УДК 004.056:34 (06)

# ЗАКОН «О ПЕРСОНАЛЬНЫХ ДАННЫХ»: САМОЦЕЛЬ, НОВЫЙ РЫНОК ИЛИ ПУТЬ К ЦИВИЛИЗАЦИИ?

**А. В. Брыкин,** директор по взаимодействию с органами госвласти «Комстар-ОТС»; советник госсекретаря Совета министров Союзного государства Россия–Беларусь по вопросам промышленности, транспорта и связи, д. э.н.; brka@mail.ru

***Ключевые слова:*** *персональные данные, информационные системы персональных данных, риски, модель угроз, информационная безопасность.*

**Введение.** С развитием информационных технологий (ИТ), созданием баз данных практически во всех сферах жизнедеятельности возникает угроза не обеспечения конституционных прав человека на неприкосновенность частной жизни, личную и семейную тайну (ст. 23 Конституции РФ) и ограничения сбора, хранения, использования и распространения информации о частной жизни (ст. 24, там же). Первыми на нее отреагировали европейские страны, принявшие в 1981 г. Конвенцию Совета Европы о защите частных лиц применительно к автоматической обработке персональных данных (ПДн), а затем, в 1995 г., Директиву Европейского парламента и Совета Европейского Союза о защите прав частных лиц применительно к обработке ПДн и о свободном движении таких данных.

В России, которая ратифицировала Конвенцию Совета Европы в 2005 г. и поэтому была обязана принять адекватное национальное законодательство, в 2007 г. вступил в силу ФЗ № 152 «О персональных данных», принятый в июне 2006 г. Государственный аппарат долго определялся с уполномоченным органом, затем со значительным опозданием стали появляться подзаконные акты (правовое поле систем защиты ПДн показано на рис. 1). Тем не менее до 1 января 2010 г. информационные системы персональных данных (ИСПДн) должны быть приведены в соответствие с требованиями закона.

Наибольшие проблемы и затраты при выполнении требований закона испытывают крупные публичные компании, работающие в сфере страховой, финансовой деятельности и телекоммуникационного бизнеса. (Соотношение субъектов ПДн в наиболее уязвимом — коммерческом — сегменте приведено на рис. 2) Однако под действие ФЗ № 152 подпадают также детские сады, школы и больницы, розничные торговые сети — все организации, так или

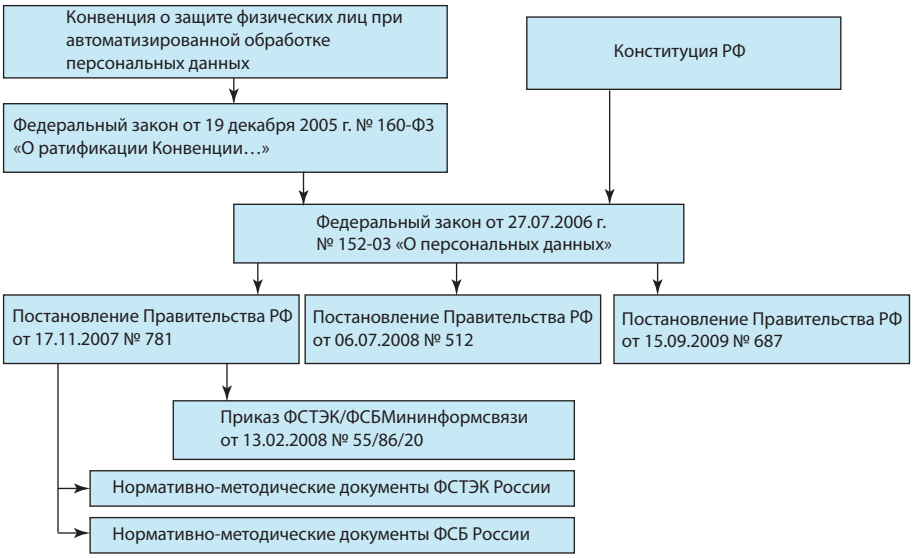


*Рис. 1*

иначе запрашивающие и обрабатывающие ПДн клиентов.

Практика применения закона выявила несколько групп проблем [1].

*Проблемы правового характера* — следствие неоднозначности положений закона, по-разному трактуемых регуляторами и операторами, требуют конкретизации, уточнений и разъяснений. В частности, это относится к конкретизации понятия «персональные данные», месте ПДн в системе информации ограниченного доступа, противоречиям между федеральными законами и др.

*Организационные проблемы* связаны с тем, что ресурсы уполномоченного органа по защите прав субъектов ПДн (Роскомнадзора) ограничены, из-за чего он не в состоянии выполнять функции надзора в полном объеме. Кроме того, нормативные правовые и методические акты уполномоченных ведомств, содержащие требования к операторам ИСПДн, были выпущены с опозданием, поэтому не все из них заложили затраты на реализацию этих требований в бюджеты 2009 г. и, соответственно, могут не успеть к сроку, установленному законом: 1 января 2010 г.

*Финансовые проблемы* обусловлены тем, что при внесении Правительством РФ в Государственную думу проекта


*Рис. 2*

ФЗ «О персональных данных» затраты на его реализацию из средств федерального бюджета не предусматривались. Тем не менее выполнение органами государственной власти и местного самоуправления, бюджетными организациями требований основных регуляторов (ФСТЭК и ФСБ) по обеспечению безопасности обработки ПДн означает резкое увеличение расходов из бюджетов всех уровней.

Среди множества вопросов, на которые нет однозначного ответа: каким образом избежать избирательных мер административного или уголовного воздействия со стороны регуляторов. Почему избирательных? Потому что в России, по подсчетам экспертов, операторами ПДн являются более 70 тыс. структур, в то время как в реестре Роскомнадзора официально зарегистрированы менее 10 тыс. Вряд ли представляется возможным в течение года организовать проверки в таком количестве структур. Ясно, что начнутся они, ско-

рее всего, не со школ и больниц, а с коммерческих структур. Здесь и возникает рулетка с вкраплением неконкурентных методов борьбы и поводами для «договоренностей».

В ситуации неопределенности многие операторы стоят перед выбором: изыскивать средства для обеспечения требований ФЗ в ущерб и без того скудным бюджетам развития на будущий год или затаиться: «авось пронесет». Однако оставим за скобками данную тему и обратимся к главному:

**Что делать** крупным коммерческим структурам, чтобы их деятельность соответствовала требованиям закона?

Начинать надо с создания ИСПДн (основные шаги по построению системы приведены на рис. 3).

Подчеркнем, что ИСПДн — это не хранилище данных с одной лишь целью организации доступа. Практически все СПДн являются специальными, т. е. кроме требований конфиденциальности должны обеспечивать целостность и/или доступность данных. Класс специальной СПДн определяется на основании модели угроз в соответствии с нормативно-методическими документами ФСТЭК и ФСБ России.

Теоретическая часть алгоритма построения систем защиты персональных данных (СЗПДн) и модели построения информационных процессов есть у многих компаний. Трудности кроются в реализации намеченных планов: это большое количество организационных процедур и изменений бизнес-процессов внутри компании. В итоге построение СПДн должно быть включено в процесс стратегического планирования и развития основного бизнеса.

| Результаты проверок Роскомнадзора | 2008 | 2009 |
|---|---|---|
| Выдано предписаний на устранение нарушений законодательства | 19 | 293 |
| Дела переданы в прокуратуру для принятия решения о возбуждении административного производства | 8 | 25 |
| Мировыми судьями составлено протоколов об административных правонарушениях | 11 | Более 30 |

Рассмотрим **примерный план работ**, который позволит привести информационные ресурсы и процессы внутри крупной компании в соответствие с требованиями закона.

*Первый шаг* — создание рабочего органа внутри компании, отвечающего за организацию работы по защите ПДн. Курировать деятельность этой рабочей группы, объединяющей представителей различных подразделений компании, должен один из топ-менеджеров, имеющий право голоса с точки зрения не только ИБ, но и выделения бюджета на реализацию намеченных действий. Оценив риски и наметив пути их решения, компания начинает долгий путь к соответствию требованиям закона с организации подготовки специалистов в области защиты ПДн — речь идет о сотрудниках не только технических, но и юридических служб.

Итогом первой итерации деятельности рабочей группы становится приказ, утверждающий детальный план мероприятий с указанием ответственных лиц и сроков исполнения, причем за каждым его пунктом закрепляются внутрикорпоративные ресурсы не только человеческого, но и материального характера. Если у компании есть дочерние общества, предстоит непростая процедура каскадирования решений и действий в аналогичные органы зависимых структур. Возможно, придется нанимать новых сотрудников, переобучать уже имеющихся. На все это потребуются время и деньги.

Позволим себе высказать собственную точку зрения: лучше отказаться от стремления сэкономить и сделать все самим. В большинстве случаев компаниям рекомендуется принять гибридную схему реализации намеченных планов, т. е. часть работы проводить самостоятельно, а часть отдать на аутсорсинг специализированным фирмам.

Сразу заметим, что лучших практик по подготовке СПДн на принципах аутсорсинга пока не сформировано и фирм, имеющих соответствующие аккредитации и возможности, немного. Поэтому выбрать аутсорсера, который гарантировал бы спокойствие перед проверками регулятора, не так просто.

В любом случае придется оформлять ТЗ, проводить тендер по привлечению аутсорсера, подписывать с ним соглашение о конфиденциальности и организовывать масштабную проектную работу в компании, опять же подкрепленную бюджетными вливаниями. Проектная деятельность неизбежно затронет многие подразделения компании, которым придется составлять свои планы мероприятий, коррелированные с общекорпоративными.

Привлекаемые аутсорсеры в большинстве случаев имеют собственные методики по организации процесса построения СПДн, но, так как никто лучше вас не знает ваш бизнес, рекомендуем принять участие в адаптации существующих методик к особенностям организационной и информационной среды компании.

Подобные проекты, как показывает опыт их реализации, могут потребовать инвестиций в размере от 3 до 8 млн. руб.


*Рис. 3*

и временны́х затрат от полутора до трех месяцев.

После того как проектная деятельность в тандеме с аутсорсером налажена, методики и целевые индикаторы согласованы, цели понятны и задачи ясны, пора переходить к практическим действиям. Для начала следует обследовать системы компании на наличие ПДн и ИСПДн, т. е. определить перечень всех существующих ИСПДн, их состав и структуру, а также технические особенности построения (средства обработки ПДн, топология), перечень и местонахождение ПДн, подлежащих защите, режим обработки ПДн в целом и их отдельных компонентов, а также осуществить категорирование ПДн.

Затем начинается подготовка к формированию так называемой модели угроз, для чего рекомендуется оценить возможность физического доступа к ИСПДн и выявить каналы возможной утечки информации, а также проанализировать риски программного и электромагнитного воздействий на ИСПДн.

Большой фронт работ охватывает не только аудит ИСПДн, но и анализ договоров компании, доработку действующих договоров с контрагентами и клиентами на предмет защиты ПДн. На этот этап рекомендуется обратить особое внимание, так как не во всех организациях есть юристы, способные осуществить данную процедуру оперативно и без рисков для будущих проверок. В крупной компании с большим количеством ИСПДн такая работа может занять от двух месяцев до полугода.

На *второй итерации* деятельности проектной группы необходимо направить в Роскомнадзор уведомление о том, что вы являетесь оператором ПДн. После этого письма можно считать дни до неизбежного визита регулятора — но об этом ниже.

Итогом второго этапа работы должны также стать документы, обосновывающие требования по обеспечению безопасности ПДн, обрабатываемых в ИСПДн: модель угроз безопасности ПДн; модель нарушителя безопасности ПДн; перечень и оценка актуальных угроз безопасности ПДн; определение класса ИСПДн; перечень мероприятий по защите ПДн в соответствии с выбранным классом ИСПДн, подкрепленный способами, мерами и средствами.

Аналогичные результаты должны быть получены касательно требований по обеспечению безопасности ПДн с использованием криптосредств.

На *третьей итерации* предстоит разработать и утвердить регламентирующие внутрикорпоративные документы по обеспечению безопасности ПДн и эксплуатации ИСПДн. В итоге в компании будет создана система управления безопасностью обработки ПДн и оптимизировано множество бизнес-процессов, связанных с обработкой, хранением и защитой ПДн.


*Рис. 4*

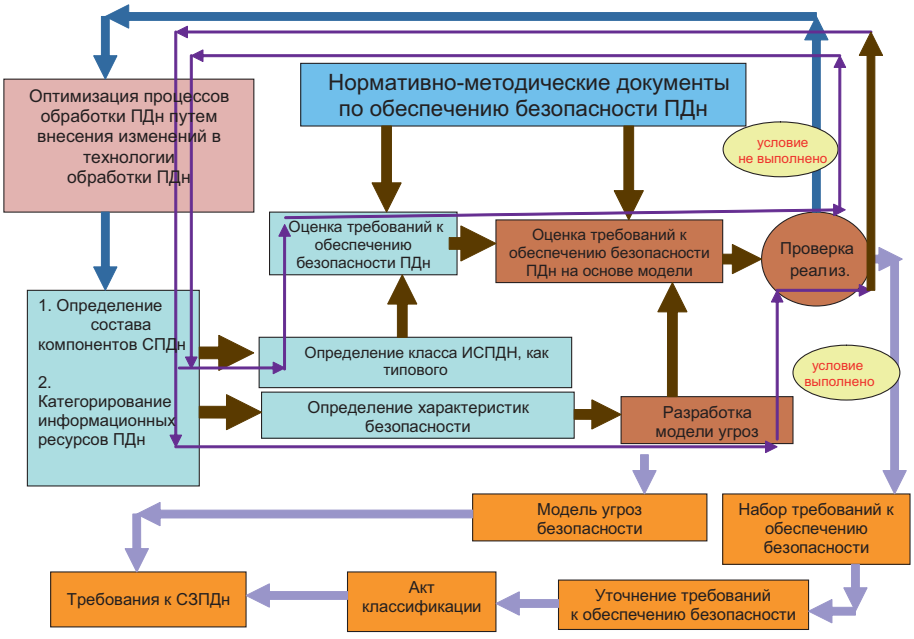


*Рис. 5*

На *третьей итерации* предстоит разработать и утвердить регламентирующие внутрикорпоративные документы по обеспечению безопасности ПДн и эксплуатации ИСПДн. В итоге в компании будет создана система управления безопасностью обработки ПДн и оптимизировано множество бизнес-процессов, связанных с обработкой, хранением и защитой ПДн.

Подтверждением, что эти три итерации пройдены успешно, будет получение от ФСТЭК России лицензии на защиту конфиденциальной информации, аттестация ИСПДн на соответствие требованиям закона, а кроме того, минимальные издержки и замечания, полученные по результатам плановой (рис. 4) или неплановой (рис. 5) проверки Роскомнадзора.

В первом полугодии 2009 г. регулятор провел 205 проверок на предмет соблюдения требований закона, из них 119 плановых и 86 внеплановых. Результаты проверок в 2008 и 2009 гг. приведены в таблице.

Типичные нарушения классифицированы следующим образом:

1. По статьям КоАП Российской Федерации:

- нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (ПДн), ст. 13.11;

● непредставление, несвоевременное или неполное представление в государственный орган сведений, предусмотренных законом, ст. 19.7;

● непредставление в уполномоченный орган уведомления об обработке ПДн, ч. 3 ст. 22;

● отсутствие в договорах с третьими лицами существенного условия обязанности обеспечения указанным лицом конфиденциальности ПДн и безопасности ПДн при их обработке, ч. 4 ст. 6, п. 1 ст. 7.

2. По процедурам, определенным постановлением Правительства РФ от 15.09.2008 № 687:

● отсутствие у оператора перечня мер, необходимых для обеспечения сохранности ПДн и исключающих несанкционированный к ним доступ;

● несоблюдение оператором условий, обеспечивающих сохранность ПДн и исключающих несанкционированный к ним доступ;

● использование электронных носителей информации, не оснащенных системой защиты.

**Цена вопроса.** Приведенный вариант работы по обеспечению соответствия требованиям ФЗ № 152 займет в крупной компании, даже по самым оптимистичным подсчетам, от полугода до года напряженной системной работы большого количества подразделений с неизбежным привлечением внешних консультантов. Организация процесса может потребовать инвестиций в размере от $2 до 7 млн.

А что в результате? Лишь минимизация рисков, связанных с проверками регулятора. Субъекты ПДн не получат ничего, кроме словесных уверений в том, что их персональные данные «охраняются еще лучше». Школы и больницы вряд ли справятся с этой задачей вообще, а коммерческие структуры осуществить все это до 1 января 2010 г., абсолютно точно, не успеют.

Если меры карательного характера не перенесут на более поздний срок, то с 1 января 2010 г. будет открыто огромное поле для недобросовестной конкуренции, а на компании ляжет дополнительная нагрузка по отстаиванию своих прав в судах. Бóльшая часть бюджетов развития компаний уйдет на обеспечение безопасности ради безопасности и судебные издержки, связанные с необходимостью отстаивать право своего бизнеса на существование. А рисков здесь множество: при выявлении нарушений в ходе проверок закон подразумевает, кроме административных взысканий, уголовное преследование, и в том числе приостановление деятельности компании на срок до 90 дней. В условиях кризиса это равносильно уходу с рынка и банкротству.

Закон отстаивает право субъекта ПДн запрашивать у оператора информацию о том, какие его данные и как обрабатываются и хранятся. Установлен предельный срок ответа на запрос — 10 дней с момента подачи. А значит, сотня, например, пенсионеров, ангажированных недобросовестными конкурентами, сможет «завалить» работой любую организацию. В случае несоблюдения сроков ответа она будет обречена на вал судебных разбирательств и дополнительные обременения.

**Заключение.** Подобную «оборону» и интенсивную модернизацию информационных систем вряд ли выдержат фирмы, работающие в сегменте низкой рентабельности, тем более в кризис. Даже сильным игрокам придется из-за

## СПИСОК ДОКУМЕНТОВ, НЕОБХОДИМЫХ ДЛЯ СОЗДАНИЯ ИСПДн В КРУПНЫХ КОМПАНИЯХ

**I. Основные организационные документы**

● **Политика** обеспечения безопасности ПДн (Общие требования по обеспечению безопасности ПДн при их обработке в ИСПДн).

● **Положение** по организации и ведению работ по обеспечению безопасности ПДн при их обработке (определяет состав организационных и технических мер защиты, порядок их реализации).

● **Регламент** обработки и защиты ПДн (Общие правила по обработке и защите ПДн персоналом ИСПДн), который должен включать:

— порядок изменения правил доступа к защищаемой информации;

— порядок изменения правил доступа к резервируемым информационным и аппаратным ресурсам;

— порядок действий должностных лиц в случае возникновения нештатных ситуаций;

— порядок проведения контрольных мероприятий и действий по его результатам.

● **Разделы должностных инструкций** персонала ИСПДн в части обеспечения безопасности ПДн.

● **Инструкции** по использованию программных и аппаратных средств защиты ПДн.

**ОРД по управлению обеспечением безопасности ПДн.**

**Приказы:**

● о допуске лиц к обработке ПДн;

● о закреплении ПЭВМ, предназначенных для обработки ПДн;

● о закреплении помещений, предназначенных для обработки ПДн;

● о назначении лиц, ответственных за обеспечение безопасности ПДн;

● о допуске лиц к работе с криптосредствами, обеспечивающими безопасность ПДн.

**II. Документация, необходимая для проведения аттестации**

● приемо-сдаточная документация на объект информатизации;

● акты категорирования выделенных помещений и объектов информатизации;

● инструкции по эксплуатации средств защиты информации;

● технический паспорт на аттестуемый объект;

● документы, регламентирующие организацию пропускного и внутриобъектового режима;

● нормативная и методическая документация по защите информации и контролю эффективности защиты.

**III. Нормативная и методическая документация по защите информации и контролю эффективности защиты включает следующие документы:**

● технологическую инструкцию администратора безопасности информации автоматизированной системы (АС) объекта информатизации;

● перечень информационных ресурсов, подлежащих защите на объекте информатизации;

● перечень программных средств, используемых в АС объекта информатизации;

● матрицу доступа пользователей к информационным и программным ресурсам АС объекта информатизации;

● инструкцию по организации парольной защиты АС объекта информатизации и др.

**Кроме того, предстоит осуществить:**

● согласование или получение заключения на частную модель угроз (требования безопасности) ПДн (ФСТЭК, ФСБ);

● сертификацию средств защиты (ФСБ, ФСТЭК);

● аттестацию ИСПДн (ФСТЭК).

**Достаточность принятых мер по обеспечению безопасности ПДн оценивается при проведении государственного контроля и надзора (ФСБ, ФСТЭК, Роскомнадзор).**

этого сокращать инвестиции в развитие. Результатом реализации закона может стать коррумпированный неконкурентный рынок, где защита ПДн станет самоцелью регуляторов и вряд ли обеспечит физическим лицам эффективную защиту их прав.

Несмотря на то что закон был издан три года назад, у операторов при построении систем защиты ПДн до сих пор возникает множество вопросов, на которые нормативные документы не дают однозначного ответа. Защита ПДн, безусловно, важная задача, но ее решение не должно быть самоцелью в ущерб основному бизнесу многих организаций. Компании поставлены в жесткие временные рамки, при том что в ситуации глобального кризиса многие максимально оптимизируют собственные материальные и временные затраты.

Кроме того, сегодня явно недостаточно компаний, имеющих лицензии на право аудита, чтобы в срок до начала 2010 г. обработать весь спектр операторов ПДн. В этой ситуации, возможно, стоит подумать о переносе сроков действия закона или определить период, в который меры Роскомнадзора в отношении соблюдения требований ФЗ № 152 будут носить предупредительный характер.

*ЛИТЕРАТУРА*

1. **Волчинская Е. К.** Некоторые правовые проблемы применения Федерального закона «О персональных данных»//Персональные данные. — 2009. — № 2.

*Получено 12.11.09*

**ИНФОРМАЦИЯ**

## «МФИ СОФТ» ПРИНЯЛА УЧАСТИЕ В ЗАСЕДАНИИ СЕКЦИИ ЭКСПЕРТНОГО СОВЕТА КОМИТЕТА ГОСУДАРСТВЕННОЙ ДУМЫ ПО БЕЗОПАСНОСТИ

Заседание было посвящено обсуждению законодательных и организационно-технических аспектов обеспечения безопасности национальной инфокоммуникационной инфраструктуры и проходило под руководством первого заместителя председателя Комитета по безопасности депутата Государственной думы **М. И. Гришанкова**. В работе экспертного совета приняли участие представители Государственной Думы, силовых ведомств и ряд экспертов в области информационной безопасности от государственных структур, общественных организаций и бизнеса. В **заседании** принял участие президент компании «МФИ Софт» **А. А. Иванов.**

Поводом для организации Совета стала высокая озабоченность общества, государственных структур и представителей инфокоммуникационного бизнеса состоянием дел, касающихся защищенности российской телекоммуникационной инфраструктуры, реализации конституционных прав граждан на доступ к открытой информации, в том числе государственным информационным услугам в рамках электронного правительства, обеспечения национальных интересов при установлении международных стандартов в области информационной безопасности, а также реализации программы обеспечения технологической независимости в сфере ИКТ от иностранных продуктов.

На заседании присутствовали такие известные эксперты в области обеспечения информационной безопасности как заместитель председателя Центрального банка РФ **М. Ю. Сенаторов,** председатель исследовательской комиссии по безопасности сектора стандартизации Международного союза электросвязи **А. С. Кремер**, руководитель антивирусных исследований «Лаборатории Касперского» **Е. В. Касперский** и др.

А. А. Иванов выступил на заседании в качестве эксперта от ведущих российских производителей телекоммуникационного оборудования и систем информационной безопасности. В своем выступлении он привлек внимание собравшихся к вопросам, касающимся обеспечения информационной безопасности операторских сетей передачи данных, несовершенства законодательной базы в этой области, отсутствия механизмов стимуляции развития российских технологий. В частности, он подчеркнул необходимость и важность использования собственных российских программно-аппаратных решений для защиты сетей связи. А. А. Иванов отметил также наличие мощного отечественного научно-технического потенциала в данной сфере и активное участие в решении имеющихся научно-технических задач ведущих специалистов в области информационной безопасности российских силовых ведомств и академических научных школ, среди которых МГТУ им. Баумана, МИФИ, МГУ им. Ломоносова, Военная Инженерно-Космическая Академия им. Можайского и др.

А. А. Иванов подчеркнул, что признанная компетенция ряда российских производителей интеллектуальных технологий и продуктов, таких как «МФИ Софт», позволяет реализовывать проекты в области защиты национальной инфраструктуры, сопоставимые по сложности и качеству с лучшими иностранными образцами.

«Важным условием успешной реализации таких проектов является совместная, синергическая деятельность бизнес-структур в направлении развития инновационной российской экономики, провозглашенной руководством России. Одновременно, развитие инноваций невозможно без собственных инвестиций российских предприятий в R&D-область. Примером такого ответственного и масштабного проекта, является совместный проект «МФИ Софт» и ОАО «Синтерра», который успешно прошел стадию тестирования в реальных условиях. В этом проекте «Синтерра» выступает в качестве инвестора и генератора бизнес-идеи, а «МФИ Софт» — научного и производственного центра», — сказал А. А. Иванов.