журнал "Бизнес-разведка" № 35

Бизнес-разведка в свете Федерального Закона «О персональных данных»

Круглый стол

30 сентября 2009 года

Вступительное слово:

Иванов Сергей Владимирович, Группа компаний «Амулет»

Емельянов Вадим Геннадьевич, Клуб сотрудников информационных служб

Доклады и выступления:

Парфенов Алексей Александрович, ЗАО «Специальная информационная служба»

Лукьянов Владимир Михайлович, «Интегрум»

Соломанидин Владимир Геннадьевич, «Власта-Консалтинг»

Баяндин Николай Иванович, Московский экономико-статистический институт

Унижаев Николай Владимирович, Институт безопасности бизнеса МЭИ (Технический университет)

Шарлот Всеволод Владимирович, эксперт

Мухин Александр Владимирович, ООО «Научно-исследовательский центр экспериментальных технологий»

Черкасс Юрий Владимирович, ЗАО «Рэйнвокс»

Казакевич Олег Юлианович (Ассоциация российских банков)

Светозаров Владимир Борисович, учредитель и редактор ж. «Бизнес-разведка»
Как регулируется работа с персональными данным в Европе и США (обзорная статья)

Иванов Сергей Владимирович (Группа компаний «Амулет»)

Сегодня мы проводим круглый стол по тематике бизнес-разведки (БР). Он организован Группой компаний «Амулет», которую представляю я, и Клубом сотрудников информационных служб, представленным Емельяновым Вадимом Геннадьевичем. Организационно-техническую сторону мероприятия обеспечила компания «Авангард». Хочу

также выразить большую благодарность тем, кто предоставил это помещение – Ассоциации защиты информации и Институту информатизации и стандартизации связи на железнодорожном транспорте.

Хочу сказать пару слов об актуальности темы. История наших круглых столов достаточно длинная, мы проводим их уже, наверное, лет 12, я имею в виду ГК «Амулет». Жизнь на месте не стоит, задачи, которые она перед нами ставит, все более сложные. Давно прошли те времена, когда мы позволяли себе дожидаться форума «Технологии безопасности», в рамках которого обычно и проводили круглые столы, и обсуждать проблемы общего характера. Сегодня мы все чаще подходим к мысли о том, что выносимые на круглый стол темы должны нести практическую направленность, соотноситься с новыми тенденциями и явлениями рынка. Выбирая тему сегодняшнего круглого стола, мы вспомнили, что через несколько месяцев вступает в силу Федеральный Закон № 152 «О персональных данных», и решили провести его обсуждение. Актуальность его, с точки зрения бизнес-разведки, (БР), на наш взгляд, весьма высока. Все мы, присутствующие здесь, - коллеги по цеху, и нам по роду своей деятельности, так или иначе, придется наверняка пересекаться в правовом поле с этим законом. Актуальность темы обусловлена тем, что и надзорные органы, которым вменяется контролировать исполнение закона, и субъекты рынка не готовы воспринять его в полной мере. Кроме того, государственная власть в лице Госдумы заинтересована в обсуждении, чтобы узнать реакцию «снизу». Я не юрист, но, читая закон, наткнулся на множество вопросов. Позволю себе бегло озвучить то, что мне показалось наиболее интересным, актуальным, в какой-то степени спровоцировав полемику.

Итак. Уже с первых строк закона натыкаюсь на формулировку персональных данных (ПД) и выясняю, что она очень размыта. Под понятие «персональные данные» в соответствии с Законом, подпадают ФИО, адрес, паспортные данные, должность, социальное положение, и далее - «другие данные». Как это понять? Если, скажем, у моей бабушки есть кот, и я, объявив об этом Интернете, преступлю закон?

Как всегда, цель принятия Закона – самая благая. Но он вызывает у специалистов множество вопросов, и главный из них - не станет ли этот закон очередным инструментом, как теперь модно выражаться, для «оборотней в погонах» и других нечистоплотных на руку людей, не сведется ли контроль и надзор за его исполнением к вопросу «сколько с меня»? Утверждают также, Закон должен следовать и соответствовать соответствующим решениям Евросоюза. Дело в том, что Евросоюз давно уже договорился в рамках своих границ об обмене персональными данными, но между ним и Россией такой договоренности нет, что явно тормозит реализацию перспективных, амбициозных, выгодных для нас проектов.

Бросается в глаза сложность исполнения Закона. Минсвязи и другие авторитетные чиновники говорят (судя по материалам СМИ), что ни финансовой, ни технической, ни организационной готовности к его исполнению нет. Ведь чтобы проверять и контролировать исполнение Закона субъектами рынка, нужно подготовить и аттестовать операторов персональных данных, а для этого потратить не один месяц и даже не один год.

Все знают о «презумпции невиновности». На мой взгляд, отчасти Закон нарушает этот принцип. В частности, в нем говорится, что я имею право оперировать данными из открытых источников – справочниками, телефонными книгами, информацией из веб-сайтов. Давайте пофантазируем. К примеру, я утверждаю, что данные моих сотрудников были когда-то заявлены в открытых телефонных книгах, таким образом, доказательство того, что эти данные являются неоткрытыми, лежит по логике на исполнительной власти. Однако, Закон этого не утверждает. Согласно Закону, как я понял, я буду должен доказать контролирующему органу, что данные, которыми я оперирую, взяты из открытых источников.

Последний момент, на который хотел бы обратить внимание, вытекает из жизненного опыта, здравого смысла. Вот любой интернет-магазин, торгующий предметами быта. Совершая сделку купли-продажи, я заполняю анкету в электронном виде со своими персональными данными, отправляю в магазин, а в ответ получаю пароль и логин, и только потом получаю право на покупку и оплату. Итак, я передаю свои персональные данные по электронной почте в интернет-магазин, но они нигде не фигурируют в виде окончательного фактического документа. Вы можете возразить, что есть электронная

подпись, и закон требует именно так поступать в этом случае. Но на сегодняшний день в России владеют электронной подписью, всего 1 или 1,5 % населения. А из них еще только процентов 15 умеют оперировать этой подписью. Таким образом, не понятно, что делать электронному магазину: ждать, когда я приеду и чернилами подпишу анкету, или автоматически нарушать закон. Субъектов рынка, которые окажутся в подобной ситуации, очень много. Это и кредитные организации, и страховые компании.

Емельянов Вадим Геннадьевич (Клуб сотрудников информационных служб)

Позвольте всех вас поблагодарить за то, что в наше перегруженное неоднозначное время нашли возможность поучаствовать в сегодняшнем круглом столе. Я надеюсь, что совместная работа сегодня, свободный обмен мнениями и опытом пойдут на пользу каждому из нас в повседневном труде, а если польза от круглого стола будет очевидной, будем стараться устраивать подобные мероприятия регулярно.

Сфера деятельности БР в преломлении закона о персональных данных. по моим наблюдениям, серьезно и глубоко еще не обсуждалась. Наверно, это объясняется тем, что БР носит довольно закрытый характер, даже зачастую и для большинства собственных сотрудников. Кроме этого, в правовом поле развитого механизма, регулирующего БР, в общем-то пока нет. Специалистов в этой области начали готовить только недавно и буквально единицы учебных заведений. Данный термин, по моему мнению, не имеет устоявшегося определения, им часто пользуются наряду с другими терминами – конкурентная разведка, деловая разведка, корпоративная разведка, коммерческая и т.д. Все эти определения существенно отличаются от понятия «промышленный шпионаж». Отличие в том, что БР собирает и использует информацию без нарушения норм законодательства, а промышленный шпионаж – любыми способами. Поэтому вступление в силу ФЗ о персональных данных однозначно ставит перед компанией, которая имеет в своем штате бизнес-разведчиков – подразделение или сотрудников – острые вопросы. Например, должна ли компания, которая имеет в структуре службу БР, интересующуюся, в том числе, и персоналиями, идентифицировать себя как оператор ИСПДМ и регистрироваться в Госкомнадзоре. Если должна, то как получать согласие субъекта на сбор данных о нем? Это же абсурдный вопрос, учитывая специфику БР. Как долго хранить архивы с ПД и какие, собственно, сведения могут в этих архивах содержаться?

Есть и другие вопросы. В рамках БР часто осуществляется сбор данных, готовятся информационно-аналитические отчеты по физическим лицам, и озвученные выше вопросы не на пустом месте возникли. Если следовать закону «О персональных данных», то может резко измениться характер конкуренции, деятельность по получению необходимой для бизнеса информации методами БР будет загнана в подполье. Не исключено, что многие владельцы бизнеса предпочтут вывести из штата своих структур соответствующих сотрудников, чтобы не вступать в противоречие с этим законом. В любом случае ФЗ о ПД профессиональную жизнь сотрудников БР явно не облегчит.

Иванов

Или ввести в штат должность журналиста. Закон позволяет. Если ты журналист, то имеешь право оперировать персональными данными в силу специфики своей творческой и профессиональной деятельности.

Емельянов

Да, и у нас все коммерсанты станут тогда владеть газетами. На сегодняшнем круглом столе мы, конечно, не ожидаем, что получим ответы на все поставленные вопросы, но даже если мы грамотно сформулируем эти вопросы, то это уже достаточно хороший, весомый результат. Будем очень рады, если прозвучат предложения о практической реализации этих вопросов. Главная задача, как я ее вижу на сегодняшний день - сохранить БР, не допуская нарушения законодательства, в том числе и ФЗ о ПД. Это важно и для нас самих,

специалистов в этой области, и для бизнеса, который является основным потребителем продукции БР.

Парфенов Алексей Александрович (ЗАО «Специальная информационная служба»)

Я буду краток, так как не готовил академичного доклада, не разбирал постатейно этот закон по простой причине, что к великому счастью мы не являемся, как указано в 3-ей статье Закона, оператором. Наша компания – чисто аналитическая, присутствие в ее названии слова «информационная» условно, так сложилось исторически. Действительно, мы сегодня занимаемся практически только аналитикой, и даже персональные данные, которые также указаны в 3 статье и в 10 статье Закона, мы практически не используем.

Шли мы к этому неоднозначно. Честно могу сказать, до сих пор по рынку мечутся люди, заказчики, которые прибегают с выпученными глазами и говорят: «дайте нам адрес генерального директора компании «Пупкин и сыновья». Я сразу спрашиваю – зачем он тебе? 90% заказчиков не могут на этот вопрос ответить.

Я тоже честно читал Закон и это «др.» меня тоже поразило. «Др.» - это не юридический термин явно. Тем не менее, я бы все-таки выделил эти ПД. Некоторые ПД, например, ФИО или дата рождения, они не меняются никак. Адрес - тоже привязка к персоналии. Их можно считать объективными. Мы в своих отчетах, не буду здесь кривить душой, в ряде случаев изучаем физические лица по заказу наших клиентов, но эти данные предоставляются нам заказчиком, а мы оперируем субъективными характеристиками. Заказчик ставит вопросы, касающиеся деловой активности исследуемого объекта, его порядочности, финансовых претензий, каких-то других качеств, которые являются, еще раз подчеркиваю, не объективными, а субъективными.

Среди ПД, которые указаны в статье 10 Закона, обращаю ваше внимание на «религиозную принадлежность», «философские воззрения» и т.п. Если честно, то я не поручусь, что наш патриарх - верующий человек. Да, у него сан - Патриарх Всея Руси, но кто честно может поручиться, что он искренне верит. Извините, может быть, за не очень корректный пример. Но я знаю много людей, имеющих научные звания, которые к науке имеют очень далекое отношение. Поэтому, было бы более корректно всегда использовать субъективные данные: как человек относится к партнеру, насколько ему можно доверять, учитывая его историю – деловую или научную, да какую угодно. Кстати, вот прозвучавший здесь пример с котом у бабушки...

Иванов

Вы знаете, Алексей Александрович, у меня есть еще один яркий пример. В одной из статей Закона указано, какие сведения не подпадают под его действие. В частности, данные, находящиеся в Едином государственном реестре индивидуальных предпринимателей (ЕГРИП). Это информация, оседающая в налоговой службе, - те же ФИО, паспорт и т.п. Но подпадают под действие сведения, содержащиеся в Едином государственном реестре юридических лиц (ЕГРЮЛ), где, в том случае, если учредитель является физическим лицом, оседают те же самые данные и даже больше.

Парфенов

Прежде чем завершить выступление, замечу, что в нашей фирме вот уже 15 лет существует журнал «Факт», в нем работают и сотрудничают журналисты, в их числе и я, специальный корреспондент, но я ни разу не доставал удостоверение и никому не показывал.

Иванов

А я тоже корреспондент, хотя нигде никогда ничего не писал, никакого удостоверения не имею. Но завтра, допустим, создам в Интернете свой блог и уже формально буду журналистом. Это подтверждает мировая практика. Вот пример: на встречу с одним из

достаточно высокопоставленных конгрессменов США было аккредитовано 100 журналистов, в их числе два человека - держатели интернет-блогов без каких бы то ни было удостоверений. Так кто такой журналист, объясните мне? Вот раньше был Союз писателей, состоишь – писатель, не состоишь – все, не писатель. А сейчас как? Кто раздает индульгенции?

Парфенов

Я выдаю.

Иванов

Я к вам записываюсь.

Парфенов

У нас официально зарегистрированный в Министерстве печати журнал «Факт» с лицензией. Соответственно, я как Генеральный директор, подписываю документы.

Иванов

Но мировая практика показывает, что можно вообще ничего не иметь и считать себя журналистом.

Парфенов

Да, это так.

Иванов

У меня еще один вопрос. Вы не оператор, но так или иначе данные по персоналу в компании имеются. По вашему персоналу, имею в виду. Может быть, есть какие-то договора с индивидуальными предпринимателями? Планируется ли какая-то работа в компании в связи с новым законом?

Парфенов

Нет, честно скажу, что нет.

Иванов
.
Почему?

Парфенов

Во-первых, такой договорной работы у нас нет, точно могу сказать.

Емельянов

Но в рамках вашей кадровой службы накопление персональных данных сотрудников должно вас к чему-то обязывать в свете Закона.

Парфенов
.
Насколько я понимаю, Закон это позволяет в связи с договорами. Если я подписываю с сотрудником договор о трудовых взаимоотношениях, то разрешается хранить эти данные и накапливать. Без дополнительной договоренности с сотрудником.

Лукьянов Владимир Михайлович

(«Интегрум»)

Баяндин Николай Иванович (Московский экономико-статистический институт): В преддверии доклада Владимира Михайловича Лукьянова, работающего в компании «Интегрум», я хотел бы два слова сказать о том, как рождался этот доклад, и на реальном примере показать, как работает система Интегрум, как конкурентная разведка использует возможности по сбору данных, в том числе и персональных. Этот доклад поднимет вопросы о том, что нам делать с теми массивами информации, которые собраны до введения Закона и которая содержит информацию, подпадающую под ПД. Такой информации видимо-невидимо. И что же - все информационные ресурсы теперь перетряхивать, переписывать историю?

Вопрос очень серьезный, поскольку, например, данные за 1991 год могут очень здорово повлиять на действие изучаемого объекта, если мы будем следовать букве закона. Итак, пример. В середине октября будет юбилей - 55 лет - очень хорошему человеку господину ХХХ. Мы на нашей кафедре решили подготовить поздравление, приветствие и для этой цели воспользовались вначале интернетом. Задали в поисковик его ФИО и Яндекс выдал нам много интересной информации. Эта информация была классифицирована вручную по различным направлениям, т.е. его деятельность, его заслуги, его связи с учебными заведениями, фотографии, его родственники, когда родился, где родился. Информация носит персональный характер. Например, имя-фамилия-отчество, дата рождения, какой ВУЗ заканчивал, профессиональный путь, ФИО жены, ФИО детей и т.д. Вся эта информация находится в открытом доступе, была опубликована, может быть, с его разрешения, а, может быть, и без – мы этого не знаем. Мы составили достаточно интересную аналитическую справку, посмотрели на блогах его учеников, их отношение к нему. Возникает вопрос: как контролировать новые сервисы, как контролировать социальные сети? Для КР все это очень интересная информация, поскольку связана с первоисточниками, но опять же возникает вопрос о Законе «О персональных данных».

Лукьянов Владимир Михайлович («Интегрум»)

Я бы хотел добавить, что сбор информации из открытых источников, действительно, достаточно трудоемкая задача, особенно если требуется назвать источник, обосновывать, откуда взят каждый конкретный факт. Наше информационное агентство на рынке уже более 13 лет, за это время собран архив из СМИ, справочных баз, там сотни миллионов документов, порядка 10 тысяч источников. И в этой информации, конечно же, фигурируют персональные данные.

Невозможно перечислить источники, по которым мы предоставляем поиск – это и регистрационные данные Росстата, и бухгалтерская отчетность, и информация об учредителях, дочерних фирмах, отчетность эмитентов. Если брать СМИ - это журналы, информационные агентства, сообщения в новостях, интернет-издания, которые зарегистрированы в Минсвязи. При этом все данные открыты, каждая статья, каждая запись имеет пометку «свой источник». Т.е. когда мы делаем отчет, мы можем всегда показать, откуда это взято, предоставлен интерфейс поиска, мы имеем рубрицированный набор источников, получаем списки найденных статей с выходными данными - тема, дата выпуска, где взято. Кроме СМИ это могут быть патентные базы, т.е. Роспатент. Если есть ФИО – находим его/её открытие или изобретение, тоже вполне объективная информация. По базам СМИ мы можем проследить профессиональную биографию – в качестве кого упоминали, какие звания имел, в какие годы.

Вспоминаю интересный случай, когда в ходе поиска по одному из политиков, не буду называть имя, вылезло звание «вор, убийца народа». Что это может быть? Заходим в источник, находим конкретное издание за дату. Все, у нас есть источник информации, открытый, дальше уже вопросы к этому изданию.

Можно проследить связи через организации – это и регистрационные данные, и источники СМИ. Мы можем проследить круг лиц, с которыми предположительно связан наш объект исследования. К примеру, уже упомянутый

Когда мы заходим в «Компанию», по ней у нас из структурированных данных возникает

связь «учредитель - дочерняя структура», получаем информацию по корпоративной структуре, открытую информацию – госконтракты с указанием сумм, сроков, тем. Арбитражные суды – сообщения о банкротствах. Вся эта информация собирается и на ее основе составляется отчет, принимается решение.

Как работать с такими данными в свете Закона? Во-первых, мы являемся информационным агентством, у нас работают журналисты, аналитики. Во-вторых, на каждую запись, на каждый факт у нас есть источник информации, и все дальнейшие вопросы уже к нему. Но остается открытым вопрос о регистрации и надзоре уже в качестве оператора.

Иванов

Владимир Михайлович, в рамках вашей системы, я знаю, огромное количество источников, в том числе и интернет-издания. Допускаете ли вы или, может быть, знаете, что среди этих изданий есть незарегистрированные, никак и нигде?

Лукьянов

Это вполне возможно.

Иванов

Вопрос-то вот к чему: завтра это издание исчезло, данные из него, накопленные за год-три, осели, а спросить уже не у кого.

Лукьянов

Мы журналисты, мы можем закрыть эту базу для себя, для внутреннего использования, но предоставлять ли доступ – уже вопрос.

Казакевич Олег Юлианович (с места).

В юриспруденции есть общее правило. Закон обратной силы не имеет, т.е. все, что было накоплено до введения Закона, под него не подпадает. С вас никто ответственности не спросит.

Иванов

Олег Юлианович, тогда разъясните такую ситуацию: у меня есть зарегистрированный 5 лет назад сайт в интернете и есть база данных, в которую входят 80% москвичей с паспортами и фамилиями. Завтра я их выкладываю на этом сайте.

Казакевич

Речь идет не об использовании или выкладывании, а о хранении.

Иванов

На сайте я могу использовать, хранить, модифицировать эти данные?
Не нарушаю ли я Закон?

Казакевич

Нет. Та информация, которая у вас была накоплена до вступления в действия этого закона, действительна.

Иванов

А как это проверить? Сайт создан пять лет назад.

Казакевич

А вы представьте себе такую ситуацию в банковской системе. Закон обязывает оператора ПД истребовать согласия на обработку персональных данных человека, вкладчика. Вы знаете, сколько к настоящему моменту, до кризиса, накоплено данных и заключено соглашений по вкладчикам, например, Сбербанка? Вы что, предлагаете перезаключить все

соглашения?

Иванов

Боже сохрани. Это документально зафиксировано.

Соломанидин Владимир Геннадьевич (Власта-Консалтинг)

Добрый день, очень приятно видеть знакомые лица, и здорово, что мы собираемся и обсуждаем вопросы, которые действительно являются существенными, определяющими для ведения бизнеса в этой сфере. Я хочу сказать, что все, что мы здесь обсуждаем, в полной мере относится и к компаниям, работающим в сфере безопасности бизнеса за рубежом. Практически один к одному, только, может быть, они несколько дальше ушли в своем развитии и в связи с этим сталкиваются с гораздо большими трудностями, чем мы в настоящее время. Говоря о бизнес-разведке, конкурентной разведке или, более мягко, об информационно-аналитическом сопровождении бизнеса, практическое поле деятельности – это касается и США и стран Евросоюза - постепенно сужается. Ряд присутствующих лиц могли в этом убедиться, участвуя в разного рода международных форумах, где эти вопросы обсуждаются. Вот, в частности, недавно в Бразилии прошла конференция Всемирной ассоциации детективов или, как сейчас она по-новому называется, Объединения профессионалов безопасности бизнеса. Там свыше 800 членов из более, чем 80 стран мира. Среди обсуждавшихся там вопросов - противодействие шпионажу. Ведь часто возникает вопрос - бизнес разведка и промышленный шпионаж, где грань между ними, как их различать? Поскольку эта тема интересует любую компанию, встает вопрос – как, что нужно делать?

Так вот, сфера деятельности сужается. Если мы говорим о ПД, то это, безусловно. В каждом штате в США есть свои законы, ограничения, но, в целом, есть общие положения, которые характерны для всех. Так, может быть, прекратить деятельность конкурентной разведки? Но это просто невозможно. Что делают в США, например? Они объединяются. У них есть Национальная ассоциация детективов, которая строится по профессиональному признаку. Детективы выступают единым фронтом и, по сути дела, лоббируют свои интересы в Конгрессе США, в своей деятельности получают поддержку от своих коллег за рубежом. То же самое сейчас происходит и в Евросоюзе. Идет политическое объединение, идет экономическое объединение и, одновременно, по профессиональному признаку. И в Европе есть аналогичная организация, которая объединяет национальные структуры различных стран, называется Ай-Ки-Де, она объединяет не членов, а организации. Эти организации выносят какие-то свои идеи, общие положения, которые лоббируются уже в европейском парламенте. В целом, это позволяет держаться на плаву.

Теперь, что касается работы компаний, которые занимаются бизнес-разведкой за рубежом. В последнее время в значительной степени ослабла позиция крупных, известных компаний, таких как «Кролл», «Контрол Риск», « Риск Эдвайзер Групп», я не буду всех называть сейчас. Эти компании оказались вовлеченными в целый ряд громких скандалов, в частности, в Германии и Великобритании. В Великобритании это во многом связано с пребыванием там представителей бизнес-элиты и олигархических кругов, которые пытаются собирать информацию в разных странах, в том числе и в России.

Ослабление «крупняков» дает возможность более активно работать средним и мелким компаниям. Крупные корпорации тратят в этой сфере колоссальные деньги, в то время как наши компании, здесь в России, выступая операторами зарубежных корпораций, получают лишь малую толику того, что забирают последние.

В процессе проработки взаимодействия с зарубежными коллегами всегда четко оговаривается, что работа должна быть выполнена в рамках действующего законодательства, т.е. ни в коем случае компания не хочет быть ответчиком в суде, не хочет, чтобы против нее выдвигали обвинения и иски. Это одна из самых примечательных для настоящего времени тенденций. Если речь идет о проверке персонала, за рубежом сформулирован и действует четкий алгоритм, который позволяет, с одной стороны

произвести нужную проверку, а с другой стороны – оставаться в поле законодательства.

Кадровые проверки за границей – вещь обычная. Проверяются не только кандидаты, но и уже работающие сотрудники. Смотрят, как меняется экономическое положение сотрудников, какая собственность приобретается, приобретения сравниваются с официальными доходами.

На это требуется разрешение самого сотрудника. Поэтому все сотрудники заполняют соответствующие документы, которые позволяют руководству корпорации проводить подобную проверку. Таким образом, они уходят от ответственности и возможных обвинений в том, что нарушаются права сотрудников, уходят от возможных серьезных обвинений в отношении компании на тот случай, если они проявили недобросовестность при приеме сотрудников. В отличие от России на Западе, если водитель какой-то компании, будучи в пьяном виде, сбил кого-то, то иск часто предъявляется компании. Может случиться ситуация, когда водитель, во внерабочее время, управляя собственной машиной, сбил человека, и при этом выясняется, что он ранее уже лишался прав или привлекался за управление транспортом в пьяном виде. В этом случае адвокаты, которые ведут дело, выдвигают обвинения против компании. Очень любят это делать. Компании вынуждены добиваться досудебного мирового соглашения, выплачивают огромные штрафы, которые исчисляются сотнями тысяч и даже миллионами. Поэтому компании должны проверять своих сотрудников, своих бизнес-партнеров.

У нас в России сейчас практикуется, что если ты ведешь бизнес, отвечаешь за то, с кем ведешь бизнес. Этот пункт не всегда понятен бизнесменам, которые здесь работают. Они говорят: «Ну, как же, мы платим все налоги, причем тут мы?». А партнеры не платят НДС и вам не только вменяют в обязанность выплатить в бюджет этот НДС, но и одновременно по результатам проверки могут возбудить уголовное дело, что, кстати, делается довольно часто.

Мы сейчас испытываем, конечно, определенные трудности. Поэтому многие отходят от того, чтобы называть себя детективным агентством, за исключением тех, кто следит за женами и мужьями. А те компании, которые занимаются достаточно серьезным бизнесом, позиционируют себя как консалтинговые компании, действующие в сфере безопасности бизнеса. Такая же тенденция в последнее время набирает оборот и у нас, и в Европе. В Америке несколько другая ситуация, там огромное количество мелких предпринимателей, частных детективов.

Крупные западные компании пытаются, используя наработанный имидж, выходить и на российский рынок. При этом часто нарушают законодательство. Например, сотрудники представительства «Кролла» во многом нарушают законодательство, понимают всю шаткость своего положения, но продолжают работать в том же ключе. Скажем, в США есть закон, который запрещает выплачивались деньги чиновникам, официальным лицам. Сотрудники же, которые занимаются у нас сбором информации, нуждаются в источниках, в нужных людях, платят им за информацию. Они осознают, что подвергаются риску, но, тем не менее, продолжают свою работу.

Хочу подчеркнуть, что взаимодействие с зарубежными компаниями, зарубежный опыт приносит много пользы. Мы перенимаем наработанные методы. Многие российские компании задумываются над тем, как проверять людей, не выходя за рамки законодательства, особенно сейчас, во время кризиса, поскольку увольняемые сотрудник пытаются каким-то образом заработать, получить деньги с компании. Используем тот же самый метод: сотрудники заполняют анкеты данными о себе, санкционируют проверку этих данных, понимая, что по истечении какого-то времени проверка может повторена.

Иванов

Вы упомянули ряд скандальных примеров, связанных с неправомерной обработкой персональные данных и их утечки. У нас таких случаев тоже сколько угодно в российской практике, однако, я не помню, чтобы субъект рынка, допустивший утечку или неправомерный сбор информации, понес за это ответственность. Закон явно не панацея, и завтра мы все равно увидим на прилавках рынка те же самые «серые» базы данных. Жизнь вряд ли сильно изменится, во всяком случае, быстро. Отсюда вопрос - на ваш взгляд, в свете выхода нового закона или вернее вступления его в силу практика наказаний возымеет место или все останется на своих местах? Спасибо.

Соломанидин

Я думаю, что какие-то вопиющие дела будут доведены до конца, в любой практике должны быть какие-то примеры, служащие прецедентом для судебных органов. Как и при защите интеллектуальной собственности, мы много об этом говорим, но практически пока никто уголовного наказания не понес. Идет лоббирование определенных интересов. На Западе такие коллизии часто решаются в досудебном порядке. Поэтому нередко те, кто занимается этим бизнесом, ведут сбор персональных данных, специально оговаривают, что информация, которая будет предоставлена, не может быть использована в суде. Для крупных корпораций очень важно получить доказательства, которые они могут использовать в суде. Для мелких и средних компаний это не нужно, это у них для «внутреннего употребления». Обнаружили, что менеджер ворует информацию, продает ее налево, его просто увольняют, поскольку открытое разбирательство скандала никому не нужно. Да и крупным компаниям скандалы не нужны.

Разбирательства с утечкой информации имеют своей целью высветить причины, закрыть прорехи, но желания судебного преследования нет ни у кого. Просто нужно быть аккуратней. Бумаги не оставлять, убирать за собой, проверять помещение на предмет подслушивающих устройств. А случаи открытого судебного разбирательства будут, конечно. Первые прецеденты важны.

Емельянов

Хотим мы того или нет, но наша бизнес-разведка очень часто, по крайней мере, в Москве, опирается на «серый» рынок баз данных, которые утекли в свое время и плодятся. Как у них там, за рубежом, существует ли «серый» рынок электронных массивов или они как-то с этим уже справились?

Соломанидин

.

Я могу сказать, что какие-то «серые» базы имеются, но в целом получение информации носит штучный характер. В Европе практически нигде вы не получите данные о судимости. Это практически невозможно, это даже не обсуждается. Они настолько запуганы, что ни за какие деньги, положим в Великобритании, делать не будут.

Для этого есть определенная процедура, когда работодатель пишет обращение по поводу сотрудника или кандидата на работу в фирме, оно будет рассматриваться, процедура эта длительная, сложная, совершенно необходимая. Допустим, частный госпиталь нанимает кого-то на должность сиделки. Потом обнаружится, что сиделка изнасиловала того, за кем должна ухаживать. При разбирательстве выясняется, что эта личность уже привлекалась за сексуальные правонарушения. И отвечать будет не она, а компания. Поэтому, хочешь - не хочешь, все равно процедуру надо проходить до конца. Конечно, алгоритм процедуры очень длительный, не позволяет принять быстрое решение, особенно неудобен, когда работодатель рассматривает несколько кандидатур и нужно быстро принять решение. Проще иметь дело с открытыми источниками. И если там можно какую-то информацию накопать, то она позиционируется как легально добытая из открытых ресурсов. Принято собирать информацию по предыдущим местам работы. Это позволяет компенсировать отсутствие или недоступность баз данных.

Емельянов

Вы считаете, что за рубежом в более или менее доступном и открытом виде базы данных не «гуляют», как у нас?

Соломанидин

Нет. В США эта проблема – настоящая головная боль, поскольку она часто связана с финансовыми рисками. Для конкурентной разведки или для информационного сопровождения бизнеса необходимо, чтобы субъект был идентифицирован. Если не идентифицирован, могут быть неожиданности, осложнения.

Для бизнеса всегда важно, кто является акционерами, это определяющий момент. И если привязки к паспорту нет и нельзя точно идентифицировать, кто есть кто на самом деле, то любой чиновник скажет, да мало ли однофамильцев - это не я и не мои это родственники. У

нас в России происходят крупные слияния, поглощения, покупки, появляются оффшорные компании за рубежом, а структура собственников не раскрывается. Никто их не знает.

Для иностранных компаний такая ситуация тревожна. Во многих случаях на Западе обязаны раскрывать структуру собственности, обязаны по закону это делать.

Иванов.

Пару минут для комментария. В 2006 году в Германии в открытом доступе появилась база данных, содержащая персональные данные на 21 млн. человек, т.е. примерно на треть населения страны. Так что утечки информации и за границей имеют место. Много раз мы слышали о подобных скандалах и в Америке, и в других странах.

Языком аналогий поясню свою мысль. Недавно вернулся из поездки по Белоруссии. Еду – идеальная европейская дорога, ни одной машины, чистота, порядок, трасса видна на три км вперед. Качусь под горочку, посреди леса висит знак «30 км». Передо мной идет 412-й «Москвич» с указанной скоростью. Я - за ним. И примерно так всю дорогу. Приехал в маленькую гостиницу к знакомому и попросил его прокомментировать столь строгое соблюдение правил дорожного движения. Он мне отвечает: «Так ведь гаишник поймает». Говорю: «Ну, дал ему денег и дальше катись» (по московским–то меркам). Ответ: «гаишник брать боится – с работы уволят». Т.е. сформулировано некое уважительное отношение к власти, суть которого – отсутствие желания играть в «сером» поле. Даже если и появилась за рубежом та или иная неправомерная с точки зрения законодательства информация, работать с ней нет желания у большинства субъектов рынка, себе же дороже.

Баяндин Николай Иванович (Московский экономико-статистический институт)

Уважаемые коллеги, еще раз добрый день. Я расскажу о деловой разведке и защите ПД на примерах работы с коллекцией БД «Лексиснексис».

Московский экономико-статистический институт – единственный в России ВУЗ, имеющий доступ к этой БД. Лексиснексис – это крупнейшая в мире полнотекстовая коллекция БД, сравнимая по своим возможностям со всем интернетом, включающая около 30 000 баз данных, объединенным единым управлением. Она была создана в 1967 году изначально как БД юридическая - для толкования законов США (в каждом штате свой закон, свои толкования, плюс общие федеральные законы, поэтому разобраться бизнесмену в этом множестве информации бывает достаточно сложно). Коллекция пришла в 1991 году на российский рынок для проверки западных компаний, занимающихся бизнесом у нас. В то время до 75% таких компаний были мошенническими. Для их проверки на предмет принадлежности к преступным группировкам, к неблаговидным намерениям тогда же, в 1991-м году, был заключен договор с этой системой, где имеется большой массив судебной информации, играющей большую роль при оценке деятельности партнера.

Когда мы говорим о проверке западных компаний, надо очень четко отличать американские компании, проверка которых достаточно проста, от тех компаний, которые работают на бирже, и от европейских компаний, которые, в основном, частные и семейные. Семейные компании вообще проверять можно только по косвенным каким-то признакам. Соответственно подход к ПД в США, Канаде, с одной стороны, и в европейских странах - с другой, различается.

В Европе, хотя они и декларируют всеобщую открытость, свободный доступ к информации затруднен, много закрытой информации. Кроме того, есть проблема различия языков. Там напринимали различного рода директивы о защите неприкосновенности частной жизни, о международных обменах персональными данными. Первый документ это конвенция Совета Европы 1981 года об охране личности относительно автоматизированной обработки персональных данных. Вообще, развитие шло по пути защиты именно автоматизированной обработки, поскольку в информационных системах накапливается огромное количество персональных данных.

«Лексиснексис» - очень серьезная система на российском рынке, там имеется много данных о вип-персонале каждой компании. Причем данные, которые можно отнести к персональным данным, например, о зарплате высших чиновников, о бонусах, которые получают они в конце года, о их передвижениях по карьерной лестнице, т.е. достаточно большое количество информации, в том числе и о тюремном заключении. Когда наша компания «Вим-Биль-Дан» выходила на американский рынок, один из владельцев компании находился в местах, не столь отдаленных. В России эта информация закрывалась, а в Штатах обязательным условием является раскрытие всей информации.

В США в 1966 году принят Акт об информации. По этому акту любая информация доступна, если она не закрыта «грифом». Если чиновник не дает ответа на информационный запрос в течение 15 дней, то должен аргументировано объяснить, почему. Если объяснение недостаточно, пользователь имеет право подать в суд на этого чиновника. Поэтому проблема получения информации, проблема западных компаний, в частности, компаний США и Канады, достаточно проста. Причем, через американские системы можно проверить и российские компании. В частности, в БД «Эдгар» такая информация имеется и по нашим чиновникам, и по нашим бизнесменам.

Важный вопрос - соотношение законодательств европейских стран, США и России. Закон, о котором мы сегодня говорим, предназначен, по моему мнению, для того, чтобы у нас была какая-то единая база с мировым сообществом. Но работать он наверно будет плохо, так как при реализации имеющихся в нем формулировок деловая разведка в России может прекратить свое существование. Проблемы будут с информационно-аналитическими системами. Ведь и «Симантический архив», и «Галактика», и «Орион» ориентированы на работу с информацией персонального характера. Строгое выполнение всех пунктов Закона приведет к ситуации, когда все информационные системы лишатся клиентов или уйдут в тень. То есть будут продолжать работу, но не вполне легально, поскольку потребность в деловой разведке существует и будет существовать всегда, а значит, найдут какие-то способы эту потребность удовлетворить. Возьмем, к примеру, «серые» базы - сколько о них говорится, а они продолжают существовать. Но главное ведь даже не в том, что в этих базах часто конфиденциальная информация, а в том, что эта информация похищена.

У нас нет закона о доступе к информации, хотя декларируется, что «страна открытая», «экономика открытая», но на самом деле деловую информацию, не составляющую коммерческую тайну, получить невозможно. Для реального вхождения в Европу потребуется и изменение законодательства, и реализация этих изменений.

О том, как Закон будет действовать, мы узнаем в скором времени после начала его действия. По-видимому, будет несколько громких, так сказать «обучающих», процессов, а потом, наверно, как-то его скорректируют под реалии современного мира.

И еще два слова. У нас в Университете мы одними из первых в России начинаем готовить специалистов в области деловой разведки. Это у нас как специализация проходит, но проблема в том, что в справочнике нет такой специальности и нет стандартов. Но я надеюсь, что стандарт «аналитик информационной безопасности» в ближайшее время появится, поскольку есть потребность и для финансового мониторинга, и для других целей.

Емельянов

Где Вы видите изучение тематики защиты персональных данных - в информационной безопасности или в деловой разведке, у вас же два направления?

Баяндин

Вообще защита ПД – это однозначно информационная безопасность, но она тесно связана и с деловой разведкой, именно в оценке той информации, которую мы получаем о конкретных лицах. Проблема в другом. Есть порядка 6 млн. операторов, библиотеки, школы и т.д. Можно приходить в любую организацию и спрашивать: «работаете с ПД?». Работают все. А дальше требовать соответствия органам ФСТЭК или чему-нибудь подобному. Ваша аппаратура соответствует этим требованиям? 90% ПО не является лицензионным. Это такая хорошая для проверяющих кормушка… Поэтому, сказать-то сказали, а вот как выполнять? Единственная надежда на то, что наши жесткие законы не выполняются.

Унижаев Николай Владимирович (Институт безопасности бизнеса МЭИ (Технический университет)

Прежде всего, хотелось бы, в очередной раз, выразить свою признательность организаторам данной конференции, продолжающим искать точки пересечения при решении задач, связанных с деловой разведкой.

Тема моего выступления: «Особенности поиска информации в социальных сетях в свете требований закона "О персональных данных"

Закону «О персональных данных» более трех лет, выполнение его мне напоминает поправку в правилах дорожного движения «О включении ближнего света вне населенных пунктов». Кто включил, кто не включил, кто-то включил подфарники, а при езде по Московской кольцевой дороге вообще не понятно, следует включать или нет. Да и ГАИ как-то к этому относится с прохладцей. Можно и без поправок обойтись, но тогда отстанем от Европы. Вот и закон «О персональных данных» следует выполнять, но по некоторым позициям выполнить невозможно.

Дадим определение, что следует понимать под термином «социальные сети»? Термин "социальная сеть" был введен в 1954 году социологом Джеймсом Барнсом. Он исследовал связи между людьми с помощью социограмм, то есть визуальных диаграмм, в которых отдельные лица представлены в виде фигур, а связи между ними - в виде линий. Первые социальные сети (иногда их называют «Социальные сети 1.0») в том виде, к которому мы сейчас привыкли, появились в середине 90-х годов и предоставляли пользователям сети интернет начальные возможности для общения, подобно ICQ. На сегодняшний день такие сетевые сервисы, как правило, не рассматриваются в качестве социальных сетей.

К современным Интернет сервисам, имеющим отношение к социальным сетям, можно отнести несколько наиболее распространенных форм организации общения с помощью веб-технологий:
1) Гостевые книги.
2) Форумы.
3) Блоги (от англ. web log — web-журнал, web-протокол).

С появлением новых технологий глобальная сеть Интернет стала способна объединить миллионы пользователей, к социальным сетям стали относить только такие крупные Интернет-ресурсы как «Одноклассники», «В контакте», «Мой мир». Их принято называть «Социальные сети 2.0». С нашей точки зрения, сюда же следует добавить и современные Интернет-игры, такие как The Sims 3, TimeZero, Perfect World, имеющие возможность формирования ролей, событий и диалогов. Сюда же следует отнести и новые ресурсы, такие как Skype. В общем можно сказать, что социальная сеть это интерактивный многопользовательский веб-сайт, контент которого наполняется самими участниками сети.

По данным аналитической службы РБК, более 75% российских пользователей интернета, входящих в данную сеть ежедневно, зарегистрированы, как минимум, в одной социальной сети. Треть активных пользователей в возрасте 15-40 лет зарегистрированы в двух и более социальных сетях. Мотивацией регистрации в социальных сетях становится, прежде всего, общение с друзьями, а также поиск утраченных контактов. В более редких случаях причинами регистрации в социальных сетях могут быть поиск работы или поиск романтических отношений. Следует также отметить, что более половины граждан России в настоящий момент не знают, что такое социальные сети Можно сказать, что социальные сети второго поколения появились в начале этого века, когда стали понятны широчайшие возможности, которые предоставляют социальные сети для всех сфер деятельности. О том, что социальные сети являются неисчерпаемым источником, сотрудникам «коммерческой разведки» известно. Я не буду рассматривать методы и способы добычи данных в социальных сетях, об этом надо говорить отдельно, возможно, посвятив данному вопросу целый семинар. Попытаюсь посмотреть на сбор информации через призму Федерального закона Российской Федерации «О персональных данных».

Использование социальных сетей для проведения аналитических исследований в области безопасности началось с момента их создания. Из четырнадцати опрошенных нами сотрудников экономической безопасности, работающих в банковской сфере, более половины сказали, что используют социальные сети для сбора того или иного рода информации, связанной с незаконной деятельностью. Данные, которые получают в свое распоряжение аналитики - самые разные, начиная с обсуждений незаконных действий и заканчивая фотосвидетельствами. Понятно, что никто не станет обсуждать в социальной сети ограбление банка. Но информацию о том, как можно обмануть, или уже обманывали сотрудников банка, найти возможно. Хотелось бы напомнить, что в соответствии с Законом под персональными данными следует понимать любую информацию, относящуюся к определенному физическому лицу. В том числе - его фамилия, имя, отчество, год, месяц, имущественное положение, образование, профессия, доходы.

Социальные сети в свои базы данных собирают самую разнообразную информацию. Мы отпустим рассуждения о том, с какой целью они это делают. Хотя зная, кто за океаном финансирует проекты социальных сетей, о целях сбора информации в социальных сетях второго поколения не сложно догадаться. Само размещение персональных данных в социальных сетях не противоречит российскому законодательству, так как, согласно статьи 8 пункта 1, с письменного согласия субъекта персональных данных такие данные могут быть размещены и в социальных сетях, попадающих в перечень общедоступных ресурсов. При регистрации каждый участник социальной сети активирует электронный флажок, трактующийся как письменное согласие субъекта. Однако не все так однозначно. Например, в социальной сети «В контакте» наш президент зарегистрирован более 90 раз и судя по размещенной там информации, вряд ли хотя бы одна запись принадлежит непосредственно нашему президенту.

Согласно статьи 9 закона о персональных данных письменное согласие на обработку персональных данных должно в частности включать:
- фамилия и номер основного документа;
- адрес;
- срок, в течение которого действует согласие, а также порядок его отзыва.

Очевидно, все это нарушается при сборе и хранении информации в социальных сетях. Информация, представленная в социальных сетях, может быть частично правильной. Например, при правильных персональных данных с использованием данного механизма вас вместо официального портала http://kremlin.ru/ перенаправят на сайт http://www.medvedev-da.ru, кстати, имеющем свой подконтрольный форум. Работая с информацией, размещенной в социальной сети, оператор не попадает под действия закона «О персональных данных» до момента обработки или использования персональных данных. Под обработкой персональных данных в Законе понимаются действия с персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, использование, распространение, обезличивание, блокирование, уничтожение персональных данных. А под использованием персональных данных следует понимать действия с персональными данными, совершаемые в целях принятия решений.

В Законе оставлена маленькая лазейка, прописанная в статье 2, которая позволяет производить, обрабатывать и использовать персональные данные без ограничения для личных целей. Закон не регламентирует сбор информации, размещенной в социальных сетях с использованием автоматизированных систем. Раз не запрещено, значит, можно считать, что разрешено. Регламентировано только принятие решения на основе исключительно автоматизированной обработки. Другими словами, оператор обязан разъяснять субъекту персональных данных, почему принято то или иное решение. Хранение персональных данных в социальных сетях также не противоречит Закону, так как чаще всего они хранятся в СУБД Oracle или MySQL, имеющих защитные функции, требуемые законом «О персональных данных»

Попробую кратко изложить проблемы, связанные с обязанностями оператора немедленно прекратить по требованию субъекта персональных данных их обработку и удалить информацию из общедоступных источников.

Ситуация первая. Данные в социальной сети появились после регистрации самого субъекта персональных данных. Для удаления данных следует поискать механизм удаления. Именно искать, так как во всех социальных сетях заложен бандитский принцип «За вход рубль, за

выход два». Например, для того, чтобы найти кнопку «Удалить Мой Мир» из ресурсов Mail, необходимо выбрать страницу «Настройки» и, выбрав закладку «Мои настройки», перейти к нижней части страницы, где и расположена кнопка. Примерно такие же действия следует произвести для удаления записи в сети «Одноклассники». Дальше всех в вопросе удаления информации зашли авторы сети «В контакте». В данной сети вообще нет возможности для удаления собственной записи. Удалить ее возможно, только последовательно изменяя записи. Причем, данный механизм, по мнению авторов, предназначен для того, чтобы исключить возможность случайного удаления. Даже после того, когда вы последовательно выберите пункты «Мои настройки» - «Приватность» - «Кто может смотреть мою старицу» - «Только я» - «Сохранить», информация будет удалена только через месяц.

Ситуация вторая. Персональные данные размещены не субъектом персональных данных. Единственная рекомендация в этом случае: обратиться к системным администраторам. Но ответа вы не получите. Несколько месяцев назад с трибуны Государственной Думы прозвучало предложение возложить ответственность за ложную и экстремистскую информацию не только на авторов Интернет-порталов, но и на руководителей хостинга, где размещен данный контент. Так что теоретически можно обратиться к хостеру об удалении информации. Но быстрее всего хостер вам сможет оказать такую услугу, только если у вас имеется решение суда. Фактически тупиковая ситуация, если и портал, и хостинг зарегистрированы вне территории России. Что в этой ситуации делать, я хотел бы спросить у вас.

Подведем итог. Автоматизированный или ручной сбор информации размешенной в «Социальных сетях» не противоречит закону «О персональных данных». Собранные и обрабатываемые оператором данные должны быть зашифрованы и защищены от неправомерного доступа с целью изменения или копирования. Обработка таких данных должна вестись с согласия субъекта персональных данных.

Емельянов

Вопрос: владельца социальной сети можно отнести к оператору ПД?

Унижаев

Насчет владельца я вам не скажу, так же как директор не обязательно будет оператором, но обязательно должно быть должностное лицо, являющееся оператором.

Емельянов

Когда у нас Закон обретет полную силу, займутся, наконец, сетями?

Унижаев

Вряд ли.

Казакевич.

Я объясню почему. Потому, что регулятор сетей – кто?

Емельянов

Там (показывая наверх).

Казакевич.

Вот именно. Не разрешат.

Унижаев

Не разрешат, но этим Законом пользуются. Я вам приведу еще один маленький пример. Недавно был репортаж из Ивановской области о том, как грамотно простой мужчина, совсем не юрист, воспользовался. Коллекторы пришли выбивать долги в какой-то поселочек: продавайте квартиры, всех выгоняем, в общем, достали всех, как у нас говорят. Нашелся один мужчина, который обратился в Следственный комитет при Прокуратуре РФ с

вопросом о том, на каком основании управляющая компания передала ПД людей в коллектор. В результате – поселковый начальник с должности снят, в управляющей компания все начальники сняты, коллекторная компания подлежит ликвидации и т.д. Так что здесь две стороны одной медали, с одной стороны – мы Закона боимся, а с другой стороны он нам нужен.

Шарлот Всеволод Владимирович, эксперт

Я буду говорить об использовании интернет-ресурсов, содержащих персональные данные, в бизнес-разведке и информационно-аналитическом сопровождении бизнеса. На сегодняшний день в Интернете содержится большое количество баз данных и информационных массивов, содержащих персональные данные, многие из которых уже упоминались предыдущими выступающими. Их наполнение может происходить как в соответствии с законом о персональных данных, так и вопреки ему. Все информационные Интернет-ресурсы, содержащие персональные данные, в той или иной мере могут быть использованы в информационно-аналитической (И-А) работе.

Информационные ресурсы, содержащие персональные данные, можно условно разделить на государственные и муниципальные (сайты министерств и ведомств, сайты региональных властей), коммерческие (сайты компаний и различные онлайновые сервисы по поиску информации в различных БД) и частные (социальные сети, персональные страницы, блоги, форумы и т.п.). В сущности, информационно-аналитическому подразделению безразлично, как формируются приведенные выше ресурсы, с нарушением закона о персональных данных или нет. Для решения поставленных перед ними задач нас больше волнует полнота и достоверность содержащейся в них информации.

Задачи, решаемые И-А подразделением, могут носить стратегический, тактический и оперативный характер.

Оперативные задачи – это краткосрочные задачи по поиску ограниченного объема и направленности информации определенной направленности, когда нужно осветить один-два вопроса. Например, установить ФИО и место работы, дату рождения и степень аффилированности. Это могут быть задачи по поиску контактной информации, идентификации людей. Например, известна фамилия, инициалы и сфера деятельности – арбитражный управляющий. Используя сайт Федеральной регистрационной службы, получаем сведения из сводного государственного реестра арбитражных управляющих http://www.rosregistr.ru/index.php?menu=4005150500. Для получения дополнительной информации используется сайт саморегулируемой организации арбитражных управляющих, сайты арбитражных судов и др. сайты в зависимости от поставленных задач..

Решенные И-А подразделением оперативные задачи – это база для принятия оперативных решений руководством (например, для установления официальных или неформальных контактов), начальные сведения для деятельности смежных подразделений и основа для постановки других более сложных задач (тактических и стратегических) для И-А подразделения. Иногда руководству требуется срочно ответить на вопрос: нет ли какой-либо компрометирующей информации на человека? На все дается час времени. При этом руководство не хочет понимать, что это не оперативная, а тактическая задача, компрометирующие данные могут и не лежать на поверхности, а их получение требует сопоставления и анализа многих фактов, которые еще нужно установить.

Тактические задачи – среднесрочные задачи по поиску информации различной направленности. К тактическим задачам можно отнести: проверку руководства партнеров, сбор информации о партнере по переговорам, проверка топ-менеджеров при приеме на работу, выявление утечек информации. Чаще всего приходится решать задачу по проверке физического или юридического лица.

Интернет-ресурсы, используемые при проверке физического лица:

• Телефонно-адресные ресурсы: адрес, состав семьи, контактные данные
• Сайт ФМС: проверка паспорта http://services.fms.gov.ru/passportpermit/

• Интернет-сервисы по поиску информации в ЕГРЮЛ: руководство или учреждение коммерческих структур. Например, «Налоговая справка» http://www.gnivc.ru/spravka.htm
• Сайты раскрытия информации ОАО (годовые отчеты): участие в акционерных обществах, места работы последние 5 лет (например, Информационный ресурс ФСФР России (отчетность эмитентов) http://e-disclosure.fcsm.ru/)
• СМИ: информация о деятельности физ. лица, позиции, которых придерживается человек: (например, ИА «Интегрум» http://www.integrum.ru/ или http://www.public.ru/.)
• Сайты с поиском работы: предыдущие места работы, дополнительная информация
• ВАС РФ: банк решений арбитражных судов РФ http://www.arbitr.ru/bras/
• Черные списки: негативная информация (например, сайт «Проверка водителе» http://drivers-test.ru/)
• Социальные сети: другая информация (http://odnoklassniki.ru/, http://vkontakte.ru/ и др.)
• Сайты выставок, конференций, специализированных изданий и т.п.

Нередко случается, что проверяемое физическое лицо за свою недолгую двадцатилетнюю жизнь уже учредило с десяток различных фирм и настолько работоспособно, что может совмещать руководство еще в пятнадцати компаниях.

Интернет-ресурсы, содержащие персональные данные, также могут быть полезны для И-А сопровождения расследования мошенничества по отношению к компании. Особенно в тех случаях, когда есть подозрения, но факт мошенничества еще не установлен. Примерный алгоритм такой работы может состоять в следующем:
• сбор установочных данных на физическое лицо, подозреваемое в мошеннических действиях
• сбор информации о деятельности подозреваемого лица
• сбор информации о группах общения

Собранная информация позволит сделать вывод о возможности и способности человека совершить мошеннические действия по отношению к фирме, а также возможные мотивы таких действий. Эта информация будет основанием для более глубокого изучения обстоятельств с целью выявления факта мошенничества.

Стратегические задачи – это изучение бизнес и социального окружения фирмы, персональный состав, позиция властных структур, от решений которых зависит бизнес компании.- вопросы, решаемые в рамках бизнес-разведки.

Здесь предметом изучения может стать:
• административное руководство региона и его окружение
• руководители владельцы конкурентов
• руководители государственных и общественных организаций региона, партий, решения/действия которых могут иметь значительное влияние на бизнес (например, руководитель экологических организаций для химических производств и т.п.)
• общественные деятели, имеющие отношение к бизнесу компании
• ученые, разработки которых могут оказать существенное влияние на бизнес
• лидеры преступных группировок, действующие в регионе и способные оказать влияние на бизнес

И-А службу будет интересовать прежде всего биография руководителя, состав его семьи, родственные и деловые связи (бизнес родственников и бывших однокурсников и коллег), членство в профессиональных сообществах, взгляды на самые различные проблемы, отраженные в интервью и самостоятельных публикациях в СМИ, отзывы (официальные и не официальные) его сослуживцев, начальников, подчиненных, экспертов, принятые за карьеру решения и успехи на предыдущих местах работы и т.п. Например, неоднократно при рассмотрении кандидатуры на должность топ-менеджера оказывалось, что он разваливал работу фирм, которыми руководил, доводя их до банкротства.

Начать изучение персоналий бизнес-окружения можно с сайтов властных структур, партий и общественных организаций и биографических БД (например, БД Лабиринт - http://www.labyrinth.ru, Русский биографический институт http://www.whoiswho.ru/, База данных «Современная Россия» http://allrus.info/main.php), но наиболее полезную информацию, видимо, дадут ресурсы содержащие публикации СМИ. Полезными также могут оказаться сайты по раскрытию информации ОАО и выписки из ЕГРЮЛ.

Можно выделить два блока задач:

• Выявление и прогнозирование угроз бизнесу со стороны государственных структур, конкурентов, общественных и политических организаций, криминальных структур (бизнес-окружения компании): лоббистские возможности конкурентов, родственные связи руководителей государственных и административных структур, негативное для компании смена руководителя госструктуры и т.п.
• Выявление возможностей для развития бизнеса (технологических разработок, использования административного ресурса, ослабления конкурентов и т.п.)

Синтез персональных данных, содержащихся в Интернет-ресурсах, позволяет в дальнейшем использовать эту информацию для создания аналитических продуктов: построения матрицы влияния, сетей связи, матрицы возможностей и угроз, PEST-анализ (выявление политических, экономических, социальных и технологических аспектов внешней среды компании) и т.п.

В силу того, что появление возможностей и угроз для бизнеса – процесс, развивающийся во времени, для отслеживания ситуации может производиться мониторинг изменений в бизнес-окружении (изменения в руководстве, среди владельцев фирмы-конкурента и партнеров, а также личных обстоятельств аффилированных лиц).

Отслеживать появление новостей по определенным ключевым словам позволяют поисковые системы Яндекс и Гугл. Такая же возможность есть у ИПС «Артефакт» ИА «Интегрум».

Как правило, персональные данные, содержащиеся в доступных ресурсах, носят поверхностный и внешний характер, но довольно большой пласт данных о личности (определение психологического типа, особенностей мышления и принятия решений) интересующего руководство компании человека может быть получен на основе анализа открытой информации. Речь идет о составлении психологического портрета личности по созданным им письменным документам или по интервью с ним, а также по форме и особенностям лица, используя физиогномику.

Таким образом, можно с полной уверенностью сказать, что чем больше ресурсов, содержащих персональные данные, появляется в Интернете, тем больше необходимой информации можно получить, тем легче в итоге работать И-А подразделению.

Иванов

Я хочу прокомментировать последнего докладчика на одном интересном примере. Этот случай документальный. В свое время группе американских ученых была поставлена задача - собрать информацию из открытых источников о состоянии дел в вооруженных силах США и в техническом плане, и в человеческом. Эта информация была собрана, после чего мгновенно засекречена. Попадание было в точку. Я это к тому, что мы часто, работая с Интернет-ресурсами, из количественного состояния информации переходим к качественному. По людям, работающими в крупном бизнесе, в политике и участвующих в каких-либо общественных организациях, можно создать зачастую достаточно яркие справки. Давайте теперь представим фирму, которая занимается этим из года в год, накапливает такой архив. Согласно закону эта справка должна быть уничтожена после достижения цели ее создания. А во-вторых, в свете Федерального закона любая проверка «отоварит» такую компанию вне очереди. Надо об этом задуматься. Мы собрали данные из абсолютно открытых источников, Интернет – это среда, которая постоянно мутирует, доказать с клавиатурой в руках, что эти данные были взяты с таких-то сайтов невозможно: сайты давно умерли, а материал нет.

Мухин Александр Владимирович (ООО «Научно-исследовательский центр экспериментальных технологий»)

Я представляю научно-исследовательский центр, который уже 15 лет занимается

разработками в области психотехнологий. Мы являемся продолжателями дела, которое начал мой учитель академик Игорь Викторович Смирнов, ныне покойный, к сожалению, по созданию диагностики подсознания и изменению поведенческой парадигмы человека. За эти 15 лет нам удалось расшифровать те алгоритмы, которыми оперирует головной мозг при обработке визуальной и слуховой информации и на основе этих алгоритмов создать систему диагностики подсознания, которая обладает двумя качествами: 1) ее невозможно обмануть даже теоретически; 2) человек при его тестировании не осознает смысла задаваемых вопросов.

Происходит это следующим образом. Мы преобразовываем исходное текстовое изображение или предложение, ответы на которые нас интересуют, обрабатываем теми самыми найденными алгоритмами, и это изображение превращается в кодированное изображение исходного вопроса. Для любого нормального человека такое изображение не несет никакой смысловой нагрузки, однако, зрительный анализатор у нас - кора головного мозга – декодирует и восстанавливает текст исходного вопроса. Таким образом, последовательно выводя на экран любого проецирующего устройства ряд закодированных изображений и регистрируя физиологические реакции, которые могут быть любые – и сложные зрительно-моторные реакции, и реакции потоотделения, и частоты сердечного ритма, есть еще очень много реакций интересных – мы можем проводить опросы и получать информацию из подсознания человека, которая нас интересует.

Подбирая соответствующие группы вопросов или формируя группы вопросов, мы можем абсолютно точно, как мы говорим, с математической точностью и статистической достоверностью не ниже 95%, получить ответы напрямую от подсознания. Кроме того, подсознание не может мыслить категориями «если», поэтому ответы строятся всегда однозначно: или он есть, или его нет – ответа. На сегодняшний день разработана действующая технология, она уже тестируется в интернет-среде, т.е. в тестовом режиме открыта для пользования в интернете.

Достоверность результатов тестирования - не ниже 95%. Достигается очень просто: мы один и тот же вопрос задаем не менее пяти раз, после этого обрабатываем статистическим модулем, который говорит, что ответ на этот вопрос абсолютно не случаен по уровню не менее 95%. Мы могли бы поставить 4 критерия, как в науке принято: 95 % - нижний предел достоверности, 99; 99,9 и в конечном итоге 99,99. Но тогда бы уже речь шла о приговоре. Чтобы не начинать с приговоров, мы выставили нижний предел достоверности данных, извлекаемых из подсознания человека по уровню 95%. Валидность данных – это мера соответствия того, насколько поставленные вопросы отвечают целям и задачам тестирования. Это значит, что если мы подбираем группу вопросов, относящихся к теме: «вор, украл данные, инсайдер ли он, занимается ли левым бизнесом, занимается откатами, сидел ли он в тюрьме, любит ли он Машу или Ларису» и т.д., и т.д., а мы не имеем ограничений по номенклатуре вопросов, т.е. по лингвистическому, смысловому, семантическому содержанию этих вопросов, то, отвечая на эти вопросы, мы математически точно и статистически достоверно восстанавливаем картину всех его эмоций, желаний и намерений. Кроме того, так как мы вопросы готовим в текстовой форме, а для подсознания является принципиально важным только устойчивый навык чтения и формирование вопросов на родном языке человека, то мы можем описать любую картину или задавать любые вопросы, которые нас интересуют, и на основании этого строить уже всю картину желаний и намерений человека в любой области, будь то личная сфера, сфера безопасности и т.д.

Наша система называется автоматизированная система мониторинга персонала, куда уже разработаны и введены соответствующие вопросы, тесты, решающие определенные задачи. Это в первую очередь задачи найма персонала, когда человек приходит, дает документы и мы начинаем по системам типа скоринговых (как собирают инфор0,мацию в банках), ГИБДД, МВД, правовых органов, где бы он мог засветиться, составлять мнение о нем. В данном случае мы этого не делаем по той причине, что подсознание обманывать не может, оно не мыслит логическими конструкциями, кроме того, предусмотрены алгоритмы математической обработки и статистической. Поэтому, когда человек в течение 5-10 минут тестируется на вопросы о воровстве, его подсознание нам отвечает – «да, был судим, сидел; да, воровал»; «я казачок засланный», если вы пришли устраиваться на работу, чтобы «слить» информацию, то, отвечая на ряд вопросов, его подсознание говорит – «да, я тот, кого вы ищете».

Тесты не только по подбору персонала, но и по выявлению инсайдеров. Проблема инсайдеров будет расти, расти и расти по мере развития информационных технологий в связи с тем, что ценность информации тоже растет. Поэтому вычислить «засланного казачка» - проблем никаких нет. Мы задаем вопрос – «вы хотите «слить» информацию из базы данных (можно конкретно название БД)?» или «вы хотите устроиться на работу в организацию для «слива» информации (название организации)?». Подсознание также отвечает – «да», вплоть до того, что если мы спрашиваем какое звание у человека, оно рассказывает - и какое звание у человека и с каким заданием пришел. Главное подобрать ряд вопросов.

Где может применяться эта технология? Я не знаю сферы, где бы она не могла применяться, начиная со сферы безопасности и заканчивая процессом обучения детей и школьников - почему у них неуспеваемость, какие у них нагрузки, какие у них проблемы дома, в семье, из-за чего агрессия возникает и т.д., и т.д. Я не буду говорить о перспективах этой технологии, для нас они определены, просчитаны, убеждать я никого не буду, надо попробовать и посмотреть, что это такое.

Фактически мы извлекаем из подсознания и формируем цифровой эквивалент психики человека. Это очень важно и принципиально по одной простой причине – как только мы получили реальный достоверный цифровой эквивалент психики человека, у нас есть принципиальная возможность обрабатывать эти данные с помощью аналитических методов. Это и системы извлечения данных скрытых, и системы прогнозирования, и системы построения моделей ситуационных. Таким образом, мы не говорим, что это у нас «детектор лжи», это был бы абсолютно не тот подход, это только вершина айсберга. Технология дает нам возможность строить по аналогии с ситуационным центром точно такую же информационно-аналитическую систему, только в области психики. Раз есть цифра, мы ее можем обработать.

Мы проводили исследование в юридическом отделе крупного банка, там из 8 юристов двое сидят на откатах. Мы ввели в систему данные контрагентов, с кем они работают (в электронном документообороте это все есть) и суммы сделок, которые они ведут, мы подсчитали даже потенциальные убытки, на которые организация могла бы «попасть». Каким образом? Суммы откатов известны – проценты от сделок, в определенных сферах в определенных сделках определенные проценты. Суммы сделок есть. Подсчитываем потенциальные убытки.

Система такова. Центральный сервер располагается в интернет-зоне, свободный доступ через логин-пароль, через регистрацию соответствующую. Заходите в систему … Да, перед этим надо получить от нас бесплатное клиентское приложение к этой системе, которое превращает любой компьютер, подключенный к интернет, в наш терминал, на котором осуществляется выбор тестов, назначение тестов (если это администратор, то он назначает тесты), анализ этих тестов, анализ данных и бухгалтерия есть. Терминал – это место тестируемое, он видит только одну-единственную вкладочку маленькую, у него существует только возможность выбора назначенных тестов, когда их пройти - сейчас или позже. Администратор управляет всей системой, аналитик следит за результатами тестирования и обрабатывает информацию, как в частности, так и в целом.

Вот заглавная вкладка: формирование структуры всей организации – поскольку центральный сервер в интернете, терминалы находится в любой точке мира, то мы можем протестировать филиал из Москвы, будь то в Нью-Йорке, будь то на Луне, лишь бы связь была вай-фай или более дальняя. Каждому тестируемому назначается свой логин и пароль, поэтому идет его идентификация, чужой не зайдет. Здесь аналитик выбирает и назначает тесты (в нашей системе на сегодняшний день более 3000 тестов) – или конкретным людям, или всему подразделению, или всей организации. Тестируемый видит только эту вкладку – слева назначенные тесты, справа кнопочка «Пройти тестирование». Результаты – выбор результатов и просмотр результатов тестов. Это осуществляет только аналитик. Данные группируются, как я уже говорил, в определенные темы, объединенные единым смыслом. И на основании таких данных мы получаем профиль человека, профиль всех его желаний и намерений. Цифровой профиль, то, о чем мы говорили.

Обнаруживается удивительная вещь – мы можем создавать, накапливать, разрабатывать новые профили, выявлять закономерные профили. Если к нам человек пришел с соответствующим профилем по каким-то темам, то система автоматически определяет – к

нам пришел казачок и он хочет получить откат от такой-то организации. Этот хочет украсть болт или гайку. И система начинает сигнализировать. И получается интересный протокол, мы его называем «индикатор угроз». Так как это все-таки аналитическая система, значит, она должна уметь сигнализировать о критическом состоянии коллектива или человека, его психики.

Удобно использовать принцип светофора – красный, желтый, зеленый. Он всем понятен, не требует объяснений. Красным загорится - мы называем это «расстрел на месте».

Четыре категории риска выдается:

1.«Расстрел на месте». Это люди, которые уже делают правонарушения с точки зрения либо закона, либо нормативной базы организации.

2. Это те, кто хотят что-то сделать, они еще ничего не сделали, но начинают предпринимать активные действия.

3. Люди, которые не имеют криминальных желаний, наклонностей, но имеют порочные связи. У нас был простой случай. В банке тестировали группу лиц. Высветились две позиции у одного человека – наркотики и обман банка, негативная реакция. Стали разбираться, более уточняющие тесты создали, ввели, оказалось, что человек знает, что употребляет наркотики, что это незаконно с точки зрения банка, и он боится потерять свое место работы. Поэтому был вынужден обманывать банк. С точки зрения безопасности бизнеса эта угроза на момент тестирования не представляет большой опасности. Почему? Потому, что у него еще не кончились деньги, еще не возникла потребность, чтобы ему кто-то дал взятку или он заработал эти деньги каким-то неправомерным деянием.

4. Абсолютно индифферентные или безопасные люди, это значит, что сфера их намерений и желаний находится вне тех тем или вне тех интересов, на которые мы их тестировали. В данном случае мы личную сферу опускаем и говорим о том, что нас не интересует, хотите ли вы поехать в Майами позагорать, или вы сейчас влюблены. Мы принимаем к сведению в первую очередь те данные, которые касаются непосредственно угроз бизнесу. Все они абсолютно легко формализованы. Вот как я вам на русском языке рассказываю, точно также мы беседуем с подсознанием. Мы формализуем все виды угроз.

Теперь мы подходим к тому, как видеть динамику. Пришел человек на работу – у него одни устремления, три месяца проработал – у него уже другие цели и задачи. Помните, раньше говорили, что директора общепита через два года надо переводить в другую столовую, кафе, ресторан. Почему? Проворовывается. Так и здесь. Пришел человек, адаптировался на рабочем месте и через полгода начинает искать источники дополнительного заработка. Если официально нет перспективы карьерного роста, значит, начинается отторжение имущественных прав от организации и т.д., использование в личных целях. Это все мы здесь видим. Опять-таки, делаем профили, отбираем людей, которые пришли, по профилям, через 5-10 минут мы отбираем из тысяч человек того, кто нас устраивает, и следим за ним. Только появился профиль угрозы безопасности бизнеса, система сама включит красный сигнал.

Информационно-аналитическая система тем и хороша, что может анализировать не только личность, но и группу людей под любыми срезами. Никто нас не ограничивает в этом плане. Я не буду сравнивать наше методологию с «детекторами лжи», хочу только сказать, что это самая нормальная аналитическая система, которая позволяет делать не только срезы текущие, но и осуществлять прогноз поведения человека.

Вот, в принципе, и все. Прошу, вопросы.

Голос из зала.

Какова стоимость?

Мухин

У нас стоимость от 9 центов до 50 долларов за тест в зависимости от его сложности. Через Web Money оплачиваете, получаете доступ в систему, точнее доступ в систему у вас есть всегда, но вот тест выбрать, пройти его, это после оплаты. 500 рублей перечислили,

попробовали – работает. Пожалуйста.

Голос из зала

На ваш взгляд, насколько законно, когда работодатель обязывает своих сотрудников проходить тестирование?

Мухин

Первое – мы работаем в правовом поле полиграфа. Второе – у нас режим тестирования не включается, пока человек не нажмет кнопочку «согласен», мы его предупреждаем, что мы собираемся в процессе тестирования извлечь сведения даже не персонального, а личного характера. Вы согласны на прохождение процедуры? И две кнопочки – «да», «нет». Все. И еще добавлю, пользование системой осуществляется на основании публичного договора оферты, где все это расписано.

Голос из зала

Сколько времени занимает прохождение теста и его обработка?

Мухин

Обработка доли секунды занимает, а время прохождения теста - в зависимости от его сложности, потому, что сложные задачи бывают, когда большое количество вопросов надо задавать, это где-то 15-20 минут. Я вам скажу: 25 минут - это 375 статистически достоверных ответов на вопросы. Для сравнения - полиграф дает 60 вопросов, статистически не будем говорить каких, за два часа.

Голос из зала

Был бы человек хороший, а статью мы вам найдем. Статья 18 ФЗ о ПД: пункт 1: «запрещается принятие на основании исключительно автоматизированной обработки решения о ПД», т.е. статью мы вам подберем.

Мухин

Отлично. Если вы обратили внимание, мы тоже подстраховались, у нас автоматизированное рабочее место аналитика. Мы даем рекомендательный характер с точки зрения законодательства. И если у него цифровые данные, то здесь многое зависит от аналитика.

Голос из зала

А честные люди вообще в бизнесе есть?

Мухин

Я вам так скажу – чем выше уровень должности, тем меньше морально-этических норм. Мы получили этому экспериментальное подтверждение на достаточно большой выборке реципиентов.

Иванов

Вы только не намекайте, никаких фамилий.

Мухин

Да нет, что вы, боже упаси. Более того, у нас предусмотрено исключение персональной информации, такой как ФИО, например, можно под номерами регистрировать и, таким образом, дистанцироваться.

Голос из зала

А скажите, пожалуйста, обследуемый человек проинформирован, на какую тему его тестируют?

Мухин

Да, конечно. И это в предупреждении выводится.

Голос из зала

И второй вопрос. Как можно легализовать результаты вашего тестирования, например, можно ли уволить человека по соответствующей статье УК?

Мухин

Наверное, самый сложный вопрос вы задали. Проблема ведь даже не в легализации результатов, а в законодательной базе. У нас даже законодательной базы по полиграфу до сих пор нет. А вы говорите – взяли, уволили. Но мы ведь взрослые люди и понимаем, что можно найти тысячу причин. Но я вам скажу другое: уволить - это не лучший выход, поверьте. Мы это знаем на большой статистике. На сайте у Варламова – автора русского полиграфа – есть уникальная информация о том, на что мало кто обращал внимание. Он распределил всех людей, и мы увидели у себя этому подтверждение, следующим образом: 10-15% - априори непорядочных людей, 75-80% - люди, которые характеризуются одной фразой «я сделаю это, если...», и у каждого свое «если», величина этого «если», и еще 10-15% - генетически порядочные люди, которые никогда, ни при каких обстоятельствах не сделают правонарушение, эти люди на костры идут и т.д. Такая статистика. Поэтому ставить в вашем контексте вопрос, я думаю, не разумно.

Продолжу свою мысль. Что происходит с тем большинством, которое составляет в среднем 75-80%? Они требуют контроля и все – тогда они будут работать честно. Но бывают ситуации... Как жизнь толкает на совершение правонарушений? Когда возникает очень большая необходимость в чем-то. Например, вопрос стоит о здоровье личном, или ребенка, или родственников. А нужны деньги. Человек попытался получить официально – не получилось. Он идет на какое-то правонарушение, если ищет какой-то источник дохода. Уникальность в том, что мы можем его перехватить в этот момент, сказать « у тебя такая проблема, но не нужно ее решать здесь, давай мы отдельно разберемся, что у тебя случилось?» В этом случае система сигнализирует о состоянии психики человека, сотрудников, и мы можем подбирать системы стимулирования. Одному нужно раз в месяц поздороваться за руку с руководителем, и он будет счастлив и отлично работать, другому – постоянно увеличивать премиальный фонд заработной платы, а третьему – новая машина. Это мотивационные характеристики человека. Все это индивидуально. В одном из банков мы разработали такую схему. Замначальника безопасности банка, проходя мимо сотрудницы-юристки через месяц после тестирования (специально выждали срок, чтобы не было явно связано), говорит: « Нехорошо, Юлия Васильевна, с той компанией играть, вы же понимаете». И ушел. Мы протестировали опять через месяц весь коллектив, 50 человек. И что вы думаете? Чиста как белый снег.

Голос из зала

Ну, так, наверно, можно говорить с любым.

Мухин

Не надо. Давайте не будем уходить на персоналии. Но я вам скажу, что вы не правы. Если человек не участвует в правонарушении и не обдумывает это участие, то вы ему, хоть говорите, хоть не говорите. Это - не значимая для него информация. Он может, кстати, обидеться, что вы его оскорбили своей подозрительностью. На это он, скорее всего, обидится, если он честный и порядочный человек.

Голос из зала

Ну и начнет зарабатывать....

Мухин

Ну не факт, кстати, у нас есть такая тема, она называется «Увольнение», когда мы точно видим, хочет человек уволиться или боится увольнения. Секретов-то теперь нет.

Емельянов

Александр Владимирович, а ваша разработка запатентована?

Мухин

Да, мы два месяца назад получили первый патент российский, и буквально неделю назад к нам пришло уведомление из-за границы о патенте Пи-Си-Ти, т.е. международном.

Емельянов

И второй вопрос. Какой-нибудь независимый эксперт или группа экспертов вашу разработку тестировали на истинность, что ли?

Мухин

Официальной сертификации еще не было, это у нас стоит в плане на ближайшие полгода. Мы отдаем в НИИ психиатрии на кафедру клинической психологии для верификации этой системы и получения официального заключения. Кроме того, у нас уже были в различных коммерческих структурах столько всяких расследований, некоторые согласились дать рекомендации.

Емельянов

И это на сайте можно увидеть, да?

Мухин

Нет. Проблема в том, что мы сайт открыли год назад и закрыли. Почему? Тема нетривиальна и пока мы еще не готовы к широкомасштабному внедрению, мы не хотим баламутить общественность преждевременно. Когда будет готово, тогда мы и откроем.

Емельянов

Каковы ваши амбиции в завоевании рынка вашей системой?

Мухин

В систему введено 60 тысяч населенных пунктов по всему миру, это официальные данные ЮНЭСКО. Все языки, которые поддерживаются Windows.

Голос из зала

Как вы так смогли «раскрутиться»?

Мухин

А мы еще не раскрутились.

Голос из зала

Какие банки профинансировали?

Мухин

Сами. Сам зарабатывал и вкладывал. Но у меня есть один инвестор, который на последней стадии помог, а так - за 15 лет, потихонечку, step by step. Все это на полу-коленке потому, что никакого бюджетного финансирования, конечно, не было. А когда к кому-то из инвесторов приходили, они говорили: «Этого быть не может, идите – гуляйте!». Так и догулялись. Теперь можно посмотреть, попробовать.

Голос из зала

Какие гарантии, что собранные вами данные не попадут к третьим лицам?

Мухин

Первое: шифруется канал передачи данных между клиентом и сервером, и второе: база данных тоже шифруется. 100%-ной гарантии, извините, дать никто не может. Я могу гарантировать, что мои сотрудники, как и я, впрочем, проходим регулярное тестирование,

и инсайдеров у нас нет. Ну а хакеры – проблема из проблем.

Голос из зала

Но у вас же обезличенная информация.

Мухин

Нет, она не обезличенная. Нам иногда вносят ФИО, данные о должности.

Баяндин

Сколько вы по времени храните персональную информацию?

Мухин

Хороший вопрос, Николай Иванович…Вообще, нам эта информация нужна. Мы делаем точно такую же систему, как сделали банки - скоринг. Скоринг формирует мнение о человеке на основании третьей информации, да? Базы чужие. Он из них выбирает информацию, формирует и говорит – вот профиль надежного заемщика. А мы общаемся с подсознанием человека и говорим, что вот этот заемщик такого-то возраста, такого-то уровня образования, может быть, место рождения, специальность, должность, пол и т.д. и т.д. – вот его профиль. Есть идея создать даже государственный центр сертификации по морально-этическим нормам государственных служащих. Вы думаете, дадут? Нет.

У нас есть тест на алкогольные предпочтения. Когда мы начинали демонстрировать свою технологию, то нам часто задавали вопрос: «А вот как в полиграфе, отгадай цифру от 1 до 10 загаданную?». Но для подсознания цифры от 1 до 10 абсолютно ничего не значат. Волевым усилием нагнать эту цифру, выдавить ее - невозможно. Нет эмоционального события в памяти, которое запечатлелось бы с этой цифрой. Думали-думали, придумали. Взяли и перечислили спиртные напитки, а потом - вопросы, связанные с этой темой – «хочу выпить», «хочу вмазать» и т.д. - т.е. сленг, мы обязаны учитывать тот сленг, на котором думает человек. И что выдумаете? И тут – поперло. Коньячок, виски, можно разновидности вносить, кто «Хеннеси» любит, кто «Блэк Лейбл».

Иванов

Александр Владимирович, если я правильно понял, подсознание испытуемого абсолютно устойчиво к условиям, в которых проходит тест. Вот меня взяли и посадили в комнату с парниковыми условиями – тишина, комнатная температура, никаких раздражающих световых факторов и вообще я в нормальном состоянии. И второй вариант – меня ввели в стрессовую ситуацию, ударили, посадили в СИЗО и туда принесли компьютер с вашей программой. С разницей в полчаса. Результат теста, профиль будет один и тот же или разный?

Мухин

Почти один и тот же. Это очень тонкий вопрос с далеко идущими последствиями. Почти один и тот же. Почему? При небольшой временной разнице почти один и тот же профиль выходит. Потому, что у нас все время крутится в подсознании, или как мы говорим, постоянно идут ментальные процессы. И если вы обратили внимание, то во многих книгах этот процесс называется «мешалка». Мы думаем об одном, когда нас везут на допрос, мы надеемся: может, сейчас в офис привезут, а не в подвал. Если в подвал привезли – у нас уже другие мысли: как бы в кресло посадили, а не к батарее пристегнули. И все это будет видно, т.е. будет временной срез. Еще есть режим интересный – характер человека. Когда мы мониторим его регулярно, например, раз в месяц, раз в квартал, статистика уже допускает вторичную статистическую обработку, и тогда мы вытаскиваем стабильные структуры в психике, которые говорят, что вот это – его характер. То, что текущее - сегодня одни мысли, завтра другие, вести себя вот так, но за определенный период – полугодовой, месячный, если мы сделаем минимум пять тестов, то мы скажем, что вот эти черты или вопросы – стабильны. Можно сделать описательную характеристику черт личности – работоспособность, энергичность и т.д. Тогда мы четко скажем, а вот это – его характер.

Иванов

Т.е. тесты накапливаются, и их корреляция дает в итоге абсолют?

Мухин

Нет. Абсолют дается сразу. Почему? Вот мы тестирование провели, статистикой обработали и это статистически достоверно, но является динамическим портретом, текущим, т.е. что он хочет сделать. В качестве примера приведу интересный случай. Приехали люди из одного города, мы их протестировали, видим, что люди – из спецслужб, потому, что соответствующее отношение и к оружию и т.д., влияет специфика работы на результаты. Так вот, у одного выпала одна единственная тема – страх. И так сильно «горит красным» тема «страх», все остальное – ерунда. Нужно было создать новый тест, чтобы узнать, в чем причина. Я ему говорю, что у него «горит» тема «страх», я не знаю почему, поскольку не было вопросов, дающих расширенное понимание этой темы. Но я тебе за пять минут соберу новый тест и точно скажу, чего ты боишься – то ли смерти, то ли кражи, то ли еще чего-то. Он говорит: «Согласен». Тут мне стало интересно и я говорю: «Объясни, откуда у тебя такая тема, ты - человек тренированный, из спецслужб, морально-политическое состояние и т.д...». Он говорит: «Ты знаешь, две недели назад купил новый джип»... А мы тогда сидели в здании, на территорию которого его автомобиль не пустили. Он говорит: «Я издалека приехал, боюсь, угонят с проезжей части и все...». Вскочил и побежал смотреть... Машина, слава Богу, на месте было.

Черкасс Юрий Владимирович (ЗАО «Рэйнвокс»)

Конечно, можно долго обсуждать достоинства или недостатки 152-го ФЗ о ПД. На мой взгляд, там много непонятных и противоречивых положений, но, тем не менее, закон этот действительно нужен, чтобы положить конец беспределу и безответственности. Необходимо государственное регулирование этой сферы. Какие-то проверки Роскомнадзор осуществляет, какие-то решения суды выносят, тем не менее, общаясь с нашими клиентами, общаясь с потенциальными заказчиками, мы видим два лагеря - одни говорят, что все плохо, другие – что все хорошо. Наверное, каждая организация, каждая компания решает для себя индивидуально: будет она выполнять требования Закона или наших регуляторов в области технической защиты (ФСТЭК и ФСБ) или будет уповать на то, что, например, документы ФСТЭКа в Минюсте до сих пор не зарегистрированы, в СМИ они не появлялись, а «потому мы их выполнять не должны».

Теперь о рисках.

Неисполнение Закона чревато серьезными рисками. Гражданско-правовыми исками со стороны клиентов и сотрудников сейчас мало кого удивишь, пострадать в нашей стране более, чем на 2 тысячи рублей маловероятно, если не причинен существенный вред здоровью.

Есть еще и репутационные риски. Здесь многое зависит от того, насколько крупная компания подвергается рискам, эти риски могут быть выражены в денежном эквиваленте.

Принудительное приостановление и прекращение обработки персональных данных.
Если крупный банк, то вряд ли он этого испугается. Это я говорю по опыту собственного общения с представителями банковской сферы. То же самое могу сказать и о крупном операторе связи. Не думаю, что наших «трех китов» лишат лицензии, если произойдет очередная утечка. Пожурить, наверно, пожурят. И достаточно сильно. Но лицензии не лишат. Все-таки их работу не остановить.

Привлечение компаний и руководителей к административной и другим видам ответственности, предусмотренной нашим законодательством. Здесь могут быть различные штрафы, вплоть до увольнения. Нарушения установленных Законом правил сбора и хранения, нарушения неприкосновенности частной жизни - далеко не весь

перечень норм законодательства, за нарушение которых сегодня предусмотрена ответственность. Если не ошибаюсь, максимальный штраф на сегодня – это 500 000 рублей для юридического лица. А также увольнения и/или запрет занимать определенную должность, отзыв лицензии и т.д.

Насколько чувствителен штраф в полмиллиона рублей для крупной компании... не знаю, тут риск каждый для себя оценивает сам. Хотелось бы привести аналогию с европейским законодательством, на которое многие уповают. Говорят, что в Европе все хорошо, они защиту информации строят, исходя из оценки ущерба и оценки риска информационных утечек. Это мировая практика – и европейская, и американская. В США за сокрытие факта утечки базы данных – уголовная ответственность, а в Европе – штраф до полумиллиона евро. Вот здесь стоит задуматься. Если бы у нас были такие штрафы, тогда можно было бы не прибегать к жесткому техническому регулированию защиты ПД, а действительно давить штрафами, тогда бы руководители организаций задумались – может, мне проще 300 тысяч на защиту потратить, чем 500 тысяч на штрафы.

Несколько слов об обязанностях по защите информации. Хочу остановиться на пункте 17 Закона, соответственно которому ответственность за защиту возлагается на разработчика. Здесь возникает вопрос о сертификации. Многие говорят, что нас обязывают использовать сертифицированные средства защиты. Мы как компания, которая занимается технической защитой, прекрасно понимаем, что полностью поменять существующий парк вычислительной техники на сертифицированный не каждая компания в состоянии. Изучая международные положения, нормы, стандарты по информационной безопасности, находим, что практически везде присутствует пункт о том, что производитель средств защиты информации должен гарантировать отсутствие в них различных угроз или уязвимости типа Бэкдор (backdoor), говоря языком наших регуляторов - не декларированных возможностей. При этом должна быть еще и соответствующая техническая документация к этим средствам защиты. Это нормальная международная практика.

В чем заключаются обязанности оператора? Начинать надо с определения перечня персональных данных, которые есть в компании. Затем в соответствии с приказом определяются категория персональных данных и цель их обработки, т.е. мы должны понять и локализовать, где эти персональные данные у нас обрабатываются. Необходимо направить уведомление в уполномоченный орган. Сроки давно истекли, но до сих пор очень многие операторы уведомление не направили. Пока это никак не карается, и будет ли караться в будущем, тоже сказать не могу. После этого надо крупными мазками разработать систему защиты ПД, подготовить документы, регламентирующие обработку ПД. Реализовать требования по инженерной защите помещения и провести аттестацию, когда это необходимо.

Можно выделить два направления работы – организационно-правовое и техническое. Если с организационно-правовым направлением все более или менее понятно, то к техническому претензий очень много, так как документы ФСТЭК по сей день являются закрытыми. Нам говорят, что региональные представительства Федеральной службы по техническому и экспортному контролю готовы их предоставить по запросу, но в открытом доступе на сегодняшний день их нет. В отличие от документов ФСБ, которые уже давно опубликованы.

Организационно-правовое направление - это выявление наличия или отсутствия признаков работы с ПД, определение, какая информация относится к ПД, формирование перечня информационных систем ПД, - то есть все действия по локализации информационной системы.

Разработка и совершенствование существующей нормативной базы. Трудовые договора с соответствующими пунктами, положения и инструкции - это нормальная практика по защите той коммерческой тайны. И ничего нового защита ПД с точки зрения внутренней нормативной базы не вносит.

Выявление наличия рисков – это анализ нормативной базы, регламентирующей деятельность предприятия, анализ функциональной структуры, анализ взаимодействия с внешними организациями. Немаловажно, что зачастую в отношениях с внешними организациями, такими как пенсионный фонд, налоговая служба, системы типа «клиент-банк» и другими, с которыми осуществляется передача и обмен ПД, очень остро встает

вопрос разграничения ответственности. Мы, полагаясь на русское «авось», думаем, что пока не случилось – ну и ладно. А когда случится, долго будем искать – кто виноват, вы или банк, вы или кредитное бюро, вы или коллекторное агентство, откуда утечка произошла.

Формирование перечня информации, относимой к ПД. Вопрос сложный и зачастую требующий согласований и оснований. Паспортные данные – это данные второй или третьей категории? С одной стороны, паспорт это документ, который позволяет однозначно идентифицировать личность. Он для этого и предназначен. С другой стороны, там есть прописка, может стоять штамп с группой крови. Здесь надо подходить с позиции здравого смысла. Если мы общаемся на фуршете и обмениваемся визитками, то абсурдно спрашивать разрешение. У каждого из нас есть мобильный телефон, у меня там более 200 записей, причем с э-мейлами, домашними адресами, днями рождения и т.д. Брать согласие в каждом случае – это же абсурд.

Выявление способов обработки ПД по классификации с использованием и без использования средств автоматизации. Принципиально разные подходы к защите. Без использования средств автоматизации – это, по сути говоря, обеспечение безопасности съемных носителей данных, бумажных носителей, флешек, съемных жестких дисков.

Выявление особенностей обработки. Та же самая локализация по подразделениям: одно подразделение, отдельный компьютер, распределенная какая-то система. Естественно, исследование возможности снижения категории. Почему выделили этот пункт? Зачастую обрабатывается излишняя информация. В одной компании, например, есть поле записи «национальность». На вопрос, нужна ли она для работы, говорят – нет. Так уберите и снижайте категорию. В некоторых организациях строго определено, к примеру, содействие оперативно-розыскным мероприятиям. Там четко перечислено, что должно предоставляться в рамках содействия, какая информация должна храниться и предоставляться.

Формирование перечня информационных систем. Есть кадровые системы, есть бухгалтерские системы, другие системы.

Определение состава и структуры каждой информационной системы ПД и технических особенностей ее построения. Состав и структура программного обеспечения, технические средства обработки, топология. Здесь мы делаем акцент на техническую защиту, при проверке все должно быть задокументировано.

Определение состава и структуры взаимодействия с внешними структурами. Это то, что я уже перечислял – коллекторские агентства, Центробанк, кредитные бюро и т.д. в зависимости от сферы бизнеса.

Разработка и совершенствование существующей нормативно-правовой базы организации. Это административно-распределительные документы предприятия, нацеленные на организацию работы.

Положения об обработке ПД. Это, наверное, самый верхнеуровневый документ, который должен быть в компании, независимо от количества информационных систем ПД, подразделений и т.д.

Инструкция о порядке обработки ПД с использованием средств автоматизации и без использования таковых.

Должностные инструкции для персонала, который выполняет обработку, соглашения и т.д.

Вообще говоря, анализ всех постановлений правительства, нормативных документов ФСТЭКа и ФСБ - это порядка 30 документов, с криптографией еще больше. Начиная от верхнеуровнего и заканчивая журналом учета носителей информации, которые должны быть в организации.

Техническое направление работ. Выявление уязвимых звеньев и возможных угроз безопасности, разработка концептуальных документов (т.е. каким образом мы вообще собираемся защищать), разработка новой или существующей нормативной базы и организация работы с ПД в рамках модернизации (если она существует), разработка новой системы обработки ПД.

Порядок классификации систем. Первичная классификация. Есть информация и оператор. Мы классифицировали, что это система ПД по признакам: ФИО, ИНН, возможно, национальность, расовая принадлежность.

Определение характеристик. Т.е. мы определили их объем, и к какой категории они относятся. И затем первичная классификация, т.е. что это у нас такое – система с использованием средств автоматизации или без использования. С выходом осенью прошлого года постановления правительства о неавтоматизированной обработке, очень много было радостных восклицаний – «Ура, нам ничего делать не надо!». Но если взять международные законодательства, например, Директивы Евросоюза, то там автоматизированной обработкой считается обработка, выполняемая полностью или частично с использованием средств автоматизации. Настольный компьютер – это средство автоматизации, поэтому та формулировка, которая дана в постановлении правительства, вызывает у меня лично некоторое недоумение, я ее не понимаю.

Характеристики безопасности персональных данных. Основные – конфиденциальность, целостность, доступность; дополнительные – учетность, аутентичность, адекватность.

Все системы обработки с использованием средств автоматизации делятся на типовые информационные системы (по классификации ФСТЭК) и специальные. Также отдельно выделены информационные системы обработки ПД по требованиям ФСБ, потому что в компетенции ФСБ находится криптографическая защита (а техническая защита - в ведении ФСТЭК).

Порядок классификации. Достаточно грустная картина, потому что практически все системы попадают в первый и второй класс. Я имею в виду более-менее крупные компании, а не кадровую службу в организации, где работают 30 сотрудников. Поэтому защита типовых систем, учитывая жесткость предъявляемых требований и отсутствие некоторой гибкости в этих требованиях, является не самым оптимальным способом защиты.

Типовая система. Алгоритм – есть требование ФСТЭКа, классифицировали, присвоили класс 1, 2, 3 или 4 (напомню – это общедоступные ПД, или обезличенные, или вообще не ПД – социальные сети), выбор меры и средств защиты (за нас уже выбрали ФСТЭК и ФСБ, все четко, по каждому типу).

Что такое «специальная система»? Информационная система относится к классу «специальная», если помимо требований конфиденциальности к ней предъявляется любое другое требование. Например, целостность или доступность. По нашему мнению 99% систем относится к классу специальных. Классический подход к обеспечению безопасности – это всегда треугольник: конфиденциальность, целостность, доступность.
Да, бывают ситуации, когда какую-то одну из этих характеристик не обязательно обеспечивать. Но это случается редко. Второе - информационные системы, в которых находятся данные по состоянию здоровья. Это более всего касается медицинских учреждений. И третье - это информационная система, которая подлежит принятию исключительно на основании автоматизированной обработки, влекущей за собой юридические последствия и т.д. Системы, которые представлены в третьем пункте, автоматически попадают в разряд «специальных». Хотя, честно говоря, если это система относится к третьему пункту, то там помимо конфиденциальности еще требуются целостность и доступность.

О конфиденциальных системах. Здесь есть некоторая гибкость. Т.е. существуют требования по защите ПД, но требования эти предъявляются на основании определения актуальных угроз. Т.е. если вы относите систему к разряду типовой, то вы на батарее должны будете ставить вибро-датчики. Так обязывает ФСТЭК. Хотя надо понимать, что иностранные спецслужбы вряд ли захотят узнать данные по вашим сотрудникам, сотрудникам вашей компании. Даже базы данных абонентов федерального уровня сотовой связи продаются, спецслужбы за этим охотиться не будут. Базы выносятся изнутри, с батареи их точно не снимают. Тем не менее, требования есть. Поэтому данный подход является более гибким. Т.е. вы говорите, что эта угроза для вас действительно не актуальна. Если в случае проверки вы документируете, что угроза утечки по вибро аккустичекому каналу для вас неактуальна, я не думаю, что вам скажут, что вы неправы, что для вас это актуально, покупайте и ставьте средства защиты. Главное, все документировать и аргументировать.

Далее - разработка специальных требований и выбор мер и средств защиты. В чем «плюс» этого подхода – выбор мер и средств защиты осуществляете вы и осуществляете в соответствии с определенными вами актуальными угрозами, т.е. защищаетесь вы только от того, что действительно актуально.

Выявление уязвимых звеньев – следующий шаг. Опять же при определении актуальности угроз вы оцениваете возможность физического доступа, каналы утечки, возможность электромагнитного излучения, заражения вирусами и т.д. Естественно, это всегда индивидуально, понятно, что информационные системы у всех разные.

Оценка ущерба. Если ущерб у вас будет на 5 рублей, а защита стоит 5 млн. рублей - наверное, это нецелесообразно. Здесь бы хотелось вспомнить концепцию 1992 года по обеспечению безопасности, где говорится, что средства защиты не должны существенно снижать функциональность информационной системы потому, что «навесить» можно столько, что она просто работать не будет.

Анализ имеющихся в распоряжении средств защиты. Здесь хочу отметить, что тоже есть много негативных отзывов. В операционной системе есть штатные средства защиты. Ввод пароля – это тоже средство защиты, если вы правильно настроили парольную политику, то выполняете требования наших регуляторов. Контроль целостности можно осуществлять также штатными средствами баз данных, просто должно быть включено логирование. Ничего дополнительно закупать не надо, достаточно правильно настроить существующую систему.

Следующий шаг - формирование требований, их обоснование в случае необходимости использования криптологической защиты. Здесь часто задают вопрос – всегда ли мы должны использовать сертифицированные средства криптологической защиты? Ответ – не всегда.

Обоснование требований при взаимодействии с внешними организациями. Здесь важен вопрос разграничения ответственности в случае чего.

Разработка концептуальных документов. Формирование требований по обеспечению безопасности ПД. Проведение оценки актуальных угроз (в рамках разработки модели угроз), разработка модели нарушителей, исследование возможностей оптимизации требований к информационной системе. Проанализировав угрозы, вы можете решать, как сократить перечень актуальных угроз. Возможно, это потребует незначительных изменений в вашей информационной системе, но при этом будет большая экономия: угроза переходит в разряд неактуальных и перечень требований к обеспечению безопасности сокращается.

Автоматизированная система по требованию ФСБ. Обязательна разработка модели нарушителей угроз. На основании этой модели выбирается класс средств криптографической защиты, ее уровень. Хочу пояснить – их шесть классов, шестой – это когда вы предполагаете, что ваши ПД представляют интерес для иностранных спецслужб.

Обоснование требований по обеспечению безопасности. Определение целесообразности использования криптосредств, о чем мы уже говорили. Не всегда это целесообразно. Вы можете не использовать криптографические средства, потому, что они вам не нужны. И тем самым не закупать дорогостоящие средства защиты.

Определение требуемого уровня технической защиты, утечки по техническим каналам и т.д., на которых реализованы криптосредства. Дело в том, что средства вычислительной техники, на которых реализуются криптографические средства защиты, тоже должны быть защищены от несанкционированного доступа, а это уже входит в ведение ФСТЭК.

Система без обработки. Здесь мы имеем больший опыт. Это и архивное делопроизводство, и сейфы элементарные, и журналы учета носителей.

Тот принцип, который пропагандирует наша компания, это принцип отраслевых стандартов. Т.е. базовые модели верхнего уровня, которые разработаны у наших регуляторов, некая прослойка отраслевой модели, где оговорен состав ПД (для разных отраслей они разные), предметные риски (для каждой отрасли они свои, например, в банках они одни, в «Телекоме» - другие, в медицинской сфере – третьи), и классы

специальных информационных систем. Т.е. некий внутренний классификатор сделан. А дальше уже на основании отраслевых неких моделей, неких классификаторов - определение тех мероприятий и требований к технической защите, которые будут реализованы в частной компании.

Организации работы с ПД в компании позволит оптимизировать бизнес-процессы, снизить категорию, а как следствие, и класс, снизить трудозатраты сотрудников, нормативно закрепить основы обработки в компании, сократить жалобы и обращения граждан, проходить проверки (попросили у вас документацию – да, пожалуйста, все есть - положения, инструкции, смотрите, проверяйте, система документирована).

Итак, что делать конкретной компании по шагам?

Разработка концептуальных документов. Кроме последнего пункта – экономического обоснования системы – документ этот не является обязательным с точки зрения руководителя организации, но является обязательным с точки зрения ответственного за безопасность ПД, потому что ему бюджет нужно обосновать перед руководителем. Поэтому здесь мы его включили.

Разработка и совершенствование нормативной базы. Здесь подробно останавливаться не буду, более 30 документов, включая различные журналы. Это задача, реализуемая внутренними силами, не такие большие документы.

И организация – непосредственно техническая часть. Кроме модернизации системы, возможно внедрение новых систем и настройка существующих, разработка эксплуатационной документации - обязательно, потому что если Роскомнадзор проверяет верхнеуровневые документы, то ФСТЭК и ФСБ будут проверять именно техническую эксплуатационную документацию. Проведение мероприятий по получению лицензий, если необходимо. Необходимо не всегда. Ну и так далее, заканчивая аттестацией, которая тоже не всегда необходима в зависимости от класса системы.

Баяндин

Два вопроса. Первый. По вашему мнению, кто на предприятии будет заниматься защитой ПД, секьюрити? Или какие-то надо создавать специальные подразделения, особенно в организациях, где раньше никогда не занимались информационной безопасностью - институтах, школах, детских садах и т.д.? Т.е. сразу потребуется расширение штата, подготовка специалистов, оснащение техникой. И второй вопрос. Вы сказали об отраслевой нормативной документации. Это очень правильная мысль. В банковской сфере все понятно – есть Центробанк, который выпускает документацию, а в других сферах, на кого это должно лечь и как это организовать?

Черкасс

По первому вопросу. Действительно, со школами, государственными и медицинскими учреждениями ситуация тяжелая, потому что в штате таких специалистов нет. Действительно, в соответствии с законодательством, необходимо ответственное лицо за защиту ПД, назначенное внутренним приказом. Каким образом это реализовать – не знаю, затрудняюсь ответить.

Баяндин

Но для тех, кто работает с информационной безопасностью, проблем-то особых нет.

Черкасс

Опять же, если взять компании, где есть IT специалисты, но нет отдельных подразделений информационной безопасности, то нормально, когда ответственность возлагается на IT службы. У меня есть информация, однако подписываться под ней не буду, что во ФСТЭК направлено письмо с просьбой разработать инструкцию, которую можно было бы разослать по образовательным учреждениям. Чтобы они, по крайней мере, двигались в едином направлении и не наломали дров. Но насколько я знаю, из ФСТЭКа пока никакого ответа нет.

Иванов

Юрий Владимирович, я правильно понимаю, что школа или любая другая коммерческая или некоммерческая организация имеет право привлечь вас, специалистов сторонних, к обеспечению выполнения закона?

Черкасс

Имеет. Но где она деньги возьмет?

Иванов

В соответствии с законом оператор ПД не имеет право передавать защиту третьим лицам. Ведь вы мне настроили систему, вы ее поддерживаете, а, следовательно, априори имеете доступ к ним…

Черкасс

Но не знакомлюсь с ними, так же как ФСТЭК во время проверок не имеет право знакомиться с ПД. Т.е. я проверяю правильность эксплуатации средств защиты, их настройки, но я не лезу с саму базу.

Казакевич Олег Юлианович (Ассоциация российских банков)

В ходе обсуждения возникли вопросы – откуда взялся этот Закон вообще? В силу активного выхода российского бизнеса на мировой рынок появились проблемы взаимодействия со своими западными партнерами, которые работают в поле несколько иных стандартов практически во всех сферах. Евросоюз потребовал от России ратификации конвенции о защите ПД. Поэтому Закон является продуктом политического решения государства.

Его опубликование вызвало бурю эмоций на всех уровнях. Когда стали заниматься прикладным исполнением Закона, то оказалось, что его концепция довольно ущербна. Произошла абсолютизация персональных данных применительно к физическому лицу. Это первый аспект. Персональные данные являются ничем иным, как идентификатором субъекта правоотношений. Это два. И, в-третьих. Два первых момента создали конфликт интересов между субъектом правоотношений (физическим лицом), юридическим лицом и государством, что мы и имеем на сегодняшний день.

Эти проблемы породили эффект очень медленного внедрения Закона в повседневную жизнь. Да, будет вам известно, что ФСТЭК и ФСБ разработали первый вариант документов только в марте этого года. Кроме того, документы не находятся в соответствии с нормативными документами, не произошла их регистрация в Министерстве юстиции и, следовательно, выпущенные руководящие документы юридической силы не имеют. До сих пор.

С учетом абсолютизации безразличных к сфере использования в различных секторах экономики, в различных отраслях народного хозяйства персональных данных, тот вариант Закона, который хотели выпустить как универсальный – не получился. И многое будет отдано, очевидно, на рассмотрение отраслевых регуляторов.

Более того, применение Закона требует очень существенной корректировки законодательства. Как уже говорил, Закон не учитывает, что ПД являются идентификатором субъекта правоотношений. Поэтому понадобится корректировка очень многих законодательных актов.

Решая для себя задачу в банковской сфере экономики, мы подготовили три проекта о внесении изменений: в Закон о банках и банковской деятельности, в Закон о Центральном банке, в сам Закон о ПД и плюс в ряд статей гражданского кодекса.

Мы работаем в тесном контакте с законодателями, в первую очередь с Комитетом по

безопасности Государственной Думы, под крышей которого был принят этот закон. Спешу вам сообщить новость, что мы и другие бизнес-структуры все-таки уговорили Комитет по безопасности ГД, который будет представлять все поступившие предложения по усовершенствованию Закона, чтобы принять решение об отсрочке исполнения данного закона на 1 января 2011 года (такое решение действительно было принято в декабре 2009 года – редакция). Почему нужен перенос? Во-первых, необходимо внесение изменений в ряд законодательных актов, во-вторых, для любого сектора экономики подготовка и реализация положений Закона, нормативных документов ФСТЭК, ФСБ и других регулирующих органов потребует достаточно много времени. И к тому же мы потеряли целый год из-за запоздалой подготовки нормативных актов, мы потеряли время для внесения в бюджеты организация расходов, связанных с внедрением систем по реализации Закона о ПД. Для банковского сектора экономики мы подсчитали, что для одного среднего банка с 5-7 филиалами внедрение этих систем (несмотря на то, что во всех банках уже существуют автоматизированные банковские системы, причем с учетом того, что там встроенная система криптографии) цена вопроса - 54 млн. рублей. Почему так получилось? Я объясню. В статье 26 Закона о банковской деятельности банковская тайна распространяется только на счета, вклады и операции. К сожалению, Закон о банковской тайне не охватывает вкладчика, носителя персональных данных.

В.Светозаров, учредитель и редактор журнала «Бизнес-разведка»

Как регулируется работа с персональными данным в Европе и США
(обзорная статья)

В Европе сегодня более 50 стран жестко регулируют использование персональных данных. Их законы базируются на принципах, зафиксированных в двух Директивах Евросоюза:

- Директива 1995/46/ЕС Европарламента о защите данных;

- Директива 2002/58.ЕС об условиях работы с персональными данными и защите личных прав в сфере электронных коммуникаций.

Первая Директива касается вопросов сбора, хранения, раскрытия и использования персональных данных. Вторая – налагает ограничения на использование персональных данных в теле и интернет-маркетинге, других видах электронной коммуникации.

Распространено мнение, что Директива 1995 года является частью законодательства каждой страны Евросоюза. На деле это не так. Директива декларирует общие принципы, реализация которых возлагается на национальные законы. В рамках этих принципов каждая страна – член Евросоюза может вводить дополнительные ограничения. Поэтому законодательства в этой области разнятся от страны к стране. К тому же надо отметить, что в ряде стран законы об ограничении использования персональных данных появились еще до Директивы 1995 года. Так, в Германии федеральный закон был принят в 1977 году, во Франции, Дании, Норвегии в 1978 году.

Европейские законы о персональных данных (далее ПД), фокусируют внимание на процессах работы с ними – сбор, запись, систематизация, хранение, передача, уничтожение. Трактовка ПД носит самый широкий смысл. Она включает практически любую информацию, относящуюся к личности. Закон защищает такую информацию как, например, телефонный номер, адрес, дата рождения, вероисповедание, членство в профсоюзе.

Компания может использовать ПД только если субъект информации однозначно дает на это свое согласие, получив от компании соответствующий запрос. Запрос должен носить подробный, исчерпывающий характер, четко указывающий, какую информацию предполагается собирать, с какой целью, кто это осуществляет, будет ли эта информация предоставлена третьей стороне, какие меры обязуется компания предпринимать для предотвращения несанкционированных утечек. Компания также должна предоставлять

субъекту право знакомиться с собранной о нем/ней информацией.

Персональные данные могут собираться исключительно для разрешенной законом цели. Вторично использовать их для иных, не декларированных задач, запрещено. Собственно данные, подлежащие сбору и применению, строго ограничиваются рамками заявленной цели. Срок хранения данных также ограничивается временем, которым исчерпывается достижение поставленной цели.

Организации, которым разрешено создавать и работать с базами персональных данных, берут на себя обязательства соблюдать конфиденциальность, исключать риск потери, злоупотребления, несанкционированного допуска, утечки, преждевременного уничтожения. Это означает, что организация обязана остановить свой выбор на провайдере, который способен предоставить достаточные гарантии безопасности и конфиденциальности. При этом требуется составление письменного документа, содержащего такие обязательства и гарантии.

Субъект имеет право не только знать, кто и зачем хочет собирать о нем/ней персональные данные, но и каковы используемые источники. То есть, знать, у кого уже имеется персональная информация, что собой она представляет, для кого она предназначается. У субъекта есть право знакомиться с этой информацией, изменять ее, если она не точна, уничтожать ее, запрещать ее использование для прямого маркетинга или в cookies.

Особо строгие ограничения оговариваются относительно прямого маркетинга. Коммерсанты не могут использовать ПД для этой цели, не получив предварительно четкое, недвусмысленное разрешение самого субъекта. Более того, уже однажды получив согласно правилам такое разрешение, скажем, его/ее электронный адрес для рекламы продуктов и услуг, коммерческая организация имеет право вторично использовать e-mail адрес только для рекламы аналогичных продуктов и услуг.

Для контроля за соблюдением закона и правил в странах Европы создана система мониторинга. Каждая организация обязана уведомлять соответствующий государственный орган (агентство) о характере и целях работы с ПД. В каждой стране уполномоченный орган власти обязан иметь регистр операций с ПД. Любой желающий может с ним ознакомиться.

Европейские Директивы ограничивают передачу персональных данных за пределы Евросоюза. Она может состояться только при условии, что страна-получатель «обеспечивает адекватный уровень защиты». На сегодняшний день Евросоюз признает таковыми немногие страны, в их числе, Аргентину, Канаду, Швейцарию. Передача ПД из Евросоюза другой стороне должна получить согласие субъекта информации.

В Соединенных Штатах регулирование в этой сфере намного либеральнее. Оно отдано на откуп отраслевым ассоциациям и бизнес-объединениям. И это различие в подходах создает проблемы для американских компаний, работающих с персональной информацией. В принципе любой проживающий в странах Евросоюза может подать в суд на американскую компанию, занимающуюся в Европе прямым маркетингом, если ее действия не соответствуют местному законодательству. Например, в случае использования электронного адреса без разрешения его владельца. Это и вопрос конкуренции, затрагивающий интересы американского бизнеса.

Американцы предложили Евросоюзу план т.н. «безопасной гавани», предусматривающий сертификацию заинтересованных организаций США при условии их обязательства соблюдать все принципы Директив. Европейцы, однако, уклоняются от принятия этого плана, но переговоры продолжаются между Министерством торговли США, с одной стороны, и Евросоюзом, отдельными его членами, с другой, с целью выработки компромиссного решения.