

## РЕГЛАМЕНТ

### «Защищенный электронный документооборот между налогоплательщиками и налоговыми органами по каналам связи»

#### 1. ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1. Настоящий регламент определяет порядок эксплуатации системы защищенного электронного документооборота «Контур-Экстерн», частью которой является «Налоговая отчетность через Интернет», участвующими в эксплуатации сторонами.
- 1.2. Настоящий регламент основывается на положениях «Порядка представления налоговой декларации в электронном виде по телекоммуникационным каналам связи», утвержденного Приказом МНС России от 02.04.2002 года №БГ-3-32/169 (в дальнейшем — Порядок), Методических рекомендациях по применению Порядка, утвержденных приказом МНС России от 10.12.2002г. №БГ-3-32/705, и применяет положения Порядка к эксплуатации конкретной системы для представления налоговой отчетности по телекоммуникационным каналам связи.
- 1.3. Для целей правильного понимания текста регламента термины, применяемые в нем, используются в следующем назначении:
  - 1.3.1. «УПРАВЛЕНИЕ» — Управление ФНС России по Тюменской области.
  - 1.3.2. «НАЛОГОПЛАТЕЛЬЩИК» — индивидуальный предприниматель без образования юридического лица или юридическое лицо, представляющие текущую отчетность по установленным законодательством формам в ИФНС по данному регламенту работы.
  - 1.3.3. «ИФНС» — Инспекция ФНС России по г. Тюмени или Межрайонная инспекция ФНС России по Тюменской области, в которой зарегистрирован НАЛОГОПЛАТЕЛЬЩИК.
  - 1.3.4. «ОПЕРАТОР» - специализированный оператор
  - 1.3.5. «ЭЦП» - Электронная цифровая подпись — цифровой код, соответствующий требованиям ГОСТ 34.10-01 «Электронная подпись» и используемый НАЛОГОПЛАТЕЛЬЩИКОМ в системе в качестве средства аутентификации при оформлении отчетов для передачи их через Интернет.
  - 1.3.6. «Интернет» — открытая телекоммуникационная сеть, по которой производится обмен информацией между НАЛОГОПЛАТЕЛЬЩИКОМ и ИФНС посредством системы «Контур-Экстерн».
  - 1.3.7. «СИСТЕМА» - система «Контур-Экстерн» — программно-аппаратный комплекс, позволяющий НАЛОГОПЛАТЕЛЬЩИКУ формировать, проверять и передавать в ИФНС налоговую отчетность по установленным законодательством формам.
  - 1.3.8. «СЕРВЕР» — компьютер и развернутый на нем Интернет-узел, находящийся у ОПЕРАТОРА, на котором открыто программное обеспечение СИСТЕМЫ для доступа зарегистрированных пользователей, отвечающее за формирование и проверку сведений, а также передачу сформированных отчетов в ИФНС.
  - 1.3.9. «Сертификат ключа ЭЦП и шифрования» — электронный документ, на основании которого генерируется ключ электронно-цифровой подписи и шифрования в соответствии с Федеральным законом №1-ФЗ 2002 г. «Об электронной цифровой подписи».
  - 1.3.10. «Центр сертификации» — компьютер, находящийся у ОПЕРАТОРА, на котором задействована система выдачи и регистрации сертификатов ключей электронной подписи и шифрования.

## **2. РАБОТА В СИСТЕМЕ «НАЛОГОВАЯ ОТЧЕТНОСТЬ ЧЕРЕЗ ИНТЕРНЕТ»**

- 2.1. УПРАВЛЕНИЕ совместно с ОПЕРАТОРОМ предоставляют НАЛОГОПЛАТЕЛЬЩИКУ возможность производить подготовку, проверку и передачу зашифрованной и заверенной электронной цифровой подписью налоговой отчетности в ИФНС с использованием СИСТЕМЫ, при условии соблюдения положений Порядка и настоящего Регламента.
- 2.2. НАЛОГОПЛАТЕЛЬЩИК, передавший налоговую отчетность в ИФНС с использованием СИСТЕМЫ, и получивший электронную цифровую подпись ИФНС на сдаваемом файле отчетности, в соответствии с Порядком, **считается исполнившим обязанность** по представлению соответствующей формы налоговой отчетности и не предоставляет ее в ИФНС в какой-либо иной форме (на бумажном или магнитном носителе).
- 2.3. Документальной базой, подтверждающей факт сдачи отчета, является пакет документов, состоящий из файлов отчетов, заверенных ЭЦП НАЛОГОПЛАТЕЛЬЩИКА и ИФНС (в терминологии Порядка этот файл называется **квитанцией о приеме сведений в ИФНС**), а также **квитанции о времени сдачи отчета**, заверенной ЭЦП ОПЕРАТОРА.
- 2.4. **Квитанция о времени сдачи отчета** формируется на сервере ОПЕРАТОРА в момент заверения НАЛОГОПЛАТЕЛЬЩИКОМ сдаваемого отчета. **Квитанция о приеме сведений в ИФНС** формируется ИФНС по факту приема соответствующего отчета НАЛОГОПЛАТЕЛЬЩИКА и пересылается НАЛОГОПЛАТЕЛЬЩИКУ в **течение одного рабочего дня**.
- 2.5. Для криптографической защиты сведений, передаваемых через Интернет при работе в Системе, стороны используют сертифицированное ФСБ средство криптографической защиты информации Крипто-Про CSP
- 2.6. В качестве средства заверения документов, как представляемых НАЛОГОПЛАТЕЛЬЩИКОМ в ИФНС, так и передаваемых ИФНС НАЛОГОПЛАТЕЛЬЩИКУ, используется электронная цифровая подпись, реализованная на базе СИСТЕМЫ с использованием сертифицированного ФСБ средства криптографической защиты информации Крипто-Про CSP.
- 2.7. **В случае выхода из строя СИСТЕМЫ**, выхода из строя программно-аппаратного обеспечения рабочего места НАЛОГОПЛАТЕЛЬЩИКА или наступления других обстоятельств, препятствующих использованию Системы, **сдача НАЛОГОПЛАТЕЛЬЩИКОМ налоговой отчетности производится другими способами** (по почте, на магнитных носителях, на бумажных носителях), допустимыми действующим законодательством. Сроки сдачи отчетности при этом не переносятся.

## **3. ПРАВА И ОБЯЗАННОСТИ УПРАВЛЕНИЯ**

- 3.1. УПРАВЛЕНИЕ обязуется:
  - 3.1.2 Обеспечить круглосуточную работу транзитного почтового сервера и проху-серверов.
  - 3.1.3 Осуществлять общий надзор и контроль за ходом информационного обмена между НАЛОГОПЛАТЕЛЬЩИКОМ и ИФНС посредством СИСТЕМЫ.
  - 3.1.4 Назначить сотрудников, ответственных за исполнение положений настоящего регламента со стороны УПРАВЛЕНИЯ.
- 3.2. УПРАВЛЕНИЕ имеет право:

- 3.2.1. Пересматривать перечень принимаемых через Интернет форм.
- 3.2.2. Пересматривать требования к логическо - арифметическому контролю информации в соответствии с изменениями в нормативных документах.
- 3.2.3. Запрашивать у ОПЕРАТОРА список отозванных и просроченных сертификатов, ранее выданных центром сертификации.

#### **4. ПРАВА И ОБЯЗАННОСТИ ИФНС**

4.1. ИФНС обязуется:

- 4.1.1. Принимать к рассмотрению налоговую отчетность, запросы по информированию о действующем налоговом законодательстве, запросы на предоставление информационной выписки об исполнении налоговых обязательств перед бюджетом, полученные от НАЛОГОПЛАТЕЛЬЩИКА через Интернет, без бумажных копий отчетных документов и копий документов на магнитных носителях при условии:
    - прохождения контроля правильности ЭЦП;
    - выполнения контроля правильности и целостности сертификата ключа ЭЦП НАЛОГОПЛАТЕЛЬЩИКА.
  - 4.1.2. Подписывать в течение **одного рабочего дня** ЭЦП ИФНС файлы отчетности, запросы на предоставление информационной выписки, запросы по информированию о действующем налоговом законодательстве и возвращать их НАЛОГОПЛАТЕЛЬЩИКУ посредством Системы.
  - 4.1.3. Проверять файлы отчетности на соответствие утвержденному формату и в течение **одного рабочего дня** направлять в адрес НАЛОГОПЛАТЕЛЬЩИКА протокол входного контроля, подписанный ЭЦП ИФНС.
  - 4.1.4. В сроки, не превышающие действующего законодательства по делопроизводству, направлять НАЛОГОПЛАТЕЛЬЩИКУ ответ на запрос по информированию о действующем налоговом законодательстве или информационную выписку об исполнении налоговых обязательств перед бюджетом, подписанные ЭЦП ИФНС.
  - 4.1.5. Немедленно блокировать прием данных от НАЛОГОПЛАТЕЛЬЩИКА, если стало известно о компрометации сертификата ключа ЭЦП и шифрования НАЛОГОПЛАТЕЛЬЩИКА или его парольной информации.
  - 4.1.6. Обеспечить хранение файлов, подписанных ЭЦП НАЛОГОПЛАТЕЛЬЩИКА и ИФНС, и образующих документальную базу для разрешения конфликтных ситуаций, в процессе установленного законодательством времени, и представлять эти файлы в судебные органы в случае необходимости проведения разбирательства.
- 4.2. ИФНС имеет право:
- 4.2.1. Отказать НАЛОГОПЛАТЕЛЬЩИКУ в принятии налоговых деклараций и бухгалтерской отчетности, в случае если они заполнены не по установленной законодательством форме.

#### **5. ПРАВА И ОБЯЗАННОСТИ НАЛОГОПЛАТЕЛЬЩИКА**

5.1. НАЛОГОПЛАТЕЛЬЩИК обязан:

- 5.1.1. Назначить ответственных лиц для работы в СИСТЕМЕ.
- 5.1.2. Не знакомить с системой формирования ЭЦП, сертификатом ключа ЭЦП, парольной информацией для входа в Систему сотрудников своего предприятия, кроме лиц, назначенных в соответствии с п.5.1.1.

- 5.1.3. Поставить в известность ОПЕРАТОРА и согласовать с ним порядок возобновления работы в СИСТЕМЕ в случае компрометации сертификата ключа ЭЦП НАЛОГОПЛАТЕЛЬЩИКА или его парольной информации.
- 5.1.4. Обеспечить хранение файлов, подписанных ЭЦП НАЛОГОПЛАТЕЛЬЩИКА и ИФНС, и образующих документальную базу для разрешения конфликтных ситуаций, в течение установленного законодательством времени, и представлять эти файлы в судебные органы в случае необходимости проведения разбирательства.
- 5.1.5. Представлять отчетность по форматам, утвержденным в соответствии с формами налоговой и бухгалтерской отчетности, действовавшими в отчетном периоде, за который предоставляется отчетность.
- 5.2. НАЛОГОПЛАТЕЛЬЩИК имеет право:
  - 5.2.1. Направить письмо установленного образца (см. приложение 1) ОПЕРАТОРУ с просьбой о присоединении НАЛОГОПЛАТЕЛЬЩИКА к СИСТЕМЕ с соблюдением настоящего регламента. Письмо заверяется подписью руководителя организации-НАЛОГОПЛАТЕЛЬЩИКА
  - 5.2.2. Изготавливать и хранить бумажные копии сформированных форм отчетности с указанием на первом листе бумажной копии, что оригинал направлен в электронном виде, а также с указанием реквизитов электронного документа-оригинала, заверенных подписью уполномоченного лица и печатью.
  - 5.2.3. В любой момент отказаться от использования СИСТЕМЫ и вернуться к сдаче отчетности другими способами, установленными действующим законодательством.
  - 5.2.4. Получать консультации по вопросам эксплуатации абонентского рабочего места СИСТЕМЫ у ОПЕРАТОРА.
  - 5.2.5. Обратиться к ОПЕРАТОРУ или в ИФНС с заявлением о непредставлении в течение установленного Порядком срока квитанции о приеме отчетности или протокола входного контроля.
  - 5.2.6. Направлять в ИФНС посредством СИСТЕМЫ запросы по информированию о действующем налоговом законодательстве и запросы на получение информационной выписки об исполнении налоговых обязательств перед бюджетом.
- 5.3. В своей деятельности, в дополнение к настоящему регламенту, ответственные лица НАЛОГОПЛАТЕЛЬЩИКА, руководствуются также положениями Инструкции (см. приложение 2).

## **6. ПРАВА И ОБЯЗАННОСТИ ОПЕРАТОРА**

### 6.1 ОПЕРАТОР обязуется:

- 6.1.1. Обеспечивать бесперебойную работу серверного модуля СИСТЕМЫ, его техническое обслуживание и сопровождение.
- 6.1.2. Своевременно вносить изменения в математическое обеспечение серверного модуля СИСТЕМЫ по мере появления изменений в действующем законодательстве.
- 6.1.3. Обеспечивать неразглашение ключевой информации.
- 6.1.4. Регистрировать в журнале факты выдачи средств криптографической защиты информации и сертификатов абонентам СИСТЕМЫ.

- 6.1.5. Поддерживать функционирование «горячей» консультационной линии для абонентов СИСТЕМЫ.
- 6.1.6. Обеспечить НАЛОГОПЛАТЕЛЬЩИКА Инструкцией по обеспечению защиты конфиденциальной информации для пользователей системы «Контур-Экстерн» (см. приложение 2) в момент заключения договора о подключении к СИСТЕМЕ.
- 6.1.7. Своевременно проходить лицензирование на право осуществлять деятельность по тем видам, которые необходимы для выполнения функций ОПЕРАТОРА, по мере истечения полученных ранее лицензий.
- 6.1.8. Не реже одного раза в квартал проводить техническую учебу с сотрудниками ИФНС по работе в СИСТЕМЕ.

6.2. ОПЕРАТОР имеет право:

- 6.2.1. Требовать от НАЛОГОПЛАТЕЛЬЩИКА проведения штатной замены сертификата через год после его выдачи.
  - 6.2.2. Требовать от представителя НАЛОГОПЛАТЕЛЬЩИКА документов, удостоверяющих его право действовать от имени организации, которую он представляет перед выдачей ему СКЗИ и сертификата.
- 6.3. В своей деятельности, в дополнение к настоящему регламенту, ответственные лица СПЕЦИАЛИЗИРОВАННОГО ОПЕРАТОРА СВЯЗИ, руководствуются также положениями должностных инструкций администратора информационной безопасности и сотрудника по выдаче сертификатов.

## **7. ПОРЯДОК ПОДКЛЮЧЕНИЯ К СИСТЕМЕ НОВОГО АБОНЕНТА**

- 7.1. Для начала работы в системе НАЛОГОПЛАТЕЛЬЩИК направляет ОПЕРАТОРУ письмо установленного образца (см. приложение 1). ОПЕРАТОР на основании письма заключает с НАЛОГОПЛАТЕЛЬЩИКОМ договор о подключении к СИСТЕМЕ, регистрирует НАЛОГОПЛАТЕЛЬЩИКА и ставит в известность ИФНС по местонахождению НАЛОГОПЛАТЕЛЬЩИКА на налоговом учете о его подключении к СИСТЕМЕ.
- 7.2. В рамках абонентского договора НАЛОГОПЛАТЕЛЬЩИК (или его представитель) приобретает у ОПЕРАТОРА комплект установки СКЗИ «Крипто-Про CSP». ОПЕРАТОР формирует и передает НАЛОГОПЛАТЕЛЬЩИКУ на магнитном носителе сертификат ключа ЭЦП и шифрования, пригодный для работы в системе по зашифрованному каналу и формирования электронной цифровой подписи. ОПЕРАТОР также передает НАЛОГОПЛАТЕЛЬЩИКУ комплект документации к СКЗИ «Крипто-Про CSP», инструкцию по работе в СИСТЕМЕ, инструкцию по защите информации.
- 7.3. После оплаты всех счетов по абонентскому договору НАЛОГОПЛАТЕЛЬЩИК самостоятельно или при содействии ОПЕРАТОРА устанавливает на свое рабочее место необходимое программное обеспечение для работы в СИСТЕМЕ, производит подключение к СЕРВЕРУ, заполняет необходимые формы и начинает сдачу отчетов через ИНТЕРНЕТ.

## **8. ПОРЯДОК ЗАМЕНЫ ПАРОЛЬНО-КЛЮЧЕВОЙ ИНФОРМАЦИИ**

- 8.1. Сертификат ключа ЭЦП и шифрования НАЛОГОПЛАТЕЛЬЩИКА, равно как и пароль доступа к базе данных НАЛОГОПЛАТЕЛЬЩИКА на СЕРВЕРЕ ОПЕРАТОРА могут быть изменены, как по заявке НАЛОГОПЛАТЕЛЬЩИКА, так и по инициативе ОПЕРАТОРА.

- 8.2. Заявка об изменении сертификата ключа ЭЦП и шифрования со стороны НАЛОГОПЛАТЕЛЬЩИКА подписывается руководителем предприятия.
- 8.3. Сообщение об изменении сертификата ключа ЭЦП и шифрования должно быть передано другой стороне не менее чем за семь рабочих дней до окончания работы в СИСТЕМЕ с применением старого сертификата.
- 8.4. Штатная замена сертификата ключа ЭЦП и шифрования, равно как и штатная замена пароля доступа к базе данных НАЛОГОПЛАТЕЛЬЩИКА производятся не реже одного раза в год.
- 8.5. Штатная замена сертификата ключа ЭЦП и шифрования НАЛОГОПЛАТЕЛЬЩИКА заключается в следующей процедуре:
- новый сертификат ключа ЭЦП и шифрования НАЛОГОПЛАТЕЛЬЩИКА генерируется центром сертификации ОПЕРАТОРА, подписывается ЭЦП ОПЕРАТОРА и шифруется с помощью старого сертификата;
  - зашифрованный с помощью старого сертификата новый сертификат передается НАЛОГОПЛАТЕЛЬЩИКУ по электронной почте или через СЕРВЕР;
  - НАЛОГОПЛАТЕЛЬЩИК расшифровывает новый сертификат и начинает использовать его для формирования ЭЦП и шифрования данных при работе в СИСТЕМЕ. Старый сертификат при этом объявляется недействительным, что регистрируется в списке отозванных сертификатов;
  - работа НАЛОГОПЛАТЕЛЬЩИКА в СИСТЕМЕ при штатной замене сертификата не приостанавливается.
- 8.6. Штатная замена пароля доступа к СИСТЕМЕ производится письмом в адрес ОПЕРАТОРА.
- 8.7. При наличии данных, позволяющих предположить, что сертификат ключа ЭЦП и шифрования или пароль НАЛОГОПЛАТЕЛЬЩИКА стал известен третьим лицам, НАЛОГОПЛАТЕЛЬЩИК немедленно информирует об этом ОПЕРАТОРА. В этом случае работа в СИСТЕМЕ с применением старого сертификата или пароля приостанавливается с момента поступления сообщения НАЛОГОПЛАТЕЛЬЩИКА.
- 8.8. Для внештатной замены сертификата, вызванной причинами, указанными в предыдущем пункте, уполномоченный представитель НАЛОГОПЛАТЕЛЬЩИКА лично получает новый сертификат у ОПЕРАТОРА.

## **9. ПРОЧЕЕ**

- 9.1. Парольная информация и сертификат ключа ЭЦП и шифрования НАЛОГОПЛАТЕЛЬЩИКА не могут быть переданы третьим лицам.
- 9.2. Для определения своевременности представления отчета используются показания системного таймера на СЕРВЕРЕ ОПЕРАТОРА (временная отметка, устанавливаемая СЕРВЕРОМ ОПЕРАТОРА в подтверждении, отсылаемом НАЛОГОПЛАТЕЛЬЩИКУ, при приеме отчета.)
- 9.3. В случае нарушения НАЛОГОПЛАТЕЛЬЩИКОМ сроков сдачи налоговой отчетности, ИФНС применяет к нему штрафные санкции в установленном законодательством порядке.

СПЕЦИАЛИЗИРОВАННОМУ ОПЕРАТОРУ СВЯЗИ

Прошу зарегистрировать в системе «Контур-Экстерн» учетную запись в соответствии со следующей таблицей:

№	Сведения об абоненте	Сведения об уполномоченном лице
1	Полное наименование: - _____ _____ _____ _____ ИНН: _____ КПП: _____ Код ИМНС по местонахождению на учете: _____ Тел./факс: _____	ФИО: _____ _____ _____ Должность: _____ ИНН: _____ Паспорт серия _____ номер _____ выдан _____ e-mail: _____

\* *Необходимые услуги отметить галочкой*

№	Наименование услуги	Кол-во	Отметка
1	Сдача налоговой и бухгалтерской отчетности ежемесячно		
2	Сдача налоговой и бухгалтерской отчетности ежеквартально		
3	Бюджетная организация		
4	Малый бизнес (ПБЮЛ)		
	Выписка с лицевого счета, неформализованный документооборот		
5	Роуминг		
6	Выезд специалиста, установка и настройка программного обеспечения		

1. Прошу сгенерировать ключи электронной подписи и шифрования и выпустить сертификаты открытых ключей электронной подписи сроком действия на один год на указанное выше уполномоченное лицо.
2. Правильность сведений, указанных в регистрационной карте, гарантирую.
3. Присоединяюсь к Регламенту «Защищенный электронный документооборот между налогоплательщиками и налоговыми органами по каналам связи» (далее – *Регламент*) и становлюсь Стороной Регламента с момента передачи Специализированному Оператору Связи настоящего заявления. С положениями Регламента, характеристиками и особенностями оказываемых по Регламенту услуг ознакомлен и согласен

АБОНЕНТ: \_\_\_\_\_ / \_\_\_\_\_ /

М.П.

## **Инструкция по обеспечению защиты конфиденциальной информации для пользователей системы «Контур-Экстерн» (налоговая отчетность через Интернет)**

Общие положения.

Поскольку в системе «Контур-Экстерн» для передачи налоговой и бухгалтерской отчетности используется открытая телекоммуникационная сеть Интернет, к *рабочим станциям*, подключаемым к системе, к самой системе и к безопасности передаваемых данных предъявляются следующие требования:

1.1. На *рабочих станциях*, которые подключены к Интернет и с которых предполагается передавать налоговую и бухгалтерскую отчетность в **обязательном** порядке должно быть установлено *антивирусное программное обеспечение* с актуальными антивирусными базами. Такому требованию удовлетворяют программы типа «Panda», «Антивирус Касперского», «Доктор WEB» и другие коммерческие продукты в которых заложена возможность обновления антивирусных баз через Интернет.

1.2. Система, обеспечивающая передачу налоговой отчетности через Интернет, должна соответствовать комплексным требованиям, направленным на безопасную передачу конфиденциальной информации от налогоплательщика в налоговый орган и обратно. Применяемая система «Контур-Экстерн» имеет Сертификат соответствия № РОСС RU.ME20.H01064, подтверждающий ее безопасность и соответствие всем предъявляемым требованиям.

1.3. *Информация*, циркулирующая в системе на всех участках передачи шифруется. Соединение компьютера налогоплательщика с сервером оператора происходит по защищенному специальным алгоритмом каналу связи, информация перед передачей на сервер шифруется и подписывается пользователем. Прочитать ее сможет лишь получатель, у которого есть открытый ключ налогоплательщика, то есть налоговый орган, которому эта информация адресована. Шифрование данных производится по ГОСТ 28147-89, электронная цифровая подпись отчетов осуществляется по ГОСТ 34.10-94 с помощью *сертифицированного ФСБ СКЗИ Крипто-Про CSP*.

1.4. Кроме того, для правильного взаимодействия субъектов внутри системы, (налогового органа, специализированного оператора, налогоплательщика), разработан Регламент электронного документооборота, который организационно определяет ответственность всех участвующих в электронном документообороте сторон.

Регламент, можно загрузить с сервера <http://s-crypto.ru> или получить в офисах ООО «Сибтел-Крипто» (г. Тюмень, ул. Энергетиков 62а, и ул. Широтная-29, корпус 2/2, оф.204). Он содержит положения о взаимном признании участниками электронной цифровой подписи (ЭЦП), а также других аспектов электронного документооборота.

Уровень защиты информации от несанкционированного доступа, достигаемый при следовании Регламенту, *существенно выше*, чем при переносе нешифрованного текстового файла на дискете (вероятность потери, кражи дискеты или бумаги с



отчетом неизмеримо больше, чем вероятность подбора злоумышленником одного ключа шифрования данных из их огромного количества).

## 2. Порядок подключения рабочей станции пользователя к системе «Контур-Экстерн».

При подключении рабочей станции налогоплательщика к системе необходимо:

- 2.1. Проверить рабочую станцию на отсутствие вирусов, при этом нужно удостовериться, что антивирусные базы актуальны, если антивирусные базы старые – сначала обновить их и после произвести проверку.
- 2.2. Если антивирусная программа на рабочей станции отсутствует, необходимо установить программу Panda Titanium \*, входящую в состав пакета пользователя, зарегистрировать ее, обновить антивирусные базы и проверить компьютер.
- 2.3. Установить СКЗИ Крипто-Про CSP (на рабочем месте, с которого будет производиться передача отчетности). Произвести настройку согласно прилагаемых инструкций.

## 3. Порядок обеспечения защиты информации налогоплательщика.

Для обеспечения защиты данных от несанкционированного доступа, на предприятии, подключенном к системе «Контур-Экстерн», должны соблюдаться следующие меры безопасности:

- 3.1. Закрытый ключ пользователя (на дискете или ruToken'е) необходимо хранить в сейфе или другом надежном хранилище.
- 3.2. Пароль на вход в систему должен быть известен ограниченному количеству людей, хранение пароля в открытом для доступа виде не рекомендуется.
- 3.4. Не допускается хранение пароля и закрытого ключа в одном месте.
- 3.5. Носитель (дискета или ruToken) с закрытым ключом пользователя должна извлекаться из сейфа только на время работы в системе.
- 3.6. Доступ к паролю и закрытому ключу должно иметь ограниченное количество постоянных сотрудников, обученных работе в системе. Для них необходимо иметь должностную инструкцию и вести журнал учета выдачи носителя (дискеты или ruToken'а) с секретным ключом.
- 3.7. При утере или хищении пароля или носителя (дискеты или ruToken'а) с закрытым ключом необходимо *немедленно* известить ООО «Сибтел-Крипто», чтобы в кратчайший срок заблокировать возможность доступа к системе.
- 3.8. Штатная смена сертификата и пароля (без личного визита, по каналу связи, защищенному старым сертификатом и паролем) должна производиться не реже одного раза в год.

\* В комплекте программного обеспечения, передаваемого пользователю на компакт-диске, находится коммерческий пакет Panda Titanium. Электронный ключ, после активации которого обеспечивается *трех-, шестимесячное или годовое* обновление антивирусных баз можно приобрести в нашей компании.