

КАТАЛОГ УСЛУГ
компании «ИНФОРИОН»®
в области ИТ-управления
и информационной
безопасности



ОГЛАВЛЕНИЕ

О КОМПАНИИ	5
НАШИ КОНСУЛЬТАЦИОННЫЕ УСЛУГИ	6
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ	7
Комплексное обеспечение информационной безопасности	7
Консалтинг в области обеспечения информационной безопасности	7
Защита персональных данных	8
Аудит информационной безопасности	9
Разработка систем обеспечения информационной безопасности	10
Разработка пакета нормативных документов по обеспечению информационной безопасности	11
Аттестация объектов информатизации	11
Услуги для телекоммуникационных операторов	12
Частные решения по обеспечению информационной безопасности	13
Аутсорсинг информационной безопасности внешнего периметра клиента	14
Аудит (инвентаризация) корпоративных информационных ресурсов	15
Нагрузочное тестирование	16
Анализ коммуникативных связей	16
Защищенные терминальные решения	17

Тренинги по продуктам и технологиям обеспечения информационной безопасности	18
Поставка, пуско-наладка и сопровождение продуктов и систем обеспечения информационной безопасности	19
ПРОДУКТЫ	20
INFORION-NAG — программно-аппаратный комплекс генерации сетевого трафика, сетевых атак и нагрузочного тестирования приложений	20
INFORION-SNC — защита сетевых соединений в информационных системах компании SAP	21
INFORION-SSF — обеспечение информационной безопасности внутреннего документооборота	22
ИТ-КОНСАЛТИНГ	23
Оптимизация и реинжиниринг бизнес-процессов предприятия	23
Содействие в выборе, дизайне и внедрении информационных систем	24
Планирование проектов и управление проектами	25
Повышение эффективности ИТ	26
Сокращение затрат и повышение операционной эффективности	27
Аутсорсинг деятельности отделов развития	28
ПРОЕКТЫ	30
ЛИЦЕНЗИИ И СЕРТИФИКАТЫ	39





О КОМПАНИИ

Компания «ИНФОРИОН» ведет свою историю с 2003 года. Она была основана успешными менеджерами, построившими свою карьеру в телекоммуникационной отрасли. Компания специализируется на оказании услуг в области информационной безопасности, а так же ИТ управленческого консультирования.

Большой опыт накоплен экспертами «ИНФОРИОН» в области моделирования бизнес-процессов и проектного управления, а в области информационной безопасности мы имеем десятки успешно завершенных проектов, в т. ч. с использованием программных продуктов собственной разработки. Принципы нашей работы это: высокое качество предоставления услуг, конфиденциальность, послепроектная поддержка. Секрет успеха компании — индивидуальный подход к заказчику и динамические рабочие группы: мы подбираем для каждого проекта именно тот состав исполнителей, который необходим для качественного выполнения именно вашей задачи.

Мы не беремся за любую работу, мы предпочитаем сложные нестандартные задачи.

Мы не оказываем услуги абстрактному понятию ЗАКАЗЧИК, мы помогаем конкретным менеджерам предприятия-заказчика в решении стоящих перед ними задач или возникших в их деятельности проблем.

На счету компании «ИНФОРИОН» несколько десятков успешных проектов в Москве, Санкт-Петербурге, Нижнем Новгороде, Ростове-на-Дону, Самаре, Воронеже, Саратове, Ярославле, Калининграде, Иркутске, Челябинске, Екатеринбурге, Владивостоке, Южно-Сахалинске и других городах России.

Заказчиками «ИНФОРИОН» являются крупные корпоративные клиенты:

- телекоммуникационные компании;
- предприятия транспортной отрасли;
- предприятия промышленности;
- государственные организации;
- системные интеграторы;
- силовые структуры (подразделения Министерства обороны и ФСБ России).

В своей деятельности специалисты «ИНФОРИОН» руководствуются международными и отечественными стандартами и нормативными правовыми актами в области информационных технологий и обеспечения информационной безопасности.

«ИНФОРИОН» является партнером многих отечественных и зарубежных ИТ-компаний. Тесное взаимодействие с лидерами в области разработки и производства средств защиты информации, вычислительной техники, телекоммуникационного оборудования и программного обеспечения позволяет эффективно решать любые виды задач — от типовых до сложных, достигая при этом поставленных целей в кратчайшие сроки и по разумной цене. Предоставляя услуги в области ИТ, «ИНФОРИОН» сотрудничает с ведущими производителями, поставщиками и интеграторами, такими как: Компания Aladdin, Корпорация American Power Conversion (APC), Компания АХОFT, Компания «Инфосистемы Джет», Группа компаний «Marvel», Seagate Technology Incorporated (Сигейт Текнолоджи Инкорпорейтед), ЗАО «ВЕРИСЕЛ ПРОЕКТЫ», ЗАО «ДиалогНаука», ОАО «ИнфоТеКС» (Информационные Технологии и Коммуникационные Системы).



НАШИ КОНСУЛЬТАЦИОННЫЕ УСЛУГИ

Полный каталог услуг «ИНФОРИОН» охватывает большинство областей управленческого консалтинга, услуг в области информационной безопасности, ИТ-консалтинг, аутсорсинг ряда функций коммерческого предприятия и даже разработку программного обеспечения. Мы рады обсудить с нашими клиентами весь спектр наших возможностей. В данном каталоге мы сосредотачиваем внимание лишь на тех аспектах деятельности предприятия, которые связаны с информацией, методами ее управления, обработки и защиты. Мы готовы обсуждать эти услуги с нашими заказчиками и потенциальными клиентами из любых отраслей экономики.

Существуют десятки различных проблем, связанных с ведением бизнеса или управлением его информационными потоками. И соответственно существуют десятки методологий и инструментов, направленных на их решение. Что предлагаем мы? Мы предлагаем как диагностику проблем, так и подбор нужных методов их решения. Это очень важно — найти правильный инструмент; так же важно, как и подобрать людей, умеющих им пользоваться.

Независимо от того, представлена та или иная услуга в нашем каталоге или нет, мы готовы найти возможность ее оказания, так как обладаем большим аналитическим потенциалом и консультационным опытом. В любом случае вы можете быть уверены, что наш профессиональный подход гарантирует вам:

- полноценный анализ Вашей проблемы, включая идентификацию причин проблемы и наиболее вероятных рисков, связанных с ее наличием;
- предложение вариантов решения проблемы, включая оценку наиболее предпочтительных (наиболее экономичных или наиболее результативных);
- план дальнейшей работы.

В обязательном порядке все наши предложения и рекомендации учитывают:

- влияние стратегии компании на ее деятельность и обратное влияние деятельности на реализацию стратегии;
- финансовые возможности компании, в том числе необходимость вести бизнес рационально и экономно;
- ориентацию любой коммерческой деятельности на клиента/потребителя;
- качество продукции/услуг предприятия, как фактор его конкурентоспособности.

Мы всегда стараемся понять ваше предприятие изнутри, так как даже самые лучшие советы и методики не смогут принести пользу, если не будут грамотно адаптированы к вашей ситуации.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Комплексное обеспечение информационной безопасности

Предоставляя весь комплекс услуг в области информационной безопасности, мы определяем для себя стратегические направления, представляющие обоюдный интерес как для нашей компании (с точки зрения развития бизнеса), так и для наших заказчиков (с точки зрения максимального удовлетворения их текущих и перспективных потребностей):

- разработка и внедрение комплексных промышленных систем обеспечения и управления информационной безопасностью;
- разработка и внедрение процессов управления безопасностью как составной части управления комплексом информационных технологий предприятия;
- обеспечение информационной безопасности корпоративных информационных систем;
- поддержка систем обеспечения информационной безопасности.

Консалтинг в области обеспечения информационной безопасности

Квалификация и опыт работы в области информационной безопасности сотрудников «ИНФОРИОН» позволяют предложить нашим заказчикам профессиональный консалтинг в области обеспечения информационной безопасности, в том числе:

- анализ, расследование инцидентов информационной безопасности;
- выделение специалистов компании в рабочие группы проектов заказчика в области обеспечения информационной безопасности;
- выполнение технико-экономического анализа продуктов и систем обеспечения информационной безопасности;
- разработку методик проведения обследований и анализа защищенности;
- разработку каталога услуг информационной безопасности для телекоммуникационных операторов;
- разработку рекомендаций по защите отдельной информационной системы;
- разработку процедур (регламентов) информационной безопасности;
- разработку требований информационной безопасности в процессах управления информационными технологиями;
- разработку специальных требований для создания комплексной системы технической защиты информации;
- разработку технического задания на создание системы обеспечения информационной безопасности;



- тестирование различного рода оборудования и программного обеспечения, организация тестовых зон для испытаний и отработки технологий в области создания средств и систем защиты информации, а так же защищенных средств и систем обработки и передачи информации;
- составление аналитического обзора продуктов информационной безопасности по критериям заказчика;
- разработку квалификационных требований к сотрудникам службы информационной безопасности;
- проведение научно-исследовательских работ в области защиты информации;
- разработку пакета нормативных документов по обеспечению информационной безопасности в компании.

Консалтинг помогает быстро и эффективно удовлетворить потребности наших заказчиков и их клиентов в решении вопросов обеспечения информационной безопасности при планировании развития корпоративных сетей и информационных систем, разработки стратегий развития и при решении других сложных вопросов обеспечения информационной безопасности.

Защита персональных данных

Действующим законодательством Российской Федерации предусмотрена обязательная защита персональных данных, как отдельной категории конфиденциальной информации, затрагивающей интересы личности (субъектов персональных данных). Федеральный закон от 27 июля 2007 г. № 152-ФЗ «О персональных данных» гласит, что основной целью при обработке персональных данных является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну; при этом статья 19 указанного закона определяет, что оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

Вопросам защиты персональных данных в России уделяется все больше внимания. С принятием пакета нормативно-правовых актов по защите персональных данных уполномоченный федеральный орган исполнительной власти по защите прав субъектов персональных данных (Роскомнадзор), а также федеральные органы исполнительной власти, уполномоченные в области обеспечения безопасности (ФСБ России) и в области противодействия техническим разведкам и технической защите информации (ФСТЭК России), обратили пристальное внимание на реализацию требований по обеспечению безопасности персональных данных и объявили об усилении контроля в данной сфере.

В связи с этим для государственных органов, муниципальных органов, юридических или физических лиц, организующих и (или) осуществляющих обработку персональных данных, а также определяющих цели и содержание обработки персональных данных (т.е. являющихся операторами персональных данных), сформировалась реальная и острая потребность в создании систем защиты персональных данных (СЗПДн) для

обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных (ИСПДн) и выполнения тем самым требований пакета соответствующих нормативно-правовых актов.

Мы готовы предоставить клиентам широкий спектр услуг в области обеспечения безопасности персональных данных — от классификации информационных систем персональных данных и выработки рекомендаций по выбору средств защиты информации до создания систем защиты персональных данных «под ключ».

Имея значительный опыт в области построения систем защиты персональных данных, специалисты «ИНФОРИОН»:

- максимально учтут особенности и возможности имеющихся у заказчика систем обеспечения информационной безопасности;
- подготовят рекомендации по оптимизации класса информационных систем персональных данных;
- помогут подобрать оптимальное решение для реализации системы защиты;
- обеспечат получение аттестата соответствия требованиям по безопасности информации;
- минимизируют финансовые и временные затраты.

Сотрудничая с «ИНФОРИОН», вы получите надежную и эффективную систему защиты персональных данных, тесно интегрированную с комплексной системой обеспечения информационной безопасности информации.

Аудит информационной безопасности

Целью проведения аудита (обследования) состояния безопасности корпоративных информационных систем и ИТ-инфраструктуры является определение текущего фактического уровня обеспечения информационной безопасности и его сравнение с декларируемым уровнем.

Обследование проводится в следующих случаях:

- анализ рисков с целью обоснования инвестиций в создание системы обеспечения информационной безопасности;
- анализ состояния информационной безопасности после внесения изменений в коммуникационную инфраструктуру, систему обеспечения информационной безопасности или информационные системы;
- периодический анализ состояния информационной безопасности;
- внеочередной анализ декларируемого и фактического уровня состояния информационной безопасности (при смене системных администраторов или администраторов безопасности, ключевых руководителей служб ИБ и ИТ, контроль состояния после разрешения инцидентов и других изменений в системах ИБ и ИТ);
- определение уязвимостей критических информационных систем или сервисов (например, путем выполнения теста на проникновение (penetration test), позволяющего определить потенциальные возможности злоумышленников по реализации несанкционированного доступа к ресурсам корпоративной сети через сеть Интернет или из внутреннего периметра сети);
- плановое обследование/самообследование организации с целью подтверждения соответствия требованиям отраслевых стандартов (например, PCI DSS);
- подготовка к созданию системы защиты персональных данных.



Опираясь на требования отечественных и международных стандартов и нормативных документов в области обеспечения информационной безопасности, наша компания разработала и успешно применяет собственную методику аудита информационной безопасности. Одним из ключевых подходов в предлагаемой методике является последовательное проведение структурного и функционального анализа, (на основе результатов инвентаризации ресурсов объекта обследования). Результаты, полученные при выполнении обследования, позволяют получить комплексную оценку уровня информационной безопасности объекта аудита, отражающую различия между декларируемым и фактическим состоянием ИБ.

Разработка систем обеспечения информационной безопасности

Система обеспечения информационной безопасности (СОИБ) является неотъемлемой частью любой корпоративной информационной системы (комплекса информационных систем). Чем выше роль и значимость информационных систем в деятельности компании, тем более жесткие требования должны предъявляться к системам обеспечения информационной безопасности.

Мы считаем, что в любой СОИБ главную роль выполняют люди, а это значит, что в основе СОИБ должны стоять правила и процедуры обеспечения безопасности и лишь потом технические средства, их реализующие. Таким образом, разрабатывая системы обеспечения информационной безопасности для наших заказчиков, мы гарантируем не только функционирование профессионально настроенных технических средств, но и работу сложного механизма «люди — процессы — информационные системы и сервисы — механизмы безопасности».



Разработка пакета нормативных документов по обеспечению информационной безопасности

В основе любой современной системы обеспечения информационной безопасности стоят не технические средства защиты информации, а правильно выстроенные процессы управления, документированные в политиках, правилах и процедурах, определяющие угрозы и риски, права и обязанности, ответственность должностных лиц и, собственно, порядок построения системы защиты и обеспечения безопасности в процессе всего жизненного цикла комплекса информационных систем. Технические средства в совокупности с деятельностью персонала всего лишь реализуют эти требования. Как показывает практика, надлежащий уровень информационной безопасности информационных систем определяется отнюдь не дорогим и многофункциональным оборудованием и ПО, а качеством функционирования развернутой системы организационно-нормативного обеспечения ИБ. Таким образом, построение эффективной подсистемы организационно-нормативного обеспечения как составной части СОИБ является залогом поддержания высокого уровня информационной безопасности.

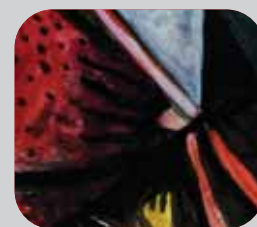
«ИНФОРИОН» предоставляет услуги по разработке нормативных документов процесса обеспечения информационной безопасности с учетом современных требований международных стандартов и успешных практик создания комплексных информационных систем и систем обеспечения информационной безопасности. В качестве типовых примеров можно указать такие документы, как:

- политики информационной безопасности, модели угроз, перечни сведений конфиденциального характера;
- специализированные политики информационной безопасности;
- правила и процедуры обеспечения информационной безопасности;
- инструкции и регламенты;
- Формализованные учетные и отчетные документы.

Аттестация объектов информатизации

Являясь лицензиатом ФСТЭК, «ИНФОРИОН» предлагает услуги по квалифицированному подтверждению соответствия объектов информатизации предъявляемым к ним требованиям по безопасности информации путем проведения аттестационных испытаний и выдачи аттестата соответствия. Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа — «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информатизации, утвержденных ФСТЭК (Гостехкомиссией) России. В качестве объектов информатизации рассматриваются предназначенные для обработки и передачи информации, подлежащей защите, автоматизированные системы различного уровня и назначения, системы связи, системы отображения и размножения документов вместе с помещениями, в которых они установлены и сами помещения, предназначенные для ведения конфиденциальных переговоров (в том числе информационные системы персональных данных).

Наличие на объекте действующего «Аттестата соответствия» дает право обработки информации с соответствующим уровнем секретности



(конфиденциальности) и на период времени, установленными в «Аттестате соответствия». Аттестация ОИ предшествует началу обработки подлежащей защите информации и вызвана необходимостью официального подтверждения эффективности комплекса используемых на конкретном ОИ мер и средств защиты информации.

Обязательной аттестации подлежат:

- объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров;
- объекты информатизации, в которых обрабатываются государственные информационные ресурсы;
- информационные системы персональных данных (в установленных случаях);
- ключевые системы информационной инфраструктуры.

После проведения аттестационных испытаний и выдачи аттестата соответствия «ИНФОРИОН» готов обеспечить сопровождение аттестованного объекта и в установленном порядке подтверждать действие аттестата при внесении изменений и расширении системы.

Услуги для телекоммуникационных операторов

Исторически компания «ИНФОРИОН» специализируется на предоставлении услуг по обеспечению информационной безопасности телекоммуникационным компаниям. В работе с операторами связи мы используем лучшие практики, которые основаны не только на действующих стандартах в области информационной безопасности, но и учитывают современные подходы к управлению информационными технологиями (ITSM), а так же процессам организации деятельности оператора (eTOM).

Для телекоммуникационных компаний мы предлагаем услуги ИБ, ориентированные как непосредственно на оператора связи, так и на их клиентов:

Информационная безопасность телекоммуникационного оператора

- защита персональных данных в информационных системах OSS/BSS;
- безопасность процессов управления (eTOM, ITSM);
- защита от DDoS атак;
- защита ИТ-инфраструктуры оператора;
- безопасность систем управления;
- нагрузочное тестирование.

Услуги информационной безопасности для клиентов оператора — от процессов до внедрения

- антивирус/антиспам;
- «родительский контроль»;
- «безопасный Интернет»;
- «дистанционная флешка».

Реализованные нами проекты для телекоммуникационных операторов представляют собой внушительный список. Вот лишь некоторые из них:

- аудит (в части защиты персональных данных) централизованной информационно-биллинговой системы и единой системы управления предприятием крупного телекоммуникационного оператора (МРК);
- создание системы защиты персональных данных биллинговой системы крупного телекоммуникационного оператора (МРК);
- разработка системы обеспечения информационной безопасности единого Интернет-портала самообслуживания абонентов телекоммуникационной компании (МРК);
- разработка системы обеспечения информационной безопасности центра обработки вызовов оператора связи (с учетом требований по защите персональных данных);
- разработка и развертывание подсистемы обеспечения информационной безопасности автоматизированной информационной системы сбора и анализа событий на сети компании-оператора магистральной сети связи;
- разработка политики информационной безопасности автоматизированной системы тарификации оператора магистральной сети связи;
- анализ предложения услуг информационной безопасности в массовых сегментах (анализ рынка услуг ИБ) в интересах федерального оператора связи;
- разработка системы обеспечения информационной безопасности ЦОД телекоммуникационной компании (системное и техническое проектирование);
- разработка подсистем обеспечения информационной безопасности для BSS-систем компании-оператора магистральной сети связи.

Частные решения по обеспечению информационной безопасности

Решение вопросов обеспечения информационной безопасности должно носить комплексный характер. Тем не менее, достаточно часто возникают потребности в быстром решении наиболее острых задач, связанных с обеспечением информационной безопасности. Кроме того, потребности в решении отдельных (частных) задач ИБ могут возникнуть при отсутствии достаточного финансирования для построения комплексной СОИБ либо при реализации поэтапного планового ввода в эксплуатацию информационных или телекоммуникационных систем, а так же при внесении изменений в конфигурацию существующих систем. В этих и других аналогичных ситуациях мы предлагаем своим заказчикам ряд частных решений:

- защита внешнего периметра сети (защита от угроз при подключении к сети Интернет);
- централизованная антивирусная защита;
- обеспечение информационной безопасности центров обработки данных;



- создание систем управления информационной безопасностью;
- развертывание виртуальных частных сетей (VPN);
- внедрение систем единого входа (SSO — single sign on);
- развертывание инфраструктуры PKI;
- аудит (обследование) состояния информационной безопасности подсистем безопасности и автоматизированных информационных систем;
- защита от спама и контентная фильтрация (в том числе услуга «Родительский контроль»);
- управление архивами электронных сообщений;
- обеспечение безопасности отдельных информационных систем и сервисов, а так же отдельных сетевых сегментов;
- настройка параметров безопасности активного сетевого оборудования широкого круга производителей.

Аутсорсинг информационной безопасности внешнего периметра клиента

Системы обеспечения информационной безопасности требуют постоянного контроля со стороны профессионального обслуживающего персонала (в ряде случаев — в режиме 24x7), периодического внесения изменений и выполнения прочих работ по сопровождению систем. В некоторых случаях с целью экономии затрат целесообразно рассмотреть возможность постановки услуг по обеспечению информационной безопасности на аутсорсинг у внешних организаций. Наша компания длительное время успешно предоставляет подобные услуги и имеет хорошо отработанные процедуры взаимодействия с заказчиком. Клиенты «ИНФОРИОН» имеют возможность сосредоточиться на ведении своей основной деятельности, в то время как опытные профессионалы возьмут на себя все тонкости и трудности управления информационной безопасностью. При этом сама система обеспечения информационной безопасности может территориально размещаться как у заказчика, так и на технологических площадках нашей компании.

При заказе услуги «Аутсорсинг информационной безопасности внешнего периметра» (обеспечение безопасности систем при их подключении к сети Интернет) заказчики, в зависимости от потребностей и технических условий, получают пакет услуг:

- развертывание системы безопасности (подсистема доступа, межсетевые экраны, системы обнаружения вторжений, средства организации VPN, антивирусные средства и т.п. — в соответствии с предъявляемыми требованиями);
- оперативное реагирование на возникающие сбои и нештатные ситуации (в т.ч. поддержка в режиме реального времени и выезд на территорию заказчика);
- внесение изменений в систему обеспечения информационной безопасности;
- разбор имевших место инцидентов и предоставление соответствующих отчетов;
- выдача рекомендаций для повышения уровня информационной безопасности по результатам анализа инцидентов, оценки активности пользователей и исследования информационных потоков.

Аудит (инвентаризация) корпоративных информационных ресурсов

В условиях современного рынка профессиональная организация информационной среды компании становится критическим фактором успешного ведения бизнеса. И многофакторная безопасность является одним из наиболее необходимых условий успешной организации этой среды.

Построение любой системы информационной безопасности должно начинаться с первичного аудита текущего состояния ИБ. Комплексный аудит ИБ включает в себя мероприятия по обследованию уровня безопасности информационных систем, проводимые в несколько последовательных этапов. Одним из ключевых этапов является инвентаризация информационных ресурсов (ИР) компании, в ходе которого определяются владельцы ИР, физические и логические «места» хранения ИР, степень конфиденциальности ресурсов.

Характерной чертой как для крупных организаций, так и для относительно небольших компаний, является отсутствие ярко выраженной структуры корпоративных ИР именно в плане конфиденциальности информации. По нашим наблюдениям очень часто в компаниях отсутствует (либо является не соответствующим действительности) перечень сведений конфиденциального характера. Зачастую без должного внимания остается весь информационный массив документов рядовых сотрудников, не входящих в руководство компании — их рабочие материалы, сообщения электронной почты, в которых могут содержаться сведения, подлежащие защите. Более того, свыше 80 % всех корпоративных информационных ресурсов являются неструктурированными — это информация в файлах, сообщениях электронной почты, заметках, докладах и планах, созданная в разных форматах и хранимая в разных системах. Данное обстоятельство указывает на необходимость проведения специального комплекса мероприятий — аудита ИР.

Мы предлагаем комплексное решение — аудит ИР, включающее в себя идентификацию, рубрикацию и категорирование корпоративных ИР. Наше решение основано на применении специализированных программных продуктов обработки разнородных информационных массивов. Реализованные в этих продуктах технологии позволяют проводить автоматизированную классификацию информационных массивов по тематическим группам (рубрикам). Причем, возможны как варианты детерминированной классификации (рубрикации по заранее определяемым темам), так и аналитические работы по выявлению структуры корпоративного контента.

После проведения аудита ИР заказчик получает полную картину внутренней структуры собственного корпоративного контента, рубрикатор контента, перечень категорий собственных ИР. Выявляются неясные конфиденциальные ИР. Оцениваются некоторые внутренние факторы, влияющие на модель угроз ИБ, например — низкая лояльность сотрудников. В случае, если аудит ИР проводился в рамках комплексного аудита ИБ, значительно повышается эффективность последнего.

По желанию заказчика применяемые при аудите ИР технические средства могут быть интегрированы в его ИТ-инфраструктуру в целях обеспечения управления корпоративными информационными ресурсами на уровне систем Knowledge Management.



Нагрузочное тестирование

Нагрузочное тестирование информационной системы предполагает целенаправленное формирование нагрузки на проверяемую ИС для качественной и количественной оценки функционирования самой системы, а также ее вспомогательных подсистем (в том числе и СОИБ).

Услуга нагрузочного тестирования предоставляется на основе применения аппаратно-программного комплекса собственной разработки INFORION-NAG. Более подробно об услуге нагрузочного тестирования и комплексе INFORION-NAG смотрите в разделе описаний продуктов компании «ИНФОРИОН».

Анализ коммуникативных связей

Компания «ИНФОРИОН» предлагает уникальную услугу на рынке информационной безопасности — анализ коммуникативных связей. Ее сутью является всесторонний анализ взаимодействия сотрудников компании между собой и с «внешними» субъектами, осуществляемого с использованием средств электронных коммуникаций. Цель такого анализа состоит в своевременном выявлении подозрительных связей на основе мониторинга данных об использовании сотрудниками коммуникационных сервисов (электронная почта, телефония, IM и др.).

Анализ коммуникативных связей позволит решать следующие задачи обеспечения безопасности деятельности организации:

- отслеживание устойчивых групп общения как между сотрудниками внутри организации, так и с посторонними лицами;
- выявление неформальных групп общения;
- выявление наиболее активных сотрудников и наиболее тесных (множественных) связей между ними;
- отслеживание взаимодействий конкретных абонентов и групп, отслеживание взаимодействий с конкретными абонентами/организациями/регионами;
- контроль взаимодействий с конкурирующими организациями;
- защита от инсайда;
- расследование инцидентов.

Дополнительно предлагаемый подход и программные средства, его реализующие, могут быть использованы для решения таких задач, как:

- анализ и оптимизация затрат на стационарную и мобильную телефонную связь;
- анализ текущей деятельности и загруженности сотрудников организации;
- временной мониторинг использования информационно-телекоммуникационных ресурсов.

Предлагаемая услуга может быть предоставлена как единовременно по запросу с применением наших технических средств, так и в форме поставки аппаратно-программного комплекса INFORION-VAT — полностью готового решения, адаптированного под задачи наших заказчиков.

В основу работы комплекса INFORION-VAT заложены интеллектуальные механизмы визуализации структурированной информации, которые позволяют выполнять агрегирование и отображение информации, полученной из различных источников (реляционных баз данных, структурированных файлов). Кроме функций визуализации используются наборы функций поиска информации, ее редактирования, формирования специ-

ализированных отчетов и синхронизации с источниками информации (в том числе и в режиме реального времени).

Услуга/продукт в первую очередь ориентированы на поддержку деятельности следующих потребителей:

- федеральные органы исполнительной власти, силовые и специальные ведомства;
- подразделения собственной безопасности банковских и коммерческих структур;
- подразделения безопасности телекоммуникационных операторов;
- подразделений информационной безопасности крупных компаний;
- подразделений, ответственных за деловую разведку (Business Intelligence) и конкурентную разведку (Competitive Intelligence).

Для анализа взаимодействия могут использоваться следующие источники данных и их комбинации:

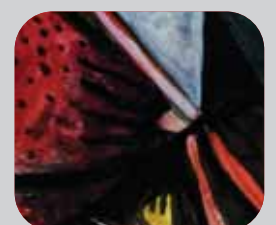
- биллинг операторов мобильной и фиксированной связи;
- биллинг корпоративных АТС (поддерживаются практически все современные станции);
- журналы регистрации событий средств защиты информации;
- журналы регистрации событий телекоммуникационных устройств;
- журналы регистрации событий почтовых серверов;
- информационные массивы (дампы) специализированных средств перехвата и анализа сетевого трафика;
- автоматизированный (операторский) ввод данных.

Для организаций, заинтересованных в анализе коммуникативных взаимосвязей, но не готовых приобрести комплекс INFORION-VAT, предлагается услуга по разовому или периодическому анализу данных и составлению заключения о существовании социальных групп и потенциальных возможностях нарушения информационной безопасности. Используя возможности комплекса, специалисты «ИНФОРИОН» готовы оказать поддержку при расследовании инцидента безопасности и сформировать элементы доказательной базы, а так же предоставить оперативный материал для профилактики подобных нарушений.

Защищенные терминальные решения

С ростом требований к системе обеспечения информационной безопасности сложность и стоимость ее обслуживания возрастает многократно. Количество инцидентов безопасности при этом растет, а эффективность реагирования на них снижается. Причинами этого является в том числе сложность эксплуатации средств защиты информации и их низкая интегрируемость в бизнес-приложения организации, что в частности может приводить к нарушению функционирования бизнес-процессов. Для уменьшения стоимости обслуживания информационных систем и повышения уровня безопасности организации, «ИНФОРИОН» предлагает использовать терминальные решения, которые, с одной стороны позволяют минимизировать расходы на СОИБ и ИТ-инфраструктуру в целом, с другой стороны — обеспечат высокий уровень защищенности информационных активов организации.

Использование терминальных решений возможно в организациях любого типа (государственные и муниципальные органы, банки,



промышленные предприятия, учебные заведения и др.); на базе таких решений может быть организована защита любой информации ограниченного доступа, будь то государственная тайна, коммерческая тайна или персональные данные.

Одним из несомненных преимуществ использования терминальных решений является сокращение расходов на содержание инфраструктуры. Стоимость эксплуатации одного рабочего места уменьшается на 35–50 %, как за счет низкой стоимости самого терминала, так и за счет отсутствия необходимости его обслуживания. В дальнейшем терминальные решения позволят:

- сократить расходы на электроэнергию (в среднем на 25–30 % в год);
- минимизировать затраты на покупку лицензий программного обеспечения (операционные системы, офисные приложения);
- минимизировать затраты на средства защиты, такие как антивирусы, персональные межсетевые экраны, локальные системы обнаружения вторжений, системы контроля внешних накопителей и портов, т.к. их не нужно устанавливать на рабочих местах.

С точки зрения безопасности терминальные решения имеют следующий ряд важных преимуществ:

- централизованное управление программными и аппаратными ресурсами, позволяющее в т.ч. ограничивать доступ к портам, принтерам и приложениям;
- строгая аутентификация пользователей на основе аппаратных ключей — безопасное и гибкое управления правами доступа к ресурсам организации;
- единая точка доступа к информационным ресурсам позволяет не только управлять, но и эффективно отслеживать злонамеренные действия и мгновенно реагировать на них;
- консолидация данных — информационные ресурсы организации хранятся исключительно на серверах;
- соответствие требованиям ФСТЭК — терминальные решения могут быть использованы в информационных системах персональных данных и системах, обрабатывающих информацию ограниченного доступа (конфиденциальная информация, государственная тайна) без использования дополнительных средств защиты на уровне автоматизированных рабочих мест.

Терминальные решения — это современный безопасный подход к построению ИТ-инфраструктуры организации, позволяющий сократить затраты на ИТ в целом и повысить качество предоставляемых сервисов без ущерба для производительности.

Тренинги по продуктам и технологиям обеспечения информационной безопасности

«ИНФОРИОН» успешно проводит обучение по технологиям и продуктам информационной безопасности. В настоящее время доступны следующие авторские курсы:

- «Управление информационной безопасностью информационных систем».

- «Обнаружение вторжений. Реагирование на инциденты информационной безопасности».
- «Межсетевое экранирование. Теория и практика защиты внешнего периметра».
- «Построение виртуальных частных сетей».
- «Обеспечение комплексной информационной безопасности информационных систем предприятия».
- «Антивирусная защита предприятий».
- «Современные сетевые технологии».
- «Сети TCP/IP».

Нами также предлагаются авторизованные авторские курсы по продуктам компании «Инфосистемы Джет»:

- «Администрирование межсетевого экрана Z2».
- «Администрирование комплекса кодирования межсетевых потоков «Тропа-Джет».
- «Администрирование системы мониторинга почтовых сообщений «Дозор-Джет».

Поставка, пуско-наладка и сопровождение продуктов и систем обеспечения информационной безопасности

Наша компания готова предложить широкий спектр оборудования и программного обеспечения, а также услуг по его пуско-наладке, поддержке и сервисному обслуживанию:

- поставка продуктов информационной безопасности (Aladdin, Cisco, Microsoft, Check Point, Symantec, Stonesoft и д.р.);
- установка, настройка и пуско-наладка средств защиты информации;
- сервисная поддержка продуктов и систем информационной безопасности.



ПРОДУКТЫ

INFORION-NAG — программно-аппаратный комплекс генерации сетевого трафика, сетевых атак и нагрузочного тестирования приложений



Компания «ИНФОРИОН» разработала программно-аппаратный комплекс генерации сетевого трафика, сетевых атак и нагрузочного тестирования приложений INFORION-NAG: Network Attack Generator.

Нагрузочное тестирование — это целенаправленное создание нагрузки на информационную систему для качественной и количественной оценки функционирования самой системы, а также ее вспомогательных подсистем (в том числе и СОИБ). В ходе тестирования система и/или ее подсистемы подвергаются различным нагрузкам, при этом целью такого тестирования является оценка способности объекта правильно функционировать не только при штатных нагрузках, но и при превышении их порогов, планируемых (наблюдаемых) при реальной эксплуатации. Такое тестирование позволяет убедиться, что система имеет определенный «запас прочности», а так же определить численные характеристики производительности (время отклика, число транзакций и пр.) и проверить эффективность работы механизмов безопасности.

Комплекс INFORION-NAG предоставляет возможности создания гибких сценариев тестирования, а именно:

- атаки и нагрузочные тесты могут выполняться одновременно с различными параметрами из разных сегментов сети;
- продолжительность выполнения каждой задачи может задаваться пользователем или зависеть от измеряемых параметров;
- для каждой выполняемой задачи можно получить статистику (например, количество переданных пакетов, количество успешных транзакций и т.п.);
- злонамеренная нагрузка имитируется несколькими видами распространенных атак типа flooding; кроме того, может быть выполнена имитация передачи вредоносного ПО (вирусов) по распространенным прикладным протоколам;
- легитимная нагрузка является эмуляцией деятельности пользователей и создается для следующего набора прикладных сетевых сервисов: SMTP (с возможностью включения в трафик спама и вирусов), FTP, HTTP, SMB, Microsoft SQL Server, Oracle SQL Server.

Проведение нагрузочного тестирования — это сложная организационно-техническая задача и один инструмент не может решить все потенциально возможные проблемы. Однако использование продукта INFORION-NAG обеспечивает максимально простое развертывание средств нагрузочного тестирования. Комплекс позволяет реализовы-

вать сложные стратегии контроля, пользуясь которыми регулярно, заказчик сможет получать ответы на такие вопросы, как:

- достаточно ли производительности используемой СОИБ для функционирования в условиях прогнозируемой нагрузки с должным уровнем обеспечения качества информационных сервисов? Достаточно ли производительность самих сервисов?
- как поведут себя в условиях обычных или распределенных атак отказа в обслуживании (DoS- и DDoS-атак) сетевые сервисы в целом и компоненты ИТ-инфраструктуры обеспечивающие их?
- правильно ли проведена настройка межсетевых экранов и средств обнаружения вторжений?
- с какой скоростью наполняются журналы регистрации событий средств СОИБ, операционных и информационных систем? Не приведет ли к отказу в обслуживании переполнение журналов событий? Есть ли необходимость в изменении правил протоколирования событий?
- успешно ли справляются со своими задачами антивирусные почтовые шлюзы и системы фильтрации спама?

Комплекс ориентирован на операторов связи, сервис-операторов, провайдеров услуг Интернет, производителей различного рода сетевого оборудования и промышленных комплексов, а также на все предприятия и организации, заинтересованные в проведении качественного исследования возможностей и защищенности ИТ-инфраструктуры.

Применение INFORION-NAG в качестве инструментального средства при проведении периодического аудита корпоративной ИТ-инфраструктуры позволит повысить уровень обеспечения информационной безопасности и непрерывности бизнеса.

Более подробную информацию о продукте, его технических характеристиках, особенностях применения можно получить на сайте нашей компании и у специалистов «ИНФОРИОН».

INFORION-SNC — защита сетевых соединений в информационных системах компании SAP

INFORION-SNC — программный продукт обеспечения защиты информации, обрабатываемой в системах SAP/R3. В основу программного продукта положена технология Secure Network Communication компании SAP AG, а в качестве криптопровайдера используется ядро «КриптоПро CSP», прошедшее сертификацию в ФСБ России.

Применение INFORION-SNC позволит существенно расширить базовые возможности обеспечения безопасности, присутствующие в стандартной поставке SAP-систем за счет реализации трех уровней защиты, определяемых технологией SNC:

- аутентификация — по терминологии SAP — «authentication only», минимальный уровень защиты, при котором выполняется только идентификация партнеров по взаимодействию, а защита данных не предусматривается;
- обеспечение целостности — возможность обнаружить изменение данных, которое может возникнуть при их передаче по каналу



связи, предполагает предварительное выполнение процедуры аутентификации;

- обеспечение конфиденциальности — шифрование сообщений как мера противодействия прослушиванию канала связи, предполагает выполнение процедуры аутентификации и гарантию целостности.

Более подробную информацию о продукте, его технических характеристиках, особенностях применения можно получить на сайте нашей компании.

INFORION-SSF — обеспечение информационной безопасности внутреннего документооборота



ИНФОРИОН разработал программный продукт INFORION-SSF, предназначенный для обеспечения информационной безопасности внутреннего электронного документооборота в системах SAP R3. Он соответствует требованиям, предъявляемым компанией SAP AG к программным продуктам такого типа.

В основу программного продукта положена технология Secure Store and Forward (SSF) компании SAP AG, а в качестве криптопровайдера используется ядро «КриптоПро CSP» от компании «Крипто-Про». Также доступна версия продукта, предназначенная для применения совместно с криптопровайдером VipNet-Криптосервис компании «Инфотекс».

Использование механизмов защиты SSF в приложениях SAP позволяет заменить обмен печатными документами, подписанными ручной подписью, на автоматизированный процесс безопасного электронного документооборота.

INFORION-SSF выступает как программная «обертка» прикладных данных в решениях SAP и может применяться в различных сценариях для защиты данных и документов с использованием механизмов на основе сертификатов X.509 и электронной цифровой подписи:

- идентификация пользователей и процессов систем документооборота;
- электронная цифровая подпись прикладных данных, обрабатываемых в решениях SAP;
- хранение данных в защищенном формате;
- защищенная передача данных через публичные сети;
- гарантирование аутентичности и целостности данных.

Более подробную информацию о продукте, его технических характеристиках, особенностях применения можно получить на сайте нашей компании.

ИТ-КОНСАЛТИНГ

Оптимизация и реинжиниринг бизнес-процессов предприятия

Как мы понимаем проблемы:

- отсутствие четкой картины разделения ответственности, недостатки в системе оценки (KPI) и мотивации труда;
- стихийный инжиниринг деятельности и взаимодействия подразделений;
- жесткие линейно-функциональные организационные структуры, тормозящие процессы принятия решений и затрудняющие движение технологического документооборота;
- недостатки процессной ориентации в организации работы компании;
- проблемы в автоматизации информационных и документарных потоков;
- недостаточное понимание сотрудниками миссии и стратегии компании, а также их реализации на операционном уровне;
- отсутствие единой методологии описания бизнес-процессов у оператора препятствует их системному анализу и повышению эффективности их функционирования.

Способы решения:

- анализ, моделирование и реинжиниринг бизнес-процессов на основе лучшего мирового опыта, а также с использованием отраслевых рекомендаций и таксономий;
- коррекция взаимосвязи маркетинговой стратегии с операционными и функциональными стратегиями;
- проведение анализа декомпозиции целей/задач и распределения ответственности между подразделениями оператора связи;
- проведение учебно-консультационных семинаров по моделированию процессов и процессному подходу;
- оптимизация процессов: устранение дублирования, простоев, лишних функций, автоматизация, тренинг, мотивация, поиск способов снижения стоимости отдельных участков;
- разработка требований к автоматизации бизнес-процессов;
- сравнение ключевых KPI компании со значениями лучших компаний целевой индустрии;
- использование знаний и опыта наших экспертов.

Мы работаем в любых нотациях (IDEF_x, DFD, EPC) и с любыми программными продуктами моделирования процессов.



Полный системный анализ перед внедрением информационной системы (ИС):

- Определение состава задач, которые должны быть решены ИС.
- Разработка концепции автоматизации, проведение НИР и изысканий в предметной области.
- Определение правил, ограничений, накладываемых на состав требований к ИС.
- Систематизация требований к ИС, снятие противоречий.
- Анализ требований на полноту и осуществимость.
- Определение приоритетов и возможной последовательности реализации требований.
- Оценка вариантов реализации.
- Спецификация требований к системам.

Выгоды для клиентов:

- построение прозрачной картины бизнес-процессов компании, сравнение с лучшим опытом, поиск возможностей для оптимизации и реинжиниринга;
- снижение стоимости и ресурсоемкости в реализации ключевых процессов, достижение установленных показателей производительности;
- повышение ответственности и мотивированности участников процесса;
- автоматизация процессов — как способ повышения их эффективности;
- внедрение единого стандарта описания бизнес-процессов, переход к использованию отраслевых таксономий;
- рост уровня информированности и вовлеченности сотрудников в достижение стратегических целей компании, оптимизация системы мотивации;
- повышение операционной эффективности работы компании за счет улучшения взаимодействия различных отделов;
- оптимизация организационной структуры.

Содействие в выборе, дизайне и внедрении информационных систем

Как мы понимаем проблемы:

- сотрудники не могут четко сформулировать требования к информационным системам или программному обеспечению, которые нужны им для продуктивной работы;
- обилие на рынке вендоров, предлагающих системы с идентичными возможностями, затрудняет выбор автоматизированной системы, оптимальной для конкретного телекоммуникационного оператора;
- модели ценообразования, которые диктует вендор системы, не всегда соответствуют ожиданиям заказчика и планам развития его бизнеса;
- у штатных сотрудников оператора связи не хватает квалификации для полноценного технико-экономического обоснования масштабных ИТ-проектов;
- любое внедрение, независимо от размера задачи, выливается в десятки-сотни тысяч долларов.

Способы решения:

- формирование технических, функциональных и бизнес-требований (ОТТ, ЧТТ, ТЗ) к информационным системам;
- создание RFI и RFP¹;
- поддержка заказчика при организации конкурсов и тендеров. Независимая экспертиза систем и решений, представленных на конкурс;

¹Request for Information — запрос на предоставление детальной информации о системе, Request for Proposal — запрос на подготовку коммерческого предложения.

- привлечение к конкурсу лучших поставщиков мирового рынка программного обеспечения и решений для бизнеса телекоммуникаций и сферы высоких технологий;
- рекомендации по выбору системы с учетом требований заказчика к системе, техническим ограничениям и бюджету;
- технико-экономическое обоснование ИТ-проектов.

Выгоды для Вас и Вашего бизнеса:

- автоматизация начинает работать на бизнес, а не бизнес на автоматизацию;
- точное формулирование потребностей заказчика к критически важным для его бизнеса информационным системам;
- независимая экспертиза и объективная оценка сильных и слабых сторон вендоров программного обеспечения и решений;
- рекомендации по лицензионной политике;
- выбор системы, наиболее полно отвечающей бизнес-требованиям, техническим ограничениям и бюджету заказчика;
- прогноз выгод от реализации системы в соотношении с затратами на ее внедрение и эксплуатацию;
- усиление команды внедренцев в сложных проектах.

Планирование проектов и управление проектами

Как мы понимаем проблемы:

- существующие проекты не укладываются в расчетные значения Времени, Бюджета или Качества полученных результатов;
- технико-экономическое обоснование проектов не выполняется;
- низкий уровень практического использования знаний в области проектного управления (Project Management);
- не разработано положение/методика о проектном управлении. Проектная деятельность в компании не отделена от регулярных функциональных обязанностей сотрудников;
- недостаток проектных менеджеров в компании;
- отсутствие авторитета у назначенных проектных менеджеров;
- на создание проектного офиса, как инструмента обеспечения проектного управления, не хватает средств.

Способы решения:

- исполнение функций проектного офиса;
- создание проектных планов: Устав Проекта, График Проекта, WBS и RBS², Бюджет проекта, план управления рисками проекта и т.д;
- предоставление услуг проектного менеджера;
- обучение/создание методических материалов в области проектного управления;
- контроль качества проектов: точечный, фазовый, непрерывный;
- аудит проектов. Восстановление проектов;
- разработка методики (положения) о проектном управлении;
- разработка плана управления рисками.

¹WBS — структурное описание работ по проекту,
RBS — структурное описание планируемых результатов проекта.



Выгоды для Вас и Вашего бизнеса:

- повышение отдачи/результативности проектной деятельности: с нужным качеством, в срок, в рамках бюджета;
- привлечение экспертизы в нужном объеме и в нужное время;
- сокращение затрат на управление проектами;
- передача рутинных/разовых функций в аутсорсинг;
- project quality review — анализ качества проектов, в том числе объективная оценка хода проектных работ и качества полученных результатов;
- восстановление/завершение проектов;
- создание документации по проекту;
- осознание рисков проекта и наличие плана управления рисками.

Повышение эффективности ИТ

Как мы понимаем проблемы:

- отдел ИТ нацелен на автоматизацию, а не на повышение эффективности бизнеса;
- отдел ИТ загружен на 100 %, но бизнес не видит от него отдачи;
- бизнес «перерос» используемые в настоящее время информационные системы, и (или) ИТ не обеспечивают необходимой поддержки бизнес-процессов;
- необходимо уменьшить стоимость владения ИТ или наоборот требуется спланировать инвестиции в ИТ;
- необходимо оценить выгоды и возможности, связанные с аутсорсингом ИТ;
- проекты, осуществляемые в сфере ИТ, не дают ожидаемых выгод и преимуществ либо выполняются с превышением сроков или перерасходом бюджета;
- стратегия в области ИТ не связана с бизнес — целями компании;
- бизнес не может сформулировать потребности на языке ИТ;
- пользователи отмечают случаи потери файлов, почты; наблюдается простой серверов, сбои в работе приложений.

Способы решения:

- разработка ИТ-стратегии;
- оценка уровня зрелости приложений и технологий;
- управление ИТ-проектами и управление изменениями;
- поддержка внедрения (контроль качества, концептуальный дизайн);
- анализ расходов на ИТ, анализ организации работы ИТ (ITIL), анализ эффективности управления ИТ (CobIT);
- управление затратами и оптимизация затрат, создание моделей затрат;
- моделирование экономических выгод и моделирование рентабельности инвестиций (ROI);
- формирование обоснованных ожиданий бизнеса от ИТ;
- обучение;

- разработка бизнес-обоснования и соглашения об уровне обслуживания (SLA, OLA);
- Разработка стратегии ИТ-безопасности;
- управление угрозами и областями уязвимости. Реагирование на кризисные и чрезвычайные ситуации в сфере ИТ-безопасности.

Выгоды для Вас и Вашего бизнеса:

- обеспечение наиболее полного соответствия между ИТ и бизнесом, демонстрация возможной отдачи от ИТ;
- возможность сократить ненужные расходы, сохранив при этом способность ИТ поддерживать стратегию бизнеса, потребности операционной деятельности и бизнес-процессов, а также соблюдение нормативно-правовых требований;
- возможность поддерживать динамичные стратегии в области бизнеса, внедрять гибкие стратегические информационные системы в запланированные сроки и без превышения бюджета, а также добиваться реализации выгод и преимуществ, являющихся значимыми с коммерческой точки зрения.

Сокращение затрат и повышение операционной эффективности

Как мы понимаем проблемы:

- высокие операционные затраты на оказание услуг или выпуск продукции;
- отсутствует понимание в каких областях деятельности предприятия возможны оптимизация и сокращение;
- планирующиеся сокращения не увязаны с изменением процессной карты компании;
- искажение реальной картины эффективности деятельности предприятия из-за ошибок в распределении затрат между функциями или подразделениями компании;
- необходимо сокращаться. С чего начать?
- нет понимания какая деятельность может и должна быть передана в аутсорсинг.
- постоянный дефицит кадров, в том числе высококвалифицированных специалистов, привел к операционным проблемам и системному кризису.

Способы решения:

- комплексный анализ проблем заказчика, построение дерева причинно-следственных связей;
- activity Based Costing — анализ затрат через призму процессов и операций в компании;
- revenue Maximizer/Cost Minimizer — специальные инструменты и методологии, направленные на сокращение издержек в компании;
- анализ возможностей для аутсорсинга и общих центров обслуживания;



Перед началом любого проекта в области аутсорсинга мы проводим предварительное обследование с целью разработки плана работ отдела развития на ближайший год

- реанимация/замораживание незавершенных проектов;
- изменение процессов с целью снижения квалификационных требований к исполнителям;
- benchmarking относительно аналогичных предприятий вашей индустрии;
- реинжиниринг процессов, направленный на повышение их результативности или снижение затрат на их поддержание.

Выгоды для Вас и Вашего бизнеса:

- сокращение затрат, упрощение процессов;
- восстановление деятельности в критически важных областях;
- оптимизация деятельности предприятия (функции, процессы, организационная структура), как результат — экономия;
- приоритезация усилий в области совершенствования деятельности предприятия;
- передача непрофильной или эпизодической работы в аутсорсинг;
- финансово-экономическое обоснование текущих проектов, инициатив, направлений деятельности.

Аутсорсинг деятельности отделов развития

Как мы понимаем проблемы:

- отделы развития, сертификации или управления бизнес-процессами не выполняют своей основной роли: повышение эффективности работы компании, повышение прозрачности управления, оптимизация организационно-штатной структуры;
- отделы развития действуют реактивно, т.е. реагируют на процессные проблемы только тогда, когда проблема не может быть решена линейными или функциональными руководителями;
- отделы развития могут описать ситуацию «As Is» (как есть), но не в состоянии предложить модель «To Be» (как должно быть);
- сертификация деятельности компании согласно стандартам качества управления (ISO 9000) не приносит ожидаемого результата в повышении эффективности работы подразделений;
- для успешной деятельности отдела требуются дорогостоящие аналитики в различных функциональных областях. Содержание узких аналитиков в штате компании нерационально. По этой причине отделы, в лучшем случае, укомплектованы техническими писателями;
- отделы развития должны тесно сотрудничать с ИТ, но, как правило, говорят с ИТ на разных языках;
- сотрудники отдела должны постоянно проходить обучение, в то время как потребность в их знаниях является эпизодической.

Предложение компании Инфорион:

- передать деятельность отдела развития в аутсорсинг;

Мы готовы рассмотреть различные формы аутсорсинга: от аутстаффинга (сдача персонала в аренду) до абонентского обслуживания компании-заказчика. Возможны любые комбинации

количества штатных сотрудников компании с объемом услуг, оказываемых со стороны Инфорион.

- передать в аутсорсинг отдельные проекты или задания: разработка инструкций, дизайн новых процессов, аудит процессов, разработка положений подразделений, построение функционального дерева компании, сертификация на ISO 9000;

Выгоды для Вас и Вашего бизнеса:

- сокращение расходов на содержание отдела развития;
- повышение качества работ, выполняемых в области процессного и функционального управления;
- доступность узкоспециализированных аналитиков по любой функциональной области заказчика;
- динамическое управление нагрузкой на отдел развития: мы готовы подключить к разовой работе столько специалистов, сколько нужно для выполнения Вашей задачи;
- тесная интеграция процессного управления и Информационных Технологий;
- повышение управляемости компании в целом.



ПРОЕКТЫ

Предлагаем ознакомиться с краткой информацией о наиболее интересных и значимых проектах, выполненных командой «ИНФОРИОН».

Создание узлов подключения к сети Интернет-вещания федеральной телерадиокомпании. Системное проектирование

Системный проект по созданию узлов подключения к сети Интернет-вещания телерадиокомпании федерального уровня выполнен в сотрудничестве с ведущим оператором связи и ориентирован на построение корпоративной информационной сети Дирекции Интернет-вещания за счет подключения к существующему сегменту двадцати региональных телерадиокомпаний. На базе единого варианта построения типового узла подключения регионального отделения ТРК к сети Интернет-вещания решены вопросы формирования архитектуры сети, выбора каналов и технологий связи, обеспечения информационной безопасности и поддержки функций распространения телевизионного контента по каналам сети Интернет в горизонте планирования до трех лет.

Аудит информационной безопасности вычислительного центра федерального министерства

Вычислительный центр — ведущая организация по эксплуатации всех информационных и телекоммуникационных систем федерального министерства. Аудит информационной безопасности ЛВС выполнен в целях поиска и анализа недостатков и уязвимостей, снижающих общий уровень информационной безопасности локальной вычислительной сети. В полной мере анализу были подвергнуты все элементы сетевой инфраструктуры, в т.ч. телекоммуникационное оборудование и сети передачи данных, вычислительные средства и периферийные устройства, информационные системы и сервисы, вспомогательные средства и системы жизнеобеспечения. Детально исследован процесс организации защиты информации в ЛВС, в т.ч. его документационное обеспечение. Выводы, подготовленные по результатам обследования, позволили определить основные вектора развития системы обеспечения информационной безопасности и перечень экспресс-мер, требующих немедленной реализации.

Аудит информационно-телекоммуникационной инфраструктуры международного аэропорта (г. Москва)

Цель проекта — определение основных направлений совершенствования и развития телекоммуникационной подсистемы и подсистем голосовой связи информационно-телекоммуникационной инфраструктуры (ИТИ).

В ходе выполнения проекта по аудиту ИТИ крупного транспортного предприятия с численностью персонала более чем 2500 человек нашей компанией применен современный подход к определению требуемых мощностей инфраструктуры на основе методологии ITIL.

На основе рекомендаций ITIL (SD/Capacity Management) нами была разработана собственная методика (бизнес-требования — информационный системы — требования к сервисам ИТИ — ресурсы ИТИ) определения требуемых мощностей инфотелекоммуникационной инфраструктуры исходя из требований бизнеса. Это позволило во-первых, определить текущие мощности инфраструктуры, а во-вторых, оценить их соответствия требованиям бизнес-процессов предприятия. Проведенный анализ помог сформулировать рекомендации относительно основных направлений развития и инвестиций в информационно-телекоммуникационную инфраструктуру в средне- и долгосрочной перспективе.

Помимо решения основной задачи по оценке соответствия мощностей инфотелекоммуникационной инфраструктуры требованиям бизнес-процессов нам удалось достичь еще одного важного результата: знания в области современных информационных технологий помогли нашим инженерам выявить недостатки сетевой архитектуры заказчика, указав при этом существующие «узкие места» и возможности более рационального использования оборудования. Практические рекомендации по оптимизации построения корпоративной сети позволили существенно повысить пропускную способность ее отдельных участков.

Система обеспечения информационной безопасности комплексной автоматизированной системы обеспечения управления и организации деятельности территориальной инспекции федерального надзорного органа. Техническое проектирование и внедрение

Основной задачей работы по созданию системы обеспечения информационной безопасности КСОУ территориальной инспекции федерального надзорного органа являлась разработка эффективного комплексного решения по защите информации, отвечающего соответствующим требованиям Федеральной службы по техническому и экспортному контролю. Специалистам нашей компании удалось реализовать успешный проект по защите территориально-распределенной сети на уровне субъекта Российской Федерации — г. Москвы. Разработанные решения основаны на применении широкого круга отечественных и зарубежных СЗИ успешно прошли экспертизу во ФСТЭК России, реализованы в масштабе всей системы защиты и применяются длительное время, полностью отвечая предъявляемым требованиям.



Система обеспечения информационной безопасности ЦОД телекоммуникационной компании МРК. Техническое проектирование

В техническом проекте системы обеспечения информационной безопасности крупного московского оператора связи воплотились концептуальные положения, выработанные на стадии системного проектирования. В рамках выполнения комплекса проектно-исследовательских работ были разработаны и обоснованы технические решения по основным сервисам информационной безопасности перспективной СОИБ ЦОД. В основу указанных решений положены лучшие программно-аппаратные средства лидеров отрасли, что обусловлено тесной связью механизмов обеспечения ИБ с технологией обслуживания абонентов. Параллельно с техническим проектированием СОИБ решен ряд вспомогательных задач, в частности — выработаны предложения по услугам ИБ, предоставляемым абонентам, проведено тестирование высокопроизводительной системы контентной фильтрации. Силами инженеров ИНФОРИОНа оперативно решена проблема борьбы со спамом в клиентском сегменте сети доступа оператора и обеспечена стабильная работа электронно-почтовой системы ISP.

Помимо технических вопросов проектная документация позволила сформировать нормативную основу организации процесса обеспечения ИБ ЦОД: были разработаны требования ИБ к процессу управления инцидентами, процедуры организации процесса обеспечения ИБ ЦОД в нотации ARIS, частные политики ИБ информационных систем ЦОД, регламенты ТО СЗИ в составе СОИБ, инструкции персоналу различных категорий.

Тест на проникновение в отношении внешней границы корпоративной ИТ-инфраструктуры регионального процессингового центра

Узкоспециализированный проект «Тест на проникновение» — это реализация пожелания заказчика, крупного регионального процессингового центра, проверить надежность защиты внешнего периметра корпоративной сети и оперативность реагирования на инциденты собственной команды администраторов безопасности. Имея в своем распоряжении в качестве исходных данных только наименование организации, являвшейся целью управляемого penetration test, специалисты «ИНФОРИОН», имитируя действия группы злоумышленников, с помощью специальных инструментальных средств и технологий выполнили сбор необходимой информации о сетевой инфраструктуре и провели ряд мероприятий, направленных на преодоление систем безопасности внешнего периметра. В ходе выполнения теста на проникновение вскрыты незначительные недостатки в организации защиты границы корпоративной сети, однако в целом принятые на ней меры обеспечения ИБ показали достаточную эффективность.

По согласованию с заказчиком был проведен экспресс-анализ безопасности операционного раздела web-сайта. Для этого специалистам «ИНФОРИОН» были выданы необходимые реквизиты доступа, по которым был осуществлен переход в требуемую зону и пробный запуск программных модулей, поддерживающих выполнение операций с пластиковыми картами. При этом на вход программных модулей подавались параметры, предположительно способные вызвать нарушения работо-

способности информационной системы вплоть до эскалации прав нарушителя в ней. Данные попытки не имели результата вследствие наличия в программном обеспечении операционного раздела механизмов фильтрации передаваемых параметров, эффективность которых была подтверждена в ходе обследования.

Аудит информационных систем персональных данных российского представительства иностранной торговой компании

«ИНФОРИОН» совместно с партнером — известным российским интегратором IBS Platformix выполнил аудит информационных систем персональных данных российского представительства иностранной торговой компании. В ходе выполнения работ был проведен детальный анализ исходных данных по системам, на основании которого заказчик получил пакет рекомендаций по созданию СЗПДн с учетом имеющихся мер по защите информации и оптимального выбора средств защиты. Особенностью выполнения проекта являлась необходимость получения взаимоувязанных решений, основанных как на требованиях по обеспечению информационной безопасности со стороны головной международной компании, так и на требованиях отечественных государственных регуляторов. Проект перешел на следующую стадию работ — разработку и внедрению СЗПДн с аттестацией объектов информатизации.

Разработка документов верхнего уровня организационно-нормативной базы перспективной системы обеспечения информационной безопасности оптовой генерирующей компании

Качественно и в срок специалистами «ИНФОРИОН» завершен проект по разработке документов верхнего уровня организационно-нормативной базы перспективной подсистемы обеспечения информационной безопасности единой информационной системы одной из оптовых генерирующих компаний электроэнергетики.

В результате выполнения комплекса работ сформирована организационно-нормативная основа для внедрения современных процессов обеспечения информационной безопасности и построения перспективной СОИБ ЕИС ОГК. Пакет разработанных на основе современных требований документов представлен:

- политикой информационной безопасности единой информационной системы ОГК;
- общими техническими требованиями к средствам информационных технологий и системе обеспечения информационной безопасности единой информационной системы ОГК;
- архитектурой перспективной системы обеспечения информационной безопасности единой информационной системы ОГК.

Эти документы — нормативный фундамент для безопасного развития корпоративной ИТ-инфраструктуры и бизнеса заказчика.



Исследование и разработка механизмов обеспечения информационной безопасности сетей подвижной связи третьего поколения. Научно-исследовательская работа

Объектом исследования в работе являлись сети подвижной связи третьего поколения (сети связи 3G). Цель работы состояла в проведении анализа используемых в сетях связи 3G механизмов обеспечения информационной безопасности, методов и средств защиты информации, анализе нормативно-правовой базы по обеспечению информационной безопасности в сетях сотовой связи, исследовании угроз информационной безопасности сетей связи третьего поколения (в том числе с определением и классификацией нарушителей), выработке требований к информационной безопасности сетей связи 3G с учетом специфики угроз и различных групп нарушителей.

В процессе выполнения работы проведен анализ технических решений по построению сетей связи UMTS и CDMA2000, организации механизмов обеспечения их информационной безопасности, а так же нормативной и технической документации по вопросам защиты информации в сетях подвижной связи.

В результате исследования осуществлен комплексный анализ вопросов обеспечения защиты информации в сетях связи третьего поколения. На основе проведенных исследований сформулированы общие принципы обеспечения информационной безопасности сетей связи 3G.

Аудит информационной безопасности автоматизированной системы управленческого документооборота сетевой компании электроэнергетики

Наша компания успешно выполнила аудит информационной безопасности автоматизированной системы управленческого документооборота крупной энергетической компании. Реализация проекта позволила получить консолидированную картину обеспечения защиты информации в одной из ключевых информационных систем крупнейшей отраслевой компании.

Аудит затронул все аспекты обеспечения информационной безопасности АСУД, включая как организационные, так и технические меры по защите информации. В рамках обследования проанализирована нормативная база компании и процессы обеспечения информационной безопасности как на уровне АСУД, так и на уровне сети компании.

В фокусе аудита оказались и меры по защите информации в АСУД, реализуемые программно-техническими средствами. Для оценки уровня защищенности системы глубокому анализу подверглась ее архитектура и особенности применения встроенных механизмов информационной безопасности, а так же порядок использования специализированных средств защиты информации.

По результатам аудита руководство заказчика получило объективную оценку защищенности АСУД и пакет практических рекомендаций по повышению уровня ее информационной безопасности.

**Система обеспечения информационной безопасности
Единого Интернет-портала самообслуживания абонентов
телекоммуникационной компании (МРК).
Техническое проектирование**

Расширение спектра предоставляемых оператором связи услуг, рост абонентской базы и наращивание каналов взаимодействия с клиентами требует внедрения в ИТ-инфраструктуру телекоммуникационной компании новых информационных систем, которые требуют пристального внимания с точки зрения обеспечения информационной безопасности. В рамках проектирования СОИБ для порталного решения одной из МРК специалистами «ИНФОРИОН» проведен широкий комплекс работ, включающий глубокий анализ объекта защиты с точки зрения изучения его особенностей, построение модели нарушителя и перечня угроз информационной безопасности, формирование схемы информационных потоков и собственно выработку технических решений. В качестве основы для построения СОИБ избрана хорошо зарекомендовавшая себя в аналогичных проектах концепция периметров информационной безопасности. Требования к сервисам ИБ в каждом периметре реализованы с помощью программных и аппаратных средств ведущих мировых производителей. Кроме того, задействованы функции безопасности интеграционной платформы, что является важным фактором с точки зрения построения эшелонированной обороны. В качестве организационно-распорядительной платформы СОИБ разработана частная политика ИБ защищаемой информационной системы, базирующаяся на положениях существующей концепции информационной безопасности и интегрированная в нормативную базу компании.

Аудит информационной безопасности программного обеспечения информационно-аналитической системы поддержки принятия решений и разработка рекомендаций по безопасному внедрению системы

Аудит информационной безопасности программного обеспечения информационно-аналитической системы, разработанной одной из российских компаний, выполнялся с целью поиска участков кода, потенциально небезопасных с точки зрения реализации направленно-деструктивных воздействий со стороны нарушителя ИБ. На основании разработанной специалистами «ИНФОРИОН» оригинальной методики контроля были проведены испытания системы, автоматизированный и экспертный анализ исходного кода ИАС. В ходе проведенных мероприятий выявлены фрагменты программного кода, требующие принятия мер по приведению его в безопасное состояние. Соответствующие рекомендации представлены заказчику в итоговом отчете. Там же приведены рекомендации по безопасным настройкам операционных систем и прикладных серверов ИАС. Помимо анализа кода подготовлены рекомендации по безопасному внедрению информационно-аналитической системы с точки зрения развертывания «традиционных» механизмов безопасности на базе СЗИ (архитектура СОИБ). Разработана и передана заказчику типовая частная политика информационной безопасности ИАС, освещающая основные организационные вопросы обеспечения ИБ системы и процедуры безопасности, связанные с ее



эксплуатацией. Проведен консалтинг по вопросу разграничения ответственности на различных этапах внедрения системы.

Система обеспечения информационной безопасности центра обработки вызовов телекоммуникационного оператора (МРК). Техническое проектирование

Объектом защиты в данном проекте выступала одна из центральных систем OSS/BSS. Помимо значительного масштаба этой информационной системы (большое количество разнообразного сложного оборудования и приложений, несколько сотен пользователей, наличие удаленных технологических площадок, значительная сетевая инфраструктура) важное значение с точки зрения проектирования системы безопасности играло то обстоятельство, что в системе планировалось обрабатывать персональные данные (ПДн). Эта особенность задала основной вектор проектирования СОИБ: ввиду наличия требований к обеспечению информационной безопасности (ИБ) системы в целом и требований к защите ПДн в составе СОИБ, разрабатывается система защиты персональных данных (СЗПДн). При этом соблюдаются все требования законодательства по защите ПДн.

Проектирование СОИБ велось с учетом наличия в ней СЗПДн, а так же принципа «СОИБ — для защиты ИС в целом, СЗПДн — для защиты ИСПДн, сформированной в составе ИС».

Были выполнены все необходимые работы, предписанные методическими документами регуляторов, в частности — закрепление перечня ПДн и правовых оснований для их обработки, разработка частной модели угроз и классификация ИСПДн, подготовка пакета нормативных документов. Разработаны две группы технических решений по обеспечению ИБ: первая группа решений ориентировалась на защиту центрального ядра системы и головного филиала, вторая — на защиту типового регионального филиала (их в структуре бизнеса насчитывается девять).

Знание существующей у заказчика системы мер по защите информации позволило использовать уже имеющиеся СЗИ и нормативные документы во вновь создаваемой системе безопасности.

Технический проект СОИБ/СЗПДн успешно прошел экспертизу в независимой организации, аккредитованной ФСТЭК в качестве аттестационного центра, где была подтверждена правильность выбранных проектных решений.

Комплексный аудит службы информационных технологий предприятия пищевой отрасли

Работы по комплексному аудиту службы информационных технологий выполнялись для решения следующих задач: содействие ИТ-команде предприятия в стратегическом планировании, анализ ИТ-потенциала предприятия в портфеле ИТ-проектов управляющего холдинга, поиск альтернативных путей развития ИТ с учетом курса на экономию затрат, рассмотрение возможностей для ИТ-аутсорсинга, оценка предстоящих инвестиций.

Работы выполнялись в рамках отдельных потоков: аудит ожиданий бизнес-пользователей, аудит ИТ-инфраструктуры, аудит архитектуры программного обеспечения, аудит ИТ-персонала и руководства ИТ, аудит процессов ИТ, аудит безопасности.

В ходе выполнения обследования выявлен значительный потенциал развития и оптимизации ИТ на предприятии.

Результаты аудита приведены в финальном отчете, который включает: описание целей и задач, которые ставит бизнес перед ИТ на ближайшие 1–3 года, заключение по возможностям ИТ-инфраструктуры/архитектуры, перспективам и целесообразности развития существующих ИТ-систем, заключение по ИТ-персоналу и управлению информационными технологиями на предприятии, текущие риски бизнеса, связанные с состоянием ИТ, возможные сценарии развития ИТ-службы в целом, в том числе включая возможности управляющего холдинга, укрупненный план ключевых мероприятий в области ИТ на период 1–3 года, рекомендации по улучшению и инжинирингу ИТ-процессов.

Подсистема обеспечения информационной безопасности автоматизированной информационной системы учета сетевых ресурсов компании-оператора магистральной сети связи. Технорабочее проектирование и внедрение


«ИНФОРИОН» выполнил техническое и рабочее проектирование подсистем обеспечения информационной безопасности автоматизированной информационной системы учета сетевых ресурсов компании-оператора магистральной сети связи и автоматизированной информационной системы сбора и анализа событий на сети компании-оператора МСС.

В ходе проектирования проведен анализ объектов защиты и выполнена разработка технических решений, направленных на противодействие угрозам информационной безопасности в рамках широкого спектра сервисов ИБ. Разработана необходимая эксплуатационная документация. Ряд решений по подсистемам обеспечения информационной безопасности потребовал разработки дополнительных оригинальных средств автоматизации работы администратора безопасности. На основе проектных документов осуществлено успешное внедрение и запуск подсистем обеспечения информационной безопасности, проведено обучение эксплуатирующего персонала.

Предпроектное обследование (аудит) информационных систем персональных данных окружного медицинского учреждения

Очередной (но не рядовой) проект в области защиты персональных данных — обследование ИСПДн медицинского учреждения — успешно завершён выпуском пакета документов: отчета об аудите (с набором рекомендаций и требований), перечней персональных данных, частных моделей угроз, актов классификации, ТЗ на создание перспективных СЗПДн. Особенность проекта — принадлежность обследуемых систем к высшему классу ИСПДн–К1, а так же уникальная специфика медицинского учреждения — деятельность в области донорства крови и ее компонентов. Наряду с решениями технических вопросов экспертная





группа «ИНФОРИОН» подготовила большое количество предложений по организационным мерам, направленным на выполнение требований действующего законодательства в области обеспечения безопасности персональных данных. Ведется работа по проектированию систем защиты персональных данных, подготовке организационно-распорядительных документов, развертыванию СЗПДн и аттестации объектов информатизации.

Обследование информационных систем персональных данных телекоммуникационной компании МРК.

Проектирование системы защиты информации централизованной информационно-биллинговой системы.

В рамках реализации стратегии обеспечения ИБ телекоммуникационной компании проведено предпроектное обследование информационных систем персональных данных уровня OSS/BSS (информационно-биллинговая система, система управления предприятием, система эксплуатационной поддержки сетей связи, система учета договоров). Проведен всесторонний анализ и выработаны предложения по реализации систем безопасности, в т.ч. — систем защиты персональных данных. Подготовлены первичные документы по организации обработки ПДн.

В ходе технического проектирования разработаны соответствующие решения по защите информации в информационно-биллинговой системе. Особенностью разработки является одновременное проектирование и механизмов безопасности, ориентированных на защиту сведений, составляющих коммерческую тайну, и системы защиты персональных данных. В последнем случае технические решения базируются как на применении классических «наложенных» сертифицированных средств защиты, так и на сертификации основного ПО системы по требованиям безопасности информации. Такой подход позволяет заказчику выбрать наиболее рациональный вариант реализации СЗПДн по таким критериям, как «стоимость», «период развертывания», «удобство эксплуатации», «производительность». Одновременно с технической документацией разработан полный пакет внутренних документов (около тридцати единиц) по организации обработки и защиты персональных данных в компании.

Разработанный «ИНФОРИОН» технический проект системы защиты персональных данных ключевой OSS-системы крупного оператора связи успешно прошел независимую экспертизу, которая была предусмотрена контрактом на выполнение работ. Заключение, полученное по результатам анализа разработанных технических решений, свидетельствует о возможности аттестации защищаемой ИСПДн по требованиям безопасности информации при условии реализации системы защиты согласно разработанного технического проекта.

ЛИЦЕНЗИИ И СЕРТИФИКАТЫ

Для осуществления своей деятельности компания «ИНФОРИОН» обладает всеми необходимыми лицензиями:

- Лицензия ФСТЭК России № 0502 от 25 июня 2009 г. на деятельность по разработке и(или) производству средств защиты конфиденциальной информации.
- Лицензия ФСТЭК России № 0836 от от 25 июня 2009 г. на деятельность по технической защите конфиденциальной информации.
- Лицензия ФСБ России №14927 от 12.08.2009 г. на осуществление работ, связанных с использованием сведений, составляющих государственную тайну.
- Лицензия ФСБ России №8489П от 03 марта 2010 г. на осуществление разработки, производства шифровальных (криптографических) средств, защищенных с использованием шифровальных (криптографических) средств информационных и телекоммуникационных систем.
- Лицензия ФСБ России №8491Р от 03 марта 2010 г. на осуществление распространения шифровальных (криптографических) средств.
- Лицензия ФСБ России №8490Х от 03 марта 2010 г. на осуществление технического обслуживания шифровальных (криптографических) средств.
- Лицензия ФСБ России №8492У от 03 марта 2010 г. на осуществление предоставления услуг в области шифрования информации.
- Сертификат соответствия № ГО00.RU.1313.P00175 (система добровольной сертификации «ГАЗПРОМСЕРТ») на проектирование, установку, пусконаладочные работы и техническое обслуживание средств защиты информации, в том числе информационных систем в защищенном исполнении.



