УДК 346.246:681.3

Н. А. Урман

ПРОБЛЕМЫ РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОГО ОБЕСПЕЧЕНИЯ НАЛОГОВОЙ СЛУЖБЫ В МИ ФНС №1 ПО РЕСПУБЛИКЕ ХАКАСИЯ

Сегодня во всем мире признано, что информация является важнейшим средством организации и регулирования частной и общественной жизнедеятельности, одной из форм закрепления и распространения имеющихся и приобретаемых знаний, действенным инструментом и материей управления. Движение к информационному обществу еще более усиливает роль информации в решении любых человеческих проблем. В таких условиях получение новой информации, хранение и поиск уже созданной, адекватное понимание и актуальное использование информации становятся очень трудным делом, требующим времени, сил и средств, создания специальных структур (систем), применения новейшей техники и технологии. Работа с информацией превращается в обширное и массовое занятие людей, а сама информация выступает основным источником интенсификации и гармонизации общественного развития. Перед обществом стоит проблема овладения информацией, ее организации, каналов движения, способов осмысления и оценки, механизмов эффективного использования на практике.

Ключевые слова: *коммуникация, информационные системы, носители информации, программные элементы, налоговая инспекция, Интернет, компьютерные сети, база данных, налоговая отчетность.*

Государство является обладателем, носителем и распорядителем публичной власти. Важнейшее и необходимое условие функционирования власти – получение, анализ, выдача и эффективное использование информации – новых сведений, характеризующих управленческую ситуацию, снижающих уровень неопределенности, воспринятых, понятых и оцененных как полезных для решения тех или иных задач управления. Поэтому информация как совокупность каких-либо сведений, характеристик чего-либо, фактов, данных о соответствующих предметах, явлениях, процессах, отношениях, событиях и т.д., собранных и систематизированных в пригодную для использования форму, составляет основу государственного управления. По существу все управленческие процессы – это не что иное, как поиск, фиксация, анализ, оценка, закрепление, распространение социальной информации, т.е. той информации, которая связана с отражением, познанием и преобразованием различных форм жизнедеятельности людей.

Массовая коммуникация – это процесс сообщения информации с помощью технических средств – средств массовой информации и коммуникации (печать, радио, телевидение, компьютерные сети и т.д.) – численно большим аудиториям. Разновидностью массовой коммуникации является коммуникация в государственных органах, осуществляющих функции государственного управления. Таким образом, коммуникация связывается, с одной стороны, с процессом передачи информации, с другой – с процессом человеческих взаимодействий, с общением. Анализ модели управления коммуникациями в налоговых органах предполагает построение классификации коммуникационных потоков. Эта классификация может быть осуществлена по ряду оснований и представлена в табл. 1.

Таблица 1

Классификация коммуникационных потоков в налоговых органах

Основания классификации	Типы коммуникационных потоков
По отношению к системе управления	Внутренние Внешние Маркетинговые
По направлению	Вертикальные сверху вниз Вертикальные снизу вверх Горизонтальные внутри отделов Горизонтальные между отделами
По содержанию передаваемой информации	Директивные Аналитические Оценочные Отчетные Согласования
По механизму трансляции	Формальные Неформальные

Информационное обеспечение органов государственной власти основывается на принципах, важнейшие из которых:

– объем и каналы информации, поступающей к органу государственной власти, должны определяться функциями, возложенными на этот орган;

– разграничение компетенции между различными структурами государственной власти и организация их взаимодействия.

Информация и процессы информационного обеспечения, с нею связанные, в настоящее время становятся основным условием функционирования любых субъектов государственной власти и принятия решений на любом уровне. Подтверждением этому является появление и глубокое проникновение во все социальные институты, прежде всего в органы государственной власти, новых информационных технологий управления.

Новые информационные технологии позволяют использовать при работе с информацией компьютерную технику и телекоммуникационные средства связи. Внедрение новых информационных технологий существенно изменяет содержание различных видов деятельности, прежде всего управленческой, повышает эффективность управления, выводит на новый, более высокий уровень информационное обеспечение процессов принятия решений органами государственной власти.

На основе совершенствования налогового администрирования необходимо создать условия упорядочения и упрощения налоговых процедур, форм и методов налогового администрирования, позволяющих увеличить количество налогоплательщиков, добровольно исполняющих свои налоговые обязательства. С этой целью в последние годы и идет реформа налоговых органов, в корне меняя управленческие инструменты и технологии.

Региональные налоговые инспекции все больше превращаются в предприятия обслуживающего типа, предоставляющие достаточно широкий спектр услуг и перерабатывающие огромные объемы информации. В то же время применение новых налоговых и информационных технологий требует структурных изменений. В период модернизации налоговых органов с 2001 по 2012 г. в Межрайонной инспекции ФНС России №1 по Республике Хакасия несколько раз менялась структура.

Структура налогоплательщиков, состоящих на учете в инспекции, приведена в табл. 2.

Таблица 2

Структура налогоплательщиков на 01.01.2013 г.

Постановка на налоговый учет	Юридические лица	Физические лица, занимающиеся предпринимательской деятельностью	Физические лица
В МИ ФНС России №1 по РХ	5 692	9 437	236 107

В инспекции стопроцентная оснащенность персонала современной вычислительной техникой. Имеются локальная вычислительная сеть на 250 пользователей и отдельная локальная сеть для доступа в Интернет. Реализована виртуальная подсеть для удаленного доступа специалистов инспекции к Федеральным Информационным Ресурсам (ФИР), сопровождаемым МИ ФНС России по ЦОД. В течение последних четырех лет на основании приказов ФНС России в инспекции ведется более 40 объемных информационных ресурсов. Финансирование осуществляется только из средств федерального бюджета. В рамках реализации ведомственных целевых программ инспекция с 2004 г. в централизованном порядке стабильно получает современную вычислительную и множительную технику, в том числе сервера для хранения, обработки и анализа поступающей информации, а также обеспечения доступа налогоплательщикам к информационным ресурсам инспекции.

Информационная политика инспекции направлена на:

внедрение эффективных налоговых технологий с учетом новых принципов взаимодействия с налогоплательщиком и новых технических средств обработки и передачи данных, осуществление модернизации механизма исчисления и взимания налога;

повышение уровня информатизации, а соответственно, и эффективности работы налоговых органов;

мониторинг общественного мнения;

взаимодействие с другими территориями и структурами;

анализ и прогнозирование (проведение аналитической работы);

формирование интегрированной информационной базы в территориальных и федеральных налоговых органах и электронного банка данных;

информирование налогоплательщиков и развитие у людей чувства сопричастности, гражданской позиции.

Здесь используются самые разнообразные инструменты коммуникаций: локальные (внутренние) и глобальные (Интернет-технологии) компьютерные сети, СМИ, коммуникационные каналы связи, «гостевые» компьютеры, организация семинаров, брифингов, пресс-конференций, информационные стенды и материалы, консультационные центры, «витринные» сервера и т.д.

Федеральная налоговая служба уже давно ведет работу по переходу всех налоговых органов на сертифицированное централизованное программное обеспечение. Наш регион не является исключением.

В настоящий момент в инспекции эксплуатируется более двадцати различных централизован-

ных программных продуктов (ПК ЭОД – местный уровень, ЕГРИП, ЕГРЮЛ, ПИК Банковские счета, ПИК НДС, СчетаФактуры, Пересечение границ, RNAL, АИС НАЛОГ, ПИК Недействительные паспорта, ПИК Совокупный доход, Беларусь обмен, ПИК Однодневка, программы статистической отчетности, ПИК Регистрация, ДКС Кадры, ПК СЭОД и др. Основным программным продуктом для инспекции является Программный Комплекс ЭОД – местный уровень. Система ЭОД на основании первичных данных о налогоплательщиках, налоговых начислениях и платежах формирует информационные базы местного уровня и обеспечивает к ним доступ в качестве пользователей всем подразделениям налогового органа.

Система ЭОД инспекции местного уровня построена в соответствии со следующими основными требованиями:

1. Обеспечение информационного обслуживания и инструментальной поддержки всех функциональных подразделений инспекции.

Обеспечивается функционированием в подразделениях соответствующих типовых автоматизированных рабочих мест (АРМ), разработанных департаментом модернизации налоговых органов ФНС России. АРМы ориентированы на прием и регистрацию налоговой информации, ее обработку, анализ и прогнозирование, информационное обслуживание, принятие управленческих решений, выпуск налоговых документов, администрирование.

2. Высокая технологичность обработки налоговой информации.

Основополагающим принципом для разработки ПК ЭОД являлась унификация методов обработки информации и пользовательского интерфейса. Вследствие чего все рабочие места спроектированы на базе унифицированного рабочего места со стандартным интерфейсом и единым методом обработки информации. Типовые методы обработки (поиск, формирование и обработка запросов, расчет пени и др.) тиражируются во все АРМы системы.

3. Создание банка данных о налогоплательщике.

Введено понятие «Досье налогоплательщика», где в электронном виде накапливается информация статистического и аналитического характера, в частности вся сигнальная информация по налогоплательщику.

4. Обеспечение персональной ответственности сотрудников инспекции за принимаемые управленческие решения.

Достигается учетом в системе ЭОД деятельности сотрудников налоговой инспекции. Ведется «Досье инспекторов», где накапливается статистика об объемах выполненных ими работ, ведется учет управленческих решений и действий, совершенных в системе.

5. Обеспечение высокой надежности и достоверности данных.

Кроме общепринятых организационных, технических и программных методов, в качестве основного метода обработки информации в системе ЭОД принят метод запрещения модификации данных за предыдущие временные периоды.

6. Широкое информационное взаимодействие на электронных носителях и по каналам связи с лицами и организациями, заинтересованными в обмене информацией.

Обеспечивается наличием средств приема массовой входной информации от сторонних организаций и лиц, наличием эффективных средств поиска информации в базе данных и наличием средств формирования массивов выходной информации.

7. Высокие аналитические возможности системы.

Обеспечивается возможностью настройки и формирования аналитической отчетности и возможностью формирования критериев для анализа и прогнозирования.

Обработка информации в системе ЭОД по юридическим и физическим лицам ничем не отличается, что соответствует организации деятельности инспекции по функциональному принципу. В системе используется и ведется более 400 таблиц нормативно-справочной информации (НСИ). Для актуализации базы данных (например, расчета пени, фиксированного сальдо), ее корректировки и формирования документов, предназначенных для печати и последующей рассылки плательщикам, в системе ЭОД используются специальные программы – Технологические процессы.

В инспекцию поступают сведения из различных регистрирующих органов: ЗАГСа, паспортно-визовой службы, Регионального управления технической инвентаризации, Росрегистрации, Роснедвижимости и др. Для обеспечения единых принципов обработки информации в ФНС России в 2005 г. были направлены предложения по разработке унифицированных единых стандартов на законодательном уровне для обмена со сторонними организациями. И только за 2006 г. на уровне ФНС России в целях обеспечения возможности представления в электронном виде сведений органами, учреждениями и организациями в соответствии с Налоговым кодексом и на основании постановления Правительства Российской Федерации было

утверждено 12 форматов файлов представления информации в инспекцию в электронном виде, что существенно позволило увеличить объемы приема и обработки поступающей информации [1].

Кроме того, в ФНС России были направлены предложения перевести часть реквизитов, участвующих в обмене данных, из «условно-обязательных» в «обязательные» (например, ИНН плательщика, который используется уже во многих государственных ведомствах и организациях).

Таким образом, применение типовой системы налоговых технологий и процедур, а также наличие современной системы электронной обработки данных (ЭОД), адаптированной к условиям функциональной организации инспекции, обеспечивает:

наиболее рациональное использование трудовых и материальных ресурсов за счет использования единых нормативных, методических, инструктивных, учебных материалов, технических, программных средств;

ослабление влияния «человеческого фактора» (влияния личных качеств сотрудника на результаты работы), так как позволяет сформировать единые требования к квалификации и подготовке персонала;

- процесс управления и контроля деятельности налоговых инспекций со стороны регионального налогового органа, за счет возможности принимать единообразные управленческие решения и контрольные действия по отношению к подчиненным налоговым инспекциям.

Развитие системы представления отчетности в электронном виде является одним из наиболее перспективных направлений работы налоговой инспекции. Работа по внедрению системы представления информации в электронном виде активно продолжается. Например, рост объемов сдачи налоговой и бухгалтерской отчетности в электронном виде в МИ ФНС России №1 по Республике Хакасия представлен в табл. 3.

Таблица 3

Динамика представления налоговой и бухгалтерской отчетности в электронном виде

Состояние на	01.01.2011		01.01.2012		01.01.2013	
Всего налогоплательщиков, сдавших отчетность	Юр.лица	Физ.л.	Юр.л.	Физ.л.	Юр.л.	Физ.л.
	2732	2167	1382	2076	1559	2228
Количество налогоплательщиков, представивших отчетность по ТКС	1246	810	802	927	1002	1058
Удельный вес	45,60%	37,4%	58%	44,7%	64,30%	47,5%

Представление данных налоговых деклараций, бухгалтерской отчетности и иных документов, служащих основанием для исчисления и уплаты налогов, в электронном виде и по телекоммуникационным каналам связи имеет свои преимущества:

– экономия рабочего времени (нет необходимости посещать налоговую инспекцию);

– отсутствие дублирования (представление данных в электронном виде по телекоммуникационным каналам связи не требует дублирования этих документов на бумажных носителях);

– избежание ошибок (при формировании данных налоговых деклараций и иных документов, служащих основанием для исчисления и уплаты налогов, и бухгалтерской отчетности с использованием средств входного контроля налогоплательщику предоставляется возможность ее подготовки в формате с контролем заполнения полей форм отчетности);

– возможность оперативного обновления форматов представления документов в электронном виде по телекоммуникационным каналам связи (в случае изменения форм налоговых деклараций и иных документов, служащих основанием для исчисления и уплаты налогов, и бухгалтерской отчетности или введения новых форм деклараций налогоплательщик автоматически получает возможность обновления версий форматов);

– возможность получения выписки, справок, уведомлений, «виртуальной» сверки и другое (отправив запрос в налоговый орган в электронном виде по телекоммуникационным каналам связи, налогоплательщик имеет возможность получить выписку о выполнении обязательств перед бюджетом, справки об отсутствии задолженности, уведомлений об уплате налогов или выявлении недоимки и другое);

– оперативное информирование (возможность получения общедоступной информации от налоговых органов, например, о действующих налогах и сборах, изменении законодательства о налогах и сборах и принятых в соответствии с ним нормативных правовых актах и др.);

– подтверждение доставки отчетности (налоговый орган высылает квитанцию о приеме налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи);

– конфиденциальность (использование ключей шифрования и электронно-цифровой подписи);

– оперативность обработки информации, избежание технических ошибок (отчетность, направленная в электронном виде по телекоммуникационным каналам связи, проходит входной контроль и не позднее следующего рабочего дня с даты регистрации в налоговом органе осуществляется ввод данных налоговых деклараций и бухгалтерской отчетности, поступивших в электронном виде по телекоммуникационным каналам связи в АИС «Налог», в том числе сумм налогов, подлежащих уплате в бюджет, по данным налогоплательщика, отраженным в налоговых декларациях, в карточках лицевых счетов налогоплательщиков).

С 2007 г. для удобства плательщиков Управление Федеральной налоговой службы по Республике Хакасия является единственным в Хакасии бесплатным удостоверяющим центром. Кроме того, во втором квартале 2007 г. проведено внедрение и опытная эксплуатация унифицированной системы круглосуточного приема, хранения и первичной обработки запросов и налоговых деклараций и бухгалтерской отчетности в электронном виде по телекоммуникационным каналам связи ПК «ГНИВЦ ПРИЕМ» и ПК «ГНИВЦ ПРИЕМ Регион» с использованием WEB-технологий («витринный» сервер).

Для бесплатного обеспечения налогоплательщика программными продуктами в холле здания инспекции установлен один «гостевой компьютер» с пишущим CD-, DVD-ROMами. Запись программных продуктов на электронные носители производится налогоплательщиком самостоятельно. При использовании компьютера на видном месте возле него размещен перечень имеющихся программных продуктов и подробная инструкция о действиях налогоплательщика при осуществлении записи этих программных продуктов.

В настоящее время Федеральная налоговая служба предлагает через Интернет заполнять налоговые платежные поручения, оформлять заявки на получение ИНН, узнавать о пенсионных отчислениях и долгах по налогам. Чтобы воспользоваться этими возможностями, нужно зайти на сайт налог.ру раздел «Электронные услуги».

На официальном сайте налоговой службы РФ налог.ру доступны следующие услуги и сервисы физическим лицам и организациям:

1. «Адрес вашей инспекции» позволяет налогоплательщику по своему адресу узнать номер своей налоговой инспекции.

2. «Интерактивная карта Управлений ФНС России по субъектам РФ» позволяет найти нужное Управление ФНС России по субъекту РФ и перейти на их сайт.

3. «Заполнить платежное поручение» – позволяет подготовить платежные документы на перечисление налогов, сборов и иных платежей в бюджетную систему Российской Федерации в электронном виде.

4. «Узнай свой ИНН» – позволяет узнать свой ИНН физическому и юридическому лицу.

5. «Обратиться в ФНС России» – является дополнительным средством для обращений физических и юридических лиц в Федеральную налоговую службу.

6. «Личный кабинет налогоплательщика» – предоставляет пользователям возможность осуществлять поиск информации о задолженности по имущественному, транспортному, земельному налогам, налогу на доходы физических лиц (только для физических лиц, граждан РФ) и распечатать платежный документ (извещение) по форме №ПД (налог).

С сентября 2011 г. ФНС запустила «Личный кабинет налогоплательщика-2», который позволяет:

– получать налоговое уведомление об уплате транспортного, земельного, имущественного налога в электронном виде;

– самостоятельно формировать и распечатывать налоговые уведомления и квитанции на уплату налоговых платежей;

– оплатить транспортный, земельный, имущественный налоги;

– обращаться в налоговые органы без личного визита в налоговую инспекцию.

7. «Подача электронных документов на государственную регистрацию» позволяет физическим лицам и организациям, регистрируемым или зарегистрированным в качестве индивидуального предпринимателя, направить документы для государственной регистрации в электронном виде через сеть Интернет.

Федеральная налоговая служба предоставляет возможность юридическим лицам и физическим лицам, регистрируемым или зарегистрированным в качестве индивидуального предпринимателя (далее – индивидуальные предприниматели), направить документы для государственной регистрации в электронном виде через сеть Интернет.

Указанный сервис действует только для г. Москвы, Санкт-Петербурга, Оренбургской и Тульской областей, на территории которых в 2011 г. проходила опытная эксплуатация программного обеспечения «Электронная регистрация».

8. «Проверь себя и контрагента» – позволяет узнать:

– сведения о юридических лицах, внесенные в ЕГРЮЛ;

– сведения о юридических лицах, в отношении которых представлены документы для государственной регистрации изменений, вносимых в учредительные документы юридического лица, и внесения изменений в сведения о юридическом лице, содержащиеся в ЕГРЮЛ;

– сообщения юридических лиц, опубликованные в журнале «Вестник государственной регистрации» о принятии решений о ликвидации, о реорганизации, об уменьшении уставного капитала, о приобретении обществом с ограниченной ответственностью 20% уставного капитала другого общества, а также иные сообщения юридических лиц, которые они обязаны публиковать в соответствии с законодательством РФ;

– сведения, опубликованные в журнале «Вестник государственной регистрации» о принятых регистрирующими органами решениях о предстоящем исключении недействующих юридических лиц из ЕГРЮЛ;

– юридические лица, в состав исполнительных органов которых входят дисквалифицированные лица;

– адреса, указанные при государственной регистрации в качестве места нахождения несколькими юридическими лицами.

9. «Получение выписки из ЕГРЮЛ/ЕГРИП через Интернет» предоставляет возможность заинтересованным лицам получить сведения из ЕГРЮЛ и ЕГРИП в виде выписки («электронной» либо на бумажном носителе) на основании запроса, направленного через Интернет.

10. «Доступ к ЕГРЮЛ и ЕГРИП» предоставляет возможность получения сведений из Единого государственного реестра юридических лиц (ЕГРЮЛ) и Единого государственного реестра индивидуальных предпринимателей (ЕГРИП) в электронном виде через сеть Интернет.

11. «Подача заявления физического лица о постановке на учет» позволяет:

заполнить заявление физического лица о постановке на учет в налоговом органе на территории РФ;

– зарегистрировать и отправить в налоговый орган заполненное заявление;

– получать информацию о состоянии обработки заявления в налоговом органе на сайте и по адресу электронной почты (если Вы укажете его в заявлении в разделе «Контактные данные заявителя»);

– распечатать заполненное заявление.

12. «Уплата госпошлины» – позволяет подготовить платежные документы на перечисление налогов, сборов и иных платежей в бюджетную систему России в электронном виде.

13. Представление налоговой и бухгалтерской отчетности в электронном виде.

14. Нормативные и методические материалы ФНС России.

15. Адреса массовой регистрации.

При эксплуатации и сопровождении централизованных программных продуктов неизбежно возникают трудности, которые невозможно преодолеть собственными силами. Из-за отсутствия возможности обращения специалистов отдела информационных технологий инспекции напрямую к разработчикам программного обеспечения возникающие проблемы решаются неоперативно. Это, в свою очередь, влечет ряд новых проблем. Остановимся на основных трудностях, с которыми инспекция сталкивается в процессе работы.

Как правило, начало года характерно вводом новых форм налоговой отчетности по основной массе налогов. Как показала практика, новые формы отчетности утверждаются и публикуются непосредственно перед сроками представления отчетности. В результате из-за отсутствия времени разработчики направляют электронные шаблоны деклараций, используемых в ПК ЭОД – местный уровень, нетестированными. Работать с такими шаблонами достаточно сложно из-за большого количества ошибок и недочетов. Затем, исправляя ошибки, разработчики направляют до семивосьми изменений на один электронный шаблон, что тоже отнимает много времени у инспекторов и администраторов на неоднократную установку, настройку и тестирование. А для программного продукта «Налогоплательщик ЮЛ», распространяемого инспекциями среди налогоплательщиков и предназначенного для сдачи налоговой отчетности на магнитных носителях, по некоторым налогам новые шаблоны деклараций зачастую бывают получены после срока представления отчетности. Кроме того, часть налогоплательщиков сочли нецелесообразным переходить на сдачу отчетности по каналам связи, поскольку, оплачивая абонентскую плату за данную услугу, они все равно из-за отсутствия электронных форм вынуждены были прийти в инспекцию, отстоять очередь и сдать отчетность на бумажном носителе.

Далее, весь этот поток бумажных носителей отдел ввода и обработки данных инспекции должен был в авральном режиме срочно ввести в систему ЭОД, исполняя требования действующих нормативных документов.

К сожалению, такая ситуация не единична. Несвоевременное представление электронных форм шаблонов значительно усложняет организацию работы по привлечению налогоплательщиков к сдаче налоговой отчетности в электронном виде, в том числе по телекоммуникационным каналам связи.

Поскольку второй этап внедрения государственной программы «Электронная Россия» согласно распоряжению Правительства России близится к завершению, то инспекции надеются, что количество приказов ФНС о внесении изменений в форматы представления форм налоговой и бухгалтерской отчетности значительно сократится.

Хотелось бы, чтобы и разработчики РНИВЦ размещали программное обеспечение в Фонд Алгоритмов и Программ (ФАП) не менее чем за 10 дней до наступления сроков представления отчетности. Кроме того, можно рекомендовать работникам отдела работы с налогоплательщиками вести постоянную агитационно-разъяснительную работу о том, что появилась возможность у налогоплательщиков формировать налоговую и бухгалтерскую отчетность в электронном виде в других лицензионных широко распространенных программных продуктах (например, 1С-Бухгалтерия, Баланс+). Разработчики таких программных продуктов гораздо более оперативно и качественно реагируют на изменения в законодательстве.

Серьезной проблемой в работе инспекции является наличие большого количества мелких централизованных программных продуктов, по существу написанных в силу объективных причин в

сжатые сроки, функции которых позднее в основном реализуются в ПК ЭОД - местный уровень.

В результате одни и те же данные приходится вводить два-три раза в разные программные продукты для ведения информационных ресурсов, что приводит к дополнительным тратам времени и неэффективному использованию трудовых ресурсов.

Нисколько не облегчает работу автоматизированный обмен данными с ПК ЭОД – местный уровень, так как на выгрузку и прием данных тоже тратится много времени, а также увеличивается время освоения программных продуктов сотрудниками инспекции. Кроме того, существенно увеличиваются затраты на администрирование большого количества баз данных, на тестирование и установку новых версий для каждого программного продукта.

Кроме того, уровень качества программного обеспечения такого, как ЕГРЮЛ, ЕГРИП, Недействительные паспорта, довольно низкий. Это выражается в несвоевременном внесении корректировок в программные продукты, связанные с изменением законодательства, наличии большого количества критических ошибок, приводящих к срыву исполнения установленных сроков.

В качестве решения этой проблемы инспекцией были направлены предложения в ФНС России о рассмотрении возможности постепенного отказа от использования дополнительных программных продуктов, полностью интегрирования их функции в единую программу. Предлагается разработать единый межведомственный программный комплекс, который бы позволил формировать и использовать в своей работе единое информационное пространство для таких государственных органов, как Министерство финансов (налоговые органы, казначейство, контрольно-ревизионная палата), Министерство внутренних дел (ГИБДД, паспортно-визовая служба), органов государственной регистрации и др.

В течение последних лет, согласно приказам ФНС России, налоговые инспекции приступили к ведению и на сегодняшний день ведут более 40 объемных информационных ресурсов, что без добавления численности работников явилось большой дополнительной нагрузкой на инспекторский состав.

Мы понимаем, что проведение данной работы преследовало:

во-первых, освобождение инспекций от ручного труда в процессе составления отчетности, которой становится все больше и больше;

во-вторых, освобождение квалифицированных кадров на местах от рутинной технической работы, заменив ее автоматизированными процессами, для создания лучших условий для выполнения основных функций;

в-третьих, формирование единого информационного пространства ФНС России, создание интеллектуальной информационно-аналитической системы автоматизированного налогового контроля, обеспечивающей единый комплексный методологический подход к решению проблем автоматизированной подготовки и проведения налоговых проверок на основе современных информационных технологий, в том числе технологии централизованной обработки данных.

На деле, учитывая все вышесказанное, достичь полной автоматизации процесса формирования отчетности, реализованной в централизованных программных продуктах, не представляется возможным.

Кроме того, ни одно изменение к централизованным программным продуктам, получаемое инспекциями, нельзя установить сразу на рабочую базу данных без предварительного тестирования, поскольку на сегодняшний день все изменения содержат ошибки. Тестирование всех изменений ложится дополнительным грузом в основном на плечи инспекторского состава. И вместо высвобождения квалифицированных кадров, мы вменяем им дополнительную нагрузку, что также негативно влияет на результаты контрольной работы.

Приказ ФНС по тестированию программных средств информационной системы налоговых органов [2] был утвержден в 2005 г. Данным приказом закреплялись конкретные территориальные налоговые инспекции России, ответственные за тестирование соответствующих централизованных программных средств. Изменения должны были выпускаться не чаще 1 раза в квартал и выкладываться на ФАП только после получения положительного протокола результатов тестирования изменений к этим программным продуктам. Тенденция исполнения данного приказа стала прослеживаться только к концу 2006 г. К сожалению, сегодня данный приказ опять не исполняется.

Но есть и субъективные проблемы, возникающие при ведении информационных ресурсов. Инспекторам из-за большой нагрузки некогда заниматься самостоятельным изучением используемых в инспекции программных продуктов. Специалисты отделов зачастую просто не знают всех возможностей программных комплексов, на которых работают, не знают всех своих обязанностей по заполнению и ведению вмененных им информационных ресурсов. В результате информационные ресурсы содержат неполные, а иногда и противоречивые сведения.

Для решения данной проблемы предлагается организовывать техническую учебу внутри отде-

лов инспекции с обязательным отрывом от производства и по окончании технической учебы проводить тестирование усвоенных знаний. В данном случае использовать дистанционное обучение (в том виде, который существует на сегодняшний день) считается малоэффективным, так как на лекции специалисты не ходят в силу большой нагрузки по основной работе, а при сдаче тестов ими привлекаются все имеющиеся в инспекции ресурсы (литература, специалисты в данной области из других отделов инспекции и управления, Интернет и др.). В результате дистанционного обучения уровень знаний работников инспекции практически не меняется.

Важным вопросом является защита информации. Число крупных утечек конфиденциальной информации из органов государственной власти в 2010 г. удвоилось по сравнению с 2009 г.

В рамках исследования «Внутренние информационно-технологические (ИТ) - угрозы в России 2010», проведенного компанией InfoWatch совместно с CNews Analytics, были опрошены сотрудники 40 органов федеральной (65%), региональной (20%) и муниципальной (15%) власти. Исследование проводилось два года подряд по единой методологии, и в представленном ниже материале ответы респондентов приведены в сравнении для 2009 и 2010 гг. [3].

Инсайдеры – главная угроза государственных органов.

Основные выводы, полученные в результате проведенного исследования, можно сформулировать следующим образом:

– Наибольшую опасность для российских органов государственной власти представляют внутренние угрозы ИТ-безопасности: кража конфиденциальной информации и халатность сотрудников. Соотношение опасности внутренних и внешних угроз информационной безопасности показано на рис. 1.

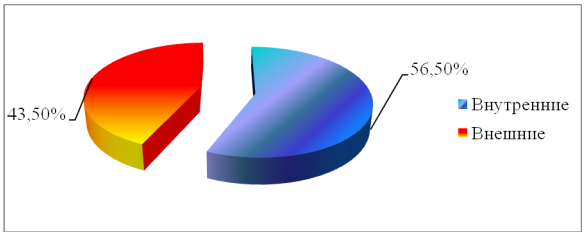

Рис. 1. Соотношение опасности внутренних и внешних угроз информационной безопасности

– Нарушение конфиденциальности информации является самой главной опасной внутренней угрозой ИТ-безопасности. Наиболее критический характер этой проблемы подтвердили все 100% респондентов.

– Органы государственной власти практически не в состоянии оценить масштабы и последствия утечки конфиденциальных данных: более 96% респондентов зарегистрировали случаи утечки или допускают их существование, но ни разу не оценивали ущерб.

– Всего лишь несколько органов государственной власти (2%) используют специализированные средства для обнаружения и предотвращения утечек конфиденциальной информации, но подавляющее большинство (83%) планирует их внедрение в течение последующих 3 лет.

– Россия опережает общемировой уровень в области профессионального подхода к ИТ-безопасности: около 40% российских органов государственной власти имеют выделенные отделы ИТ-безопасности или специалистов в этой сфере. В то же время в общемировой практике этот уровень составляет 27%. Органы государственной власти больше всего озабочены следующими угрозами: кража информации (64%), вредоносные программы (49%), хакерские атаки (48%), спам (45%) и халатность сотрудников (43%).

Респонденты отметили, что внутренние угрозы – кража информации и халатность сотрудников вызывают у них большую озабоченность, чем внешние атаки. Это лишний раз подтверждается резким снижением обеспокоенности органов государственной власти вирусными атаками: 60% – в 2009 г., но уже 49% – в 2010 г. Таким образом, респонденты отчетливо сознают опасность утечки конфиденциальных данных.

По мнению аналитического центра InfoWatch, спад обеспокоенности органов государственной власти такими проблемами, как вредоносные коды и спам, вызван, прежде всего, тем, что организации уже выработали эффективные средства противодействия этим атакам. Действительно, все 100% респондентов используют антивирусные средства, а практически каждый пятый – еще и фильтры спама. Данные об оснащении такими средствами защиты, имеющиеся в распоряжении CNews Analytics, прямо свидетельствуют о высокой ИТ-вооруженности органов государственной власти в этой сфере. В то же время готовность к новым угрозам можно определить как «крайне низкую».

Внутренние угрозы, напрямую связанные с человеческим фактором и организационными мерами, вызывают у органов государственной власти большую озабоченность, по сравнению с обеспечением внешней защиты, так как опыт использования систем защиты от инсайдеров еще очень мал (лишь 2% госорганов применяют их на практике), а сами утечки обладают более высоким уровнем латентности.

Чтобы изучить структуру внутренних угроз ИТ-безопасности, респондентам было предложе-

но ответить на вопрос о том, какие внутренние ИТ-угрозы являются самыми опасными. Органы государственной власти однозначно (100%) указали на нарушение конфиденциальности информации, как на самую опасную угрозу из всех перечисленных.

В 2010 г. многие органы государственной власти столкнулись с утечками собственных баз данных, а те, которым все же удалось сохранить свою информацию в секрете, оказались под впечатлением громких утечек начала и конца 2010 г. При этом специфика органов власти состоит, во-первых, в более высоких рисках потери репутации, так как каждая утечка наносит удар по имиджу всей страны, а, во-вторых, в необходимости обеспечить защиту государственной тайны. Таким образом, сохранение конфиденциальности данных – самый главный приоритет органов государственной власти.

Остальные внутренние угрозы следуют с существенным отрывом: искажение информации (54%), сбои в работе информационной системы (23%), утрата информации (5%), кража оборудования (4%) и другие (23%).

Как показывают данные исследования, наибольшую обеспокоенность респондентов вызывают мобильные накопители информации (91%). Популярность этого канала утечки данных возросла за последние двенадцать месяцев. Так, портативные устройства опередили прошлогодних лидеров в лице электронной почты (86%), интернет-пейджеров (85%) и других веб-служб (80%). Остальные угрозы фигурируют в опросе на эпизодическом уровне: печатающие устройства – 30%, фотопринадлежности – 5%, другие каналы утечки – 35%.

Такая структура ответов вызвана спецификой инсайдерских угроз именно в органах государственной власти. Как известно, на черном рынке России особой популярностью пользуются базы данных правительственных организаций, часто имеющие довольно большой объем. По некоторым оценкам, размеры особо насыщенных баз могут достигать нескольких сотен гигабайт. Очевидно, что выкрасть столько информации можно, используя только емкие накопители информации. Например, съемные жесткие диски, USB-память, компакт-диски и т.п.

Такие объемы данных – нескольких сотен гигабайт – не могут передать инсайдеры по электронной почте или Интернету, так как это, как минимум, вызовет перегрузку канала и станет заметным персоналу, не имеющему к ИТ-безопасности никакого отношения. Более того, пересылка этими средствами протоколируется, может быть заблокирована и использована в качестве доказательства вины злоумышленника. Наконец, далеко не во всех органах власти разрешен свободный доступ к почте и существует прямое подключение к другим сетевым сервисам.

Таким образом, для защиты от возможной утечки больших баз данных, содержащих конфиденциальную информацию, можно использовать ограничение доступа (физически отключать от питания, если это возможно, либо опечатывать) к USB-портам, пишущим CD-, DVD-ROMам компьютера.

Между тем лишь 9% министерств и ведомств уже сейчас применяют защиту от утечек, хотя среди коммерческих компаний эта доля в среднем равна 10,5% [3]. Другими словами, лишь каждая 11 государственная организация пытается взять под контроль утечки, что, конечно же, очень невысокий показатель. По мнению аналитического центра InfoWatch, относительно невысокая защищенность госсектора (9% против 10,5%) объясняется, прежде всего, тем, что государственные организации не теряют конкурентоспособность вследствие утечки, так как у них попросту отсутствует конкуренция.

Что именно мешает госструктурам внедрять системы защиты от утечек? [4] Как оказалось, наибольший вес для российских министерств и ведомств имеет отсутствие стандартов (31%). Причем под стандартами здесь понимаются не только нормативные или рекомендательные акты, а еще и единое видение системы внутренней безопасности. Так, многие респонденты отмечали, что сегодня еще не сформировался единый подход к решению этой проблемы. В результате организациям сложно планировать бюджеты и выбирать продукты для внедрения. Отсюда вытекает еще одна проблема – бюджетные ограничения (21%).

Наиболее эффективными внутренними средствами защиты информации являются внедрение комплексных решений на основе информационных технологий (разграничение прав и доступа, сетевые фильтры, антивирусные программы, использование средств криптографической защиты, программы мониторинга и др.). Не менее важны и организационные мероприятия по защите информации от несанкционированного доступа (разработка Порядка обмена документами по электронной почте, Положения о постоянно действующей комиссии по защите служебной тайны, Инструкции о порядке работы абонентских пунктов пользователей локальной вычислительной сети, Положения о разрешительной системе допуска работников к служебной информации, Порядка по использованию сети Интернет, Положения по ведению информационных ресурсов и др.). Третьим эффективным направлением в работе по защите информации является ограничение связи

с внешними сетями и источниками (компьютеры, подключенные к Интернету, не должны быть подключены к локальной вычислительной сети организации, вести учет вычислительной техники с открытыми дисководами, USB-портами, съемными CD-, DVD-дисками, вести журнал учета и выдачи небумажных носителей документов «Для служебного пользования» и др.).

Таким образом, наиболее эффективным способом минимизации инсайдерских рисков является комбинация различных способов. Правда, базовой основой все равно должно быть комплексное решение на основе ИТ, так как только с его помощью можно закрепить положения политики безопасности на рабочих местах. В то же время проведенное исследование позволяет сделать некоторые выводы:

– российские госструктуры более всего обеспокоены именно внутренними угрозами ИБ. Инсайдерские риски превалируют над внешними угрозами в соотношении 6:4;

– наибольшую опасность для государственных организаций представляют утечки персональных данных граждан. Такой точки зрения придерживается абсолютное большинство респондентов (77%);

– министерства и ведомства озабочены халатностью собственного персонала (51%), так как безалаберность служащих может привести к утечке или искажению данных;

– только 15% респондентов могут уверенно заявить, что не допустили ни одной утечки в прошедшем году. При этом 40% госструктур допустили более одной утечки в году;

– государственные организации обеспокоены ситуацией. Хотя стимулов внедрять защиту у них намного меньше, чем у коммерческих компаний, 91% министерств и ведомств планирует внедрить то или иное средство защиты уже в ближайшие 3 года.

Введение новых обязанностей при работе с налогоплательщиками, конечно, легло дополнительной нагрузкой на плечи, прежде всего, налоговых инспекторов. Для того чтобы в полной мере предоставить налогоплательщикам всю необходимую им информацию, как оказалось, недостаточно только констатации в законе. Общение с налогоплательщиками, работа с ними, направленная на восполнение пробелов в их знаниях и воспитание в них ответственного отношения к уплате налогов, требуют серьезных усилий и средств. Выявился целый ряд проблем – организационных, материально-технических, содержательных.

В организационном плане информационно-разъяснительная работа потребовала значительных затрат времени. Налоговые инспектора занятые, прежде всего, налоговым контролем, часто просто не успевают в должной мере уделять внимание вопросам каждого налогоплательщика. Если же речь идет о таких формах информирования, как проведение семинаров, наглядная агитация, издательская деятельность, то это самостоятельное направление работы, которое требует отдельных специалистов. Уровень качества работы с налогоплательщиками зависит от того, насколько услуги, предоставляемые налоговыми органами, соответствуют потребностям и запросам налогоплательщиков. Расширение спектра информационных услуг является ключевым фактором повышения уровня добровольного исполнения налогоплательщиками своих обязательств, что, в свою очередь, значительно упрощает контроль за уплатой налогов, сокращает административные затраты и способствует высвобождению людских ресурсов, которые могут быть дополнительно направлены на работу с налогоплательщиками.

Материально-технические проблемы ни для кого не новость. Законодатель предусмотрел, безусловно, правильное положение о бесплатности информационно-разъяснительной работы с налогоплательщиками. Право на информацию – неотъемлемое право каждого. Однако, как известно, ничего бесплатного не бывает. Любые действия, в том числе государственных органов, как-то оплачиваются: иногда на хозрасчетной основе, чаще – из бюджета. Но если не предусмотрено ни выделение из бюджета средств (пусть скудных), ни иных источников финансирования, то оказывается, что на изготовление стендов с информацией, издание специальной литературы, проведение семинаров с налогоплательщиками, а тем более на внедрение новых информационных технологий денег нет. В результате – низкий уровень информирования не с точки зрения качества информации, а с точки зрения ее оформления. В последнее время ситуация стала меняться. С начала 2006 г., момента утверждения и реализации федеральной целевой программы «Совершенствование работы с налогоплательщиками», инспекцией было получено и освоено достаточное финансирование на издание литературы и информационных материалов, в том числе новых стендов, выступлений в СМИ, оплаты работы инспекторов за участие в семинарах. Кроме того, инспекцией в централизованном порядке получено 2 сервера и 103 комплекта современной вычислительной техники с соответствующим лицензионным программным обеспечением, а также самостоятельно приобретено лазерное коммуникационное оборудование.

Кроме того, наряду с оснащением налоговых органов современной вычислительной техникой и внедрения новых информационных технологий необходимо создавать условия для доступа налогоплательщиков к данным услугам за мини-

мальную (условную) плату, организовывать консультационные и удостоверяющие центры, четко законодательно разграничивать полномочия государственных органов.

Но все перечисленное не так важно в сравнении с содержательными проблемами, в связи с которыми налогоплательщики задают свои вопросы. Анализ обращений налогоплательщиков за письменными разъяснениями, к сожалению, подтверждает, что налоговое законодательство далеко от совершенства. Возникает неизбежное расхождение в толковании норм налогоплательщиками и налоговыми органами, что влечет конфликты.

К сожалению, в практике встречается слишком много таких вопросов, которые не имеют однозначных ответов. Это нередко приводит к тому, что налогоплательщик, обращаясь за разъяснениями в несколько налоговых органов (например, в нижестоящий и вышестоящий), получает разные ответы. Эта ситуация не выгодна ни налогоплательщикам, ни государству. Но установление на уровне закона права получать разъяснения и введение на уровне ведомственного акта обязанности вести учет обращений налогоплательщиков за информацией и разъяснениями создают хорошую возможность для обобщения и унификации практики. На этой основе могут делаться обоснованные законодательные предложения и формироваться внутриведомственная информационно-правовая система, содержащая ответы на типовые вопросы налогоплательщиков.

Руководством ФНС России ставится задача по формированию досье налогоплательщика для достижения большей результативности при выполнении контрольных функций, которая предусматривает обмен информацией со сторонними организациями. Основным реквизитом, по которому можно идентифицировать данные по плательщику, для налоговых органов является Идентификационный Номер Налогоплательщика (ИНН).

К сожалению, законодательно до сих пор не решен вопрос об обязательном включении реквизита «ИНН плательщика» в представляемые в налоговые органы данные. Например, в представляемых данных из Управления федеральной регистрационной службы ИНН плательщика зачастую просто отсутствует, так как согласно приказу МНС России [5] данный реквизит не является обязательным. В результате инспекция не может идентифицировать в среднем до 20% получаемых данных из РУТИ об имуществе плательщика, так как те, в свою очередь, получают их неполными от Управления федеральной регистрационной службы. В итоге, инспекция располагает неполной и соответственно, недостоверной базой для исчисления налога на имущество. Аналогична ситуация по сведениям, служащим базой для исчислений налога на землю, транспортного налога и т.д. То есть необходима преемственность программных продуктов на законодательном уровне в части идентификации налогоплательщиков при электронном обмене с организациями, регистрационными и лицензионными органами, банками, фондами и другими организациями, заинтересованными в информационном обмене. К сожалению, даже полученные и проидентифицированные инспекцией данные от регистрирующих органов содержат недостоверную информацию на 10–15%, так как, продав, купив, подарив или унаследовав имущество, владельцы не спешат переоформлять соответствующие документы.

Кроме того, поступающие на бумажных носителях в больших объемах данные от организаций и учреждений, в соответствии со ст. 85 Налогового кодекса, инспекция не в состоянии обработать в указанные законодательством сроки имеющейся численностью, 50 % которой составляет контрольный блок. В результате, данные вводятся без должного анализа и с большой задержкой. Что также приводит к тому, что информационные ресурсы теряют свою актуальность. Т.е. назрела необходимость представления сведений в рамках исполнения ст. 85 Налогового кодекса РФ только на магнитных носителях в установленных форматах. Минфину России в последнее время все больше удается договориться и подписать двусторонние взаимовыгодные нормативные документы по электронному обмену данными. Также инспекциям разрешено на собственном уровне подписывать соглашения двустороннего обмена с администрациями, банками, ГИБДД и другими организациями, не нарушая нормативных документов о неразглашении сведений, составляющих служебную тайну или относящихся к сведениям «Для служебного пользования».

Таким образом, проведя анализ по совершенствованию информационно-коммуникационного обеспечения деятельности налоговых органов, можно сделать вывод, что достижение поставленных задач невозможно без внедрения новых информационных технологий в налоговой службе, что важно не только оснастить инспекции современной вычислительной техникой и обеспечить централизованным высокотехнологичным программным обеспечением, но и создать условия для возможности эффективного использования данных технологий не только специалистами налоговых органов, но и непосредственными потребителями предоставляемых услуг.

Литература

1. *Постановление* Правительства Российской Федерации «О совершенствовании процедур государственной регистрации и постановки на учет юридических лиц и индивидуальных предпринимателей» от 26.02.2004 №110.

2. *Приказ ФНС* России «Об организации работ территориальных органов ФНС России по тестированию программных средств информационной системы налоговых органов» от 11.04.2005г. №САЭ-3-13/149@.

3. *Защита* информации // CNews Analytics. – 2011. – №8 (17) сентябрь. – С. 36–76.

4. *Рынок* информационных технологий 2011. Итоги года // CNews Analytics. – 2012. – №4 (23) апрель. – С. 42–54.

5. *Приказ МНС* России «Об утверждении структуры и форматов текстовых файлов информации, поступающей в соответствии с налоговым законодательством в налоговые органы от организаций и учреждений».