ЭЛЕКТРОННОЕ УПРАЗДНЕНИЕ ПРОДАЖ: УГРОЗА НАЛОГОВЫМ ПОСТУПЛЕНИЯМ

OECD

ОРГАНИЗАЦИЯ ЭКОНОМИЧЕСКОГО СОТРУДНИЧЕСТВА И РАЗВИТИЯ

ОЭСР - уникальный форум, обеспечивающий сотрудничество правительств ряда стран мира в поиске ответов на порождаемые глобализацией экономические, социальные и экологические вызовы. ОЭСР находится в авангарде усилий, предпринимаемых по осознанию новых проблем, - таких, как вопросы корпоративного управления, информационная экономика и вызовы, связанные с проблемой старения населения,- и оказанию содействия правительствам в поиске соответствующих решений. Организация обеспечивает для национальных правительств платформу, в рамках которой они могут сопоставлять опыт реализации мер государственной политики в тех или иных областях, искать ответы на общие вызовы, выявлять примеры передовой практики и осуществлять координацию реализуемых ими мер внутренней и международной политики.

Членами ОЭСР являются Австралия, Австрия, Бельгия, Канада, Чили, Чешская Республика, Дания, Эстония, Финляндия, Франция, Германия, Греция, Венгрия, Исландия, Ирландия, Израиль, Италия, Япония, Южная Корея, Люксембург, Мексика, Нидерланды, Новая Зеландия, Норвегия, Польша, Португалия, Республика Словакия, Словения, Испания, Швеция, Швейцария, Турция, Великобритания, США. В деятельности ОЭСР принимает участие и Европейская Комиссия.

фото кредитов:© Patryk Kosmider - Fotolia.com

Оглавление

О докладе

Техника утаивания доходов от продаж с помощью компьютерных технологий способствует уклонению от налогов и во всемирных масштабах приводит к значительным потерям бюджетов различных стран от несобранных налогов. Применяемые в розничном секторе системы электронных кассовых терминалов (СЭКТ) – ключевой компонент комплексных систем продаж и бухгалтерского учета. На них полагаются как на действенный инструмент реализации функции бухгалтерского учета, необходимый для управления предприятием. Соответственно, ожидается, что они будут содержать исходные данные, которые могут проверять налоговые инспекторы. В реальности же подобные системы не только позволяют осуществлять такназываемый «скимминг», т.е. хищение поступающих наличных средств с использованием компьютерных технологий, подобно тому, как это делается вручную при краже средств из кассовых аппаратов предшествующих поколений), но и функционируя на основе ПО, призванного обеспечить утаивание выручки от продаж, они способствуют появлению куда более изощренных видов мошенничества, поскольку позволяют перепрограммировать вносимые записи для того, чтобы последние не позволяли замечать результаты скимминга.

Из-за недостоверных данных о результатах продаж и доходах, скрытых с помощью подобной техники ухода от налогообложения, национальные налоговые органы теряют миллиарды долларов/евро. Канадская ресторанная ассоциация оценила объем утаиваемой всего за один год ресторанами страны выручки от продаж на уровне 2,4 млрд. канадских долларов. Со времени начала деятельности Рабочей группы ОЭСР по налоговым и другим финансовым преступлениям (РГНФП) и, благодаря ее работе по повышению осведомленности об этом явлении, ряд стран (включая Францию, Ирландию, Норвегию и Великобританию) провели проверки предприятий розничного сектора и обнаружили наличие в нем значительных проблем. В этой связи следует особо отметить быструю реакцию Ирландии: в стране было незамедлительно принято законодательство по борьбе с подобного рода нарушениями закона. Правительства ряда стран полагают, что активная работа в данном направлении – важный компонент стратегии по уменьшению разницы между суммой подлежащих выплате предприятиями налогов и фактически собираемым в бюджет объемом налогов.

В настоящем отчете описываются функции систем СЭКТ и конкретные области, в которых сконцентрированы соответствующие риски. В нем детально представлены выявленные экспертами виды и способы утаивания доходов от продаж, в частности, мошенническое ПО и программы на внешних носителях (т.н. *Zappers*), а также продемонстрировано, как налоговые аудиторы и следователи могут выявить использование подобных методов. В документе также отмечается постоянное совершенствование инструментов утаивания доходов с помощью компьютерных технологий и необходимость быть готовым незамедлительно реагировать на изменения в этой сфере.

В данном докладе собран и проанализирован ряд используемых национальными правительствами методов борьбы с правонарушениями, возникающими в результате использования техники утаивания доходов от продаж с использованием компьютерных технологий, а также представлены некоторые примеры передовой практики в данной области. Последние включают совершенствование практики соблюдения требований закона с упором на добровольность принятия бизнесом соответствующих обязательств в рамках отраслевых организаций, работу по повышению уровня информированности всех ключевых заинтересованных сторон, включая широкую общественность, совершенствование профессиональных умений и навыков представителей налоговых и следственных органов, деятельность по сбору и обмену данными и использованию технических решений – таких, как сертифицированные СЭКТ.

Авторами доклада представлены следующие рекомендации:

- Национальные налоговые администрации должны в рамках комплексного подхода к проблеме соблюдения налоговой дисциплины разработать стратегию борьбы с практикой утаивания доходов от продаж с использованием компьютерных технологий для того, чтобы она стала адекватным ответом рискам, порождаемым системами утаивания доходов от продаж с использованием компьютерных технологий; кроме того, в рамках данной стратегии следует пропагандировать принципы добровольного следования нормам закона, а также совершенствовать меры по выявлению фактов вышеуказанной практики и борьбе с этими явлениями.

- Следует разработать программу коммуникаций, нацеленную на повышение информированности всех ключевых заинтересованных сторон о преступной природе использования подобного рода техники и серьезных последствиях, которые влекут за собой расследование и привлечение к ответственности за совершение подобного рода правонарушений.

- Налоговым администрациям следует периодически проводить анализ на предмет соответствия их установленных законом полномочий задачам проверки и судебной экспертизы СЭКТ.

- Налоговым администрациям следует уделить особое внимание повышению квалификации сотрудников, совершенствованию их умений, навыков и инструментария в части проведения проверок и расследований, связанных с СЭКТ, включая повышение роли высококвалифицированных специалистов-аудиторов по электронным платежам и расчетам и – там, где это будет признано целесообразным, - использование экспертов по компьютерам и ПО.

- Налоговым администрациям следует рассмотреть возможность разработки рекомендаций в части законодательства, криминализирующего поставки, владение и использование ПО в целях утаивания доходов от продаж с использованием компьютерных технологий.

Введение

К истории вопроса

Использование техники утаивания доходов от продаж через электронные кассовые терминалы с помощью компьютерных технологий – тревожная тенденция в сфере уклонения от налогов. Рост количества правонарушений в этой области регистрируется в течение уже более десяти лет. За истекший период основные усилия по борьбе с этим явлением отмечались, главным образом, в Канаде, Германии, Нидерландах и Германии. С момента, когда в этом направлении стала действовать Рабочая группа ОЭСР по налоговым и прочим финансовым преступлениям, чья деятельность привела к повышению информированности об указанном явлении, решительные действия по борьбе с подобного рода преступлениями предприняли и ряд других государств (включая Францию, Ирландию, Норвегию и Великобританию). Цель настоящего доклада – ознакомить с указанной проблемой более широкую аудиторию и продемонстрировать, что обращение к ней требует выработки различного рода решений: технических, функциональных, стратегических, а также решений, лежащих в плоскости государственной политики. Кроме того, цель доклада состоит также в представлении практических рекомендаций для национальных налоговых администраций и правительств.

Используемые в розничном секторе модели современных кассовых аппаратов функционируют как комплексные системы учета продаж. В них зачастую используются стандартные программные решения для бизнеса, и на них полагаются как на действенный инструмент реализации функции бухгалтерского учета, необходимого для управления предприятием. Соответственно, ожидается, что они содержат набор исходных данных для проверки их налоговыми инспекторами, включая персонал налоговых органов, отвечающий за исполнение предприятиями требований налогового законодательства в части НДС или налога с продаж. Сегодня стало очевидно, что этими системами можно манипулировать, чтобы с их помощью осуществлять скимминг кассовых чеков, точно так же, как это делалось с кассовыми аппаратами предыдущих поколений (тех, у которых имелся один или более выдвижной ящик для денег). Проблема в том, что функционируя на основе ПО, призванного обеспечить утаивание выручки от продаж, они способствуют возникновению куда более изощренных видов мошенничества, поскольку позволяют перепрограммировать записи для того, чтобы не позволить заметить результаты скимминга.

Для обозначения современных контрольно-кассовых аппаратов часто используются термины «электронный кассовый аппарат» (ЭКА) или же «электронный кассовый терминал» (ЭКТ), но для целей настоящего доклада они вместе или по отдельности, а также их гибридные модели, носят общее родовое название «Системы ЭКТ» (СЭКТ).

Для сбора необходимой для подготовки настоящего доклада информации были задействованы судебные эксперты, аудиторы-специалисты по электронным платежам и расчетам, налоговые следователи, а также участвующие в процессе принятия решений представители государства.[1] Они также приняли участие в разработке набора пособий (включая наборы методических материалов, руководств и составление библиотеки технической информации) для налоговых аудиторов и следователей. Они использовали накопленный опыт для того, чтобы их собственные высокопрофессиональные умения и навыки, а также разработанные ими пособия стали незаменимым орудием для их коллег в других налоговых органах.

В настоящем отчете рассматриваются функции современных контрольно-кассовых аппаратов и роль их изготовителей, поставщиков и других сторон, вовлеченных в процесс пользования ими. Авторы доклада анализируют выявленные различного рода инструменты и виды техники утаивания доходов от продаж, а также следственные методы, которые привели к их раскрытию. В отчете также исследуется имеющиеся оценочные данные о распространенности использования указанных инструментов и техники утаивания доходов от продаж и соответствующих потерь бюджета вследствие недополученных налогов. В докладе также приводится описание ряда национальных стратегий по обеспечению выполнения требований законодательства и расследований соответствующих правонарушений, которые национальные правительства могут взять на вооружение, а также содержатся рекомендации о действиях, которые необходимо предпринять в этой связи.

Другие проекты в данной области

В настоящем докладе упор сделан на преступное поведение как элемент правонарушений, связанных с использованием техники утаивания доходов от продаж с помощью компьютерных технологий, а также на деятельности органов уголовного следствия по выявлению, пресечению и привлечению к ответственности за подобного рода поведение. В рамках Форума ОЭСР по налоговому администрированию и программы ЕС «Fiscalis» реализуется деятельность, которая в большей степени ориентирована на обеспечение исполнения требований налогового законодательства и стоящие перед представителями налоговых органов вызовы.

Реализуемый под эгидой программы «Fiscalis» проект **Евросоюза «Проектная группа по контрольно-кассовым аппаратам»**[2] обеспечил разработку в 2006 г. «Руководства по передовой практике в части контрольно-кассовых аппаратов».[3] Соответствующий документ включает комплексный обзор законодательства всех стран-членов ЕС, существующих программно-аппаратных систем для контрольно-кассовых аппаратов, каталог существующих рисков, а также рекомендации по передовой практике проверок кассовых аппаратов и СЭКТ.

В апреле 2010 г. **Форум по вопросам налогового администрирования** опубликовал **руководящие указания**, включая рекомендации по порядку обеспечения достоверности сделанных в электронной форме записей.[4]

Во втором полугодии 2010 г. в рамках существующего проекта **ЕС «Проектная группа по электронным проверкам»** была создана Рабочая группа по запперам и мошенническому ПО (ZAPAT). Цель проекта – на основе новых

решений и практической деятельности в области налоговых проверок стран-членов ЕС интегрировать передовую практику в данной сфере и, таким образом, способствовать повышению качества электронных проверок СЭКТ. В задачи Рабочей группы также входит создание на основе результатов исследований руководящих указаний в части электронных проверок СЭКТ для нужд представителей налоговых органов стран-членов ЕС. Этот документ дополнит собой результаты деятельности по подготовке настоящего доклада.

Оценки потерь национальных бюджетов от неуплаты налогов и других видов мошенничества

По оценкам Канадской ассоциация ресторанов и услуг общественного питания, в 2009 г. объем утаенной предприятиями общепита Канады выручки от продаж может составлять **2,4 млрд. канадских долларов**.

Потери бюджета провинции Квебек от неуплаты налогов в период 2007-20008 гг. оцениваются на уровне **417 млн. канадских долларов**

В результате проведения в течение 4 лет 2 тыс. налоговых проверок правительство Швеции дополнительно взыскало в бюджет **150 млн. евро**

В рамках лишь одного дела о взыскании налогов правительство Южной Африки добилось отмены экспатриации суммы в размере **22 млн. евро**

В рамках лишь одного дела о взыскании налогов правительство Норвегии взыскало ранее незадекларированную сумму в размере **7 млн. евро**

Оценки потерь национальных бюджетов в связи с использованием компьютерных технологий для утаивания выручки были произведены для определенных отраслей и конкретных географических территорий. Эти данные могут стать ориентировочными для оценки возможных налоговых потерь в других регионах мира. Так, имеется достоверная статистика по Канаде, в основе которой – неоспоримые свидетельства, полученные в результате раскрытых правонарушений. В частности, по оценкам *Revenu Québec*, ведомства, ответственного за администрирование и сбор налогов на доходы и потребление в провинции Квебек, потери регионального бюджета от применения указанной техники в 2007-2008 гг. составляют 417 млн. канадских долларов.

В 2008 г. Налоговая служба Канады предъявила обвинения владельцам всего лишь 4 ресторанов в уклонении от уплаты налогов посредством проведения около 200 тыс. транзакций с использованием запперов (о запперах см. соответствующий раздел ниже по тексту- *прим. перев*.) (т. н. «заппинга»)) на общую сумму 4,6 млн. канадских долл. По оценкам Канадской ассоциация ресторанов и услуг общественного питания, объем «фантомных» продаж за наличные средства предприятиями общепита страны в 2009 г. может составлять 2,4 млрд. канадских долларов.

В подготовленном германским федеральным аудиторским ведомством «Годовом отчете об управлении федеральными финансами за 2003 г.» выражается озабоченность относительно потерь бюджета от укрытия доходов от продаж при помощи компьютерных технологий и содержится вывод о том, что «учитывая объем финансовых транзакций, достигающий десятков миллиардов евро, не следует недооценивать риск уклонения от налогов».[5]

Некоторые другие показатели в этой связи.

- В рамках одного расследования правительство Норвегии взыскало ранее незадекларированную сумму налогов в размере 7 млн. евро
- В рамках одного дела о взыскании налогов в Южной Африке был выявлен вывод средств из страны представителями сектора оптовой торговли на сумму, эквивалентную 22 млн. евро.
- В ходе предпринятого словенскими налоговыми органами расследования в отношении магазинов розничной торговли в конце рабочего дня, выяснилось, что зафиксированный в их системах объем продаж в действительности оказался в три раза выше, чем в другие дни.

Налоговая служба Швеции изучила эту проблему в контексте разницы между суммами начисленных и реально выплаченных налогов. Согласно оценке шведских налоговиков, общий оборот компаний, осуществляющих продажи за наличные в стране, составляет 100 млрд. евро. Размер предполагаемой разницы для этих компаний оценивается в 2 млрд. евро, что составляет примерно одну шестую от зафиксированной в общенациональном масштабе разницы.

В период с 2006 по 2010 гг. в стране были инициированы более 2 тыс. проверок ресторанов, парикмахерских, магазинов одежды и продуктовых точек, т.п. Было установлено, что подвергшиеся проверкам компании не доплатили в бюджет около 150 млн. евро, включая неуплату налогов на доходы, НДС и социальные отчисления за работников. В ходе проверок было также установлено, что они укрыли от налогообложения от 20 до 40% своего оборота – средства, которые питают серую или подпольную экономику, а в отдельных случаях - и организованную преступность.

Существуют свидетельства того, что использование запперов и мошеннического ПО - широко распространенное в мире явление, что порождает постоянно растущую угрозу объему налоговых поступлений. Некоторые поставщики ПО, скажем, для устанавливаемых в ресторанах СЭКТ в открытую продвигают на международных рынках свою продукцию со встроенной функцией утаивания доходов. Что до прогнозов на будущее, налоговики и следователи, работающие по данному направлению, сообщают о постоянном процессе разработки новых видов методик, позволяющих избежать выявления правонарушения, и растущую изощренность этих методов.

Вместе с тем не были выявлены случаи использования схожего рода методов для завышения показателей продаж, например, в целях отмывания полученных преступным путем доходов. Однако подобные случаи вполне могут иметь место, и налоговым администрациям следует осознавать наличие подобных рисков.

Примечания

1. Координатором данной группы экспертов выступила Норвегия, а участие в ней приняли представители Бельгии, Канады, Франции, Германии, Греции, Ирландии, Нидерландов, Норвегии, Португалии, Швеции, Турции, Великобритании и США.

2. Цель работы Проектной группы заключалась в выявлении рисков в сфере контрольно-кассовых аппаратов и систем ЭКТ и разработке методов противостояния им. В своей деятельности данная группа преследовала следующие цели:

   - Сбор информации о различных правилах и требованиях, предъявляемых налоговыми органами стран-членов к контрольно-кассовым аппаратам и СЭКТ, а также их применением на практике, включая перечень правил и условий для производителей программно-аппаратных комплексов;
   - Сбор, распространение информации, повышение осведомленности и распространение передового опыта в части технических характеристик контрольно-кассовых аппаратов и СЭКТ;
   - Определение различий в концептуальных подходах и обмен опытом в целях совершенствования использования данных по транзакциям в коммерческом секторе для целей налоговых проверок; а также
   - Сбор информации о том, каким образом различного рода системы могут стать объектом возможных правонарушений.

3. *Cash Register Good Practice Guide*, EU Fiscalis Project Group 12, 2006 г. (Документ для служебного пользования).

4. *Guidance and Specifications for Tax Compliance of Business and Accounting Software*, Forum on Tax Administration, OECD, апрель 2010 г..

5. Federal Parliament circular 15/2020 at 197-198 (24 ноября 2003 г.).

Системы электронных кассовых терминалов

Системы ЭКТ

Когда в 1879 г. Дж. Ритту изобрел первый кассовый аппарат, цель его состояла в создании системы фиксирования осуществляемых за наличный расчет транзакций, чтобы персонал принадлежавшего ему салуна не мог больше воровать прибыль. Одна из первых его моделей рекламировалась как «Неподкупный кассир», и вскоре кассовые аппараты стали для бизнеса ключевым инструментом управления финансами. Точное фиксирование транзакций по продаже товаров и сохранность записей о них остаются ключевым требованием бизнеса к кассовым аппаратам. Они выдают кассовые чеки, которые становятся документом, подтверждающим продажу предприятием товара потребителю. Такие чеки – первичный документ или подтверждение содержания данной транзакции. Функции кассового аппарата с течением времени эволюционировали и стали включать документирование не только транзакции, но и данных, необходимых для бухгалтерского и налогового учета.

Эволюция кассовых аппаратов продолжалась, и сегодня бизнес использует современные СЭКТ по целому ряду причин: они обеспечивают безопасность и контроль за движением и сохранностью наличных средств, они стали быстродействующими, снижают вероятность ошибки при осуществлении транзакции, упрощают ведение бухгалтерского, налогового, товарного учета, позволяют отслеживать работу персонала, выдают кассовые чеки и, в целом, способствуют формированию профессионального имиджа предприятия.

Важную роль кассовые аппараты играют в процессах управления бизнесом в таких отраслях экономики, как розничные продажи и гостиничное хозяйство. Введение в кассовый аппарат данных о заказе потребителя или транзакции – отправной момент для последующих действий: например, заказ блюд в ресторане может быть автоматически передан на кухню с помощью электронных средств связи, в то время как ответственность за обслуживание клиента возлагается на конкретного официанта. В рамках полностью интегрированных систем ведения бизнеса СЭКТ становится одной из многих подсистем, но именно она остается той системой, которая инициирует коммерческую транзакцию и передает информацию другим процессам. В этом случае между кассовыми аппаратами, логистическими системами, системами учета и прочими системами, задействованными в бизнес-процессах, появляются интерфейсы.

С точки зрения функциональной сложности, СЭКТ варьируются от довольно простых до крайне сложных. Вполне возможна ситуация, когда конкретный коммерческий потребитель активирует не все внедренные поставщиком в данную систему функциональные решения. Системы средней или высшей сложности зачастую включают сенсорные панели или экраны и в качестве опции могут быть подсоединены к локальной компьютерной сети и сканирующим

устройствам. Реализованные в таких системах сложность и разнообразие технических решений могут представлять проблему для налогового инспектора, которому необходимо понять, как наиболее действенным образом осуществить их проверку.

Проверки СЭКТ: правовые основы

Крайне важно обеспечить ситуацию, при которой правовые основы проведения налоговых проверок учитывали бы необходимость проверки и цифровых систем для ведения бизнеса, включая ЭКТ. В законодательстве большинства стран присутствуют положения, требующие от предприятий создавать соответствующие информационно-учетные системы ведения бизнеса. При этом предприниматели не ограничены в том, чтобы в рамках предприятия самостоятельно устанавливать системы, которые соответствуют указанным принципам. Ниже приведены некоторые общие черты такого рода законодательства или регуляторных норм:

- Необходимо, чтобы генерируемые подобными частными информационно-учетными системами данные, которые влияют на налоговые обязательства экономических агентов, сохранялись в течение определенного периода времени.
- Владелец бизнеса несет ответственность за обеспечение того, что все учетные записи сохраняются в таком виде, чтобы их можно было проверить в разумные сроки.
- Перевод данных в электронном формате в бумажный позволителен, только если такого рода перевод не затрудняет проведение проверки.

В ряде стран действуют особые нормы регулирования в отношении требований ведения бухгалтерского учета предприятиями, которые осуществляют продажи за наличный расчет. Такие регуляторные нормы учитывают использование СЭКТ, и в них могут быть конкретно определены виды предоставляемых такими предприятиями отчетности, формат, язык отчетов, а также сроки их хранения. Такова, например, практика Норвегии.

Существует и ряд стран, где использование конкретных видов сертифицированных СЭКТ – обязательное условие для всего бизнес-сектора либо определенных отраслей розничного бизнеса или сферы услуг. Такого рода инструменты известны как «фискальные регистраторы». Их описание приведено ниже по тексту, в разделе «Ответные меры со стороны государства».

Требования налоговых органов

Требования к управлению информационными ресурсами предприятия с точки зрения налоговой проверки в полной мере совпадают со стандартными потребностями бизнеса. В дополнение к вышеуказанным параметрам для целей налоговой проверки особые рекомендации по ним включают следующие моменты:

- Сохранение детализированной информации об осуществленных транзакциях в электронном формате;
- Наличие подробных записей, доступных налоговой проверке по требованию;

- Сохранение в полном виде архива записей о проведенной продаже; а также
- Принятие надлежащих мер по предотвращению возможности внесения последующих изменений в данные и обеспечению целостности сохраненных массивов данных.

Детализированная информация о процессе ведения бизнеса необходима для проведения проверки на предмет полноты представленных данных о продажах. С точки зрения налоговой проверки, требования к информации о деятельности предприятия относительно просты – записи с данными по продажам должны обеспечивать полное и точное представление о последних. Эти записи должны позволить представителям налоговых служб в течение разумного периода времени осуществить проверку представленных цифр на предмет полноты и точности предоставленных фактов продаж. Эти данные должны представлять доказуемую, полную и точную картину этих продаж.

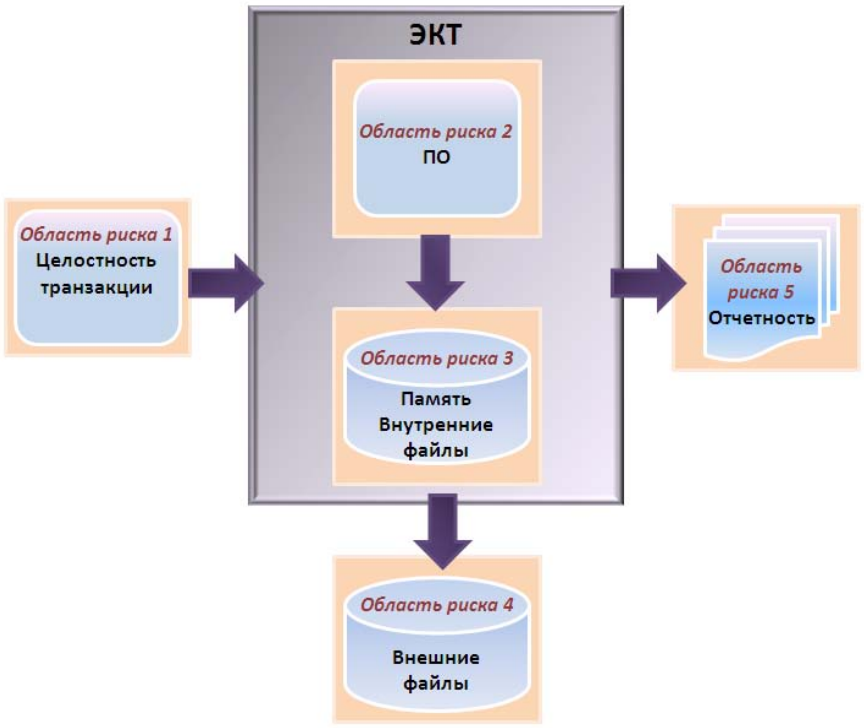
Указанные требования созвучны требованиям общего рода к коммерческим предприятиям в части используемых ими технологий поддержки систем ведения коммерческих операций: ожидается, что с момента фиксации данной транзакции информация о ней сохраняется в неискаженном виде. Кроме того, предполагается, что такие транзакции полностью и точно представлены в отчетах, которые можно сделать в любой момент, и вплоть до, по крайней мере, момента сверки учетных данных предприятия.

Более крупные по размеру компании предпринимают соответствующие меры для безопасного сохранения критических для их бизнес-процессов данных. Ответственным управленцам в таких компаниях необходимо прочно держать рычаги власти в своих руках. Эти данные нужны им, чтобы располагать информацией, которая лежит в основе принятия решений, влияющих на успех предприятия в долгосрочной перспективе, а также для того, чтобы осуществлять подготовку должного качества финансовой отчетности для акционеров компании и бухгалтерской отчетности – для регулирующих органов.

Риски, связанные с СЭКТ

Эксперты полагают, что слабые с точки зрения утаивания доходов от продаж с помощью компьютерных технологий места присутствуют в определенных несущих в себе риски сегментах конфигурации систем ЭКТ. Каждая из этих областей риска чревата возможностью удаления данных, их подмены или же – в случае фактического осуществления транзакции – отсутствия записи о ней. На приведенном ниже схематическом рисунке[1] представлены пять областей риска.

Рис.1. Модель рисков системы ЭКТ



Источник: информация представлена Нидерландами

Цельность транзакции. Для защиты цельности транзакции в кассовом аппарате должно быть предусмотрено наличие мер по обеспечению полноты, точности и актуальности вводимых данных о транзакции. Если эти данные неполны, неточны и неактуальны, система генерирует недостоверную коммерческую информацию и порождает такие риски, как уменьшение способности принимать верные управленческие решения и представлять правильные данные в налоговой декларации.

ПО. Необходимо, чтобы ПО разрабатывалось таким образом, чтобы обеспечить цельность, конфиденциальность и доступность выполняемых кассовым аппаратом процессов. Если система неспособна обеспечить указанные цельность, конфиденциальность и доступность, то, опять-таки, результатом станет появление недостоверной информации, порождающей вышеуказанные риски. В этой связи важно обеспечить такой режим функционирования ПО, при котором сохраняется вся информация по всем действиям системы кассового аппарата и обеспечивается

ее архивирование для целей проверки. Это необходимая для реализаций функций действенного управления и контроля за полным циклом бизнес-процессов мера.

Внутренняя память. Сохраняемые в памяти и внутренних файлах данные о транзакции – основа всех видов отчетности, а также элемент подлежащего проверке и расследованию комплекса данных. Именно в этой области проявляются самые серьезные риски из-за использования ПО в целях утаивания доходов от продаж (или других методов воздействия на файлы) путем манипулирования содержащейся в данных о транзакции информацией.

Внешние файлы. Риск здесь связан с передачей и хранением данных о транзакциях в оффлайновом режиме – в файлах, нужда в которых возникает, например, когда исчерпана емкость журнала электронных записей в ЭКТ. Национальное законодательство ряда стран обычно содержит требования к предприятиям хранить в течение определенного периода соответствующие записи и проводки, включая также и носители данных, на которых размещаются записи о них. Законодательством отдельных стран предусмотрено, что хранение подобных записей и проводок должно быть организовано таким образом, чтобы обеспечить возможность налоговому аудитору осуществлять их проверку в течение разумного периода времени. Внешними файлами также могут быть и файлы, которые в ежедневном режиме переносятся с системы ЭКТ на установленную на отдельном компьютере резервную систему. Такие резервные файлы могут храниться либо на внешних носителях, либо на жестком диске самой системы, но в другой папке. Такие резервные файлы могут содержать информацию, очень важную для выявления использования компьютерных технологий для утаивания доходов от продаж в рамках контрольно-кассовой системы.

Отчетность. Эта область рисков тесно связана со второй зоной рисков – ПО, которое управляет отчетностью, - и, следовательно, открывает возможности для манипулирования данными в процессе создания отчетности, а также ее форматом. Такие отчеты важны для управленцев и используются для переноса информации в систему бухгалтерской отчетности для создания налоговой отчетности и т.п. В случае утери данных о транзакциях важно, чтобы владелец бизнеса мог полагаться на бумажные копии отчетов, которые отражают все входящие данные по транзакциям и хранятся в памяти контрольно-кассового аппарата.

Примечания

1. В целях обеспечения соблюдения налоговых обязательств голландские поставщики СЭКТ совместно с налоговыми органами страны разработали модель рисков для указанных систем. Эта работа стала частью общенационального проекта “Знак качества для надежных систем ЭКТ», который рассматривается ниже по тексту в разделе «Ответные меры со стороны государства». Экспертная группа ОЭСР по проблемам применения компьютерных технологий для утаивания доходов от продаж использовала голландскую модель для создания концептуальной модели учета рисков в СЭКТ.

Методы утаивания доходов от продаж с помощью компьютерных технологий

Проблема, порождаемая использованием компьютерных технологий для утаивания доходов от продаж, заключается в том масштабе уклонения от уплаты налогов, который она порождает, благодаря возможности не предоставлять точную отчетность по продажам и прибыли. В данной главе описывается, как используемые и сегодня простые методы скимминга были автоматизированы и интегрированы в СЭКТ.

Утаивание данных о продажах, также известное как скимминг, в той или иной форме существовало всегда, в частности, для того, чтобы обеспечивать уклонение от налогов. Скимминг реализуется с помощью различного рода простых действий, как то:

- Неисполнением функции занесения фактов продаж за наличные в кассовый аппарат; при этом неучтенные наличные идут непосредственно в карман владельцу бизнеса; или
- Перенаправлением наличности в другой, «теневой», кассовый аппарат.

Такого рода методы наиболее характерны для малых и средних предприятий, поскольку у них имеется меньшее число механизмов внутреннего контроля и их владельцами зачастую является узкая группа лиц. В некоторых случаях практикующие скимминг предприятия ведут параллельную отчетность: «официальная» предназначена налоговых органов, а «теневая» - для владельца предприятия, поскольку он может захотеть при продаже бизнеса продемонстрировать потенциальному покупателю реальную картину продаж. В одном австралийском ресторане скимминг осуществлялся ближе к вечеру путем простой остановки работы кассовых аппаратов. В результате владельцы ресторана были признаны виновными в мошенничестве в особо крупных размерах и сумма доначисленных налогов и наложенных на них штрафов, исчисленных на основе оценки укрытых ими от налогообложения доходов, составила 8,4 млн. австралийских долларов.

Современные технологии позволили автоматизировать подобного рода мошеннические действия с использованием особого мошеннического ПО для утаивания доходов от прибыли (если оно встраивается в СЭКТ) и запперов (внешнего ПО, зачастую размещаемого на USB-ключах). Это ПО обеспечивает возможность реализовывать скимминг в полностью компьютеризованной среде, что позволяет владельцу бизнеса осуществлять деятельность, на первый взгляд, самым обычным способом (когда все продажи заносятся персоналом в электронный кассовый терминал, где генерируются записи о них как о транзакциях по продаже товаров или услуг). Эта технология также позволяет владельцу бизнеса активировать функцию утаивания доходов от продаж в удобное для него время (обычно ближе к концу рабочего дня). Эта функция может принимать форму некой

установленной на каждый день денежной суммы или же просто определенного процента от продаж за наличные. Таким образом, больше нет нужды в «черной кассе»: все полностью компьютеризовано и находится у владельца бизнеса под рукой. Все, что ему нужно, чтобы получить доступ к этому ПО, - это простые программные решения, например, контактная карта или же скрытая кнопка на экране его компьютера, с помощью которой активируется особое меню. Следователи также отмечают случаи, когда активация такого меню происходила посредством набора определенных символов на клавиатуре компьютера.

В прошлом ключевым элементом любого типа скимминга было наличие существенного объема продаж за наличные. В то же время продажи по кредитным и дебетовым картам редко становились предметом скимминга, поскольку такого типа транзакции было значительно легче отследить в ходе проверки. Однако в последнее время отмечались также и факты утаивания доходов от карточных продаж. В настоящее время ряд стран предприняли расследования, чтобы понять, представляют ли собой подобные действия новую тенденцию и как можно бороться с этими явлениями. Работа в этом направлении не продвинулась достаточно далеко, чтобы ее результаты были освещены в настоящем докладе.

Что касается стоимости мошеннического ПО или запперов, полученные из Канады и США свидетельства позволяют установить, что она может либо быть включена в стоимость СЭКТ, что в особенности типично для мошеннического ПО, либо – в случае использования заппера - равняется примерно 1,500 канадским долл. за штуку, и в таком случае эта сумма приплюсовывается к стоимости системы ЭКТ.

Злонамеренное использование функций ПО для ЭККА/ЭКТ

У современных ЭКТ имеются различные программные опции, некоторые из которых могут быть использованы для утаивания доходов от продаж. Так, например, ЭКТ может быть запрограммирован для того, чтобы:

- Предотвращать фиксирование определенных действий, как то: возвраты средств, отмены транзакций и прочие негативные транзакции,- в отчетности или в журнальном файле;
- Предотвращать включение определенных действий, как то: возвраты средств, отмены транзакций и прочие негативные транзакции, - в итоговые суммы;
- Функционировать в режиме обучающей симуляции (либо все устройство, либо только для определенного его оператора), что означает, что продажи не фиксируются в обычной отчетности;
- Обнулять итоговые суммы и прочие подсчеты или в некоторых случаях приводить их к некой заранее заданной величине, а также
- Обеспечивать отсутствие некоторых товарных позиций в отчетности или журнальном файле.

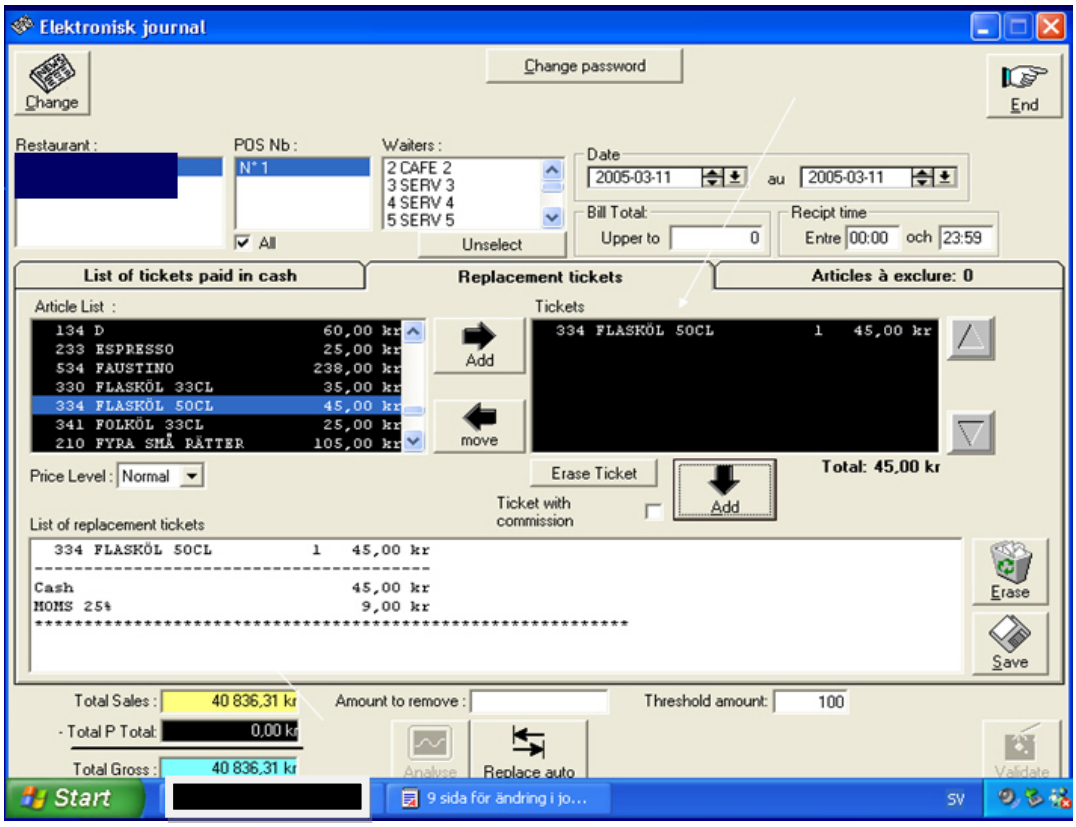
В отличие от мошеннического ПО варианты программирования для выбора подобных опций не запрятаны в меню программирования и приведены в руководстве по работе с ЭКТ или разработанной поставщиком инструкции; однако подобное руководство конечному потребителю обычно не предоставляется – оно доступно только для официальных дилеров. Программирование большинства

современных контрольно-кассовых аппаратов осуществляется посредством введения кода, что требует от осуществляющего программирование лица некоторых технических знаний. Большинство компьютеризованных СЭКТ также имеют сходные опции, но в этом случае, чтобы работать с ними, владельцу бизнеса не нужно быть семи пядей во лбу.

Мошенническое ПО

Мошенническое ПО – это предустановленная в прикладное бухгалтерское ПО ЭККА или компьютеризованная ЭКТ-программа. Она спрятана от не подозревающего о ее существовании пользователя, и доступ к ней осуществляется посредством клика на до поры невидимую кнопку на экране компьютера, введением особой последовательности команд или набором особой последовательности символов на клавиатуре. Эти действия активируют меню опций для выборочного удаления транзакций и/или печати отчетов о продажах, с пропусками в них некоторых строк. После удаления фактических подтверждений продаж во избежание очевидных несоответствий программа автоматически корректирует подробную информацию о товарных остатках; при активации опции пропуска строк может изменяться лишь отчет о продажах. Если производятся изменения в бухгалтерских проводках, программа позволяет распечатать архив удаленных транзакций, чтобы владелец бизнеса мог управлять этими изменениями (и отслеживать их). Наглядный пример использования такой программы предоставила Швеция: речь идет о программе для ресторанов, которая агрегирует данные из компьютеризованной СЭКТ и сохраняет их в электронном журнале. Приведенный скриншот позволяет увидеть возможность легкого осуществления подмены транзакций в системе, а именно по разделам «Список оплаченных счетов» и «Замененные счета».

Рис. 2. Пример мошеннического ПО



Источник: информация предоставлена Швецией

На данном примере использования мошеннического ПО можно убедиться, что продажи на самом деле не удаляются, но корректируются посредством подстановки более дорогих позиций меню вместо более дешевых. Такой вид утаивания доходов от продаж с помощью электронных средств более изощренный, чем простое удаление данных, так как позволяет избежать пробелов в списке порядковых номеров осуществленных транзакций, которые возникают в результате простого удаления данных. Таким образом, аудитор должен знать о том, что в данном случае используются определенные виды мошеннического ПО, которые удаляют данные о продажах и присваивают оставшимся транзакциям новые порядковые номера в новой последовательности. Таким образом, сам факт присутствия ненарушенной последовательности номеров транзакций не исключает возможности наличия факта утаивания доходов от продаж.

Запперы

Запперы – это внешнее ПО для реализации функции утаивания доходов от продаж. Они размещены на таких носителях, как USB-ключи, CD, или же доступны в Интернете. Разработкой, технической поддержкой и продажей запперов занимаются те же лица, которые разрабатывают СЭКТ для соответствующих отраслей экономики, хотя участие в этой работе принимают и независимые подрядчики. С функциональной точки зрения, запперы схожи с мошенническим ПО, но их труднее обнаружить,

поскольку как программный продукт они более сложны, а также потому, что незаконное ПО в таких случаях не размещается в самом компьютере на постоянной основе. Опыт Канады показывает, что запперы были обнаружены в значительном числе ресторанов страны и в каждом случае для их активации использовалось USB-устройство. При активации последнего на экране СЭКТ возникало новое окно, которое позволяло владельцу ресторана начать работу по удалению и/или внесению изменений в записи о продажах.

Резюме

Имеющиеся данные позволяют предположить, что, независимо от вида используемого ПО, в поставляемые через каналы розничных продаж СЭКТ уже инсталлировано ПО, позволяющее использовать их в мошеннических целях. Такое ПО может служить для обучения работы на СЭКТ или к нему могут прилагаться инструкции для пользователей, причем порой такие опции уже включены в стоимость поставляемого устройства..

В случае наличия и использования мошеннического ПО и запперов пользовательский интерфейс обычно носит профессиональный вид и им удобно пользоваться. Как правило, такого рода интерфейс разрабатывается одним из специалистов, принимающих участие в создании операционного ПО для СЭКТ, и формат его зачастую схож с последним, так что внешне и по субъективным ощущениям ПО для утаивания доходов от продаж неотличимо от стандартного «фирменного», лицензированного ПО. Выбор товарных позиций для манипулирования – обычно простая операция, зачастую требующая лишь клика по мышке для того, чтобы удалить данную позицию или заменить ее на более дешевую, или же введения суммы или процента от продаж для удаления (заппинга) последних. Для этих же целей могут служить фильтры, позволяющие с помощью заппера удалять определенные категории продаж. К примеру, в случае незаконного найма на работу какого-либо служащего владелец бизнеса может стереть все записи об осуществленных этим работником продаж; аналогичным образом, если владелец предприятия продает контрабандные товары (скажем, табачные изделия), то с помощью заппера он может удалить факты соответствующих продаж для устранения свидетельства его участия в этой незаконной деятельности.

Функции систем утаивания доходов от продаж с помощью компьютерных средств можно в обобщенном виде представить в виде следующего алгоритма:

- Доступ к скрытому ПО;
- Представление деталей транзакций за наличные (в настоящее время появились также свидетельства того, что аналогичные действия предпринимаются в отношении карточных транзакций);
- Удаление избранных позиций продаж и соответствующих записей учета движения товара;
- Замена избранных товарных позиций на более дешевые;
- Автоматическое удаление определенных товарных позиций для снижения суммы продаж до определенного уровня (например, если владелец бизнеса стремится к тому, чтобы закамуфлировать выводимые из бизнеса средства в размере, скажем 1 тыс. евро в день и согласен с тем, что ПО самостоятельно определяет, какие позиции подлежат удалению);

- Удаление архивных файлов и других следов транзакций; а также
- Сохранение исходных данных в другом месте

Вместе с тем не были выявлены случаи использования схожего рода методов для завышения показателей продаж, например, для целей отмывания полученных преступным путем доходов. Однако подобные случаи вполне могут иметь место, и налоговым администрациям следует осознавать наличие подобных рисков.

Финансовый аудит

Передовая практика проведения налогового аудита предлагает ряд достаточно универсальных и действенных способов определения того, имеются ли причины полагать, что данное предприятие практикует утаивание доходов от продаж с помощью компьютерных методов.

Врезка 1. Методы аудита

- **Расчет личного потребления** позволяет на основе дохода, наличных расходов и динамики активов установить, какими суммами для личного пользования располагает данный налогоплательщик. Если установлено, что личное потребление находится на очень низком уровне или характеризуется отрицательными цифрами, это означает, что у подозреваемого больше средств, чем он/она задекларировал(а). Это, в свою очередь, означает возможное наличие незадекларированного дохода, источником которого могли стать утаенные денежные поступления. Другие возможные методы - метод чистой стоимости и метод банковских вкладов.
- **Отрицательный баланс денежной наличности** означает, что подозреваемый налогоплательщик изъял из данного кассового аппарата бóльшую, чем приведена в фактической отчетности, сумму наличности, что в теории невозможно и становится признаком наличия неких необъясненных или скрытых поступлений наличных средств.
- **Анализ валовой прибыли** используется для анализа продаж. Сначала продажи анализируются путем расчета теоретической валовой прибыли на основании официально представленных налогоплательщиком закупочных и отпускных цен. Затем валовая прибыль рассчитывается на основе данных бухгалтерской отчетности (закупок и продаж) налогоплательщика. Зафиксированная в этой отчетности валовая прибыль, которая оказывается ниже расчетных цифр, - указание на то, что в отчетности был отражен не весь объем продаж.
- **Контроль объема** используется для анализа товаропотоков. Такой анализ может выявить, не продает ли данное предприятие товаров больше, чем закупает и имеет на складах, что означает наличие неучтенных продаж. Этот метод обычно используется в паре с анализом валовой прибыли.
- **Движение денежных средств от текущей деятельности/чистая выручка**: это часть, которую составляет движение денежных средств от текущей деятельности в процентах от чистой выручки, или дохода (согласно отчетности о доходах) компании. Чем выше это процентное значение, тем прозрачнее ведущий продажи за наличные бизнес; если это значение ниже, чем ожидалось, тем больше вероятность, что предприятие данного сектора предоставляет недостоверную отчетность. Следует отметить, что значения эти могут сильно разниться в зависимости от конкретного сектора и профиля предприятия. В одном конкретном случае при анализе деятельности ресторана представленные в отчетности

значения данного показателя не отклонялись от средних статистических данных по стране, но в реальности после того, как была выявлена практика утаивания доходов от продаж, подлинные цифры составили сумму, гораздо больше представленных государственными органами статистики средних величин

- **Тайные операции** могут использоваться налоговой администрацией для отслеживания деятельности данного предприятия и могут дать аудиторам важную информацию об использовании СЭКТ. Представители налоговой администрации могут также сыграть роль потенциальных пользователей для приобретения копии соответствующего ПО для его анализа.

- **Прочие используемые данным предприятием финансово-управленческие системы**, - такие, как учет товарных остатков и формирование счетов и накладных, - зачастую тесно привязаны к его контрольно-кассовой системе продаж. Извлеченная из этих систем информация может оказаться важной с точки зрения проверки содержащихся в ЭКТ данных

Аудитора можно научить тому, как извлекать полезную информацию из СЭКТ. Он может также научиться тому, как перепрограммировать ККТ, чтобы выявлять утаенные факты продаж и транзакции и распечатывать отчетные документы, содержащие соответствующую детальную информацию. Такой подход был принят на вооружение в Великобритании, где были организованы трехдневные курсы повышения квалификации для аудиторов. В результате реализации проекта штрафные санкции были наложены на 68% от общего числа подвергшихся аудиту предприятий.

Аудит в сфере электронной торговли

Аудиторы в сфере электронной торговли, или *e*-аудиторы, известны также под названием Специалисты по аудиту электронной торговли (Electronic Commerce Audit Specialists (ECAS)). СЭКТ зачастую содержат данные о тысячах транзакций, что делает их проверку невозможной без использования компьютеризованных инструментов и методик аудита (Computer Assisted Audit Tools and Techniques (CAATTs)),- таких, как ПО, известное, как «Интерактивное извлечение и анализ данных» (Interactive Data Extraction and Analysis (IDEA)). Этот вид инструментов позволяет аудитору выгружать данные практически из любых форматов или видов файлов и проводить самого различного рода анализ этих данных, а также составлять отчеты и графики (примеры которых приведены ниже по тексту). Этот инструмент может дополнять традиционные формы аудита и виды анализа, а также помогать выявлять нетипичные транзакции, наличие которых может указывать на факты мошенничества или отмывания денежных средств. ECAS-аудиторы – это специалисты, которые прошли специализированную подготовку по использованию CAATTs. Учитывая все более широкую практику использования электронных СЭКТ в сегменте предприятий, осуществляющих торговлю за наличные, на ECAS-аудиторов возлагается задача проведения анализа сложных систем и получения соответствующей ключевой информации для ее тестирования с помощью аудиторского ПО - такого, как IDEA, ACL или SESAM. Отбор файлов данных не простая линейная процедура, – в особенности, если предприятие использует электронную ККТ-систему или гибридную систему, а не более традиционную СЭКТ на основе ПК. Кроме того, ECAS-аудиторы обладают должным уровнем подготовки и компетенций в части углубленного анализа больших и сложных массивов данных электронных ККТ-систем для выявления признаков утаивания

доходов от электронной торговли и других нарушений закона. ECAS-аудиторы могут также передавать выявленные сведения другим членам группы аудиторов, работающей по данному делу, для сравнения их с данными, полученными силами налоговых аудиторов.

Использование методов криминалистической компьютерной экспертизы

Криминалист-программист при расследовании дела использует многие из числа тех инструментов, которые находятся в распоряжении аудиторов в сфере электронной торговли. Для обеспечения юридической состоятельности подобного рода криминалистического анализа необходимо, чтобы в лабораторию криминалистики была представлена подлинная СЭКТ; иными словами, как и в процессе «обычного» уголовного расследования, необходимо обеспечить наличие улик, включая использованные для совершения преступления инструменты. После их изъятия (обычно на основании ордера на обыск) делается копия содержимого их памяти (часто это описывается, как процесс «клонирования» жесткого диска устройства), и после этого можно приступать к процедуре криминалистической экспертизы.

Отслеживание «следов» правонарушений

Специалистами ОЭСР составлен подробный список «следов» правонарушений, которые может выявить «обычный» аудитор, ECAS-аудитор и эксперт-криминалист. Этот список предназначен для служебного пользования.

Методы уголовного следствия

Когда речь заходит об утаивании доходов от продаж с помощью компьютерных технологий, то, как и при других попытках избежать уплаты налогов, роль следователя заключается в проведении уголовного расследования в отношении действий подозреваемых в уклонении от налогов юридических и физических лиц в финансовой области для целей привлечения их к уголовной ответственности.

В случае утаивания доходов от продаж при помощи компьютерных технологий следователь по уголовным делам продолжает использовать традиционные методы расследования для сбора улик с помощью судебных ордеров на обыск (для изъятия СЭКТ, архивов электронных данных и резервных файлов, переданной по электронной почте корреспонденции и других видов данных в электронном формате), судебных приказов о предоставлении информации или других видов административных предписаний для получения финансовой информации, а также опроса потенциальных свидетелей в месте нахождения предприятия, в отношении которого ведется расследование, а также третьих сторон, как то производителей СЭКТи т.п.

В отношении производителей ПО следователь по уголовным делам может также использовать секретные операции или совместные с другими правоохранительными органами действия. Секретные операции требуют высочайшего уровня квалификации и тщательности планирования. Они могут позволить следователю получить непосредственные улики преступления и обеспечить существенные основания для получения ордера на обыск. Существует также более высокая вероятность того, что при получении и предъявлении улик

обвиняемым они признают себя виновными. Так, Канада прибегла к секретной операции в отношении некоего разработчика ПО, в ходе которой представители правоохранительных органов изображали состоятельных зарубежных рестораторов в поисках возможности открыть ресторанный бизнес в Ванкувере и проводили с ним переговоры по поводу закупки заппера. Собранные улики обеспечили достаточные основания для получения ордера на обыск производственных помещений компании–разработчика ПО.

После того как собрано достаточно улик, которые безусловно указывают на наличие вины, в адрес прокуратуры направляется представление для последующего обвинения в совершении налоговых и/или других уголовных преступлений. Цель любого привлечения к уголовной ответственности заключается в том, чтобы, помимо наказания правонарушителя, отвратить других лиц от совершения схожего рода преступлений и повысить уровень их законопослушания, послав им сигнал о том, что уклонение от налогов – это уголовное преступление, которое влечет за собой уголовное преследование, результаты которого предаются гласности.

Расследование «следов» правонарушений

Для случаев использования ПО в целях утаивания доходов от продаж можно предположить, что меры по сокращению оборота наличности также в большей степени затруднят или сделают невозможным раскрытие фактически полученных доходов с помощью «обычного» аудита бухгалтерской отчетности и учетных документов. Это подтвердилось в ходе проведенных в последнее время расследований по использованию мошеннического ПО: было сделано заключение о том, что для выявления реальной картины происшедшего следователи в значительной степени нуждаются в инструментах криминалистической экспертизы. Однако даже если зачастую у аудиторов нет возможности прибегнуть к инструментам цифровой криминалистической экспертизы, умения и навыки в области аудита электронной торговли все равно могут позволить аудитору обнаружить и скопировать ценные для следствия резервные и прочие файлы.

Представленные Швецией и Норвегией практические примеры – иллюстрация того, как вносились изменения в функционал ПО для утаивания доходов от продаж, чтобы усложнить его обнаружение. Ранние версии мошеннического ПО в оставляли в базовой системе управления бизнес-процессами большое число следов, связанных с внесенными изменениями. Более того, в ней оставались файлы с исходными данными о продажах. Налоговые органы раскрыли наличие подобного ПО, о чем стало известно производителю этих программных продуктов. В ходе проведенного затем расследования выяснилось, что эти программы подверглись изменениям, чтобы таких следов больше не оставалось: более поздние версии этого ПО уже удаляли бóльшую часть следов исходных транзакций и обрели функционал, который, как представляется, предназначался для предотвращения раскрытия факта наличия программы в ходе цифрового исследования данной системы, в частности, путем подмены временны*х* меток для файлов данных и т.п.

Для целей выявления случаев использования мошеннического ПО и программных продуктов, предназначенных для обеспечения утаивания доходов от продаж, крайне необходимо наличие правовых полномочий и технического потенциала для обеспечения безопасности СЭКТ и компьютеров. Несмотря на то, что такое ПО может оказаться в состоянии генерировать весьма убедительные

свидетельства подлинности фактов заниженного товарооборота и избавляться от всех следов истинного положения дел на предприятии, необходимо работать в предположении о том, что электронные улики останутся в других, более глубоких слоях системы, например, в операционной системе и системе файлов. Однако во многих случаях они могут стать объектом исследования только в ходе проведения криминалистической экспертизы.

Использование запперов также может оставлять следы в операционной системе и системе файлов. Однако в отличие от мошеннического ПО запперы после использования отсоединяют от системы и, как следствие, их невозможно подвергнуть анализу на основе материалов, к которым может получить доступ судебный эксперт-криминалист. При обнаружении заппера он может стать объектом такого анализа, однако в большинстве случаев для его проведения необходимо иметь соответствующие юридические полномочия в части изъятия личного имущества.

Цифровая криминалистическая экспертиза проводится также путем контролируемого сбора и анализа данных. Сбор данных включает изъятие достоверных копий источников цифровых данных, которые могут иметь отношение к данному предприятию и его деятельности; анализ же этих данных осуществляется с помощью методов и мер следствия, предназначенных для интепретации изъятой цифровой информации.

Изъятие источников цифровых данных

При том, что основной упор при изъятии данных делается на СЭКТ, существуют и другие источники цифровых данных предприятий, которые могут оказаться полезными для целей следствия: это могут быть компьютеры, обслуживающие бизнес-процессы предприятия, и внешние носители, которые могут быть связаны с использованием запперов и мошеннического ПО. При условии наличия юридически правомочного разрешения на изъятие и анализ подобного рода источников проблема заключается в обеспечении доступа к данной информации для целей ее копирования: существует риск ее повреждения или удаления, что может иметь серьезные последствия для ставшего объектом следствия предприятия и уменьшить возможность проведения анализа исследования его оборота. Решением в этой связи может стать осторожность и описанное ниже квалифицированное использование инструментов и техники.

Для сбора вышеуказанных данных имеется целый набор инструментов и ПО, которые по сути обеспечивают сохранность не подвергшихся какому-либо изменению цифровых данных предприятия и наличие копии данной информации, которая проверяется на соответствие ее оригиналу.

В случае необходимости обеспечить безопасность данных, содержащихся в специализированных системах предприятия, таких, как ЭКТ с хранением данных в ПЗУ[1], может оказаться необходимым проведение предварительных (до изъятия информации) тестов на аналогичном оборудовании, что требует должного уровня подготовки для использования данной технологии до начала налогового расследования.

Инструменты для обеспечения сохранности цифровой информации включают следующие системы.

- EnCase (разработчик - Guidance Software): это ПО способно выгружать данные с различных носителей информации и часто используется в сочетании с программным обеспечением для предотвращения записи, которое предназначено для сохранения цельности исходных данных.
- Forensic Toolkit Imager (разработчик - Access Data): это ПО может использоваться вместе с программами для предотвращения записи и выгрузки данных – действий, которые выполняются на работающей в этот момент системе.

Эти лишь отдельные примеры из имеющихся на сегодня программных продуктов. Эти продукты могут меняться, но принципы их использования остаются неизменными. На практике может случиться так, что вышеуказанные инструменты могут оказаться недостаточно адекватными, – в этом случае ключевой проблемой становится уровень профессиональной компетентности технических экспертов-криминалистов. Это, в свою очередь, предъявляет высокие требования к качеству соответствующей документации, а также обязывает проводить следственные мероприятия в соответствии с принципом, гласящим, что задачи должны быть выверены и их впоследствии можно будет воспроизвести.

Анализ цифровой информации

Порядок анализа хранимой информации разнится в зависимости от специфики отдельно взятого дела, доступа к ресурсам, квалификации налоговиков и следователей, а также законодательства, которым они руководствуются в своей работе. Таким образом, трудно дать общее представление о том, как осуществлять типовой анализ, но, вероятно, правильно было бы начинать с поиска и ознакомления с относящимися к фактам продаж записями.

Процедура судебной экспертизы должна начинаться с оценки и анализа всей имеющей отношение к данному налоговому аудиту информации. Это может быть информация, хранящаяся в архивах системы, в операционной системе, ПО или находящаяся в различного рода прочих файлах. Упор в процессе анализа следует делать на выявлении свидетельств использования ПО для утаивания доходов от продаж и вида использовавшегося ПО (мошенническое ПО или запперов).

Файлы, которые содержат зафиксированные факты продаж, необходимо сверять с временны*ы*ми метками [2] в памяти /системе файлов. Если записи о продажах подвергались изменениям в период времени, когда обычно они не заносятся в СЭКТ, это может служить указанием на использование ПО для утаивания доходов от продаж. Архивные файлы могут также содержать данные, которые могут служить доказательством ранее замеченных следов утаивания. Обычно надежным источником определения времени создания, изменения или последнего по времени использования файла может служить информация в файловой системе. Другими источниками могут стать записи, вносимые в обеспечивающие безопасность приложения, такие, как антивирусные программы, которые могут нести в себе информацию об именах и размерах файлов. Наличие разницы между размерами данного файла, зарегистрированного антивирусной программой, и размером файла в изъятой системе может служить доказательством произведенных в его содержании изменений. Цель анализа подобных файлов заключается, главным образом, в выявлении факта использования ПО для утаивания доходов от продаж.

Типовые инструменты, используемые в процессе анализа цифровой информации, следующие:

- EnCase (разработчик - Guidance Software) – программа, совместимая с большинством архивных систем и удобная для общего анализа собранной цифровой информации (*www.guidancesoftware.com/*).
- Forensic Toolkit from (разработчик - Access Data)- ПО, которое поддерживается большинством стандартных систем памяти и которое позволяет осуществлять процесс поиска посредством использования индексирования содержания собранной цифровой информации (*www.accessdata.com/*).
- IDA (разработчик - Hex-Rays) - программа, которая поддерживается большинством приложений и позволяет детранслировать файлы приложений (*www.hex-rays.com/idapro/*).
- Forensics WinHex (разработчик - X-Ways Software Technology) - шестнадцатеричный редактор со множеством аналитических функций (*www.x-ways.com/*).

Если в процессе анализа цифровой информации упор делается на выявление наличия ПО для утаивания доходов от продаж, в центре внимания эксперта оказываются, главным образом, программные файлы и вносимые в операционную систему записи. Порядок проведения подобного анализа может быть разным и включать различные виды экспертизы. Одним из часто используемых и весьма продуктивных подходов является анализ извлеченного из сохраненных материалов прикладного ПО. Это можно сделать, запустив данную программу на другом физическом компьютере или *виртуальной машине*. Можно привести ряд примеров, когда такого рода попытки привели к выявлению скрытых функциональных возможностей этого ПО. Этот метод - также удобный способ раскрытия способности программы занижать объемы оборота (продаж) с помощью других, не скрытых функций. Более сложный подход заключается в использовании методов детранслирования программных файлов, что означает, что содержание их, которое состоит, в основном, из инструкций для данной машины, переводится в программный код, доступный ис-)следователю для чтения. Этот процесс отнимает много времени, а степень его успешности может оказаться различной. Еще одним подходом, который выказал достаточно высокую эффективность, является выделение из программных файлов окон диалога и графических данных, которые могут выявить скрытые функциональные возможности и содержать ссылки на функциональность, относящуюся к занижению данных о продажах.

Примечания

1. Постоянное запоминающее устройство (ПЗУ) – память компьютера, которая может постоянно сохранять данные и приложения.
2. Временн***а***я метка – момент времени, в который компьютер фиксирует *событие,* например транзакция по продаже.

Ответные меры со стороны государства

Утаивание доходов от продаж с применением компьютерных технологий в системах электронных кассовых терминалов имеет место уже несколько лет, и уровень осведомленности правительств и налоговых администраций об этой проблеме неуклонно растет. Включению этого вопроса в повестку дня правительств ряда стран способствовала деятельность Рабочей группы ОЭСР по налоговым и другим финансовым преступлениям (РГНДФП). В ходе первого Форума по налогам и преступности, состоявшегося в Осло в марте 2011 г., этот вид налоговых рисков был представлен вниманию более широкого круга налоговых чиновников и представителей правоохранительных органов.

Рабочая группа ОЭСР по налоговым и другим финансовым преступлениям провела исследование подходов к решению этой проблемы в разных странах мира. Полученные данные послужили основой для анализа эффективности ответных мер, реализуемых правительствами разных стран в целях решения проблем и преодоления рисков, связанных с утаиванием доходов от продаж с применением компьютерных технологий.

Эти меры можно подразделить на следующие основные категории:

- Меры по повышению налоговой дисциплины;
- Информационно-разъяснительная работа;
- Выявление нарушений, аудит и расследования;
- Сбор оперативной информации;
- Использование фискальных регистраторов и сертифицированных СЭКТ.

Проблема утаивания доходов от продаж с применением компьютерных технологий довольно сложна, поэтому для ее эффективного решения необходим целый комплекс мер из разных - если не из всех - вышеперечисленных категорий. По этой причине для разработки пакета адекватных ответных мер необходим некий стратегический подход.

Стратегический подход

Некоторые налоговые администрации считают свою деятельность в этой сфере элементом реализации более общей стратегии, направленной либо на преодоление так называемого «налогового разрыва» (между предполагаемыми и реальными поступлениями в казну), либо на борьбу с теневой экономикой.

Для того чтобы разработать стратегический подход к решению проблемы утаивания доходов от продаж с применением компьютерных технологий, налоговой администрации нужно определиться с характером рисков, которые могут иметь место в этой ситуации. Для этого ей, в свою очередь, может быть полезна та информация, которая содержится в настоящем документе; кроме того,

весьма ценные сведения могут быть получены от более опытных сотрудников налоговых органов других стран, которые продвинулись по пути решения этой проблемы несколько дальше.

Что касается типов рисков, то их можно установить с помощью специальных аудиторских проверок определенных категорий предприятий - как тех, где фактор риска присутствует априори, так и тех, где его наличие не столь очевидно. Такой подход был использован в целом ряде стран, при этом проблема утаивания доходов от продаж с применением компьютерных технологий была выявлена в обоих случаях. Расширив охват таких выборочных проверок, можно определить, в каких секторах розничной торговли и сферы услуг риски нарушений являются наиболее высокими. Во многих странах первоочередное внимание налоговиков уделяется ресторанному бизнесу, однако высокие риски нарушений обнаруживаются также и в сетях небольших супермаркетов, в розничных аптеках, в парикмахерских и в других заведениях сферы услуг.

Полезно также бывает понять характер рынка СЭКТ, выяснить, кто их поставляет – как на внутреннем рынке, так и на международном, - и как между поставщиками распределены доли рынка.

Некоторые налоговые администрации продемонстрировали свои стратегические намерения бороться с утаиванием доходов от продаж с применением компьютерных технологий, закрепив соответствующие положения в законодательствах своих стран. Органы прокуратуры должны иметь возможность опереться на законодательство, криминализирующее поставки, владение и использование программного обеспечения, предназначенного для утаивания доходов от продаж с применением компьютерных технологий; это поможет ускорить процесс противодействия мошенническим фирмам (который зачастую бывает очень длительным), а также подать ясный и недвусмысленный сигнал соответствующим производителям и поставщикам. Такое законодательство недавно вступило в силу в Ирландии1, а в настоящее время вводится также в некоторых штатах США (в том числе во Флориде, в Мэне и в Нью-Йорке).

Меры по повышению налоговой дисциплины

Как сказано в отчете о работе Форума по налоговому администрированию Monitoring Taxpayer’s Compliance («Соблюдение налогоплательщиками налоговой дисциплины»)2, «в идеальном мире все граждане и все предприятия будут добросовестно выполнять все свои обязательства, предусмотренные налоговым законодательством и касающиеся учета, добровольного декларирования доходов и своевременной уплаты всех причитающихся налогов, размер которых вычисляется правильно и в полном объеме, в соответствии с действующим законодательством». Вопрос соблюдения налогоплательщиками этих основных обязательств можно также рассматривать с точки зрения тех средств, с помощью которых это соблюдение достигается: является ли оно добровольным («добровольное соблюдение» требований налогового законодательства) или обеспечивается за счет проверок и/или соответствующих мер принудительного характера со стороны налоговой администрации («принудительное соблюдение» требований налогового законодательства). С точки зрения налогового администрирования это различие имеет огромное значение, поскольку «принудительное соблюдение» влечет за собой затраты, и зачастую очень немалые.

Добровольное соблюдение требований налогового законодательства

В Руководстве ОЭСР по ведению бухгалтерского учета[3] преимущества добровольного соблюдения требований налогового законодательства описаны следующим образом:

«Обеспечение соблюдения налогового законодательства посредством частых проверок, тщательного аудита и преследований за нарушения – это дорогостоящий способ достижения надлежащего уровня соблюдения, поэтому большинство налоговых администраций пытаются максимально повысить уровень соблюдения добровольного, которое предполагает поощрение налогоплательщика к сотрудничеству с налоговыми органами и к действенному соблюдению им своих налоговых обязательств. Такой подход позволяет снизить издержки налогового администрирования, но реализовать его на практике можно только в том случае, если требования налогового законодательства хорошо понятны, если налогоплательщикам относительно легко их выполнить, и если бизнес в целом их понимает и принимает». «Добровольного соблюдения налогового законодательства… легче всего добиться там, где требования к предоставлению налоговой отчетности объединены с действующими системами учета и бухгалтерской отчетности. Если эти системы достаточно надежны, то издержки соблюдения налоговой дисциплины (как для предприятий, так и для налоговых администраций), скорее всего, будут минимальными».

В рамках деятельности по повышению уровня «соблюдения требований налогового законодательства, основанного на принципах сотрудничества», Форум по налоговому администрированию в своей Рекомендательной записке под названием «Общие принципы разработки коммерческого и бухгалтерского программного обеспечения и требования к его техническим характеристикам» («Guidance and Specifications for Tax Compliance of Business and Accounting Software»), дает серию соответствующих рекомендаций как для налоговых органов, так и для разработчиков программного обеспечения. Эти рекомендации касаются всех видов бухгалтерского и коммерческого программного обеспечения и, соответственно, распространяются также на программное обеспечение для кассовых аппаратов и СЭКТ. Как указано в этой Рекомендательной записке, условия, в которых приходится работать налоговым администрациям, всегда различны: это касается и политики, и особенностей законодательства, и системы управления, и культурных традиций страны, - и все эти факторы необходимо надлежащим образом учитывать.

Во многих странах налоговые администрации стремятся наладить сотрудничество с налогоплательщиками, а с крупнейшими налогоплательщиками работать в режиме так называемого «расширенного взаимодействия». Такие взаимоотношения строятся на основе взаимного доверия, прозрачности и взаимопонимания. Со стороны налоговых органов для этого необходимы понимание нужд и коммерческих интересов налогоплательщика, объективность, беспристрастность, сбалансированный подход, открытость и способность к быстрому и непосредственному взаимодействию с налогоплательщиком; со стороны налогоплательщиков же требуются раскрытие информации и прозрачность. Одним из преимуществ вовлечения бизнеса в расширенное взаимодействие с налоговыми органами является получение в результате такого взаимодействия скорейшей определенности в налоговых вопросах. Организуя режим расширенного взаимодействия с крупным бизнесом, налоговые

администрации обращают внимание на действующую на соответствующих предприятиях систему внутреннего контроля. Одним из элементов системы внутреннего контроля предприятия является бухгалтерское программное обеспечение (в том числе для электронных кассовых аппаратов и СЭКТ). При работе с предприятиями малого и среднего бизнеса налоговые администрации, обсуждая вопросы соблюдения требований налогового законодательства, зачастую обращают внимание на какие-то конкретные сектора их деятельности, а также на деятельность ассоциаций предприятий, и стараются достичь определенности по налоговым вопросам заблаговременно. В качестве примеров здесь можно привести Канаду и Нидерланды, где налоговые администрации вовлекают в обсуждение вопросов соблюдения требований налогового законодательства представителей местного ресторанного бизнеса.

Очень важной группой заинтересованных сторон здесь являются разработчики программного обеспечения и поставщики систем электронных кассовых терминалов. В ряде стран налоговые администрации рассматривают возможность работы в режиме расширенного взаимодействия с разработчиками и поставщиками электронных кассовых терминалов. Цель заключается в создании такой деловой среды, в которой в подавляющем большинстве кассовых терминалов не будут использоваться никакие методы утаивания доходов от продаж. Для этого налоговые администрации стремятся наладить сотрудничество с этими заинтересованными сторонами и поставить перед ними задачу избавиться от программного обеспечения, предназначенного для утаивания доходов от продаж. Здесь очень важно повлиять не только на поведение налогоплательщиков, но также и на деятельность разработчиков и поставщиков программного обеспечения; по сравнению с проведением индивидуальных проверок такой подход был бы гораздо более эффективным, поскольку он носит упреждающий характер и предполагает коллективный охват. В этой связи необходимо определить те стандарты, которым должны соответствовать электронные кассовые аппараты, и обязать разработчиков и продавцов программного обеспечения эти стандарты соблюдать.

Наглядный пример такого подхода продемонстрировало налоговое ведомство Ирландии. Там была развернута кампания по обеспечению соблюдения требований налогового законодательства при использовании систем электронных кассовых аппаратов, ориентированная на три основных категории заинтересованных сторон: владельцев предприятий (конечных пользователей), поставщиков кассовых аппаратов и/или программного обеспечения для них и их соответствующие представительные органы. Всем им были разосланы письма, к которым прилагалась изданная Комиссией налогового ведомства Ирландии новая брошюра с описанием новых правил. В этой брошюре было четко указано, что должен сделать каждый налогоплательщик для того, чтобы соблюсти требования по НДС за 2008 год, и, в частности, как именно требование к ведению отчетности применяется к использованию электронных кассовых аппаратов. Эта информация была также опубликована на сайте налогового ведомства Ирландии (см. *www.revenue.ie/en/tax/vat/leaflets/cash-registers.html*).

Знак качества

Инновационный подход к обеспечению добровольного соблюдения требований налогового законодательства применила налоговая администрации Нидерландов. В рамках этого подхода была создана специализированная отраслевая организация по сертификации качества СЭКТ, продаваемых в

Нидерландах. Пока что голландская система присвоения Знака качества4 является уникальной, но, по всей видимости, со временем ее можно будет приспособить и для других юрисдикций. Когда в Нидерландах эта система будет реализована в полном объеме, было бы полезно изучить возможности ее применения в международном масштабе. Следует обеспечить возможность применения специальных международных стандартов в отношении СЭКТ: в перспективе такой подход сулит очень большие преимущества, к числу которых можно отнести, например, существенное сокращение открытого рынка для утаивания доходов от продаж с применением компьютерных технологий, предоставление налоговым администрациям, разработчикам программного обеспечения и пользователям гарантии качества СЭКТ, а также снижение издержек соблюдения налоговой дисциплины для всех сторон.

Налоговая администрация Нидерландов и производители кассовых аппаратов участвуют в этом проекте на добровольных началах. В настоящее время проект успешно функционирует и получает поддержку со стороны многих производителей, а специализированная организация по присвоению Знака качества действует как полностью независимый орган. Идея этого проекта заключается в том, что электронные кассовые аппараты, удовлетворяющие установленным стандартам, получают маркировку «Знак качества». Организация по присвоению Знака качества устанавливает стандарты, которым должна соответствовать надежная СЭКТ, и отслеживает соблюдение этих стандартов производителями (а также правомерность использования ими Знака качества).

Рис. 3. Знак качества, присваиваемый электронным кассовым терминалам в Нидерландах

Источник: www.keurmerkafrekensystemen.nl

При проведении аудиторских проверок Налоговая администрация Нидерландов в своей системе управления рисками будет принимать во внимание, что на тех предприятиях, где электронные кассовые терминалы имеют этот Знак качества, риски нарушений должны быть заведомо меньше, чем на остальных.

Информационно-разъяснительная работа

Планомерное и постепенное повышение осведомленности о проблеме утаивания доходов от продаж с применением компьютерных технологий и о последствиях этого явления может оказаться полезной мерой. В ряде случаев такая информационно-разъяснительная работа может проводиться с привлечением или даже по инициативе СМИ и журналистов, занимающихся независимыми расследованиями: именно такой подход используется в Канаде, Нидерландах и Норвегии.

Налоговым администрациям, вероятно, нужно будет организовать диалог с ключевыми заинтересованными сторонами, к числу которых относятся производители, поставщики и представители делового сектора. Благодаря такому диалогу у налоговых администраций появится возможность обеспечить, чтобы эти заинтересованные стороны понимали:

- как применяются положения действующего законодательства к тому аппаратному и программного обеспечению, которым они пользуются;
- каких действий государство ожидает от них в этой связи;
- что им следует предпринять, чтобы соблюсти требования законодательства;
- какими могут быть последствия несоблюдения этих требований.

Если речь идет о конечных пользователях, то в ходе такого диалога можно рассмотреть следующие вопросы:

- бухгалтерский учет и правовые требования к ведению учетной документации;
- использование систем электронных кассовых аппаратов в контексте соответствия требованиям действующего законодательства;
- преимущества соблюдения требований действующего законодательства для обеих сторон (взаимная выгода): предприниматели получают наиболее актуальную деловую информацию, а налоговые органы - сведения об используемых кассовых терминалах и уверенность, что данный налогоплательщик относится к «категории более низкого риска» (что, соответственно, позволяет высвободить ресурсы для проведения аудита тех налогоплательщиков, которые относятся к «категории более высокого риска»).

При таком подходе могут использоваться такие средства коммуникации, как специальные брошюры с описанием использования систем кассовых аппаратов, специальные страницы на официальном сайте налоговой администрации, а также информационно-разъяснительные кампании более узкой направленности.

В ходе общения с поставщиками речь может идти, главным образом, о таких вопросах, как:

- положения действующего законодательства и требования к ведению бухгалтерской отчетности в отношении разработки, установки и использования систем электронных кассовых терминалов;
- специальные требования, которым должны удовлетворять системы электронных кассовых терминалов;
- преимущества соблюдения требований действующего законодательства для обеих сторон (взаимная выгода): например, разработчики/ поставщики получают возможность конкурировать на равных условиях, а налоговым органам соблюдение ими действующих требований обеспечивает некоторую «страховку» (меньший риск, возможность высвободить ресурсы для проведения аудита тех налогоплательщиков, которые относятся к «категории более высокого риска»).

Здесь основными средствами коммуникации являются организация и проведение встреч с представительными органами, а также личные встречи с поставщиками.

Кроме того, используя средства массовой информации, информационно-разъяснительную кампанию можно ориентировать на самый широкий круг лиц. Для этого нужно публиковать в СМИ сведения об обвинительных приговорах в

отношении нарушителей действующего законодательства: это будет способствовать повышению налоговой дисциплины. В Канаде, например, освещение в СМИ и публикация материалов об успешных судебных преследованиях нарушителей налогового законодательства является ключевым фактором успеха Программы уголовных расследований Налогового управления. В некоторых случаях - как, например, с запперами - к освещению дела в СМИ можно прибегнуть на этапе выдачи ордеров на обыск, когда уголовное расследование уже идет. Публикация материалов о ходе судебного преследования нарушителей и о вынесении им приговора является неотъемлемым элементом системы самооценки налогоплательщика; кроме того, это действует как фактор сдерживания для тех, кто подумывает об уклонении от уплаты налогов. Пример такого освещения в СМИ приведен на рисунке 4. Эта история была подхвачена также в вечерних программах теленовостей.

Рис 4. Использование запперов: освещение проблемы в СМИ

Источник: газета «The Province» от 11 декабря 2008 г., первая страница: «Tax - Cheating software bust – Something's fishy at these restaurants (…and it's not the sushi)» («Афера с мошенническим программным обеспечением раскрыта: в этих ресторанах что-то дурно попахивает (… и это не суши)»).

Аудит и налоговые расследования

Налоговые администрации не только проводят выборочные аудиторские проверки отдельных налогоплательщиков, но и применяют некоторые системные

подходы к анализу и аудиту возможных фактов утаивания доходов от продаж с помощью компьютерных технологий. Отбор дел для таких проверок может производиться на основании целого ряда факторов. Важную роль здесь играют программное обеспечение, используемое для анализа рисков (например, описанная выше система IDEA), а также знание конкретных видов бизнеса и секторов, где оборот наличности традиционно очень высок. В налоговые органы поступают самые разные сигналы, и бывают случаи, когда на основании таких сигналов может быть выявлено программное обеспечение и другие средства, используемые для утаивания доходов от продаж, а также их поставщики.

Проверки и расследования деятельности поставщиков электронных кассовых терминалов, в отношении которых у налоговых органов имеются подозрения в использовании компьютерных технологий для утаивания доходов от продаж, позволяют получить клиентские базы этих поставщиков, выявив таким образом пользователей этого программного обеспечения. Эти сведения можно использовать для разработки программ по проверке конкретных видов электронных кассовых аппаратов. Кроме того, это позволяет получить больше информации о тех изменениях, которые вносятся в проверяемые системы кассовых аппаратов.

Наиболее серьезные нарушения должны преследоваться в уголовном порядке, и сведения о таких случаях необходимо предавать гласности, с тем чтобы у других налогоплательщиков был повод задуматься о своих действиях и устранить возможные нарушения. У налоговых администраций многих стран есть программы добровольного раскрытия информации, цель которых состоит в том, чтобы у налогоплательщиков появился стимул сделать шаг навстречу налоговым органам и исправить ситуацию, если ранее ими были допущены те или иные нарушения.

Для всех налоговых администраций ключевым элементом борьбы с утаиванием доходов от продаж является уверенность в высоком уровне профессионализма специалистов, контролирующих вопросы соблюдения клиентами установленных норм и требований. Такими специалистами являются налоговые аудиторы, аудиторы - специалисты по электронным платежам и расчетам, компьютерно-технические эксперты и следователи по уголовным делам. Для того чтобы все они могли осуществлять свои функции на должном уровне, необходимо изыскать ресурсы и обеспечить подготовку специалистов соответствующей квалификации.

Налоговый аудитор

Если в основе подхода к борьбе с утаиванием доходов от продаж лежит соблюдение определенных «принципов», т.е. если налоговые администрации исходят из того, что налогоплательщики добросовестно выполняют свои налоговые обязательства, надлежащим образом ведут документацию и бухгалтерскую отчетность, то функции налогового аудитора заключаются в следующем. В ходе проверки он должен посетить те производственные помещения налогоплательщика, где есть электронные кассовые терминалы (так, например, он должен узнать название производителя СЭКТ, посмотреть, нет ли там каких-то старых СЭКТ, «которые больше не используются», и т.д.), побеседовать с налогоплательщиком и его сотрудниками (например, для того, чтобы выяснить, каковы функции данных кассовых терминалов и как они используются, узнать, каковы должностные обязанности налогоплательщика и его сотрудников в рамках действующих бизнес-процессов и системы внутреннего контроля), провести косвенную проверку

доходов налогоплательщика (для этого, например, он должен будет проверить источники дохода и характер использования средств, провести анализ чистой стоимости имущества) и проверить результаты работы самих электронных кассовых терминалов (например, сравнить отчетный объем продаж за предыдущие периоды с аналогичным показателем на момент проведения аудиторской проверки).

Кроме того, как и в случае с передачей дела в отдел по уголовным расследованиям налоговой администрации или в соответствующие правоохранительные органы при выявлении возможных фактов уклонения от уплаты налогов, аудитор также должен иметь в виду, что налогоплательщик может использовать мошенническое программное обеспечение для утаивания доходов от продаж. В этой связи аудитору необходимо организовать проверку самих кассовых терминалов, договорившись об этом со специалистами по вопросам электронной коммерции или с аудиторами, специализирующимися в области электронных платежей и расчетов.

Если же в основе подхода к борьбе с утаиванием доходов от продаж лежит соблюдение определенных «правил» (а не «принципов»), то роль аудитора расширяется. Этот подход предусматривает, что государство требует от пользователей использовать только определенное, «одобренное государством» оборудование и программное обеспечение и соблюдать установленный порядок ведения отчетности. В этом случае наряду с обычными проверками, о которых шла речь выше, аудиторам придется также тщательно проверить ЭКТ и электронные кассовые аппараты на предмет их физической целостности (не были ли они взломаны с целью несанкционированного вмешательства в их работу), а также проверить соответствующую документацию. В некоторых странах аудиторы делят эту функцию с аудиторами - специалистами по электронным платежам и расчетам.

Аудиторы передают дело в органы следствия или в соответствующие правоохранительные органы во всех случаях обнаружения фактов возможного уклонения от уплаты налогов, включая те, которые связаны с использованием компьютерных технологий для утаивания доходов от продаж.

Аудиторы - специалисты по электронным платежам и расчетам и компьютерно-технические эксперты

Если налогоплательщики используют СЭКТ, то большую помощь в работе налоговых аудиторов могут оказать аудиторы, являющиеся специалистами по электронным платежам и расчетам. Именно эти специалисты обладают необходимой квалификацией для того, чтобы получить доступ к компьютерной системе налогоплательщика и предоставить налоговому аудитору копии электронных документов его ЭКТ.

Следует отметить, что после того, как в 1990-х годах были выявлены первые случаи использования мошеннического программного обеспечения для утаивания доходов от продаж, роль аудиторов - специалистов по электронным платежам и расчетам расширилась: если раньше они обеспечивали только пассивную помощь налоговикам, то теперь их роль в проведении проверок стала активной. В странах, где такие должности были созданы, квалификация специалистов по электронным платежам и расчетам существенно повысилась: теперь они в состоянии производить сложнейшие компьютерные операции (дешифровать пароли, выявлять функциональные ключи управления, обнаруживать изменения в программных

кодах и т.п.). Кроме того, они проводят беседы с владельцами и сотрудниками предприятий, задавая им вопросы о функционировании кассовых терминалов. Обычно результаты работы этих специалистов передаются налоговым аудиторам, которые затем приобщают их к материалам проверок.

В случае серьезных нарушений дело может быть передано в органы уголовного расследования, и тогда уже на первый план выходят компьютерно-технические эксперты. Эти специалисты, как и их коллеги - аудиторы - специалисты по электронным платежам и расчетам, - обладают необходимой квалификацией для проведения выемки и судебной экспертизы компьютерных и других электронных данных. Они получают доступ к компьютерам и СЭКТ налогоплательщика и, используя различные технологии судебной экспертизы (анализ меток даты/времени, контрольных сумм и чисел, дублирование систем для проведения проверки, анализ электронных писем, уличающих в нарушениях, восстановление удаленных электронных писем, файлов и данных и т. д.), помогают следователям по уголовным делам установить наличие такого элемента состава преступления, как преступный умысел (mens rea), который обычно требуется для предъявления обвинения в совершении уголовного преступления. Как правило, результаты работы этих специалистов также передаются следователю по уголовным делам, чтобы он смог приобщить их к материалам дела.

Вне зависимости от того, какой из этих подходов использует налоговая администрация для целей борьбы с утаиванием доходов от продаж с применением компьютерных технологий, роль аудиторов - специалистов по электронным платежам и расчетам и компьютерно-технических экспертов здесь является ключевой. При этом очень важно организовать работу таким образом, чтобы аудиторы - специалисты по электронным платежам и расчетам и компьютерно-технические эксперты имели возможность эффективно взаимодействовать как друг с другом, так и с работниками налоговой администрации.

Уголовное расследование

Угроза уголовного расследования и преследования является самым сильным сдерживающим фактором, который большинство налоговых администраций могут использовать для целей борьбы с серьезными нарушениями налогоплательщиками требований налогового законодательства, в том числе с такими, как применение методов и средств утаивания доходов от продаж. Как и остальные правоохранительные органы, налоговая администрация должна собрать улики, подтверждающие преступный умысел, а также доказать наличие у налогоплательщика не отраженных в его отчетности доходов.

Для сбора доказательств следователи применяют обычные методы расследования (например, сбор доказательств и свидетельских показаний с использованием ордеров на обыск, судебных приказов о предоставлении информации, а также опроса ключевого персонала – как по месту осуществления коммерческой деятельности налогоплательщика, так и по месту нахождения изготовителя программного обеспечения, используемого для утаивания доходов от продаж, и т.д.). Вместе с тем могут применяться и другие методы расследования - например, секретные операции (описанные выше) или операции, проводимые совместно с другими правоохранительными и регулирующими органами; целью таких операций является получение ключевых доказательств, подтверждающих использование технологий по утаиванию доходов от продаж. Еще одной, побочной

целью здесь является создание фактора сдерживания посредством повышения осведомленности общества о растущей угрозе утаивания доходов от продаж с применением компьютерных технологий и получения теми, кто использует такие методы, несправедливых преимуществ по отношению к остальным участникам рынка. Благодаря огласке, которую получают такие случаи, те, кто прибегает к этой форме уклонения от уплаты налогов или мошенничества, будут знать, что налоговая администрация в курсе этой ситуации и не намерена с ней мириться. К тем, кто участвует в таких махинациях, будут применены жесткие наказания, штрафы и, возможно, даже тюремное заключение.

Источники оперативной информации

Помимо упомянутых выше специалистов, которые работают с налогоплательщиками непосредственно, есть еще те, кто, «оставаясь в тени», помогают им делать все, что необходимо для эффективной борьбы с утаиванием доходов от продаж. Это специалисты самого разного профиля: от сотрудников финансовой разведки, которые, используя информацию из открытых источников, а также сведения, которые собирают налоговые аудиторы и следователи (например, клиентские базы поставщиков оборудования и программного обеспечения), составляют на их основе сводки оперативной информации, до инструкторов, осуществляющих необходимую подготовку и обучение всех четырех категорий специалистов, непосредственно работающих с клиентами, так чтобы те могли выполнять свои задачи надлежащим образом.

Выявление и расследование нарушений требуют глубоких знаний в области функционирования СЭКТ. Информация о различных системах ЭКТ может быть:

- собираемой открыто из открытых источников; или
- собираемой тайно (например, путем анонимного приобретения технической документации).

Нормативно-правовая база деятельности по сбору информации - это вопрос конкретного национального законодательства. Есть большое количество правовых систем, в основе которых лежат правовые традиции и понимание публичных прав. В большинстве стран-членов ОЭСР существует разграничение между законодательством о правоприменительной деятельности и налоговым законодательством. Обмен информацией между налоговой администрацией и правоохранительными органами, как правило, жестко регулируется. Сбор информации и обмен ею все чаще происходят в тех случаях, когда возникают обоснованные подозрения в совершении преступления (в настоящее время или в прошлом). Когда речь идет о манипуляциях и мошенничестве с использованием цифровых систем - например, таких, как СЭКТ, - ключевую роль играет наличие у правоохранительных и других государственных органов достаточных правовых оснований для сбора и анализа информации. Это необходимо для того, чтобы организовать наиболее адекватные ответные меры и выявить системы ЭКТ, используемые недобросовестно.

Налоговые администрации могут обмениваться друг с другом собираемыми сведениями, пользуясь имеющимися в их распоряжении механизмами обмена информацией по налоговым делам. В частности, свою полезность уже доказало использование спонтанного обмена информацией о производителях, работающих на международном рынке. Кроме того, в последнее время весьма успешным

оказалось применение Конвенции о взаимной административной помощи по налоговым делам, которая предусматривает обмен информацией между странами. Эту конвенцию пока подписали не все страны-члены ОЭСР, но число подписантов неуклонно растет.

Сбор оперативной информации

Для следователя сбор оперативной информации является той основой, которая позволяет ему определиться с рамками расследования. В ходе уголовного преследования оперативная информация в качестве доказательства использоваться не может, но она помогает следователю получить необходимые улики. Для следователя польза такой информации состоит в том, что она помогает ему понять, что именно он должен искать (и как это выглядит).

Системы утаивания доходов от продаж с применением компьютерных технологий обладают целым рядом признаков, указывающих на то, что эти системы должны попасть в поле зрения следователей. В таких случаях полезными методами сбора информации могут быть:

- Агентурные операции: этот метод используется некоторыми подразделениями по налоговым расследованиям в целях проведения секретных расследований. Этот подход требует очень детального правового, технического и оперативного планирования. Результатами применения таких методов поделиться можно, но в некоторых юрисдикциях, ввиду действия положений о неприкосновенности частной жизни, поставка, получение и использование такой информации в уголовном процессе невозможны.
- Технические методы сбора информации: к ним относятся контроль передачи данных / прослушивание телефонных переговоров подозреваемых, слежка за личным автотранспортом подозреваемых, аудиомониторинг помещений и другие «пассивные» технические операции (пассивные в том смысле, что они не предполагают взлома компьютерных систем и других подобных мероприятий). Эти методы используются для получения информации и могут включать в себя также и более «агрессивные» меры.
- Использование конфиденциальных источников и информантов.

Библиотеки информации

В некоторых странах создаются библиотеки актуальной информации, которая может послужить подспорьем для проведения проверок и расследований в отношении СЭКТ. На уровне одной страны такая библиотека может содержать не только общедоступную информацию о производителях, поставщиках и имеющихся на рынке СЭКТ, но также и техническую информацию, полученную в ходе аудиторских проверок и расследований. В этой связи возник вопрос о возможности ведения таких библиотек на международном уровне и предоставления доступа к ним налоговым органам разных стран, однако при реализации этого подхода есть вероятность столкнуться с некоторыми проблемами, касающимися защиты данных и обмена информацией. Возможной альтернативой здесь было бы создание некоего шаблона для обмена информацией об использовании СЭКТ для целей утаивания доходов от продаж, который можно было бы применять в рамках обычных

механизмов обмена информацией между странами, ведущими собственные библиотеки.

Использование фискальных регистраторов и сертифицированных систем электронных кассовых терминалов

В борьбе с недобросовестным использованием СЭКТ для целей уклонения от уплаты налогов пробовали применять самые разные подходы. В настоящее время диапазон возможных решений в этой сфере довольно широк - от итальянских «фискальных регистраторов» (аппаратов, у которых в конце торгового дня в памяти записывающего устройства сохраняются данные о продажах за этот день) до португальского «сертифицированного программного обеспечения для СЭКТ» (которое обеспечивает генерирование в системе зашифрованных данных о продажах, защищенных электронной цифровой подписью, которая удостоверяет подлинность транзакций). Одним из главных новшеств в этой области является то, что теперь данные в СЭКТ защищены с момента их генерации, в отличие от старых систем, в которых это происходило только в конце торгового дня. Подробное описание особенностей фискальных регистраторов и сертифицированных систем электронных кассовых терминалов содержится в Приложении.

В настоящем докладе нет рекомендаций об использовании каких-то конкретных технических решений в этой области; скорее, его авторы хотели предоставить читателю сведения о возможных решениях. При этом, однако, нельзя не отметить, что в настоящее время предпочтение все чаще отдается таким системам, которые обеспечивают защиту кассовых данных с момента их генерации и включают в себя такие технологии, как шифрование данных и использование электронной цифровой подписи.

Примечания

1. В 2011 г. в законодательство были введены следующие положения:

   ‘‘(ба) сознательно или преднамеренно владеет или использует для целей уклонения от уплаты налогов компьютерные программы или электронные компоненты, модифицирующие, исправляющие, удаляющие, отменяющие, скрывающие или иным образом изменяющие какую бы то ни было информацию, хранящуюся или сохраняемую с помощью каких бы то ни было электронных устройств, без сохранения исходных данных и сведений об их последующих модификациях, исправлениях, отмене, сокрытии или изменении,

   (бб) предоставляет или делает доступными для целей уклонения от уплаты налогов компьютерные программы или электронные компоненты, модифицирующие, исправляющие, удаляющие, отменяющие, скрывающие или иным образом изменяющие какую бы то ни было информацию, хранящуюся или сохраняемую с помощью каких бы то ни было электронных устройств, без сохранения исходных данных и сведений об их последующих модификациях, исправлениях, отмене, сокрытии или изменении.

   Такие правонарушения преследуются в порядке суммарного производства; наказание за правонарушения, совершенные по состоянию на 14 марта 2008 года или после этой даты, предусматривает штраф в размере до 5000 евро (или до 3000 евро, если преступление совершено до указанной даты), который может быть уменьшен до суммы, составляющей не менее одной четвертой части этого штрафа, или, по усмотрению суда, лишение свободы на срок до 12 месяцев, либо оба указанные вида наказания, а в случае осуждения за преступление, вмененное по обвинительному акту, - штраф в размере до 126970 евро или, по усмотрению суда, лишение свободы на срок до 5 лет, либо оба указанные вида наказания.”

2. См. OECD (2008) *www.oecd.org/dataoecd/51/13/40947920.pdf*.

3. Издания по налоговому руководству – Ведение учета *www.oecd.org/dataoecd/29/25/31663144.pdf*.

4. Брошюра, где описана концепция «Знак качества», доступна также на английском языке, см. *www.belastingdienst.nl/download/1419.html.*

Заключение

С тех пор как Рабочая группа ОЭСР по налоговым и другим финансовым преступлениям начала вести среди налоговых администраций работу по повышению их осведомленности о проблеме утаивания доходов от продаж с применением компьютерных технологий, налоговые администрации существенно активизировали свою деятельность по выявлению и устранению тех угроз для казны, которые такое утаивание представляет. Однако одновременно с этим повысилась и изощренность методов, которыми стали пользоваться мошенники и недобросовестные поставщики СЭКТ для сокрытия операций, осуществляемых в целях уклонения от налогов. В настоящем докладе содержатся рекомендации для налоговых администраций по вопросу разработки стратегий борьбы с утаиванием доходов от продаж и приводится конкретная информация, которая может помочь налоговым аудиторам и следователям в их деятельности по выявлению, расследованию и пресечению практики уклонения от налогов.

Оценка рисков и выбор наиболее подходящей и эффективной стратегии в этом вопросе остаются за каждой конкретной налоговой администрацией. Ниже мы приводим ряд рекомендаций относительно тех действий, которые должны быть элементами такой стратегии.

Процесс работы над этим докладом группы его авторов оказался чрезвычайно полезным сам по себе. Так, например, обмен опытом между экспертами позволил выявить дополнительные области для исследования, а в некоторых случаях способствовал установлению международного сотрудничества в сфере борьбы с преступностью – вплоть до сотрудничества по вопросам проведения рейдов по проверке производственных помещений и выдачи международных ордеров на арест. Благодаря этому было положено начало процессу устранения того дисбаланса, из-за которого поставщики мошеннического программного обеспечения и запперов, пользуясь отсутствием обмена информацией между странами, имели возможность свободно оперировать на международном рынке.

Рекомендации

Налоговые администрации должны разработать стратегию решения проблемы утаивания доходов от продаж с применением компьютерных технологий, укладывающуюся в рамки их общего подхода к обеспечению соблюдения налоговой дисциплины. Такая стратегия должна способствовать снижению рисков, связанных с использованием систем утаивания доходов от продаж, добровольному соблюдению требований налогового законодательства, а также совершенствованию системы мер по выявлению нарушений и противодействию им. В идеале эта стратегия должна предусматривать заблаговременный сбор информации об используемых налогоплательщиками системах: это позволит

выявлять потенциальные риски нарушений заранее и выделять для решения возникающих проблем необходимые ресурсы.

Следует разработать программу коммуникаций между всеми заинтересованными сторонами, направленную на повышение их информированности о преступном характере использования методов утаивания доходов от продаж и о тех серьезных последствиях, которыми такая практика чревата (уголовное преследование).

Налоговым администрациям рекомендуется также исследовать вопрос о наличии у них необходимых правовых полномочий для проведения проверок и судебной экспертизы систем электронных кассовых терминалов.

Налоговым администрациям следует вкладывать соответствующие ресурсы в приобретение необходимой квалификации и инструментов для проведения проверок и расследований в отношении СЭКТ. Сюда, в том числе, относится также введение в случае необходимости должности аудиторов, являющихся специалистами по электронным платежам и расчетам, и привлечение к работе компьютерно-технических экспертов. В рамках борьбы с утаиванием доходов от продаж с применением компьютерных технологий следует также предусмотреть механизмы, обеспечивающие эффективное сотрудничество между специалистами различных профилей.

Налоговым администрациям следует рассмотреть возможность разработки рекомендаций о внесении в действующее законодательство положений, криминализирующих поставки, владение и использование программного обеспечения для целей утаивания доходов от продаж с использованием компьютерных технологий.

Приложение. Использование фискальных регистраторов и сертифицированных систем электронных кассовых терминалов

Фискальные регистраторы

В некоторых странах фискальные регистраторы были законодательно введены в обращение более 25 лет назад, а недавно интерес к этим устройствам снова стал расти. По своей сути фискальный регистратор - это кассовый аппарат, который должен удовлетворять ряду технических требований в отношении безопасного хранения данных и контроля событий внутри системы. Впервые фискальные регистраторы появились в Италии еще в 1983 году, когда правительство страны, пытаясь снизить объем теневой экономики, ввело в отношении некоторых категорий предприятий требование об обязательной выдаче клиентам фискальных чеков с использованием электронных фискальных кассовых аппаратов. Этот же подход был использован в Греции и в ряде других стран. Какую именно информацию должна сохранять система ЭКА, в какой форме должны в ней храниться данные, какие результаты (отчеты / файлы и чеки) и в каком формате система должна выдавать для сохранения данных для последующих налоговых проверок - все это определяло правительство каждой конкретной страны.

Специальные требования в этой области таковы:

- Сохранение детализированных данных о совершенных транзакциях – в специальном электронном формате, надлежащих образом зашифрованных и на специальных носителях;
- Хранение детализированных данных, доступ к которым, в случае необходимости, может получить только налоговый аудитор;
- Сохранение в полном объеме контрольного журнала системы, а в некоторых случаях – архива мониторинга событий в системе;
- Система должна быть оснащена определенной контрольной аппаратурой; и
- Другие технические требования, обеспечивающие защиту данных от последующих изменений и сохранение их целостности.

Первые фискальные регистраторы позволяли сохранять данные только по состоянию на конец торгового дня, современный же подход предусматривает возможность сохранения данных непосредственно в момент их генерации.

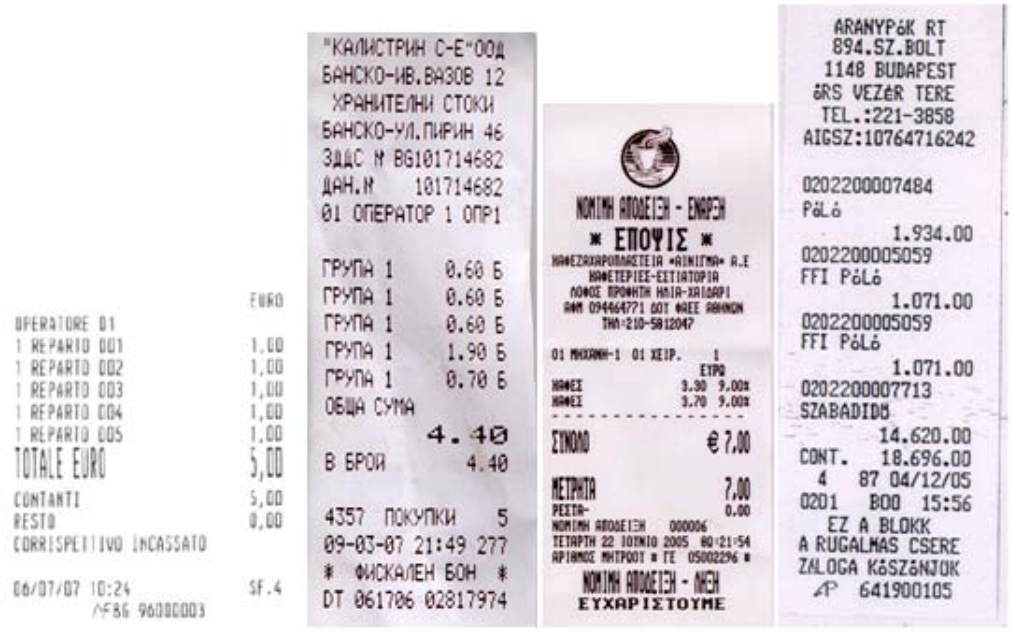
В общих словах эту технологию можно описать следующим образом. В конце каждого торгового дня предприниматель должен составлять кассовый отчет за день (ежедневный финансовый отчет). Затем общие суммы продаж, указанные в этих отчетах, записываются в защищенную память фискального устройства, счетчики которой обновляются при записи данных о продажах за соответствующий день. Впоследствии в некоторых странах эти счетчики были усовершенствованы и могли

запоминать также данные с терминалов, выдающих электронные билеты с номером очереди, общую сумму выданной сдачи и другие параметры.

Изначально эта защищенная память (ПЗУ) опечатывалась и хранилась в самом кассовом аппарате: она крепилась к его корпусу с помощью канифоли или эпоксидной смолы. Но по мере развития технологий и все большей привязки кассовых аппаратов к компьютерным системам помещение защищенной памяти внутрь корпуса перестало быть обязательным; теперь этот блок может находиться в отдельно стоящем принтере системы (впоследствии он получил название фискального принтера).

В печатаемом чеке четко указывается, является ли он подлинным фискальным чеком, отражающим совершенную транзакцию, или же он напечатан в целях обучения, в качестве примерного счета-фактуры, или это копия билета с номером очереди. Фискальные чеки также имеют внизу штамп, содержащий фискальный логотип, который должен отвечать некоторым специальным требованиям, предъявляемым к шрифтам и формату чека.

Рис. 5. Примеры фискальных чеков (слева направо: Италия, Болгария, Греция, Венгрия)



Источник: Информация предоставлена Италией, Болгарией, Грецией и Венгрией.

В разных странах сертификация (подтверждение соответствия системы требованиям закона) осуществляется либо налоговой администрацией, либо частным органом по сертификации.

«Фискальные регистраторы» были ведены в обращение во многих странах, включая Аргентину, Бразилию, Болгарию, Венгрию, Венесуэлу, Грецию, Латвию, Литву, Мальту, Польшу, Россию и Турцию. В определенных обстоятельствах такие системы по-прежнему уместны. В некоторых развивающихся странах при использовании этих систем производится автоматическая передача данных с них в компьютерную систему налоговой администрации.

Сертифицированные системы электронных кассовых терминалов

В последнее время все больше стран стремятся повысить уровень соблюдения налогоплательщиками налоговой дисциплины путем обязательного использования на всех предприятиях, деятельность которых предполагает оборот наличных денег, либо на всех предприятиях какого-то конкретного сектора экономики (например, ресторанного) «сертифицированных» систем электронных кассовых терминалов. Этот подход предполагает использование дополнительного оборудования, которое, с помощью технологии шифрации данных, добавляет ко всем или к некоторым элементам данных электронную цифровую подпись. Такое оборудование может включать в себя контрольное устройство для хранения данных чеков и электронных подписей и для обновления общих итоговых значений параметров в защищенной памяти.

Защита данных чеков электронной цифровой подписью и хранение данных в памяти контрольного устройства

Технические решения такого характера предусматривают не только добавление к некоторым данным чека электронной цифровой подписи, но и отслеживание содержащихся в этих чеках данных, существенных для налогообложения. Такой подход внедрен или внедряется в настоящее время в налоговых администрациях Бельгии, Греции, канадской провинции Квебек и Швеции.

Греция

Министерство финансов Греции первым ввело порядок добавления электронной цифровой подписи[1] к данным чеков и счетов. Печать электронной цифровой подписи на чеке или счете и ее запоминание в исходных данных позволяют получить достаточно хороший инструмент для проверки и обеспечения целостности данных в СЭКТ.

Рис. 6. Греческое фискальное устройство по формированию электронной цифровой подписи

Источник: информация предоставлена Грецией

Квебек

В провинции Квебек было разработало и внедрено контрольное устройство - модуль учета продаж, которое запоминает соответствующие данные чека и генерирует электронную цифровую подпись.2 Подпись в виде двухмерного штрих-кода печатается также на чеке, который получает клиент. Открытый ключ принадлежит налоговой администрации (которая является поставщиком модуля учета продаж).

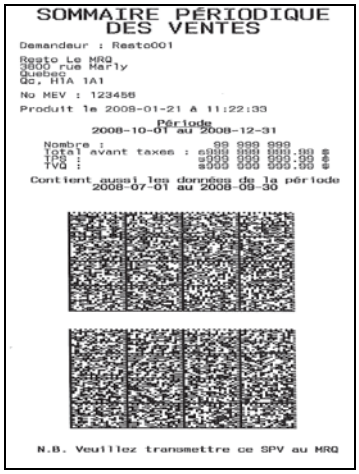
Рис. 7. Модуль учета продаж, используемый в провинции Квебек

Источник: Информация предоставлена налоговой администрацией провинции Квебек

Сканируя этот штрих-код ручным сканером (с программным обеспечением с открытым ключом), легко проверить действительность электронной цифровой подписи. Недействительность подписи однозначно укажет на то, что содержание чека подвергалось каким-то манипуляциям.

Кроме того, этот модуль учета продаж может выдавать периодические отчеты, также представленные в форме двухмерного штрих-кода. Такой отчет может быть отправлен в налоговую администрацию Квебека либо обычной почтой, либо в электронном виде, путем копирования на USB-ключ и последующей загрузки в защищенную компьютерную систему налоговой администрации.

Рис. 8. Пример отчета о продажах, сформированного модулем учета продаж в виде штрих-кода


SOMMAIRE PÉRIODIQUE
DES VENTES

Demandeur : Resto001

Resto Le MRQ
3800 rue Marly
Quebec
Qc. H1A 1A1

No MEV : 123456

Produit le 2008-01-21 À 11:22:33

Période
2008-10-01 au 2008-12-31

Nombre : 99 999 999
Total avant taxes : $999 999 999.99 $
TPS : $999 999 999.99 $
TVQ : $999 999 999.99 $

Contient aussi les données de la période
2008-07-01 au 2008-09-30

N.B. Veuillez transmettre ce SPV au MRQ

Источник: информация предоставлена Канадой.

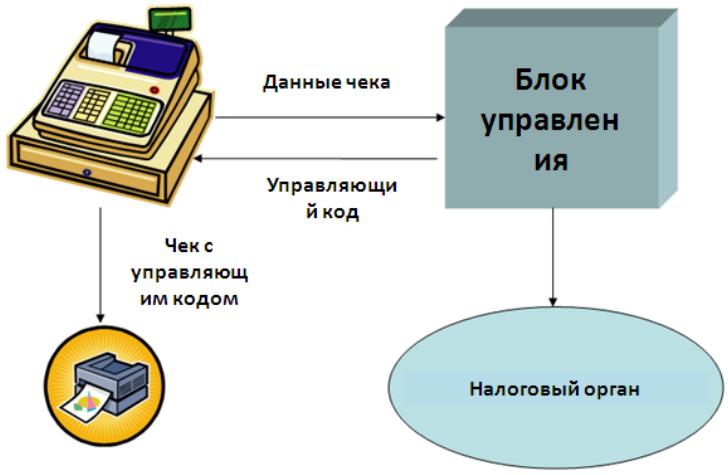
Это устройство было введено в эксплуатацию только в ресторанном секторе. Более подробную информацию об этом можно найти на сайте Налогового управления провинции Квебек3.

Швеция и Бельгия

В 2010 году полностью вступило в силу новое законодательство Швеции, предусматривающие обязательное использование систем контрольно-кассовых аппаратов на всех предприятиях, деятельность которых сопряжена с интенсивным оборотом наличных средств (с некоторыми исключениями, под которые подпадают, в частности, очень мелкие предприятия, открытые рынки и крупные компании с хорошей системой внутреннего контроля).

В соответствии с новым законодательством, СЭКТ должны удовлетворять строгим техническим требованиям, при этом в законе прописаны как обязательные функции, которыми СЭКТ должны обладать, так и те функции, которые в этих системах запрещены. Каждый кассовый аппарат производитель обязан регистрировать в налоговых органах.

Рис. 9. Шведский блок управления



Источник: информация предоставлена Швецией.

Кроме того, блок управления должен быть подключен к системе. Исходя из содержимого чека, он формирует электронную цифровую подпись4. Эта подпись (она печатается на чеке) позволяет производить простую проверку целостности данных чека. Соответствующие данные чека хранятся в защищенной базе данных блока управления, в которой содержится также большое количество счетчиков, обновляющихся при выдаче каждого чека. Простая процедура копирования позволяет аудитору получить полную копию базы данных блока управления, что дает возможность, пользуясь специальным программным обеспечением, легко производить необходимые проверки.

Бельгия намерена ввести подобную систему в 2013 году, но пока что это нововведение коснется только ресторанного бизнеса, точнее, только тех ресторанов, где не менее 10% годового торгового оборота приходится на продажу блюд, сервируемых не навынос.

Основное отличие бельгийской системы от шведской заключается в том, что в Бельгии контрольное устройство будет состоять из двух частей - контроллера данных о продажах, похожего на шведский блок управления, и смарт-карты НДС. Этот сертификат с предоставляемым налоговой администрацией закрытым ключом встраивается в смарт-карту НДС, которая будет персонализирована посредством подключения к ней номера НДС, генерации пары ключей и запоминания открытого ключа в базе данных налоговой администрации. Производители контроллеров этого ключа знать не будут.

Рис. 10. Бельгийская «сертифицированная система ЭКА»

Источник: информация предоставлена Бельгией.

Этот подход предполагает не только тщательную проработку технических аспектов, но и полную сертификацию каждого элемента этой «сертифицированной системы ЭКА»; таким образом, все заинтересованные стороны (производитель, продавец, пользователь, налоговая администрация) будут знать свои обязанности и полностью осознавать свою ответственность в этой связи.

Так же, как в Швеции и в Квебеке, в Бельгии выдача (фискального) чека стала обязательной, а информация о сертифицированных системах теперь будет публиковаться на сайте налоговой администрации.

В настоящее время различные варианты обеих этих концепций рассматриваются и в других странах ЕС; в том числе рассматривается возможность введения в управляющий модуль функции работы в режиме «псевдореального времени».

Снабжение данных чека электронной цифровой подписью, хранение необходимых данных в памяти контрольного устройства и безопасная передача данных в налоговые органы в режиме реального времени

В некоторых странах наиболее оптимальным и экономичным решением может стать снабжение данных чека цифровой подписью, хранение необходимых данных в памяти контрольного устройства и обеспечение налоговой администрации возможности удаленного доступа к данным (например, с помощью технологии GPRS). Удаленный доступ может осуществляться как автоматически (в этом случае в определенные фиксированные моменты времени на центральный сервер налоговой администрации производится отправка полной копии массива необходимых данных), так и «по запросу» (данные отправляются на сервер налоговой администрации, если необходимо провести аудиторскую проверку). Автоматическая загрузка данных может рассматриваться как официальная подача налоговой декларации.

Снабжение данных чека электронной цифровой подписью с помощью сертифицированного программного обеспечения для СЭКТ

Самый свежий пример использования сертифицированного программного обеспечения для СЭКТ для целей добавления к данным чеков электронной цифровой подписи представляет Португалия. При этом подходе контрольное устройство не требуется: в его основе лежит система шифрования данных, с помощью которого документ снабжается подписью с помощью асимметричной схемы и алгоритма RSA. Открытый ключ разработчик программного обеспечения передает в налоговую администрацию, а закрытый ключ известен только самому разработчику. Налоговая администрация проверяет соответствие программного обеспечения установленным требованиям, и если результат проверки оказывается положительным, то сертифицирует это ПО и соответствующим образом обнародует сведения об этой сертификации.

Начиная с 2008 года в Португалии действует требование об обязательном использовании в СЭКТ программного обеспечения, которые называется «Стандартный файл данных аудита для целей налогообложения» (SAF-T). Этот файл включает цифровую подпись следующих полей каждого документа: дата чека; дата входа в систему; номер чека; общая сумма продажи; подпись предыдущего документа той же серии.

В результате:

- по чеку легко определить, использовалось ли при его выдаче сертифицированное программное обеспечение;
- цифровая подпись на чеке должна соответствовать цифровой подписи на хэше чека в файле SAF-T (если аудитор запросит проверку такого соответствия); и
- используя открытый ключ, данные чека и цифровую подпись чека, анализатор SAF-T может определить:
  - производились ли с данными чека какие-либо манипуляции;
  - была ли электронная цифровая подпись сформирована с помощью правильного закрытого ключа; и
  - была ли нарушена последовательность данных чека.

Более подробную информацию и сведения об анализе цифровой подписи можно найти на сайте налоговой администрации Португалии (см. http://info.portaldasfinancas.gov.pt/pt/apoio_contribuinte/news_saf-t_pt.htm). Там также есть перевод закона о сертификации программного обеспечения на английский язык.

Примечания

1 Для этого был использован алгоритм криптографического хэширования SHA-1 с открытым исходным кодом.

2. В этом устройстве используется инфраструктура открытого ключа и алгоритм цифровой подписи Райвеста-Шамира-Адлемана (RSA).

3. См. *www.revenuquebec.ca/en/a-propos/evasion_fiscale/restauration/secteur.aspx*

4. Алгоритм, составленный на базе алгоритма цифровой подписи Райвеста-Шамира-Адлемана (RSA); инфраструктура открытого ключа; закрытый ключ в блоке управления.

ЭЛЕКТРОННОЕ УПРАЗДНЕНИЕ ПРОДАЖ: УГРОЗА НАЛОГОВЫМ ПОСТУПЛЕНИЯМ

Техника утаивания доходов от продаж с помощью компьютерных технологий способствует уклонению от налогов и во всемирных масштабах приводит к значительным потерям бюджетов различных стран от несобранных налогов. Применяемые в розничном секторе системы электронных кассовых терминалов (СЭКТ) – ключевой компонент комплексных систем продаж и бухгалтерского учета. На них полагаются как на действенный инструмент реализации функции бухгалтерского учета, необходимый для управления предприятием. Соответственно, ожидается, что они будут содержать исходные данные, которые могут проверять налоговые инспекторы. В реальности же подобные системы не только позволяют осуществлять так называемый «скимминг», т.е. хищение поступающих наличных средств с использованием компьютерных технологий, подобно тому, как это делается вручную при краже средств из кассовых аппаратов предшествующих поколений), но и функционируя на основе ПО, призванного обеспечить утаивание выручки от продаж, они способствуют появлению куда более изощренных видов мошенничества, поскольку позволяют перепрограммировать вносимые записи для того, чтобы последние не позволяли замечать результаты скимминга.

В настоящем отчете описываются функции систем СЭКТ и конкретные области, в которых сконцентрированы соответствующие риски. В нем детально представлены выявленные экспертами виды и способы утаивания доходов от продаж, в частности, мошенническое ПО и программы на внешних носителях (т.н. Phantomware, Zappers), а также продемонстрировано, как налоговые аудиторы и следователи могут выявить использование подобных методов. В документе также отмечается постоянное совершенствование инструментов утаивания доходов с помощью компьютерных технологий и необходимость быть готовым незамедлительно реагировать на изменения в этой сфере. В особенности, доклад содержит ряд рекомендаций, нацеленных на оказание помощи странам в решении этой важной области риска.

Оглавление: