкладом в ваше собственное будущее, а грамотно выстроенные управленческие курсы придадут вам особую ценность.

В рамках этого направления Учебный центр МАСКОМ предлагает 32 курса продолжительностью от 8 до 24 часов.

ТЕХНИЧЕСКОЕ ОСНАЩЕНИЕ УЦ МАСКОМ

Занятия проводятся в комфортабельных классах, оборудованных всем необходимым для учебного процесса. Их оснащенность 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

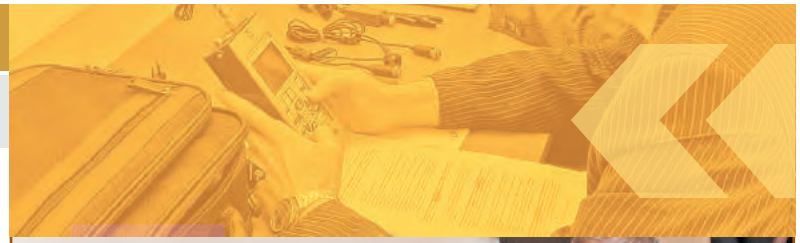
Предназначен для отработки действий по выявлению закладочных устройств

Аппаратура:

- Комплекс радиоприемной аппаратуры «Кассандра-К21»
- 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 «СИГУРД» 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. таину, 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-ух вариантах: очно-заочный формат курсаосуществляется 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 окончанию курса проходитвебинар.

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, строительно-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

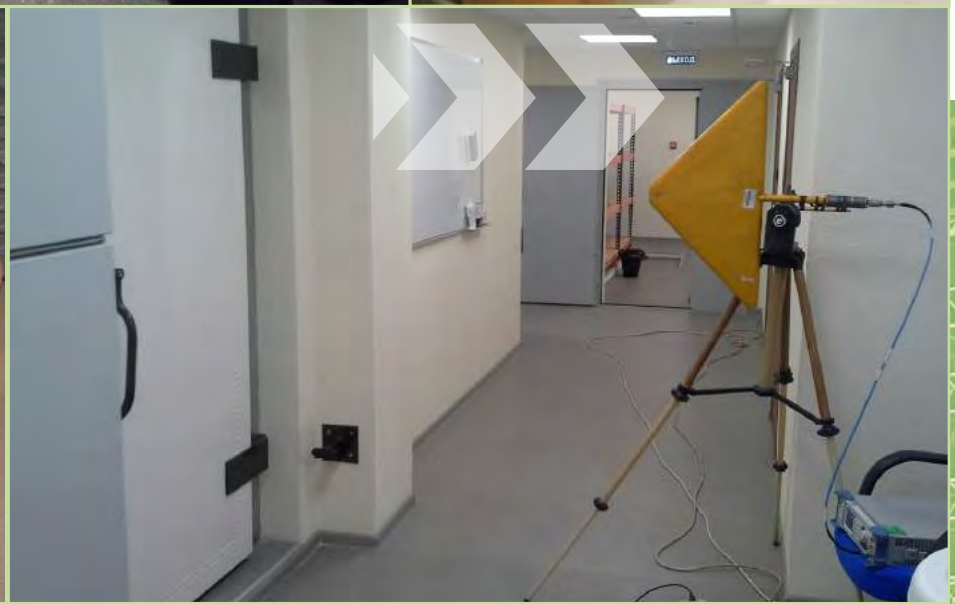
СПЕЦИАЛЬНЫЕ ИЗМЕРИТЕЛЬНЫЕ ЛАБОРАТОРИИ

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.

Учебный лабораторный комплекс

- **Специализированная лаборатория «Защита информации от утечки за счет НСД»**
- **Специализированная лаборатория «Защита информации от утечки за счет ПЭМИН»**
- **Специализированная лаборатория «Защита информации от утечки за счет АВАК»**
- **Специализированная лаборатория «Поиск и выявление демаскирующих признаков ЭУНПИ»**

Специализированная лаборатория

- Учебный лабораторный стенд
- Средства защиты информации
- Средства контроля защищенности информации
- Учебно-методические материалы
- Выставка демонстрационного оборудования

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 недекларированных возможностей (НДВ) программного обеспечения. Существующие методы выявлениями 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 выявление 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


SDV-6-2+
ТЕХНИЧЕСКИЙ ЭКСПЛУАТАЦИЯ

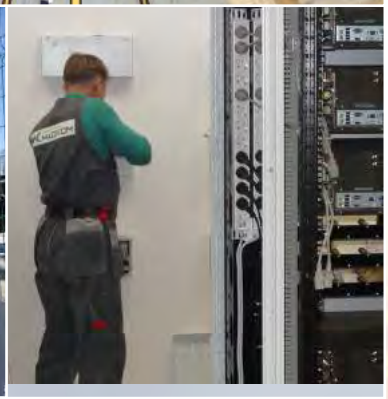
ОБЪЕКТЫ

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, бщекосмодромного и локальных центров управления и мониторинга безопасности

Выполненные работы:

- Разработка концептуальных материалов по анализу уязвимомти 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.

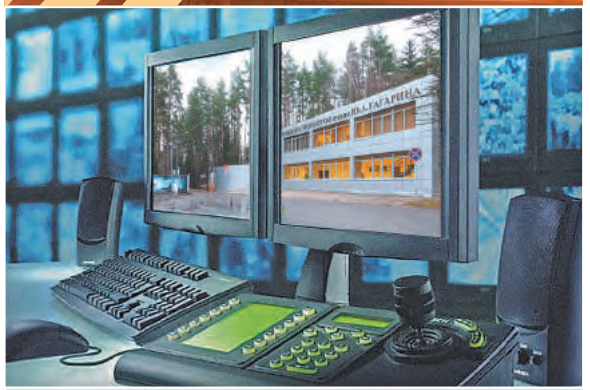
Проект реализуется для ФКА России

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.

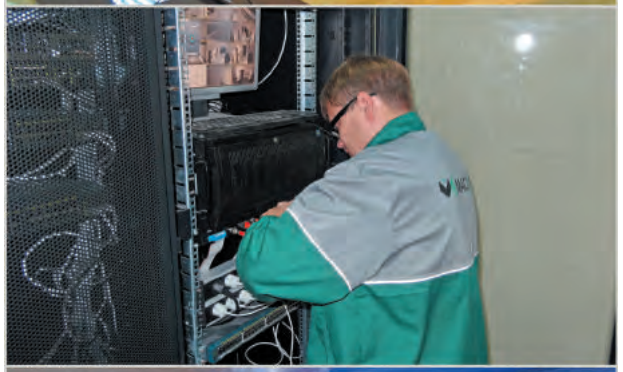
Проект реализован для ФКА России

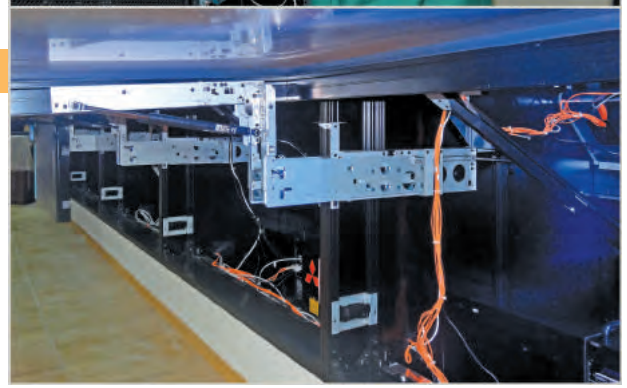
ПРОЕКТИРОВАНИЕ И СТРОИТЕЛЬСТВО СПЕЦИАЛИЗИРОВАННОГО ЗДАНИЯ ЦЕНТРА АСУ С ЦЕНТРОМ БОЕВОГО УПРАВЛЕНИЯ И ПОЛНЫМ ТЕХНИЧЕСКИМ ОСНАЩЕНИЕМ

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.

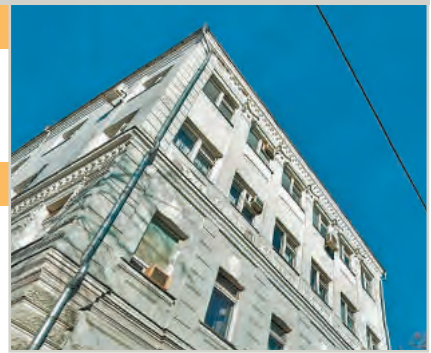
Проект реализован для МВД России

ПРОЕКТИРОВАНИЕ СИСТЕМ ЗАЩИТЫ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ, ВИБРАЦИОННОМУ, ОПТИКО-ЭЛЕКТРОННОМУ И 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

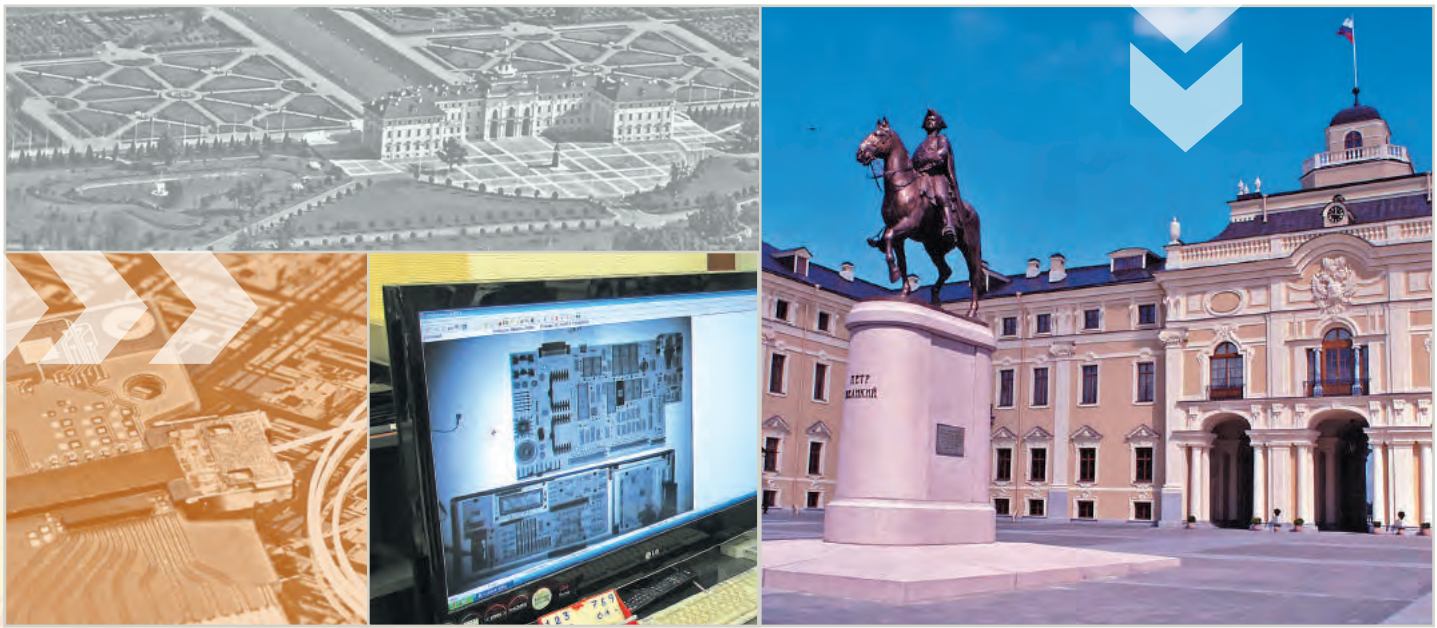
Выполненные работы:

- 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 эффективености

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 нагрузку 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

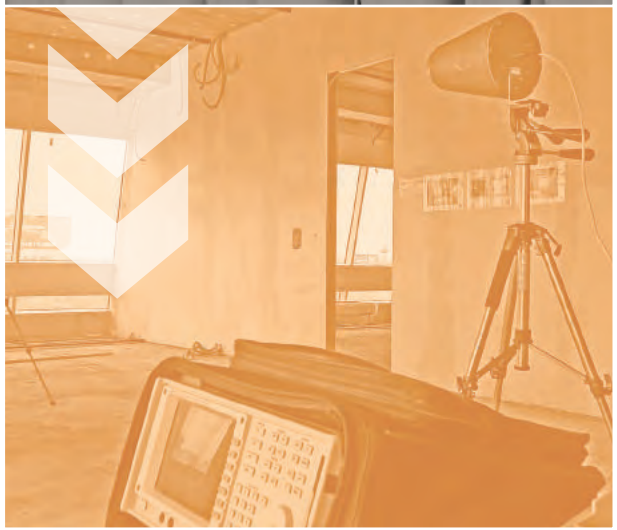
Выполненные работы:

- 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:

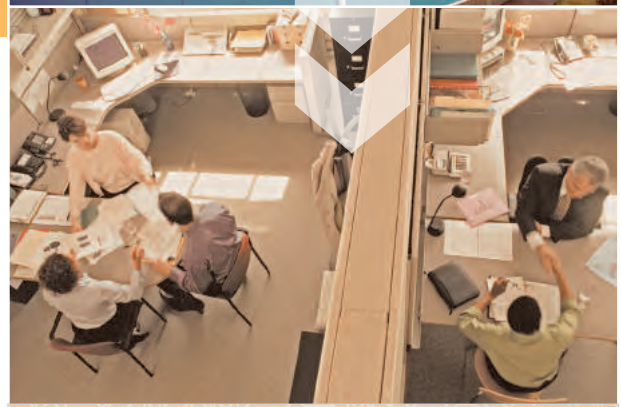
- Проектирование с последующей реализацией комплексной системы защиты информации, включающей в себя:
  - Систему защиты информации от утечки по техническим каналам в соответствии с требованиями руководящих документов ФСБ России и ФСТЭК России
  - Систему защиты аудио-визуальной информации от утечки по 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, разворачиваемые 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 стредствами 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
- Возможностью 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 локалных 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 внутриплощадные сети связи.

Проекты выполнены для Министерства обороны Российской Федерации

СОЗДАНИЕ ЗАЩИЩЕННОЙ IT-ИНФРАСТРУКТУРЫ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

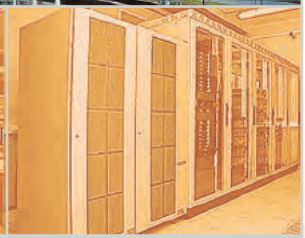
Цель проекта: Провести аудит защищенности, разработать и реализовать технические решения по созданию защищенной IT-инфраструктуры центра обработки данных

Выполненные работы:

- Проектно-изыскательские работы
- Разработка технических решений по созданию безопасной IT-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.

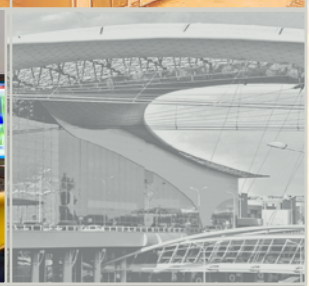


СОЗДАНИЕ ЗАЩИЩЕННОЙ IT-ИНФРАСТРУКТУРЫ ЦЕНТРА ОБРАБОТКИ ДАННЫХ

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

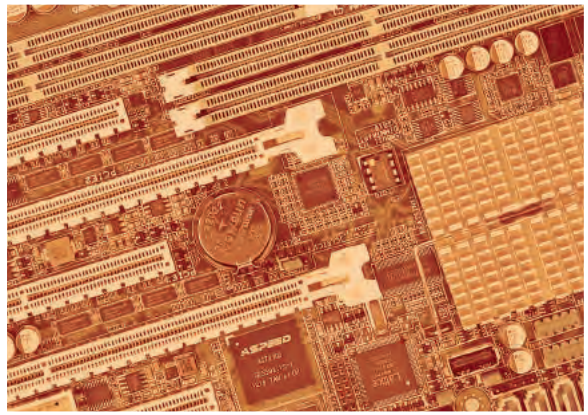
Выполненные работы:

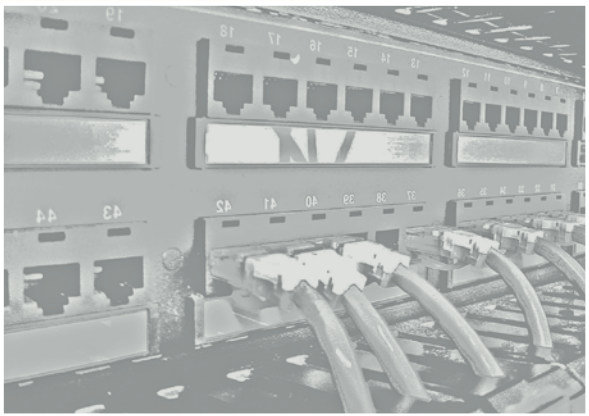
- Проектно-изыскательские работы
- Поставка, монтаж и пуско-наладка оборудования локальной вычислительной сети
- Поставка, монтаж и пуско-наладка оборудования супервычислительного комплекса
- Поставка, монтаж и пуско-наладка средств защиты информации
- Специальные работы по защите информации
- Аттестация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

Проект выполнен для НИЦ «Курчатовский институт»





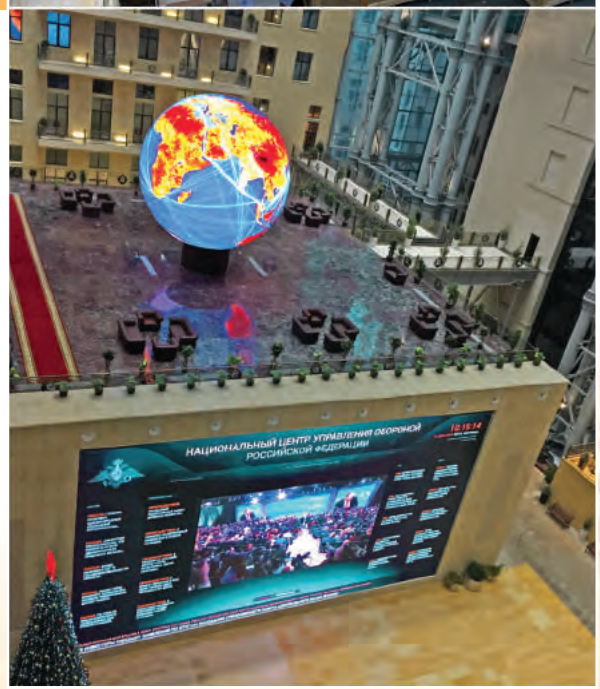
3 ДОМ МО РФ

Специальная проверка (СП) и специальные исследования (СИ) высокотехнологичной системы отображения информации и видеокоммутации (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»

КАТАЛОГ ОБОРУДОВАНИЯ

Сиситемы оценки защищенности

СИГУРД - А10 › › › › ›

Система автоматизированная измерительная

Система измерительная автоматизированная «Сигурд-А10» предназначена для измерений параметров электромагнитных излучений и наводок при проведении специальных исследований технических средств.

Система «Сигурд-А10» обеспечивает:

- Исследование технического средства с целью оценки его защищенности по каналу побочных электромагнитных излучений и наводок (ПЭМИН).
- Расчет показателей защищенности технического средства от утечки информации по каналу ПЭМИН в соответствии с актуальными нормативно-методическими документами.

Выполнение заявленных функций осуществляется в соответствии с требованиями следующих нормативно-методических документов:

- «Требования по технической защите информации, содержащей сведения, составляющие государственную тайну» (ФСТЭК России, Москва, Приказ № 025 от 20.10.2016 г.).
- «Методика оценки эффективности защиты информации, обрабатываемой объектами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, Москва, Приказ № 043 от 27.11.2017 г.).

Технические характеристики

Параметр и характеристика	Значение
Рабочий диапазон частот при измерении напряженности электрического поля	9 кГц – 10 ГГц
Рабочий диапазон частот при измерении напряженности магнитного поля	9 кГц – 30 МГц
Рабочий диапазон частот при измерении силы тока и напряжения переменного тока, наведенного электромагнитным полем	9 кГц – 400 МГц
Точность расчета показателей R2, r1 и r1' для объектов 1-й, 2-й и 3-й категории для стационарных, возимых и носимых средств разведки	не хуже предельных значений, заданных в нормативных документах

Комплектация

Анализатор спектра	1 к-т
Комплект измерительных антенн	1 к-т
Пробник напряжения	1 шт.
Штатив	1 шт.
Управляющая ПЭВМ ноутбук	1 шт.
Комплект программного обеспечения	1 к-т
Комплект укладок для транспортировки	1 к-т
Комплект документации	1 к-т

Свидетельство об утверждении типа средств измерений (на стадии оформления).

Оформляется сертификат ФСТЭК России на СПО.

СИГУРД - М8Р

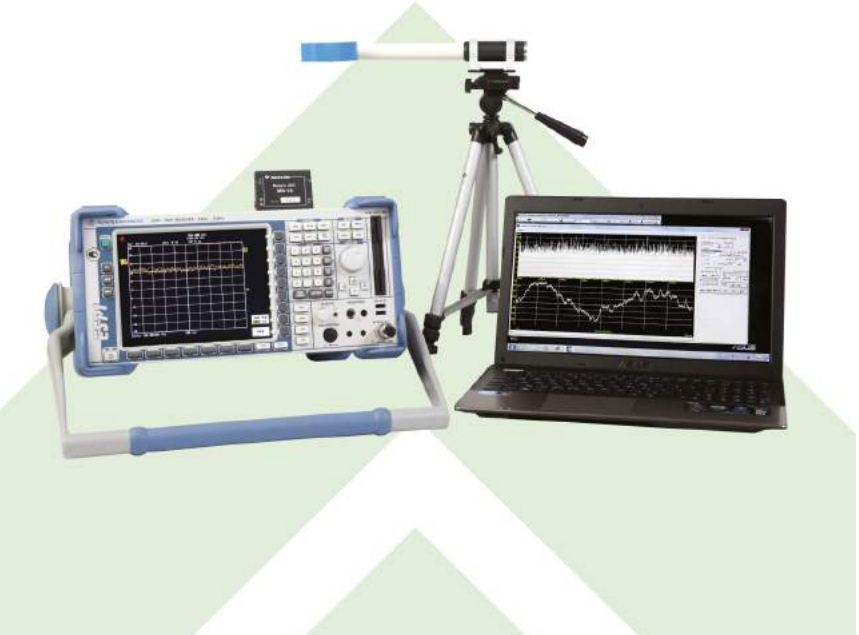
Система автоматизированная измерительная

Система измерительная автоматизированная «Сигурд-М8Р» предназначена для измерений параметров электромагнитных излучений и наводок при проведении специальных исследований технических средств.

Система «Сигурд-М8Р» обеспечивает исследование технических средств с целью оценки его защищенности по каналу побочных электромагнитных излучений и наводок (ПЭМИН) в соответствии с требованиями следующих нормативно-методических документов:

- «Требования по технической защите информации, содержащей сведения, составляющие государственную тайну» (ФСТЭК России, Москва, Приказ № 025 от 20.10.2016 г.).
- «Методика оценки эффективности защиты информации, обрабатываемой объектами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, Москва, Приказ № 043 от 27.11.2017 г.).
- «Сборник методик для организаций, имеющих лицензию ФСБ России на право осуществления мероприятий и (или) оказания услуг в области защиты информации в части проведения специальных исследований на побочные электромагнитные излучения и наводки технических средств».

Сиситемы оценки защищенности



Технические характеристики

Параметр и характеристика	Значение
Рабочий диапазон частот при измерении напряженности электрического поля	100 Гц – 12 ГГц
Рабочий диапазон частот при измерении напряженности магнитного поля	100 Гц – 30 МГц
Рабочий диапазон частот при измерении силы тока и напряжения переменного тока, наведенного электромагнитным полем	100 Гц – 400 МГц
Точность расчета показателей R2, r1 и r1' для объектов 1-й, 2-й и 3-й категории для стационарных, возимых и носимых средств разведки	не хуже предельных значений, заданных в нормативных документах

Комплектация

Анализатор спектра	1 шт.
Комплект измерительных антенн	1 к-т
Пробник напряжения	1 шт.
Управляющая ПЭВМ ноутбук	1 шт.
Комплект программного обеспечения	1 к-т
Комплект укладок для транспортировки	1 к-т
Комплект документации	1 к-т

Свидетельство об утверждении типа средств измерений.

Оформляется сертификат ФСТЭК России на СПО.

СТЕНТОР - МИНИ

Сиситемы оценки защищенности

Система для измерения коэффициентов реального затухания электромагнитных сигналов

Система «Стентор-Мини» обеспечивает расширение функциональных возможностей автоматизированной системы «Сигурд» и предназначена для измерения коэффициентов реального затухания электромагнитных сигналов.

Система «Стентор-Мини» обеспечивает измерение коэффициентов реального затухания электромагнитных сигналов в соответствии с требованиями следующих нормативно-методических документов:

- «Требования по технической защите информации, содержащей сведения, составляющие государственную тайну» (ФСТЭК России, Москва, Приказ № 025 от 20.10.2016 г.).
- «Методика оценки эффективности защиты информации, обрабатываемой объектами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, Москва, Приказ № 043 от 27.11.2017 г.).

Технические характеристики

Параметр и характеристика	Значение
Максимальная длина трассы измерений реального затухания электромагнитного сигнала в эфире	200 м
Максимальный измеряемый коэффициент реального затухания электромагнитного сигнала в эфире	не менее 80 дБ
Максимальный измеряемый коэффициент реального затухания электромагнитного сигнала в линии	не менее 60 дБ
Диапазон рабочих частот при измерении реального затухания сигналов в эфире	100 Гц – 12 ГГц
Диапазон рабочих частот при измерении реального затухания сигналов в линии	100 Гц – 400 МГц
Максимальный уровень тестового сигнала на выходе генератора	26 дБм (23 дБм – для частот от 8,5 до 12 ГГц)

Комплектация

Генератор сигналов	1 шт.
Антенная система	1 к-т
Точка доступа	1 к-т
Индуктор магнитный	1 шт.
Комплект программного обеспечения	1 к-т
Комплект укладок для транспортировки	1 к-т
Комплект документации	1 к-т

СПЕЦИАЛЬНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «СИГУРД»

Пакет специального программного обеспечения «Сигурд» предназначен для автоматизации управления процессом измерений и расчетов показателей защищенности технических средств от утечки информации по каналу побочных электромагнитных и наводок (ПЭМИН), а также показателей эффективности систем активного зашумления.

Актуальная версия СПО «Сигурд» разработана в соответствии с требованиями «Методики оценки эффективности защиты информации, обрабатываемой объектами вычислительной техники, от утечки за счет побочных электромагнитных излучений и наводок» (ФСТЭК России, Москва, Приказ № 043 от 27.11.2017 г.).

СПО «Сигурд» обеспечивает:

- Автоматический поиск и измерение параметров электромагнитных сигналов исследуемого технического средства в соответствии с подготовленным заданием.
- Автоматизированное исследование технического средства на наличие ПЭМИН в соответствии с актуальными нормативно-методическими документами ФСТЭК России.
- Возможность управления поворотным столом, получение диаграмм направленности излучения.
- Дистанционное управление по ИК-каналу работой программы, предназначенной для управления состоянием исследуемого технического средства, с целью получения сигналов ПЭМИН заданного вида.
- Расчет показателей защищенности технических средств от утечки информации по каналу ПЭМИН (в том числе в отходящих линиях) в соответствии с нормативно-методическими документами ФСТЭК России.
- Возможность ввода/корректировки всей номенклатуры исходных данных для расчета оператором вручную.

Поддерживаемые СПО «Сигурд» анализаторы спектра:

- Rohde&Schwarz серия FSV
- Rohde&Schwarz серия ESRP
- Rohde&Schwarz серия FSL
- Rohde&Schwarz серия FSH
- Rohde&Schwarz серия ESPI
- Keysight (Agilent) E4402B/ E4405B/E4407B
- Rohde&Schwarz серия FSC
- Rohde&Schwarz серия FSP
- IFR 2394/2394A/2395A/2399/2399C

Сиситемы оценки защищенности

Комплектация

Специальное программное обеспечение «Сигурд» в составе: - Программная оболочка «Сигурд-Лайт». - Динамически подгружаемый программный модуль управления системой «Сигурд-Интерфейс». - Программный модуль расчета показателей защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок (ПЭМИН) «Сигурд-Дельта».	1 к-т
Ключ защиты от несанкционированного использования	1 шт.
Комплект документации	1 к-т

Оформляется сертификат ФСТЭК России на СПО.

СПДУ - 1 › › › › ›

Дополнительное оборудование

Стол поворотный диэлектрический управляемый

Наиболее эффективно использовать СПДУ-1 в составе специализированных автоматизированных систем, например, таких как система оценки защищенности 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.

Технические характеристики

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 ˚/с
Диапазон вращения столешницы по углу поворота	0 – 360˚
Длина оптического соединительного кабеля	10 м
Время непрерывной работы изделия без ухудшения рабочих характеристик	не менее 8 часов
Напряжение сети электропитания изделия	220 ±20 В
Частота сети электропитания изделия	50 ±2 Гц
Максимальная допустимая мощность, потребляемая испытуемой аппаратуры	1000 Вт

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.

ШЕПОТ- М1 › › › › ›

Система оценки защищенности выделенных помещений по виброакустическому каналу

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

Система «Шепот-М1» обеспечивает:

- Автоматические измерения уровня звукового давления тестового сигнала вблизи от его источника, а также уровня наведенного им акустического давления/виброускорения.
- Использование данных измерений для расчета показателей защищенности выделенных помещений по виброакустическому каналу утечки речевой информации.
- Формирование и ведение информативной базы данных о результатах выполненных измерений в каждой контрольной точке.
- Составление отчета по результатам измерений в форме, отвечающей требованиям нормативных документов.
- Автоматический и/или ручной режим ввода данных для расчета показателей защищенности выделенных помещений по виброакустическому каналу.
- Возможность перехода на ручное управление аппаратурой системы.

Технические характеристики

Параметр и характеристика	Значение
Диапазон рабочих частот	не менее 80 – 11300 Гц
Диапазон измерений звукового давления	не менее 20 – 125 дБ (20 мкПа)
Диапазон измерений виброускорения	не менее $2 \cdot 10^{-3}$ – 200 м*с$^{-2}$
Погрешность измерений уровня звукового давления и виброускорения	не более ±1 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)	не менее 100 дБ

Системы оценки защищенности

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.
Колонка акустическая активная	1 шт.
Комплект измерительных и соединительных кабелей	1 к-т
Штатив	3 шт.
Комплект программного обеспечения	1 к-т
Комплект укладок для транспортировки	1 к-т
Комплект документации	1 к-т

Система находится в стадии разработки.

ТАЛИС - НЧ - М2

Системы оценки защищенности

Система измерительная автоматизированная

Система «Талис-НЧ-М2» 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 различных технических средств от утечки речевой информации.

Система «Талис-НЧ-М2» обеспечивает:

- Предоставление оператору пользовательского интерфейса, позволяющего установить все необходимые параметры для работы системы в режиме автоматического выполнения задания и в режиме ручного исследования сигналов.
- Автоматический поиск и измерение параметров сигналов в соответствии с подготовленным заданием.
- Визуализацию обнаруженных в процессе исследования сигналов (в виде спектра сигналов).
- Проведение расчета показателя защищенности технических средств от утечки информации по каналу АЭП в отходящих от них линиях в соответствии с актуальными нормативно-методическими документами.

Технические характеристики

Параметр и характеристика	Значение
Диапазон рабочих частот	не менее 100 – 11200 Гц
Диапазон измерений напряжения переменного тока	не хуже $5*10^{-8}$ – 3 В
Диапазон измерений звукового давления	не менее 20 – 125 дБ (20 мкПа)
Максимальное звуковое давление тест-сигнала на расстоянии 1 м от излучателя (интегральное)	не менее 100 дБ

Комплектация

НЧ-анализатор спектра	1 к-т
Комплект первичных преобразователей	1 к-т
Измерительный блок (шумомер)	1 шт.
ICP микрофон	1 шт.
Источник калиброванного звукового давления	1 шт.
Комплект соединительных и измерительных кабелей	1 к-т
Генератор тестового акустического сигнала	1 к-т
Экранированная акустическая колонка	1 шт.
Штатив	1 шт.
Управляющая ПЭВМ ноутбук	1 шт.
Комплект программного обеспечения	1 к-т
Укладка для транспортировки	1 к-т
Комплект документации	1 к-т

Система находится в стадии разработки.

ТАЛИС - М1 › › › › ›

Системы оценки защищенности

Система автоматизированная измерительная

Система «Талис-М1» предназначена для проведения исследований характеристик технических средств с целью оценки наличия акустоэлектрических преобразований в технических средствах и отходящих от них линиях, возникающих в них при воздействии акустическим сигналом.

Система «Талис-М1» обеспечивает:

- Автоматизированное исследование технических средств на наличие эффекта высокочастотных акустоэлектрических преобразований (ВЧ АЭП) в паразитных излучениях.
- Установку всех необходимых параметров для работы системы через интерфейс программного обеспечения.
- Возможность формирования заданий с указанием параметров настройки измерительной аппаратуры для автоматического поиска сигналов заданного вида.
- Автоматический поиск и измерение параметров сигналов исследуемого технического средства в соответствии с подготовленным заданием.
- Проведение расчетов показателей защищенности технических средств от утечки информации по каналу ВЧ АЭП с выводом результатов в файл стандарта HTML или DOC.

Технические характеристики

Параметр и характеристика	Значение
Рабочий диапазон частот при измерении напряженности электрического поля	100 Гц – 12 ГГц
Рабочий диапазон частот при измерении напряженности магнитного поля	100 Гц – 30 МГц
Рабочий диапазон частот при измерении силы тока и напряжения переменного тока, наведенного электромагнитным полем	100 Гц – 400 МГц
Минимальный измеряемый коэффициент (индекс) модуляции	не хуже $1*10^{-5}$
Динамический диапазон измерений напряженности электромагнитного поля, силы тока и напряжения переменного тока (с учетом переключения входного аттенюатора)	не менее 80 дБ

Комплектация

Анализатор сигналов и спектра	1 шт.
Комплект измерительных антенн	1 к-т
Пробник напряжения	1 к-т
Устройство управления исследуемым техническим средством	1 к-т
Генератор тестового акустического сигнала	1 к-т
Экранированная акустическая колонка	1 шт.
Измерительный блок (шумомер)	1 шт.
ICP микрофон	1 шт.
Источник калиброванного звукового давления	1 шт.
Комплект измерительных и соединительных кабелей	1 к-т
Штатив	2 шт.
Управляющая ПЭВМ ноутбук	1 шт.
Комплект программного обеспечения	1 к-т
Комплект укладок для транспортировки	1 к-т
Комплект документации	1 к-т

Свидетельство об утверждении типа средств измерений (на стадии оформления).

ТЕЛЕФОН - Н2

Телефонный аппарат стандарта GSM в защищенном исполнении

Телефон-Н2 представляет собой телефонный аппарат стандарта GSM в защищенном исполнении, оснащенный аппаратными средствами, исключающими утечку акустической речевой и визуальной информации, циркулирующей в выделенных помещениях, по каналам сотовой связи. А также обеспечивающими защиту информации, обрабатываемой основными техническими средствами и системами (ОТСС) от утечки по техническим каналам, возникающим при размещении изделия на режимных объектах.

Телефон-Н2 предназначен для ведения открытых переговоров и допускается к вносу в выделенные помещения до второй категории включительно, в том числе в помещения органов государственной власти Российской Федерации.

Телефон-Н2 обеспечивает:

- Возможность ведения открытых разговоров по сотовой связи стандарта GSM любого оператора сотовой связи, действующего на территории Российской Федерации.
- Исключение утечки акустической речевой и визуальной информации, циркулирующей в выделенном помещении, от утечки по каналам сотовой связи при нахождении в помещении телефона с активированной системой защиты.
- Исключение утечки информации, обрабатываемой основными техническими средствами и системами (ОТСС), за счёт перехвата побочных электромагнитных излучений (ПЭМИ).

Технические средства в зищищенном исполнении

Технические характеристики

Параметр и характеристика	Значение
Стандарт связи	GSM 900/1800/1900
Тип SIM-карты	микро-SIM
Диагональ дисплея/ размер изображения	2,4 дюйма/240x320
Тип дисплея	цветной
Емкость аккумулятора/тип	800 мАч/ Li-Ion
Интерфейс	USB
Габаритные размеры	52x102x17 мм
Масса	не более 90 г

Комплектация

Телефонный аппарат стандарта GSM в защищенном исполнении «Телефон-Н2»	1 шт.
Зарядное устройство	1 шт.
Комплект документации	1 к-т

Сертификат ФСБ России.

Сертификат ФСТЭК России (в процессе получения).

Декларация о соответсвии Федерального агентства связи (РОССВЯЗЬ) № Д-ТАРТ-11074 от 18.12.2017 г.

Экспертное заключение Роспотребнадзора.

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).
- Возможность управления включением произвольной нагрузки, подключенной к блоку питания и управления.
- Возможность работы от внешнего источника питания 12 Вольт.
- Учёт времени наработки системы.

Сертификат ФСТЭК России.

Санитарно-эпидемиологическое заключение.

Решение о соответствии требованиям пожарной безопасности.

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 -40 до +45 °С)
Максимальное количество излучателей, подключаемых к БПУ-1	35 шт.

КЛЮЧ - ВП (ИТ) › › › › ›

Управляемый размыкатель линии

Управляемый размыкатель линии «Ключ-ВП (ИТ)» предназначен для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, циркулирующей (обрабатываемой) в помещениях, от утечки за счет акустоэлектрических преобразований в линиях компьютерных сетей и телефонии, отходящих от технических средств. Изделие может использоваться автономно или в составе системы «Шорох-5Л».

Изделие при автономном использовании обеспечивает:
- Размыкание цепей защищаемой линии при подаче на изделие электропитания.
- Замыкание защищаемой линии при отсутствии на изделии электропитания.
- Детектирование входящего вызова на подключенный к изделию телефонный аппарат в режиме защиты.

Изделие при совместной работе с системой «Шорох-5Л» обеспечивает:
- Размыкание цепей защищаемой линии при включении электропитания на блоке питания и управления БПУ-1, из состава системы «Шорох-5Л».
- Замыкание цепей защищаемой линии при выключении электропитания на блоке БПУ-1.
- Дистанционное размыкание и замыкание цепей защищаемой линии при использовании пульта ДУ из состава дополнительных опций системы «Шорох-5Л», подключенного к блоку БПУ-1.

Технические характеристики

Параметр и характеристика	Значение
Диапазон рабочих частот, кГц	не менее 0,1 – 10
Затухание в полосе рабочих частот, дБ	не менее 60
Количество проводов защищаемой линии, шт.	8
Напряжение питания, В	12
Ток потребления, мА	не более 80
Коммутируемый ток, А	не более 0,5
Дистанционное управление	имеется
Масса, г	не более 65
Габаритные размеры, мм	не более 109x54x30

Комплектация

Управляемый размыкатель линии «Ключ-ВП (ИТ)»	1 шт.
Комплект документации	1 к-т

Сертификат ФСТЭК России (при использовании в составе системы «Шорох-5Л») на стадии оформления.

Соответствует требованиям Технического регламента таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования» и Технического регламента таможенного союза ТР ТС 020/2011 «Электромагнитная совместимость технических средств».

КЛЮЧ - ВП (220)

Управляемый размыкатель линии

Управляемый размыкатель линии «Ключ-ВП (220)» предназначен для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, циркулирующей (обрабатываемой) в помещениях, от утечки за счет акустоэлектрических преобразований в линиях электропитания, отходящих от технических средств. Изделие может использоваться автономно или в составе системы «Шорох-5Л».

Изделие при автономном использовании обеспечивает:
- Размыкание цепей защищаемой линии при подаче на изделия электропитания.
- Замыкание защищаемой линии при отсутствии на изделиях электропитания.

Изделие при совместной работе с системой «Шорох-5Л» обеспечивает:
- Размыкание цепей защищаемой линии при включении электропитания на блоке питания и управления БПУ-1, из состава системы «Шорох-5Л».
- Замыкание цепей защищаемой линии при выключении электропитания на блоке БПУ-1.
- Дистанционное размыкание и замыкание цепей защищаемой линии при использовании пульта ДУ из состава дополнительных опций системы «Шорох-5Л», подключенного к блоку БПУ-1.

Технические характеристики

Параметр и характеристика	Значение
Диапазон рабочих частот, кГц	не менее 0,1 – 10
Затухание в полосе рабочих частот, дБ	не менее 60
Количество проводов защищаемой линии, шт.	3
Напряжение питания, В	12
Ток потребления, мА	не более 80
Коммутируемый ток, А	не более 7,0
Коммутируемое переменное напряжение, В	220±22
Дистанционное управление	имеется
Масса, кг	не более 0,2
Габаритные размеры, мм	не более 113x69x90

Комплектация

Управляемый размыкатель линии «Ключ-ВП (220)»	1 шт.
Комплект документации	1 к-т

Сертификат ФСТЭК России (при использовании в составе системы «Шорох-5Л») на стадии оформления.

Соответствует требованиям Технического регламента таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования» и Технического регламента таможенного союза ТР ТС 020/2011 «Электромагнитная совместимость технических средств».

КЛЮЧ - ВП (СЛ)

Управляемый размыкатель линии

Управляемый размыкатель линии «Ключ-ВП (СЛ)» предназначен для защиты акустической речевой информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом, циркулирующей (обрабатываемой) в помещениях, от утечки за счет акустоэлектрических преобразований в слаботочных линиях, отходящих от технических средств. Изделие может использоваться автономно или в составе системы «Шорох-5Л».

Изделие при автономном использовании обеспечивает:
- Размыкание цепей защищаемой линии при подаче на изделие электропитания.
- Замыкание защищаемой линии при отсутствии на изделии электропитания.

Изделие при совместной работе с системой «Шорох-5Л» обеспечивает:
- Размыкание цепей защищаемой линии при включении электропитания на блоке питания и управления БПУ-1, из состава системы «Шорох-5Л».
- Замыкание цепей защищаемой линии при выключении электропитания на блоке БПУ-1.
- Дистанционное размыкание и замыкание цепей защищаемой линии при использовании пульта ДУ из состава дополнительных опций системы «Шорох-5Л», подключенного к блоку БПУ-1.

Технические характеристики

Параметр и характеристика	Значение
Диапазон рабочих частот, кГц	не менее 0,1 – 10
Затухание в полосе рабочих частот, дБ	не менее 60
Количество проводов защищаемой линии, шт.	4
Напряжение питания, В	12
Ток потребления, мА	не более 80
Коммутируемый ток, А	не более 1,0
Коммутируемое напряжение, В	не более 60
Дистанционное управление	имеется
Масса, г	не более 65
Габаритные размеры, мм	не более 109х54х30

Комплектация

Управляемый размыкатель линии «Ключ-ВП (ИТ)»	1 шт.
Комплект документации	1 к-т

Сертификат ФСТЭК России (при использовании в составе системы «Шорох-5Л») на стадии оформления.

Соответствует требованиям Технического регламента таможенного союза ТР ТС 004/2011 «О безопасности низковольтного оборудования» и Технического регламента таможенного союза ТР ТС 020/2011 «Электромагнитная совместимость технических средств».

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, выполнение 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.В011.022** от 26.11.2003 г.
- Аттестат аккредитации испытательной лаборатории при ФСТЭК России **№ СЗИ RU.094.БО25.058** 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.Р00268** на следующие услуги (работы): монтаж, пусконаладочные работы, ремонт и техническое обслуживание инженерно-технических средств охраны
- Сертификат соответствия Системы сертификации Euro-Standart **№ РОСС RU.ОС/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

ЦБИ МАСКОМ
121596, г. Москва ул. Горбунова, д. 2, стр.5
Тел. +7 (495) 136-40-10
Тел. +7 (495) 136-40-20
mascom@mascom.ru
Департамент оборудования:
121596, г. Москва ул. Горбунова, д. 2, стр.5
Департамент комплексных работ:
121596, г. Москва ул. Горбунова, д. 2, стр.5
Тел. +7 (495) 136-40-10
Тел. +7 (495) 136-40-20

НОУ ДПО УЦБИ МАСКОМ
117630, г. Москва, Старокалужское шоссе, д.62, стр.1
Тел. +7 (495) 136-40-10 (доб.1310)
Тел. +7 (495) 136-40-20 (доб.1310)
www.mascom-uc.ru
mascom-uc@mascom-uc.ru

М СОФТ
121596, г. Москва ул. Горбунова, д. 2, стр.5
Тел. +7 (495) 136-40-10
www.mascomsoft.ru
info@mascomsoft.ru

МК-СПЕЦМОНТАЖ
121596, г. Москва ул. Горбунова, д. 2, стр.5
Тел. +7 (495) 660-06-08

МАСКОМ ВОСТОК

ДСЦБИ МАСКОМ
680038, г. Хабаровск, ул. Яшина, д. 40
Тел. +7 (4212) 45-46-33
Факс +7 (4212) 76-48-78
www.mascom-dv.ru; info@mascom-dv.ru

МАСКОМ-АМУР
675000, г. Благовещенск, ул. Калинина, д. 126
Тел. +7 (4162) 222-843
Факс +7 (4162) 222-839
www.mascom-amur.ru; amur@mascom-amur.ru

СТАНДАРТ ТЕЛЕКОМ
680038, г. Хабаровск, ул. Яшина, д. 40
Тел. +7 (4212) 91-20-34
www.stnt.ru
info@stnt.ru

МАСКОМ-ПРИМОРЬЕ
690001, г. Владивосток, ул. Светланская, д. 165
Тел. +7 (423) 230-23-30
Факс +7 (423) 224-04-40
www.mascomvl.ru; info@mascomvl.ru

МАСКОМ ТЕХЛАЙН
680038, г. Хабаровск, ул. Яшина, д. 40
Тел. +7 (4212) 45-46-32
Факс +7 (4212) 76-48-78
www.mascom-it.ru; info@mascom it.ru

МАСКОМ-ИНСТРОЙ
680038, г. Хабаровск, ул. Яшина, д. 40
Тел. +7 (4212) 45-46-31
Факс +7 (4212) 76-48-78
www.mascom-instroy.ru; info@mascom-instroy.ru

МАСКОМ-СИБИРЬ
630091, г. Новосибирск, ул. Фрунзе, д. 5, оф.325
Тел. +7 (383) 218-87-18
Факс +7 (383) 221-12-41
sideria@mascom-vostok.ru

МАСКОМ ЮГ
350015, г. Краснодар, ул. Кузнечная, д. 6
Тел. +7 (988) 367-08-18
Тел. +7 (918) 211-30-71
mascom-u@mascom.ru; www.mascom-ug.ru