

УТВЕРЖДЕНО
Решением Правления
ОАО «Витабанк»
протокол № 31
от «26» ноября 2003
Председатель Правления



**ПЕРЕЧЕНЬ МЕР,
направленных на предотвращение неправомерного
использования служебной информации при осуществлении
профессиональной деятельности на рынке ценных бумаг,
установленных в ОАО «Витабанк»**

Санкт-Петербург
2003г.

1. Общие положения

1.1. Настоящее Положение разработано в соответствии с требованиями Федерального закона РФ № 39-ФЗ от 22.04.1996 г. «О рынке ценных бумаг» (в ред. Федеральных законов от 26.11.1998 г. № 182-ФЗ, от 08.07.1999 г. № 139-ФЗ, от 07.08.2001 г. № 121-ФЗ, от 28.12.2002 г. № 185-ФЗ), Постановлений ФКЦБ России № 03-34/пс от 13.08.2003 г. «О положении о внутреннем контроле профессионального участника рынка ценных бумаг», № 10 от 15.08.2000г. «Об утверждении порядка лицензирования видов профессиональной деятельности на рынке ценных бумаг Российской Федерации» (в ред. Постановлений ФКЦБ РФ от 21.03.2001 г. № 4, от 18.07.2001 г. № 14, от 05.02.2003 г. № 03-5/пс, от 12.02.2003 г. № 03-11/пс, от 01.04.2003 г. № 03-15/пс).

1.2. Меры, направленные на предотвращение неправомерного использования служебной информации при осуществлении профессиональной деятельности на рынке ценных бумаг, а также при оказании услуг финансового консультанта на рынке ценных бумаг, установленные в ОАО «Витабанк» (далее - Банк), включают в себя:

- перечень ограничений по доступу к служебной информации;
- требования по разграничению прав доступа и обеспечению конфиденциальности информации;
- меры защиты служебной документации и информации от неправомерного использования;
- меры защиты рабочих мест и мест хранения документации и информации от несанкционированного доступа;
- информирование Регистрирующего органа о выявленных Банком нарушениях, допущенных Клиентом, в процессе осуществления финансового мониторинга;
- требования к работникам Банка;
- систему мер ответственности за несанкционированное предоставление работниками подразделений Банка служебной информации работникам других подразделений Банка и посторонним лицам.

1.3. В настоящем документе используются следующие термины и определения:

Банк – ОАО «Витабанк», осуществляющее профессиональную деятельность на рынке ценных бумаг.

Клиент – юридическое или физическое лицо, которому Банк оказывает услуги, связанные с его профессиональной деятельностью на рынке ценных бумаг, а также эмитент, которому Банк оказывает услуги финансового консультанта на рынке ценных бумаг.

Регистрирующий орган – государственный орган исполнительной власти РФ, к полномочиям которого отнесена государственная регистрация выпусков ценных бумаг Клиента.

Финансовые рынки – рынки ценных бумаг и срочных сделок.

Финансовый инструмент – ценные бумаги и срочные контракты, базовым активом которых являются ценные бумаги.

Финансовый консультант на рынке ценных бумаг - юридическое лицо, имеющее лицензию на осуществление брокерской и/или дилерской деятельности на рынке ценных бумаг, оказывающее эмитенту услуги по подготовке проспекта ценных бумаг.

Служебная информация – любая информация, имеющаяся в распоряжении Банка, не являющаяся общедоступной и содержащая сведения об эмитенте и выпущенных им эмиссионных ценных бумагах, об операциях (сделках) Банка и ее клиентов на рынке ценных бумаг, которая ставит работников Банка, обладающих такой информацией в силу своего

служебного положения или трудовых обязанностей, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг.

Раскрытие информации - обеспечение ее доступности всем заинтересованным в этом лицам независимо от целей получения данной информации по процедуре, гарантирующей ее нахождение и получение.

Лента новостей - информационный ресурс, обновляемый в режиме реального времени и предоставляемый информационным агентством, уполномоченным Федеральной комиссией по рынку ценных бумаг РФ на публичное предоставление информации, раскрываемой на рынке ценных бумаг.

Меры – меры, препятствующие несанкционированному доступу к служебной информации и ее неправомерному использованию, в том числе при совмещении различных видов профессиональной деятельности на рынке ценных бумаг.

1.4. Целью Мер является:

- исключение возможности несанкционированного доступа к служебной информации и ее использования работниками Банка и третьими лицами в собственных интересах в ущерб интересам клиентов Банка и интересам самого Банка;
- повышение уровня доверия к Банку со стороны клиентов.

1.5. Настоящие меры разрабатываются Службой внутреннего контроля и согласовываются со Службой защиты информации и главным юристом.

1.6. Контролер Банка осуществляет текущий контроль за соблюдением Мер сотрудниками Банка, а также проводит проверку эффективности защиты служебной информации с помощью указанных Мер.

2. Перечень Мер

2.1. Ограничение доступа посторонних лиц в помещения структурных подразделений Банка, предназначенные для осуществления профессиональной деятельности на рынке ценных бумаг или эксплуатации информационно-технологических систем, предусматривает следующие мероприятия:

2.1.1. Размещение помещений структурных подразделений Банка и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая работников других подразделений. Сотрудники подразделений Банка, осуществляющие различные виды профессиональной деятельности размещаются в разных помещениях по функциональному признаку. После окончания рабочего дня дверь каждого помещения закрывается на ключ. Контейнер с ключом в опечатанном виде сдается под роспись сотруднику поста охраны Банка. Каждое помещение Банка оборудовано охранно-пожарной и тревожной сигнализацией (ОПТС). При сдаче ключей сотрудник охраны Банка ставит помещение на ОПТС. Все помещения имеют разные замки. Дубликаты ключей от помещений Банка хранятся в хозяйственном отделе Банка в запираемом и опечатываемом шкафу, ключи от которого находятся у начальника хозяйственного отдела Банка. В случае ухода из помещения в течение рабочего дня всех работников, дверь помещения закрывается на ключ. Работники каждого подразделения, расположенного в отдельном помещении, не должны покидать своего рабочего места, оставляя в нем без присмотра посторонних лиц, включая работников других подразделений

Банка. Контроль за соблюдением установленного порядка возложен на старшего по должности в каждом помещении согласно приказу по Банку.

2.1.2. Проведение переговоров с клиентами Банка осуществляется в специально оборудованном помещении.

2.1.3. Обеспечение контроля за входом (выходом) в Банк. С этой целью в Банке в холле первого этажа располагается пост охраны из сотрудников вневедомственной охраны, введен пропускной режим входа (выхода) в Банк. Помещения, в которых эксплуатируется информационно-технологическая система, имеют двери с кодовыми замками. Введено ограничение доступа посторонних лиц в помещения во внерабочее время. Доступ сотрудников в помещения Банка по выходным и праздничным дням, а также в рабочие дни после 20 часов, осуществляется только по предварительному распоряжению Председателя Правления.

2.2. Разграничение прав доступа при вводе и обработке данных с целью защиты от несанкционированных действий работников разных подразделений Банка, а также ограничение доступа работников Банка к служебной информации, предусматривающее следующие мероприятия:

2.2.1. Четкое разграничение прав и обязанностей работников Банка. С этой целью для каждого сотрудника Банка составлена должностная инструкция, в которой определены его функции, права и обязанности.

2.2.2. Доступ к данным только ограниченного круга лиц, являющихся непосредственными исполнителями, обеспечивающими осуществление конкретного вида профессиональной деятельности Банка. Доступ работников Банка только к сведениям, необходимым им для выполнения своих прямых служебных обязанностей в пределах предоставленных полномочий. В Банке издается приказ, определяющий круг лиц, имеющих доступ к служебной информации. Доступ сотрудников к информационным ресурсам осуществляется на основе уникального имени и пароля. Сложность паролей обеспечивает минимальную вероятность их подбора. При генерации пароля следует избегать использования имен, дат рождения, других простых последовательностей символов, причем новый пароль должен быть отличен от уже использовавшегося. Предоставление доступа сотрудникам Банка к информационным ресурсам Банка производится по служебной записке начальника структурного подразделения Банка на имя Председателя Правления и заявкам, согласованным со службой защиты информации. В заявке указывается необходимые права доступа к сети, а также другим информационным ресурсам. При предоставлении доступа сотрудникам Банка к информационным ресурсам ему присваивается имя, уникальный номер и пароль, являющиеся индивидуальными для каждого конкретного сотрудника. Пароли выбираются каждым пользователем самостоятельно по рекомендации лиц, осуществляющих функции администраторов доступа и обновляются не реже одного раза каждые 6 (Шесть) месяцев.

Удаление и модификация прав доступа пользователей к информационным ресурсам Банка производится на основании мотивированной служебной записки на имя Председателя Правления, согласованной со службой защиты информации. Смена пароля пользователя производится также по мотивированной просьбе пользователя или в других случаях, когда возникает предположение о компрометации пароля.

Запрещается хранение паролей в явном или зашифрованном виде на бумаге или на машинных носителях. Запрещается предоставление какого-либо пароля в распоряжение

сотрудников, не имеющих доступа к защищаемой информации, а также лиц, не являющихся сотрудниками Банка, равно как и использование паролей, известных уволенным сотрудникам.

В случае увольнения или перемещения сотрудника, удаление его из числа пользователей соответствующими информационными ресурсами Банка производится не позднее суток с момента подписания обходного листа.

Контроль за правильностью использования и своевременностью смены парольной защиты возлагается на лицо, осуществляющее функции администратора информационной безопасности.

2.2.3. Наличие системы разграничения доступа к разным уровням баз данных и операционной среды используемого программного обеспечения, состоящей из системы разграничения доступа на уровне локальной сети. Для каждого сотрудника Банка в информационной базе определяется уровень полномочий. При описании доступа к пунктам меню система позволяет задавать маску отдела, минимальные и максимальные полномочия. Для сотрудников, отделы которых не указаны, данный пункт меню на экране не отображается, сотрудники отдела с полномочиями ниже минимальных также не будут видеть пункт меню на экране. Производится поддержка системы безопасности, предусматривающая постоянное отслеживание технологии работы подразделений Банка, изменение должностных обязанностей работников, а также корректировка системы безопасности при каждом изменении, происходящем в подразделениях Банка.

2.2.4. Доступ к данным только с определенных автоматизированных рабочих мест. Практические рекомендации: наличие персонального компьютера, доступ к которому возможен только через имя пользователя и личный пароль.

2.2.5. Ведение автоматизированного журнала регистрации пользователей информационной системы и регистрации попыток несанкционированного доступа к данным, содержащим служебную информацию. Все сотрудники Банка, являющиеся пользователями информационных систем, зарегистрированы в автоматизированном журнале. При приеме на работу и при увольнении работников данные обновляются. При взломе или несанкционированном входе в информационную систему производится регистрация указанных происшествий. Попытки несанкционированного доступа к данным, содержащим служебную информацию, доводятся до сведения Председателя Правления Банка. Виновные лица привлекаются к дисциплинарной ответственности за попытки несанкционированного доступа к служебной информации.

2.2.6. Своевременное уничтожение всех не подлежащих хранению документов. В случае если документ, содержащий служебную информацию, утратил силу, устарел и не может представлять никакой важности (ценности) в будущем, то такой документ уничтожается при помощи специального оборудования.

2.3. Защита рабочих мест и мест хранения документов от беспрепятственного доступа и наблюдения, защита служебной информации от неправомерного использования, предусматривающая следующие мероприятия:

2.3.1. Размещение рабочих мест сотрудников осуществляется таким образом, чтобы исключить возможность несанкционированного просмотра документов и информации, отраженной на экранах мониторов. Расположение мониторов персональных компьютеров работников вне зрительной видимости от других работников. Использование жалюзи для

защиты окон в помещениях, находящихся на нижних этажах. После окончания рабочего дня все информационно-техническое оборудование (компьютеры, принтер, ксерокс) отключается от системы питания. В случае отлучения работника со своего рабочего места во время рабочего дня необходимо отключить монитор персонального компьютера или заблокировать вход в информационную систему в целях защиты от просмотра данных посторонними лицами, включая работников других подразделений. Работникам Банка не разрешается обсуждать сделки клиентов с другими работниками Банка или иными лицами, не имеющими отношение к этим сделкам.

2.3.2. Использование надежных систем защиты служебной информации от неправомерного использования. При осуществлении профессиональной деятельности используются системы защиты информационно-технических систем, предохраняющие от потери информации в информационно-технических системах и базах данных, утечки служебной информации по каналам связи.

2.3.3. Хранение документов, содержащих служебную информацию, в запираемых шкафах или сейфах. Все документы, содержащие служебную информацию, хранятся в указанных шкафах или сейфах, запираемых на ключ, который хранится у ответственных сотрудников Банка. При отсутствии необходимости работы с документами, содержащими служебную информацию, указанные документы не должны находиться на рабочих столах сотрудников.

2.3.4. Инвентаризация хранилища. В Банке проводятся инвентаризации мест хранения документов, содержащих служебную информацию. Факты обнаружения недостачи, порчи, утери документов доводятся до сведения Председателя Правления Банка. К виновным лицам применяются меры дисциплинарной ответственности.

2.3.5. Защита документов при доставке их Клиенту. При заключении договора на брокерское обслуживание клиент уведомляется о рисках, связанных с возможным несанкционированным доступом к документам, направляемым клиенту, во время их доставки. В договоре на брокерское обслуживание устанавливается способ доставки Банком документов клиенту (например, при передаче документов в бумажном виде – использование указанной клиентом курьерской службы, в том числе и курьерской службы Банка, при доставке документов с помощью электронных средств связи – использование защищенных каналов передачи информации). Банк должен использовать все возможные средства для минимизации рисков, связанных с возможным несанкционированным доступом к документам, направляемым клиенту.

2.3.6. Защита документов, полученных от Клиента в процессе осуществления финансового мониторинга при оказании Банком услуг финансового консультанта на рынке ценных бумаг. К указанным документам относятся:

- ★ копии сообщений, публикуемых Клиентом на этапах эмиссии ценных бумаг;
- ★ копии зарегистрированного проспекта ценных бумаг Клиента;
- ★ копии зарегистрированного отчета об итогах выпуска (дополнительного выпуска) ценных бумаг Клиента;
- ★ копии сообщений о существенных фактах Клиента;
- ★ копии ежеквартальных отчетов Клиента.

До момента, когда соответствующая информация должна быть раскрыта Клиентом в порядке, предусмотренном законодательством РФ, Банк при оказании услуг финансового консультанта не вправе раскрывать полученную от Клиента информацию.

В договоре на оказание услуг финансового консультанта устанавливается способ доставки Банком документов Клиенту (например, при передаче документов в бумажном виде – использование указанной Клиентом курьерской службы, в том числе и курьерской службы Банка, при доставке документов с помощью электронных средств связи – использование защищенных каналов передачи информации). Банк должен использовать все возможные средства для минимизации рисков, связанных с возможным несанкционированным доступом к документам, направляемым Клиентом в Банк.

2.4. Своевременное информирование Регистрирующего органа о выявленных Банком нарушениях, допущенных Клиентом при раскрытии информации, предусмотренной законодательством РФ, в процессе осуществления финансового мониторинга при оказании Банком услуг финансового консультанта на рынке ценных бумаг, включающее следующие мероприятия:

2.4.1. Направление в Регистрирующий орган сведения о выявленных Банком нарушениях, допущенных Клиентом при раскрытии информации, предусмотренной законодательством РФ, не позднее следующего дня после выявления таких нарушений.

2.4.2. В случае нарушения требований по раскрытию информации, в том числе информации об исполнении обязательств или неисполнении обязательств (дефолте) по облигациям и опционам Клиента, которые предусмотрены законодательством Российской Федерации либо решением о выпуске (дополнительном выпуске) ценных бумаг Клиента, - раскрытие Банком информации о таком нарушении с указанием содержания нарушения, а также причин такого нарушения (если они известны Банку). В случае нарушения Клиентом требований по раскрытию информации о неисполнении обязательств (дефолте) по облигациям и опционам Клиента Банк дополнительно раскрывает причины такого дефолта (если они известны Банку).

Раскрытие Банком информации о нарушении Клиентом требований по раскрытию информации осуществляется путем:

- ★ направления соответствующей информации в Регистрирующий орган;
- ★ опубликования такой информации в Ленте новостей каждого из информационных агентств, уполномоченных Федеральной комиссией по рынку ценных бумаг РФ на публичное предоставление информации, раскрываемой на рынке ценных бумаг, не позднее следующего дня после даты нарушения Клиентом требований по раскрытию информации;
- ★ опубликования такой информации на странице в сети "Интернет", используемой Банком для раскрытия информации о Клиенте, в срок не позднее следующего дня после даты нарушения Клиентом требований по раскрытию информации, но не ранее даты опубликования такой информации в ленте новостей.

В сообщении, публикуемом Банком в Ленте новостей, указывается адрес страницы в сети "Интернет", которую Банк использует для раскрытия информации о Клиенте в соответствии законодательством РФ.

В случае невозможности дальнейшего исполнения Банком функций финансового консультанта на рынке ценных бумаг, в том числе по причинам:

- ★ принятия уполномоченным органом Банка решения о ликвидации;
 - ★ приостановления либо аннулирования лицензии профессионального участника рынка ценных бумаг на осуществление брокерской и/или дилерской деятельности на рынке ценных бумаг;
 - ★ несостоятельности (банкротства) Банка;
- финансовый мониторинг должен осуществляться иным финансовым консультантом.

2.5. Управление персоналом, предусматривающее:

2.5.1. Наличие письменного обязательства работников Банка о не разглашении служебной информации внутри Банка и за ее пределами. В трудовом договоре работника, имеющего доступ к служебной информации, определяются условия наступления и объем ответственности в случае разглашения служебной информации.

2.6. Применение мер ответственности за несанкционированное предоставление работниками подразделений Банка служебной информации работникам других подразделений Банка и посторонним лицам, предусматривающее:

2.6.1. Применение дисциплинарной ответственности и административных мер, в т.ч. наложение материальных взысканий на работников Банка за несанкционированное предоставление служебной информации работникам других подразделений Банка и посторонним лицам.

2.7. Взаимодействие подразделений Банка, осуществляющих различные виды профессиональной деятельности, предусматривающее:

2.7.1. Разработку правил обмена служебной информацией и их соблюдение. Передача служебной информации между отдельными подразделениями Банка или между сотрудниками, ответственными за осуществление различных видов профессиональной деятельности допускается при наличии необходимости. По каждому факту составляется служебная записка, в которой указывается причина и объем запрашиваемой информации. Передача информации производится с разрешения руководителя подразделения и Службы внутреннего контроля. В Банке организован контроль за соблюдением утвержденных правил обмена служебной информацией между отдельными подразделениями Банка или работниками, участвующими в операциях на рынке ценных бумаг.

2.7.2. Документальная фиксация фактов привлечения сотрудников одного подразделения Банка для временной работы в другом подразделении. При этом в обязательном порядке отражается следующая информация:

- фамилия, имя, отчество привлекаемого сотрудника;
- продолжительность его пребывания в указанном подразделении;
- основания для пребывания;
- перечень установленных для него ограничений.

Привлекаемые сотрудники обязаны соблюдать конфиденциальность полученной информации. С этой целью оформляется дополнительное обязательство о неразглашении служебной информации.