



## Валерий ПУСТАРНАКОВ: «В условиях жесткой конкуренции необходимо постоянно развиваться»

Основа безопасности любого предприятия — профессионализм команды, которая эту безопасность обеспечивает. Компания «Газинформсервис», системный интегратор и разработчик средств защиты информации, по праву гордится своими компетенциями в области систем безопасности и информационных технологий, значительной научно-технической базой и богатым опытом реализации ответственных проектов. Клиентами компании являются многие крупные предприятия по всей России. О бизнесе компании, актуальных задачах в области обеспечения информационной безопасности и путях их решения мы беседуем с генеральным директором ООО «Газинформсервис» Валерием Федоровичем ПУСТАРНАКОВЫМ.

– Компания «Газинформсервис» была основана в 2004 г., но очевидно, что она имеет более глубокие «исторические корни». Какова предыстория основания компании? Что послужило мотивом для ее создания, какие задачи стояли перед командой вновь образованной компании?

– Ядро нынешней компании «Газинформсервис» сформировалось еще в 90-х гг. прошлого века на базе профессорско-преподавательского состава ВКА им. А.Ф. Можайского. Группа специалистов в области информационных технологий и информационной безопасности, в том числе и я, несколько лет работала единой командой во ФГУП «Желдоринформзащита». Спустя некоторое время, поняв актуальность и перспективность развития направления информационной безопасности, мы решили создать свою компанию, которая будет заниматься этими вопросами.

Первоначально деятельность компании включала в себя три основных направления: информа-

ционную безопасность, инженерно-технические средства охраны и удостоверяющий центр. Одновременно начались работы по созданию собственных программных продуктов. Свидетельством востребованности и успешности наших решений, а также подтверждением высокого уровня компетенции «Газинформсервис» стало сотрудничество с ОАО «Газпром».

Одним словом, становление компании происходило поэтапно и в соответствии с развитием потребностей предприятий ОАО «Газпром» в обеспечении информационной безопасности в рамках комплексных целевых программ по обеспечению безопасности объектов ОАО «Газпром».

Впоследствии перед нами ставились новые, более сложные задачи, которые необходимо было решать, и именно это потребовало от нас разработки нового и эффективного подхода к информационной безопасности и повышению уровня компетенции сотрудников. К настоящему моменту общая численность

сотрудников превышает 500 человек, включая персонал филиалов.

– Каковы сегодня основные направления деятельности и ключевые компетенции компании? Насколько широк спектр выполняемых работ? Кто основные заказчики компании «Газинформсервис»?

– Хочется подчеркнуть, что на сегодняшний день бизнес компании сосредоточен на вопросах информационной безопасности, которая заключается в обеспечении надежной безотказной работы информационной инфраструктуры в условиях внешних воздействий и внутренних атак инсайдеров, а также расследование подобных инцидентов, защита конфиденциальной информации и т. д. В рамках этих направлений ведется весь перечень работ: выполнение НИОКР, разработка программного обеспечения, проектирование, внедрение, сопровождение, подготовка специалистов заказчика, а также участие в разработке нормативной документации.

Основу деятельности компании «Газинформсервис» составляют проектирование и внедрение систем как информационной, так и физической безопасности для достаточно крупных территориально распределенных компаний. Наши специалисты разрабатывают и внедряют наиболее передовые решения таких крупных западных вендоров, как Oracle, IBM, Symantec, Microsoft, Citrix, Cisco, VMware, Check Point и др.

Другими словами, деятельность «Газинформсервис» включает в себя весь комплекс услуг по обеспечению безопасности – это информационная безопасность, в том числе разработка средств защиты информации, физическая безопасность объектов, услуги удостоверяющего центра, испытательной лаборатории и услуги по обучению сотрудников служб безопасности наших клиентов.

Сегодня нашими заказчиками являются предприятия ТЭК, федеральные службы России, государственные учреждения, компании финансовой и банковской сферы, транспортной отрасли, промышленного сектора, телекоммуникационные компании, медицинские центры, электронные торговые площадки и проектные институты.

**– К настоящему времени «Газинформсервис» существенно расширил географию деятельности, создав несколько филиалов. Есть также несколько аффилированных компаний. Какими направлениями занимаются эти компании, какова их специализация?**

– Как я уже говорил, количество выполняемых проектов росло с каждым годом, что, несомненно, способствовало накоплению уникального опыта внедрения и сопровождения объектов защиты, в том числе находящихся на значительном удалении от базовой площадки в Санкт-Петербурге. Именно ввиду того, что большая часть наших объектов территориально находится слишком далеко от Санкт-Петербурга и разбросана по всей стране, возникла необходимость расширения собственного присутствия в регионах. Это потребовало создания региональных «точек роста» компании. На сегодняшний день это аффилированные компании: НОУ ДПО «Центр предпринимательских рисков» (Санкт-Петербург), ООО «Научно-испытательный институт систем обеспечения комплексной безопасности» (Москва), ООО «УЦСБ» (Екатеринбург), ООО «ИЦ РЕГИОНАЛЬНЫЕ СИСТЕМЫ» (Волгоград), а также филиалы в Москве, Новом Уренгое, Омске и Самаре.

**– Одним из направлений работы компании является удостоверяющий центр. Причем речь идет о расширенных сервисах УЦ (стало быть, только выдачей сертификатов работа УЦ не ограничивается). Что входит в перечень услуг удостоверяющего центра «Газинформсервис»?**

– Да, удостоверяющий центр сегодня – это одно из наиболее динамично развивающихся подразделений компании. УЦ «Газинформсервис» аккредитован на всех федеральных электронных

торговых площадках (РТС-Тендер, Сбербанк-АСТ, ЕЭТП Росэлторг, Заказ РФ, ММВБ), отобранных Минэкономразвития РФ в соответствии с законом № 94-ФЗ, входит в Ассоциацию электронных торговых площадок, аккредитован в качестве доверенного УЦ в ФНС, ПФР, ФСС, Росстате, зарегистрирован в Едином Государственном реестре уполномоченных лиц удостоверяющих центров (ЕГР), а также является доверенным для задач взаимодействия с органами исполнительной власти и органами местного самоуправления с использованием Интернета согласно постановлению Правительства РФ от 15 июня 2009 г. № 478. Конечно, в первую очередь УЦ оказывает стандартные услуги по изготовлению и обслуживанию сертификатов ключей электронной подписи для работы во множестве информационных систем, в области электронной торговли, государственного заказа и электронного документооборота с использованием инфраструктуры открытых ключей.

Но, как известно, в условиях жесткой конкуренции необходимо постоянно развиваться как в области собственных компетенций, так и за счет расширения «ассортиментного портфеля», а в случае УЦ – развития дополнительных сервисов.

Работая в этом направлении, компания «Газинформсервис» активно сотрудничает с ведущими разработчиками программного и аппаратного обеспечения в области криптографической защиты информации и использует его в своей деятельности для обеспечения конфиденциальности данных при их передаче по сетям общего пользования.

В настоящее время в УЦ «Газинформсервис» можно получить не только сертификаты ключей электронной цифровой подписи. УЦ оказывает консультации по участию в государственных закупках в форме электронных аукционов на большинстве электронных торговых площадок Российской Федерации, предоставляет оперативную информацию о проводимых и предстоящих аукционах, осуществляет сбор и проверку пакета документов для участия в электронных торгах. С недавнего времени УЦ «Газинформсервис» начал подключение к системам сдачи отчетности в

контролирующие органы в электронном виде по телекоммуникационным каналам связи. Проще говоря, теперь УЦ изготавливает сертификаты ключа подписи и для сдачи отчетности в электронном виде в ФНС, ПФР, ФСС и Росстат.

**– На недавнем семинаре, проведенном компанией «Газинформсервис», неоднократно поднимался вопрос о качестве услуг УЦ. Что ваша компания вкладывает в понятие «качество услуг удостоверяющего центра»?**

– В нашем понимании «качество услуг удостоверяющего центра» – это не только наличие определенного, регламентированного регулирующими органами набора услуг и товаров. Это касается и уровня сервисного обслуживания клиентов. И тут УЦ «Газинформсервис» имеет большие конкурентные преимущества по сравнению с прочими УЦ. Например, большое значение имеют оперативность и полнота оказания услуг, простота и легкость, доступность и широкий спектр консультаций. Приведу лишь некоторые из дополнительных сервисов, которые УЦ «Газинформсервис» активно внедряет и успешно развивает: принцип «одного окна», когда клиенту достаточно зайти на сайт УЦ, заполнить бланк заявления, где для удобства большая часть данных вносится автоматически, и принцип «одного визита» – клиенту достаточно один раз прийти с паспортом и доверенностью в офис УЦ, где в его присутствии сформируют ключи, сертификат ключа подписи и подготовят необходимый пакет документов в течение одного часа.

Другой показатель качества услуг – это, безусловно, полнота набора услуг. Например, для участия в электронных торгах наш УЦ предлагает сбор и проверку пакета документов, консультации и помощь в прохождении аккредитации на ЭТП, по участию в электронных торгах, поиск и подбор конкурсов по тематике клиента, помощь в получении банковских гарантий и финансового обеспечения.

Говоря о качестве услуг УЦ нельзя обойти понятие качества ЭЦП (или, в терминологии нового ФЗ-63, – Электронной подписи). Именно этот смысл мы прежде всего обсуждали на нашем семинаре.

Классически составляющими качества ЭЦП считают качество криптографических алгоритмов, длину криптографических ключей, защищенность ключевых носителей.

Наш УЦ, как я уже упоминал, прошел множество аккредитаций, таким образом подтвердив соответствие требованиям по качеству этих составляющих.

**– Многие компании, работающие в области информационной безопасности, заявляют о готовности предоставить решение по комплексной автоматизации процессов управления информационной безопасностью. Есть ли подобные предложения у вас? Что в данном случае стоит за словом «комплексная»?**

– Тенденции современного рынка требуют постоянного совершенствования и ускорения многих бизнес-

По своей сути КСЗИ – это совокупность организационных и инженерно-технических мероприятий, которые направлены на обеспечение безопасности информационной инфраструктуры автоматизированных систем.

Мы не только внедряем различные системы защиты информации, направленные на предотвращение угроз ИБ, но и занимаемся разработкой систем, обеспечивающих поддержку и автоматизацию деятельности сотрудников подразделений служб безопасности наших заказчиков.

В данном случае мы можем предложить порталные решения по автоматизации процессов управления информационной безопасностью и услуги по разработке организационно-распорядительной документации по ИБ в соответствии с требованиями

обеспечивают информационно-технологическую поддержку и контроль основных процессов управления ИБ за счет автоматизации деятельности подразделений ИБ, сбора и анализа информации о состоянии ИБ объектов предприятия и его филиалов. САПУИБ реализуется на основе порталного решения с использованием технологий Microsoft Office SharePoint.

Проще говоря, комплексный подход в нашем понимании – это внедрение технических мер защиты информации, с одной стороны, и обеспечение автоматизации на базе порталных решений Microsoft Office SharePoint – с другой. Такой подход позволяет ввести систему метрик по измерению эффективности процессов управления ИБ в компаниях-заказчиках, прогнозировать и обоснованно принимать решения по совершенствованию системы защиты в целом.

**– Многие специалисты утверждают, что основным источником утечек информации на предприятии являются умышленные или неумышленные действия собственного персонала. Какие решения по контролю персонала есть в арсенале вашей компании? Какие подходы вы предлагаете использовать для решения этого вопроса?**

– Я бы даже сказал, что сегодня инсайдерская угроза – самая актуальная проблема, которая решается прежде всего путем управления правами пользователей, что является важнейшим элементом корпоративной системы безопасности. До недавнего времени такое управление реализовывалось исключительно организационными мерами. Сегодня для решения задач управления и контроля доступа сотрудников к внутренним информационным и техническим ресурсам применяются DLP-системы. Под DLP-системой подразумевается автоматизированное средство, позволяющее распознавать и/или блокировать перемещение существенных объемов конфиденциальных данных за пределы защищаемой информационной системы по любым каналам, используемым в повседневной работе. Более того, в настоящее время DLP является самым быстрорастущим новым сегментом рынка ИБ.

Наша компания готова предложить DLP-решения, разработанные

**Мы особенно гордимся тем, что нам доверяют и поручают проводить работы ОАО «Газпром», а также регулирующие структуры в области информационной безопасности России, такие как ФСТЭК и ФСБ.**

процессов, что, в свою очередь, способствует стремительному развитию информационных технологий, обеспечивающих решение данных задач. С другой стороны, ежегодно возрастает количество угроз: это и вирусы, и сетевые атаки злоумышленников, и нарушения конфиденциальности информации внутри компании, приводящие к финансовым потерям, зачастую весьма серьезным. Решение вопросов защиты данных в современных информационных системах будет успешным только при условии реализации комплексного подхода к построению системы обеспечения безопасности информации. В силу этого одним из направлений деятельности нашей компании являются разработка и создание комплексных систем защиты информации (КСЗИ).

ми законодательства РФ и регулирующих органов в области ИБ.

Сегодня, в условиях нарастающей зависимости эффективного функционирования предприятия от ИТ-инфраструктуры, усиливаются требования по ИБ со стороны как международных стандартов (ISO/IEC 27001:2005, ISO/IEC-17999:2005) и нормативных актов (Sarbanes-Oxley Act, Basel II, PCI DSS, FISMA, GLBA и др.), так и российских (СТО БР ИББС-1.0-2006, Федеральный закон «О персональных данных» (№ 152-ФЗ), СТР-К, ГОСТ Р ИСО/МЭК 17799-2005), и необходимо иметь инструментарий в интересах системы управления информационной безопасностью предприятия.

Наши системы автоматизации процессов управления информационной безопасностью (САПУИБ)

на базе Symantec и других ведущих вендоров. Кроме того, мы предлагаем собственные решения для защиты от несанкционированного доступа к информационным ресурсам. В частности, СЗИ «Блокхост-сеть» позволяет контролировать и ограничивать доступ корпоративных пользователей к сетевым сервисам, устройствам печати и внешним носителям, в том числе USB-накопителям. Для мобильных пользователей (использующих в своей работе ноутбуки и хранящих на них конфиденциальную информацию) мы предлагаем продукт «Блокхост-МДЗ», в котором реализованы функции прозрачного шифрования системного и логических дисков, в том числе с использованием российских сертифицированных криптографических алгоритмов. Это поможет защитить мобильного пользователя от утечки информации даже в случае утери или кражи ноутбука.

**– «Газинформсервис» ведет разработку собственных программных продуктов. Какие это категории продуктов, для каких целей и каких категорий заказчиков они предназначены?**

– Я уже упоминал, что разработка собственных средств защиты информации является одним из основных направлений деятельности «Газинформсервис».

Сейчас разработка СЗИ ведется по трем направлениям: защита информации от несанкционированного доступа (НСД) – ТМ «Блокхост»; контроль сетевых устройств – ТМ «ЭФРОС»; контроль отсутствия недеklarированных возможностей (НДВ) – ТМ «IRIDA». В линейку «Блокхост» входят также разработанные нами информационные системы «Блокхост-АСЗП» – автоматизированная система заказа пропусков и «Блокхост-КСКПП» – комплекс средств контроля подъездных путей к охраняемым объектам.

Программные продукты и решения «Газинформсервис» имеют сертификаты ФСТЭК России и системы добровольной сертификации «Газпромсерт» и успешно используются в органах государственной власти, на предприятиях нефтегазодобывающей отрасли, в сфере образования и в коммерческих организациях.

**– В среде специалистов-«безопасников» известен афоризм:**

**«Безопасность удобной не бывает». Вы бы согласились с этим? Способно ли современное решение безопасности быть комфортным или незаметным для пользователя? Или оно неизбежно будет требовать от пользователей неких дополнительных усилий?**

– Безусловно, полностью незаметным для пользователя никакое современное решение по защите информации быть не может в принципе. Увы, за безопасность надо платить. Например, при двухфакторной аутентификации от пользователя будут требоваться введение дополнительного пароля и/или некоторые другие дополнительные манипуляции. Кроме того, любое СЗИ – это в первую очередь программное обеспечение, и естественно, при его запуске используются ресурсы самой рабочей станции, что может привести к некоторому замедлению работы компьютера при запуске различных сервисов. С другой стороны, удобство и комфортность в вопросе защиты информации в большей степени относятся к ориентированности компаний-разработчиков на клиентов, и тут еще предстоит много работы.

**– Представители компаний, как работающих на рынке информационной безопасности, так и имеющих собственные службы ИБ, нередко сетуют на сложность кадрового вопроса: молодые специалисты могут иметь неплохую теоретическую подготовку, но слабую практическую. Поэтому обучение и повышение квалификации специалистов – очень актуальная тема. Может ли «Газинформсервис» как-либо помочь другим организациям в деле обучения специалистов?**

– Конечно, эта проблема существует. В нашей компании для решения этой проблемы применяются технологии дистанционного обучения. Специально созданное подразделение занимается разработкой комплектов учебно-методических материалов для дистанционного обучения по информационной безопасности и комплексной защите инженерно-технических средств охраны (ИТСО).

Мы можем помочь нашим заказчикам определиться с образовательными потребностями и в обосновании создания системы

профессиональной подготовки и переподготовки специалистов, основанной центром дистанционного обучения с программно-аппаратным комплексом.

Кроме того, одна из аффилированных компаний, НОУ ДПО «Центр предпринимательских рисков», находящаяся в Санкт-Петербурге, проводит обучение в области экономической и информационной безопасности.

**– Что бы вы отнесли к числу наиболее весомых достижений компании за последнее время? Поделитесь дальнейшими планами ее развития.**

– Своим успехом наша организация обязана высокой квалификации персонала, внедрению проектного управления, наличию испытательно-стендовой базы, на которой проверяется работоспособность отдельных технических решений, отрабатываются информационные взаимодействия между ними, а также активному использованию архива и накопленного опыта.

На сегодняшний день компания сформировала и продолжает укреплять положительный имидж и высокую репутацию надежного партнера в бизнесе. Мы особенно гордимся тем, что нам доверяют и поручают проводить работы ОАО «Газпром», а также регулирующие структуры в области информационной безопасности России, такие как ФСТЭК и ФСБ.

Сегодня компания «Газинформсервис» соответствует растущим требованиям рынка, а ее динамика развития соответствует запросам и предпочтениям заказчиков, даже таких взыскательных, как ОАО «Газпром» и его дочерние общества и организации.

Особое внимание уделяется разработке программных продуктов, что требует значительных капиталовложений. Мы разработали и продолжаем разрабатывать программные продукты и решения, наглядно демонстрирующие инновационный потенциал компании, который наряду с нашими постоянными заказчиками из нефтегазовой отрасли отмечает и высоко оценивает экспертный совет ежегодной Национальной отраслевой премии «За укрепление безопасности России» («ЗУБР»). ■