



Адрес
г. Ярославль,
ул. Угличская, 39В



Телефон
+7 (4852) 587-300



E-mail
info@yarsec.ru



Режим работы
Пн.-Чт.: 9:00 - 18:00
Пт.: 9:00 - 17:00



WWW.YARSEC.RU



С Т А Н Д А Р Т
БЕЗОПАСНОСТИ
БЕЗОПАСНОСТЬ КАК СТАНДАРТ



WWW.YARSEC.RU



С Т А Н Д А Р Т
БЕЗОПАСНОСТИ
БЕЗОПАСНОСТЬ КАК СТАНДАРТ



Дорогие друзья, уважаемые коллеги!

С момента своего основания в 2008 году «Стандарт безопасности» прошел большой путь и достиг выдающихся результатов, чем мы чрезвычайно гордимся!

От всего сердца выражаю слова глубокой благодарности всем нашим Клиентам! Ориентированность «СБ» на долгосрочную и стабильную работу является основополагающим принципом нашей культуры и ставит перед нами гораздо более фундаментальные цели, нежели способность просто инвестировать в новые проекты.

Нашими важнейшими преимуществами являются портфель первоклассных предложений в сфере Информационной и Инженерно-технической безопасности, характеризующихся высокой степенью проработки, минимизированными рисками и низкими инвестиционными потребностями.

В регионах своего присутствия мы стремимся работать ответственно и вести бизнес в соответствии с лучшими мировыми корпоративными и этическими стандартами.

Мы помогаем нашим Клиентам реализовывать любые проекты в сфере безопасности оптимальным образом, с минимальными затратами и 100% гарантией результата.

Большое спасибо Вам за доверие и сотрудничество! Мы сделаем всё возможное, чтобы, обратившись к нам, Вы испытали желание остаться с нами надолго.



МИХАИЛ РАЧКОВ
Генеральный директор

С уважением, Михаил Рачков
Генеральный директор
«Стандарт безопасности»



КТО МЫ?

- Наша компания ООО «Стандарт безопасности» - системный интегратор в области безопасности.
- Компания ООО «Стандарт безопасности» (г. Ярославль) была образована в 2008 году. Компания работает, разделяя имя и бренд своего учредителя – Акционерного Общества «Стандарт безопасности» г.Москва.
- Наша миссия – помощь в создании безопасного пространства жизнедеятельности и коммуникации правового гражданского общества.

КАКИЕ ЗАДАЧИ МЫ РЕШАЕМ?



Стандарт безопасности специализируется в вопросах защиты информации различного уровня конфиденциальности, обеспечивая защиту клиента от финансовых и репутационных потерь.

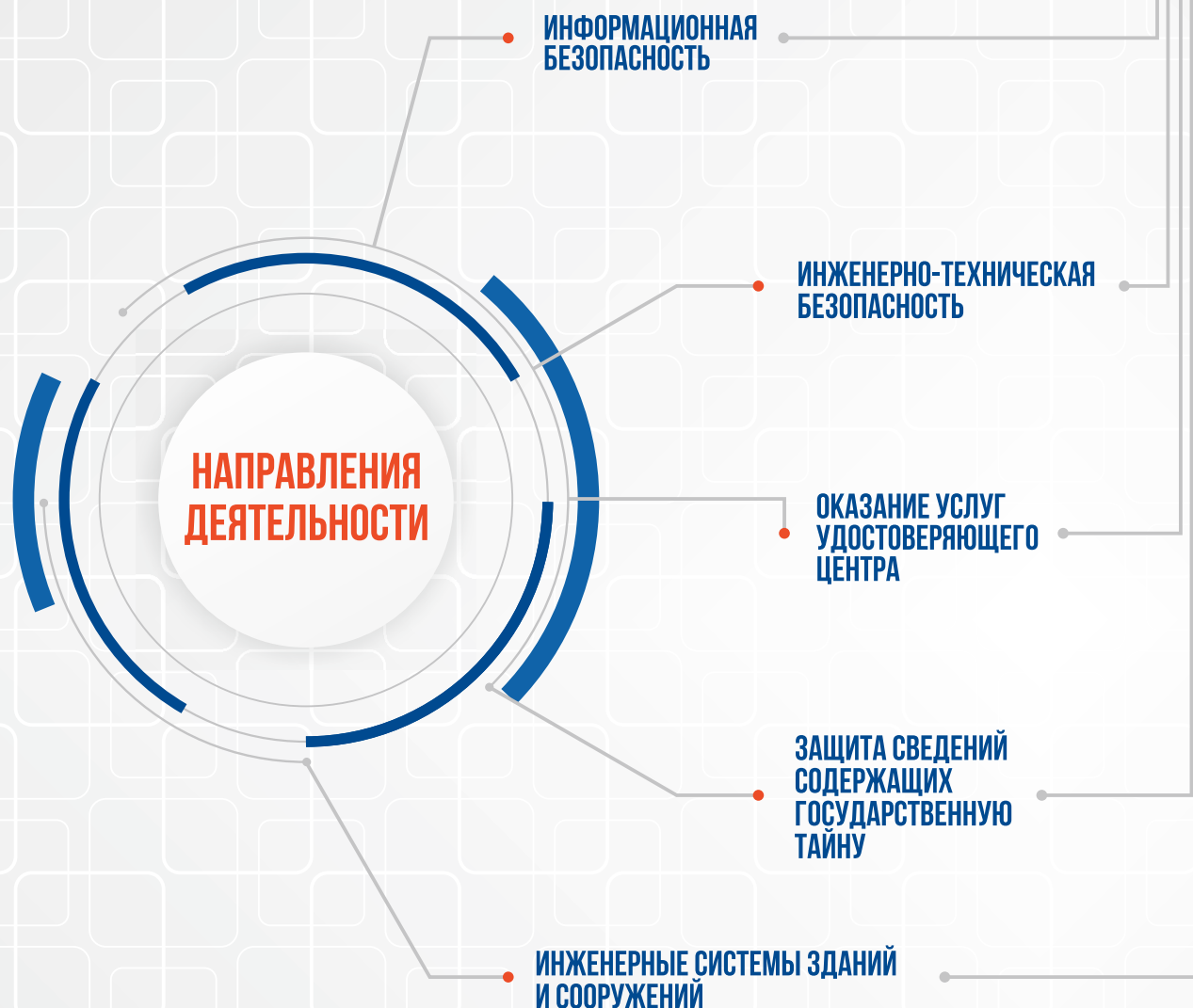
Мы создаем решения с высокой интеллектуальной составляющей, аккумулирующей опыт как отдельных экспертов, так и компании в целом.



Наши специалисты обладают экспертными знаниями в области информационной и технической безопасности, а также защиты сетевой инфраструктуры, чтобы помочь клиентам защитить текущие бизнес-процессы, улучшить операционную кибер-безопасность.

У нас опыт реализации более 3500 масштабных проектов. Высокий уровень компетенций «Стандарта безопасности» позволяет с успехом решать задачи на высоком профес-сиональном уровне.





Предложение по этим направлениям клиент получает в максимально оптимизированном виде с учетом бизнес потребностей и передовых на текущий момент времени технических решений.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

АНАЛИТИЧЕСКИЕ

- Аналитическое обследование информационных систем
- Инструментальный анализ защищенности информационных систем
- Моделирование угроз безопасности

ВНЕДРЕНИЕ

- Поставка средств защиты информации
- Поставка оборудования и программного обеспечения
- Монтаж и пусконаладка средств защиты

ОБСЛУЖИВАНИЕ И ПОДДЕРЖКА

- Обслуживание системы защиты информации и информационных систем.



ПРОЕКТНЫЕ

- Разработка модели защиты информационных систем
- Проектирование систем защиты информации

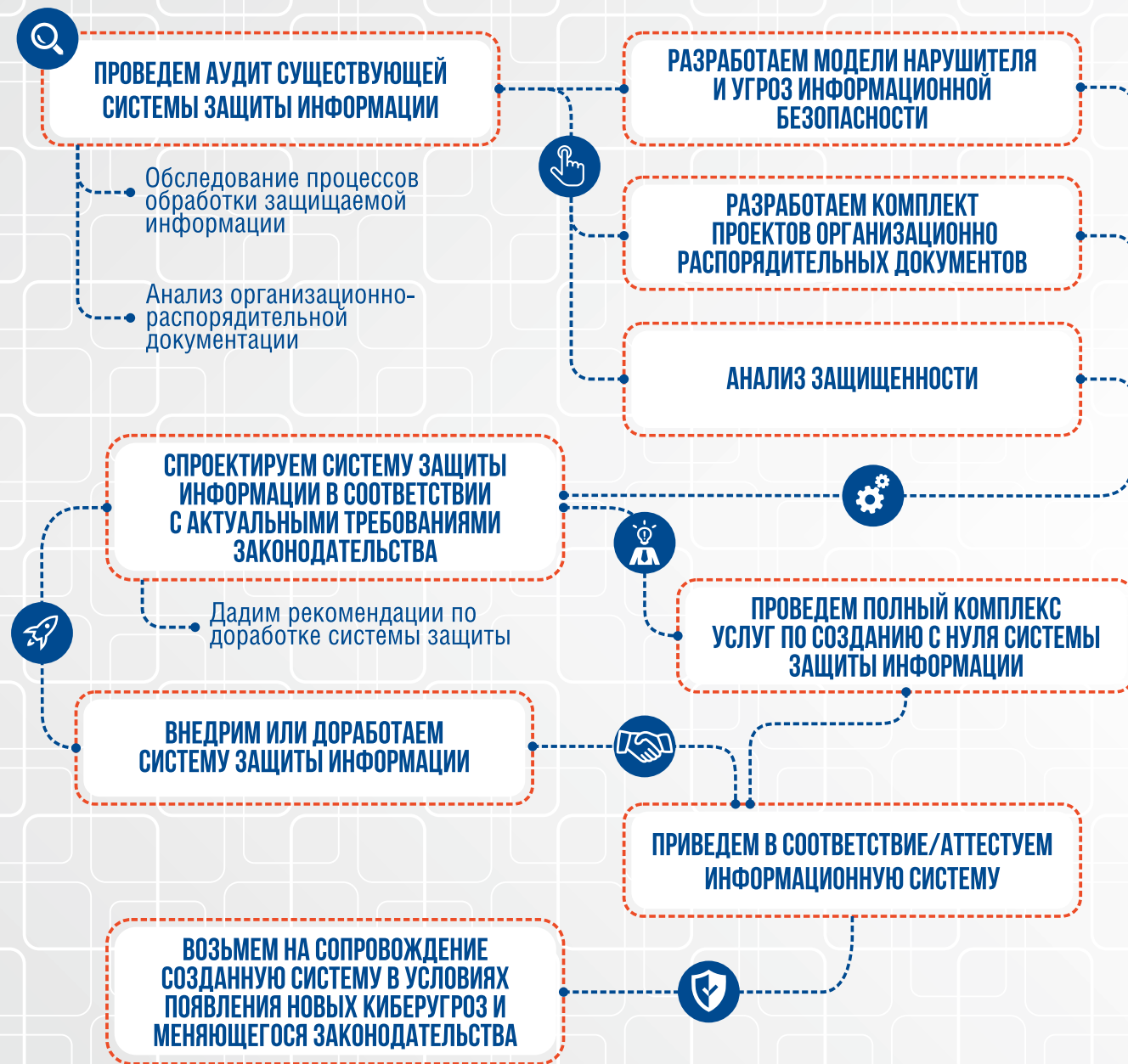
АТТЕСТАЦИОННЫЕ МЕРОПРИЯТИЯ

- Аттестация информационных систем
- Ежегодный мониторинг эффективности системы защиты информации
- Моделирование угроз безопасности

МЫ ЗАЩИЩАЕМ:



- Государственную тайну
- Информацию для служебного пользования
- Коммерческую тайну
- Персональные данные, в том числе в соответствии с GDPR
- Объекты критической информационной инфраструктуры
- Государственные и муниципальные информационные системы
- Автоматизированные системы управления технологическими процессами
- Открытые и общедоступные информационные ресурсы



ЗАЧЕМ ПРОВОДИТЬ АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

- понять как работает информационная система;
- понять насколько эффективна система защиты информации на текущий момент;
- выявить слабые места в системе защиты информации;
- выявить слабые места в процессах управления ИБ;
- наметить пути повышения уровня информационной защищенности компании.

ВОЗМОЖНЫЕ РЕЗУЛЬТАТЫ АУДИТА:

- Отчетный документ по результатам аналитического обследования информационных систем, содержащий описание технологических процессов обработки информации и схемы информационных потоков.
- Модели нарушителей и угроз информационной безопасности
- Техническое задание на систему защиты информации
- Комплект проектов организационно-распорядительных документов
- Заключение по результатам анализа защищенности

ЗАЧЕМ МОДЕЛИРОВАТЬ НАРУШИТЕЛЕЙ И УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ?

- ответить на вопрос «Кто враг?»;
- сделать предположение о том как «враг» будет нападать.

РЕЗУЛЬТАТЫ МОДЕЛИРОВАНИЯ

- модели нарушителей и угроз информационной безопасности.

ЗАЧЕМ ПРОЕКТИРОВАТЬ СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ?

- выстроить план обороны от «врага», начертить карту укреплений, препятствующих реализации его вероятных атак



РЕЗУЛЬТАТЫ ПРОЕКТИРОВАНИЯ:

- проект на систему защиты информации

ЗАЧЕМ ВНЕДРЯТЬ СИСТЕМУ ЗАЩИТЫ ИНФОРМАЦИИ?

- не стать жертвой первого встречного



РЕЗУЛЬТАТЫ ВНЕДРЕНИЯ:

- система защиты информации, внедренная в соответствии с требованиями проектной документации

ЗАЧЕМ АТТЕСТОВЫВАТЬ ИНФОРМАЦИОННУЮ СИСТЕМУ?

- не обмануться при внедрении системы защиты информации



ВОЗМОЖНЫЕ РЕЗУЛЬТАТЫ АТТЕСТАЦИИ:

- программа и методики оценочных испытаний;
- протокол оценочных испытаний;
- заключение по результатам оценки соответствия

ТАКТИКА ЗАЧЕМ ПРОВОДИТЬ АНАЛИЗ ЗАЩИЩЕННОСТИ И ПЕНТЕСТ?

- понять насколько эффективна система защиты здесь и сейчас;
- выявить слабые места в системе защиты информации.

ВОЗМОЖНЫЕ РЕЗУЛЬТАТЫ АУДИТА:

- Заключение по результатам анализа защищенности с рекомендациями по закрытию уязвимостей.

В РАМКАХ АУДИТА И КОНСАЛТИНГА ИБ «СТАНДАРТ БЕЗОПАСНОСТИ» ПРЕДОСТАВЛЯЕТ СЛЕДУЮЩИЕ УСЛУГИ:

- Аудит информационной безопасности по любым видам требований.
- Анализ защищенности и тестирование на проникновение (в том числе, согласно требованиям Стандарта PCI DSS)
- Разработка модели нарушителей и угроз.
- Разработка технического задания на систему защиты информации.
- Разработка технического проекта и рабочей документации на систему защиты информации.
- Внедрение и подготовка к сертификации Системы управления информационной безопасностью (СУИБ) в соответствии с требованиями международного стандарта ISO 27001.
- Внедрение отдельных процессов ИБ (передача знаний работникам Заказчика, демонстрация, наблюдение и контроль выполнения) и соответствующей административной документации.

ЧТО ТАКОЕ АТТЕСТАТ СООТВЕТСТВИЯ И ЗАЧЕМ ЭТО НУЖНО?

АТТЕСТАТ – это документ, который подтверждает, что автоматизированная информационная система соответствует требованиям безопасности информации, а также дает право определенное время обрабатывать конфиденциальную информацию.

Аттестат соответствия выдается сроком на 3 года, в течение которых должна быть обеспечена неизменность условий функционирования объекта и технологии обработки защищаемой информации.



АТТЕСТОВАТЬ ИНФОРМАЦИОННУЮ СИСТЕМУ НЕОБХОДИМО, ЕСЛИ:

- Информационная система является государственной или муниципальной на соответствие требованиям, утвержденным приказом ФСТЭК России от 11.02.2013 № 17;
- В ней обрабатываются сведения, составляющие государственную тайну
- В ней обрабатываются сведения, составляющие служебную тайну на соответствие требованиям нормативно-методического документа «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденного приказом Гостехкомиссии России от 30.08.2002 № 282.
- Аттестация автоматизированных информационных систем требуется для получения лицензии ФСТЭК России или ФСБ России.

УСЛУГИ УДОСТОВЕРЯЮЩЕГО ЦЕНТРА



Оформление и выдача квалифицированного сертификата электронной подписи



Продажа сертифицированных ключевых носителей.



Продажа программного обеспечения для работы с электронной подписью.



Продажа средств криптографической защиты информации.



Организация защищенного канала связи на основе собственной сети VipNet.



Мы предоставляем организациям (юридическим лицам) услуги по изготовлению и сопровождению ключей электронной подписи пользователей информационных систем. Наш УЦ осуществляет и другие сервисные функции, связанные с использованием электронных подписей, шифрованием, обеспечением электронного юридически-значимого документооборота.

КТО МОЖЕТ ОБРАТИТЬСЯ В УДОСТОВЕРЯЮЩИЙ ЦЕНТР?

- Юридические лица и врачи для электронных больничных.
- Продавцы алкоголя, леса, меха для ЕГАИС
- Кадастровые инженеры для Росреестра
- Для регистрации кассы в ФНС
- Предпринимателю для регистрации ЮЛ и ИП
- Директору ТСЖ, ЖСК и УК для ГИС ЖКХ
- Для регистрации недвижимости в Росреестре

ДЛЯ ЧЕГО?

Для работы на сервисах:

- Госуслуги
- nalog.ru
- ЕГАИС
- Росреестр
- ГИС ЖКХ
- Росимущество
- СМЭВ
- Для отчетности и документооборота
- и других сервисах

ПОЧЕМУ С НАШИМ УЦ ВЫГОДНО СОТРУДНИЧАТЬ?



У нас индивидуальный подход в зависимости от потребностей клиента.



Быстрота исполнения.



Мы оказываем техническую поддержку (установка и настройка ПО, сертификатов, браузеров для работы с электронной подписью на различных порталах.)



Надежность нашей подписи подтверждены соответствующими лицензиями и сертификатами.

КАКИЕ СИСТЕМЫ РАЗРАБАТЫВАЕТ И ВНЕДРЯЕТ «СТАНДАРТ БЕЗОПАСНОСТИ»:



Системы безопасности в т.ч.:

- Системы диспетчеризации инженерных систем зданий
- Системы охранного и технологического видеонаблюдения,
- Системы контроля и управления доступом,
- Системы охранной и/или пожарной сигнализации,
- Системы пожаротушения (ПТ) и системы автоматизации пожаротушения (АПТ).
- Системы дымоудаления,
- Системы охраны периметра,
- Системы оповещения и управления эвакуацией людей,
- Системы газоанализа промышленных и офисных помещений,
- Системы хранения ключей и ценностей,
- Интегрированные платформы для всех подсистем безопасности управления и фиксации событий.



Системы связи в т.ч.:

- Структурированные кабельные системы (СКС),
- Локальные вычислительные сети (ЛВС), в т.ч. сети беспроводной связи WiFi,
- Системы телефонной связи в аналоговом (TDM-телефония) или цифровом виде (IP-телефония),
- Системы видеоконференцсвязи (ВКС),
- Конгресс-системы,



Системы звукоусиления, звуковоспроизведения и звукозаписи



Системы электроснабжения и освещения зданий и сооружений



Системы кондиционирования (бытовые и полупромышленные системы)

КАКИЕ ВИДЫ РАБОТ ВЫПОЛНЯЕТ СТАНДАРТ БЕЗОПАСНОСТИ В СФЕРЕ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ БЕЗОПАСНОСТИ И ПОСТРОЕНИЯ ИНЖЕНЕРНЫХ СИСТЕМ ЗДАНИЙ И СООРУЖЕНИЙ?

ПРЕДПРОЕКТНОЕ ОБСЛЕДОВАНИЕ, В Т.Ч.:



- анализ текущего состояния инженерных систем,
- разработка эскизных вариантов построения инженерных систем,
- составление ведомостей объемов работ;



РАЗРАБОТКА ПРОЕКТНО-СМЕТНОЙ ДОКУМЕНТАЦИИ, В Т.Ч.:

- подготовка проектной документации,
- подготовка рабочей документации,
- подготовка сметной документации по сборникам Росстроя;

СТРОИТЕЛЬНО-МОНТАЖНЫЕ РАБОТЫ, В Т.Ч.:



- монтаж инженерных систем,
- авторский надзор в процессе монтажа систем,
- оформление разрешительных документов в процессе монтажа (акты входного контроля, скрытых работ, ведомости смонтированного оборудования и пр.);



ПУСКО-НАЛАДОЧНЫЕ РАБОТЫ, В Т.Ч.:

- разработка программ пуско-наладочных работ,
- разработка программ-методик испытаний инженерных систем, выполнение пуско-наладочных работ,
- оформление разрешительных документов в процессе наладки,
- сдача инженерных систем в эксплуатацию Заказчику.



ИНЖЕНЕРНЫЕ СИСТЕМЫ ЗДАНИЙ И СООРУЖЕНИЙ ДЛЯ ЧЕГО НУЖНА СИСТЕМА ДИСПЕТЧЕРИЗАЦИИ?



для оперативного контроля и управления различными инженерными системами здания или площадки, такими как: вентиляция, теплоснабжение, электроснабжение, водоснабжение и т.п.;



для организации единого центра контроля и управления всеми инженерными системами здания и площадки в реальном времени;



упрощает эксплуатацию инженерных систем, т.к. предоставляет возможность: анализа загрузки оборудования систем; планирования профилактических и ремонтных работ; автоматизации реакции систем в нештатных ситуациях и т.п.;



повышает эффективность использования энергоресурсов



сокращает расходы на эксплуатацию инженерных систем за счет более эффективного использования обслуживающего персонала;



повышает безопасность функционирования инженерных систем;



уменьшает риски появления нештатных ситуаций при работе инженерных систем;

НАША КВАЛИФИКАЦИЯ В ОБЛАСТИ ИНЖЕНЕРНЫХ СИСТЕМ

КОМПАНИЯ ООО «СТАНДАРТ БЕЗОПАСНОСТИ» ЯВЛЯЕТСЯ СЕРТИФИЦИРОВАННЫМ ПАРТНЕРОМ:



компании **SIEMON**, статус «Certified Installer» (оборудование и решения для построения Структурированных Кабельных Систем); компания имеет в штате сертифицированных SIEMON специалистов Certified Designer/Installer;



компании **Panduit Corp.**, статус Silver Enterprise Structured Cabling Certified Company (оборудование и решения для построения Структурированных Кабельных Систем); компания имеет в штате сертифицированных Panduit Corp. специалистов Panduit Certified Technician;



компании **Тайле**, статус «Авторизированный Инсталлятор» (оборудование и решения для построения Структурированных Кабельных Систем); компания имеет в штате сертифицированных NIKOMAX специалистов по проектированию, монтажу и обслуживанию Структурированной кабельной системы NIKOMAX на основе МЕДНЫХ и ОПТИЧЕСКИХ РЕШЕНИЙ.



компании **Cisco Systems**, статус «Registered Partner» (оборудование и решения для построения сетей передачи данных с интеграцией услуг); компания имеет в штате сертифицированных Cisco Systems специалистов CCNA.



компании **Honeywell**, в области систем пожарной и охранной сигнализации, а также систем диспетчеризации зданий.

ЗАЩИТА СВЕДЕНИЙ СОДЕРЖАЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

Аттестация объектов информатизации (по требованиям ФСТЭК):

выделенных (защищаемых) помещений, автоматизированных рабочих мест (АРМ), автономных ПЭВМ, распределенных вычислительных сетей и телекоммуникационных систем; разработка программно-методического обеспечения для проведения аттестационных испытаний объектов информатизации;

Разработка технико-экономического обоснования необходимости создания систем защиты информации (СЗИ)

объектов информатизации, таких как выделенные помещения, автоматизированные рабочие места (АРМ), автономные ПЭВМ, распределенные вычислительные сети и телекоммуникационные системы; авторский надзор и методическое сопровождение реализации мероприятий, предусмотренных проектной документацией на объект информатизации в части СЗИ;

Организация специальных проверок (СП) и лабораторных специальных исследований (СИ)

Анализ существующей системы защиты государственной тайны и защиты информации в организации

проектирование и создание объектов информатизации любых классов защищенности от пространственно-распределенных вычислительных сетей (в том числе ЗЛВС) до выделенных помещений (зданий и объектов в информационно-защищенном исполнении), оснащенных системами видеотрансляции и звукоусиления;

Специальные исследования (СИ):

- побочные электромагнитные излучения и наводки (ПЭМИН);
- акустоэлектрические преобразования (АЭП);
- высокочастотное навязывание (ВЧН);
- высокочастотное облучение (ВЧО),
- закупка, установка и настройка систем вибро-акустической защиты (СВАЗ)

Закупка оборудования, монтаж и пусконаладочные работы по вводу в эксплуатацию системы защиты информации:

на базе генераторов шума сертифицированных по требованиям безопасности информации (ФСТЭК); поставка ПЭВМ в защищенном исполнении (закупка и доработка ПЭВМ) выдача открытой законодательной и нормативно-методической документации по защите государственной тайны и технической защите информации; разработка подготовительной аттестационной документации и выдача самого аттестата.

закупка, установка и настройка систем защиты ПЭВМ от несанкционированного доступа к информации; различные виды испытаний и исследований каналов утечки информации (защита от НСД) организация защиты информации в автоматизированных системах.

организация и выполнение проектных и строительно-монтажных работ для специальных объектов; оснащение объектов техническими системами; оценка эффективности средств защиты информации (СЗИ) выделенных помещений, автоматизированных рабочих мест (АРМ), распределенных вычислительных сетей и телекоммуникационных систем;

ПРОЕКТЫ, КОТОРЫМИ МЫ ГОРДИМСЯ:



Заказчик **Сбербанк:**

Монтаж и пуско-наладка одной из крупнейших систем контроля и управления доступом, создание рабочих мест локально-вычислительной сети



Заказчик **Федеральная служба по надзору в сфере транспорта:**

Разработка системного проекта развития ИТИ ЕАИС с учетом требований по информационной безопасности, создание и внедрение защищенной распределенной сети передачи данных масштабов всей страны



Заказчик **КБП имени Шипунова:**

Проектирование, монтаж, пуско-наладка интегрированных систем контроля и управления доступом, видеонаблюдения, ОПС, систем охраны периметра, автоматизации пожаротушения и вентиляции для крупных оборонных предприятий холдинга



Заказчик **Газпром:**

Разработка и реализация проектов обеспечения информационной безопасности предприятий, входящих в холдинг ОАО "Газпром", реализация комплексных проектов по защите информации, созданию защищаемых переговорных комнат.



Заказчик **Многофункциональный центр по Ярославской области:**

Централизованное внедрение систем защиты информации, комплексное построение распределенной защищенной сети передачи данных, сопровождение системы, а также постоянное решение трудновыполнимых.



Заказчик **Управление ЗАГС Правительства Ярославской области:**

Создание защищенной системы защиты информации областного масштаба, обслуживание системы Находка ЗАГС с организацией защищенного взаимодействия со сторонними организациями ПФР РФ, ФНС РФ, Органы социальной защиты населения, ТФОМС, УВД, УФМС, ФСБ и др. с использованием механизмов электронной подписи, защищенной сети передачи данных компании, запуски модулей взаимодействия со СМЭВ, разворачивание инфраструктуры для обеспечения работы ЕГР ЗАГС.



Департамент
здравоохранения
Ярославской области

Заказчик **Департамент здравоохранения Ярославской области:**

Проектирование и создание защищенной сети передачи данных областного масштаба для единой государственной системы здравоохранения Ярославской области, с учетом элементов межсетевого экранирования и сегментов объединения различных информационных систем здравоохранения, моделирование нарушителей и угроз безопасности для системы и ее элементов.

НАШИ ПРОЕКТЫ БЫЛИ УСПЕШНО РЕАЛИЗОВАНЫ У КЛИЕНТОВ:

Органы власти:

Мэрия города Ярославля, Органы государственной власти Ярославской области, Департамент здравоохранения (другие департаменты ЯО), Управление ЗАГС Правительства Ярославской области, Управление Министерства Юстиции по Ярославской области, Правительство Москвы, ГКУ ЦОДД Москвы, Федеральная служба по надзору в сфере транспорта, Министерство транспорта РФ, Федеральное агентство по Управлению имуществом РФ (Росимущество), Правительство Ханты-Мансийского автономного округа Югры, Многофункциональный центр по Ярославской области.

Силовые ведомства:

Управление ФСБ по Ярославской области и Костромской области, Управление федеральной службы исполнения наказаний по Ярославской и Костромской областям, Академия МЧС России, Управление Федеральной Миграционной службы по Ярославской, Костромской, Ивановской, Владимирской областям.

Предприятия нефте-газового сектора:

Газпром, ГК Газпромнефть (более 20 предприятий), Межрегионгаз по Ярославской области, Транснефть.

Частный бизнес:

Завод Алюмет, Медицинские учреждения.

Предприятия военно-промышленного комплекса:

Ростех, РТ-Информ, Высокоточные комплексы, Щегловский вал, КБП имени Шипунова, Тульский Оружейный Завод, ЦНИИАГ, Объединенная двигателестроительная корпорация, НПО Сатурн, Ярославский радиозавод, Ярославский судостроительный завод, Тулаоборонстрой, Роскосмос.

Учреждения здравоохранения:

Управления делами Президента РФ, Тверская медицинская академия, более 100 различных государственных учреждений здравоохранения в центральной России, ТФОМС Ярославской области, ТФОМС Костромской области.

Финансовый сектор:

Сбербанк России, Центробанк России, ряд банков входящих в топ-20 РФ.

А так же:

Ростовский кремль, Ярославский государственный университет (более 50 вузов по Российской Федерации), и более 1000 других уважаемых нами клиентов.

СПИСОК ЛИЦЕНЗИЙ СТАНДАРТ БЕЗОПАСНОСТИ

- На осуществление деятельности в области использования источников ионизирующего излучения (генерирующих) (за исключением случая, если эти источники используются в медицинской деятельности) Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека Лицензия № 76.01.10.002.Л.000001.03.16 от 10.03.2016 г.
- На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны Центр по лицензированию, сертификации и защите государственной тайны ФСБ России Лицензия ЛСЗ № 0098225 от 18 января 2017 года
- 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) Центр по лицензированию, сертификации и защите государственной тайны ФСБ России Лицензия ЛСЗ № 001438 от 31 января 2017 года.
- На деятельность по монтажу, техническому обслуживанию и ремонту средств обеспечения пожарной безопасности зданий и сооружений Министерство РФ по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий Лицензия № 76-Б/00096
- Телематические услуги связи Роскомнадзор Лицензия №83394 от 27 декабря 2015 года
- 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) Управление ФСБ России по Ярославской области Лицензия ЛСЗ № 0005612 от 6 декабря 2013 года
- На проведение работ, связанных с созданием средств защиты информации ФСТЭК России Лицензия № 2622 от 5 октября 2015 года
- На осуществление работ с использованием сведений, составляющих государственную тайну Управление ФСБ России по Ярославской области Лицензия №876 от 04 апреля 2014 года
На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны (в части технической защиты информации) ФСТЭК России Лицензия №2621 от 5 октября 2015 года

- На деятельность по технической защите конфиденциальной информации ФСТЭК России Лицензия №0814 от 5 мая 2009 года
- На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны Управление ФСБ России по Ярославской области Лицензия №996 от 19 августа 2016 года
- На осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны проведение специальных экспертиз предприятий, учреждений и организаций при их допуске к проведению работ с использованием сведений, составляющих государственную тайну Управление ФСБ России по Ярославской области Лицензия № 878 от 04 апреля 2014 года

Аттестаты и свидетельства:

- Сертификат, подтверждающий право на проектирование, монтаж и обслуживание СКС NIKOMAX с предоставлением системной гарантии от производителя сроком на 25 лет
- Свидетельство о допуске к определенному виду или видам работ которые оказывают влияние на безопасность объектов капитального строительства
- Членский билет ООО "Стандарт безопасности" Ярославской областной торгово-промышленной палаты и ТОРГОВО-ПРОМЫШЛЕННОЙ ПАЛАТЫ РОССИЙСКОЙ ФЕДЕРАЦИИ.
- Свидетельство о членстве Некоммерческого Партнерства содействия развитию информационной безопасности в организациях и предприятиях "Союз защитников информации»
- Свидетельство о членстве Ассоциации "Транспортная безопасность»
- Свидетельство об аккредитации организации на проведение оценки уязвимости объектов транспортной инфраструктуры и транспортных средств. Министерство транспорта РФ. Федеральное дорожное агентство (РОСАВТОДОР) № 0000197 от 24 апреля 2013 года.
- Свидетельство о допуске к определенному виду или видам работ, которые оказывают влияние на безопасность объектов капитального строительства
- Аттестат аккредитации органа по аттестации. ФСТЭК России Аттестат № СЗИ RU.2621.B259.499 от 29 октября 2012 года

ПОЛНЫЙ СПИСОК ЛИЦЕНЗИЙ НА САЙТЕ:
www.yarsec.ru/company/licenses/



ПОЧЕМУ СТАНДАРТ БЕЗОПАСНОСТИ?



Мы ведем честный и открытый диалог. У нас индивидуальный подход в зависимости от потребностей клиента.



Быстрота исполнения.



Мы несем ответственность за результат и оказываем техническую поддержку на всех этапах выполнения работ.



Высокоспециализированная экспертиза. У нас опытная команда имеющая многолетний опыт построения и эксплуатации инженерных систем.



Мы ценим уважение клиентов.

