ФЕДЕРАЛЬНАЯ КОМИССИЯ

ПО РЫНКУ ЦЕННЫХ БУМАГ

СОГЛАСОВАНО

25 июля 2003 г.

(подпись)_____ Колесников Г.И.

УТВЕРЖДЕНО

Правлением открытого акционерного общества коммерческий банк «Центр-инвест»

(Протокол № 32 от «18» июня 2003 г.)

Председатель Правления

(подпись)_____ А.Я. Черенков

ПЕРЕЧЕНЬ МЕР, НАПРАВЛЕННЫХ НА ПРЕДОТВРАЩЕНИЕ НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ СЛУЖЕБНОЙ ИНФОРМАЦИИ.

г. Ростов-на-Дону

2003 г.

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Банк - открытое акционерное общество коммерческий банк "Центр-инвест".

1.2. Клиент - юридическое или физическое лицо, которому Банк оказывает услуги, связанные с профессиональной деятельностью на рынке ценных бумаг.

1.3. Сотрудник Банка - физическое лицо, осуществляющее свою деятельность на основании трудового или гражданско-правового договора с Банком и имеющее доступ к конфиденциальной информации в пределах необходимых для выполнения обязанностей, определенных его должностной инструкцией.

1.4. Должностное лицо Банка - штатный сотрудник Банка, имеющий право на получение конфиденциальной информации для выполнения обязанностей возложенных на него внутренними документами Банка.

1.5. Служебная информация - информация, поступающая и предоставленная Банку, а также созданная и используемая Банком в процессе осуществления профессиональной деятельности на рынке ценных бумаг в качестве профессионального участника рынка ценных бумаг.

1.6. Конфиденциальная информация - часть служебной информации, которая не подлежит разглашению и передаче любым способом любому лицу или группе лиц, не имеющих доступа к ней в силу своих обязанностей.

1.7. Настоящий Перечень мер, направленных на предотвращение неправомерного использования служебной информации (далее - Перечень) в Банке является внутренним документом и определяет порядок обращения служебной информации, а также ответственность сотрудников и. должностных лиц Банка в случае совершения ими действий, повлекших неправомерное использование служебной информации.

1.8. Перечень, а также изменения и дополнения к нему рассматриваются и утверждаются Правлением Банка и вступают в действие с момента их регистрации Федеральной комиссией по рынку ценных бумаг Российской Федерации.

2. ОРГАНИЗАЦИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ.

2.1. Основу соблюдения режима доступа к служебной информации составляют следующие способы обеспечения защищенности служебной информации от несанкционированного доступа и неправомерного использования:

2.1.1. правовое регулирование защиты информации;

2.1.2. разграничение и контроль лрав доступа к информации;

2.1.3. учет входящей и исходящей информации;

2.1.4. инженерно-техническая защита информации;

2.1.5. криптографирование входящих и исходящих потоков информации.

2.2. Правовое регулирование защиты информации включает в себя:

2.2.1. Наличие во внутренних положениях Банка, контрактах заключаемых с Сотрудниками, в должностных инструкциях Сотрудников и Должностных лиц Банка положений и обязательств по защите конфиденциальной информации.

2.2.2. Формулирование и доведение до сведения всех сотрудников Банка (в том числе не связанных с конфиденциальной информацией) положения о правовой ответственности за разглашение конфиденциальной информации, несанкционированное уничтожение или фальсификацию документов.

2.2.3. Разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите информации.

2.2.4. Ответственность за выполнение мер правового регулирования защиты информации несут руководители подразделений Банка на основании должностных инструкций.

2.3. Разграничение и контроль прав доступа к информации.

2.3.1. Система разграничения доступа предназначена для предоставления каждому Сотруднику и Должностному лицу Банка только тех данных и прав, которые ему необходимы для работы и ограждения информации от несанкционированного доступа.

2.3.2. Для защиты информации от несанкционированного доступа применяется система персональных паролей, идентифицирующих команд и разграничения доступа к автоматизированной банковской системе, а также прочим файлам, находящимся в общебанковской сети на основе средств, заложенных в используемые операционные системы и аппаратные средства.

2.3.3. Сотрудник или Должностное лицо Банка получает доступ к информации после регистрации в системе и ввода пароля. Регистрация делается с помощью стандартных средств операционной системы и базы данных, что обеспечивает достаточную надежность за счет шифрования паролей и их централизованной проверки.

2.3.4. После регистрации в системе сотрудник или должностное лицо Банка работают с помощью специализированного программного обеспечения, позволяющего им выполнять только допустимый набор действий.

2.3.5. Для защиты информации от несанкционированного доступа применяется также система мер по регламентации доступа в отдельные помещения Банка с помощью идентифицирующих кодов, шифров.

2.3.6. Мероприятия по разграничению доступа к информации и контроль за его соблюдением осуществляет отдел внутреннего контроля на основании Положения о внутреннем контроле.

2.4. Учет входящей/исходящей документированной информации, позволяет разграничивать конфиденциальную информацию от иной служебной информации. Информация, заявленная отправителем/получателем как конфиденциальная, учитывается отдельно от иной служебной информации.

2.5. Инженерно-техническая защита информации предназначена для пассивного и активного противодействия средствам технической разведки и формирования рубежей охраны территории, здания, помещений и оборудования с помощью комплексов технических средств и включает в себя:

2.5.1. сооружения физической (инженерной) защиты от проникновения посторонних лиц на территорию, в здание и помещения;

2.5.2. средства защиты технических каналов утечки информации при работе ЭВМ, средств связи и других приборов и офисного оборудования, при проведении совещаний, беседах с посетителями и сотрудниками и т.п.;

2.5.3. средства защиты помещений от визуальных способов технической разведки;

2.5.4. средства обеспечения охраны территории, здания и помещений;

2.5.5. средства противопожарной охраны;

2.5.6. технические средства и мероприятия, предотвращающие вынос персоналом из помещений документов, дискет, специально маркированных предметов и т.п.

2.6.Ответственность за организацию, инженерно-технической защиты информации несет Заместитель Председателя Правления банка по вопросам безопасности.

2.7. Криптографирование входящих и исходящих потоков информации является дополнительным способом обеспечения защищенности информации от несанкционированного доступа.

2.8. Все серверы баз данных Банка и сетевое оборудование размещены в специальных помещениях, допуск в которые имеет ограниченный круг администраторов сети и баз данных Банка.

3. ПОЛНОМОЧИЯ СОТРУДНИКОВ И ДОЛЖНОСТНЫХ ЛИЦ БАНКА ПО ПРЕДОСТАВЛЕНИЮ И ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИИ.

3.1. Председатель Правления Банка имеет право использовать и предоставлять любую служебную информацию, в том числе и конфиденциальную, в соответствии с внутренними документами Банка.

3.2. Члены Совета Директоров Банка используют служебную информацию в пределах необходимых для осуществления ими своих обязанностей и не вправе предоставлять служебную информацию от имени Банка.

3.3. Должностные лица Банка используют служебную и конфиденциальную информацию, за исключением случаев специально оговоренных во внутренних документах Банка и вправе предоставлять конфиденциальную информацию только в случаях специально оговоренных во внутренних документах Банка или по распоряжению Председателя Правления Банка.

3.4. Сотрудники Банка вправе предоставлять и использовать служебную информацию в пределах, необходимых для осуществления ими своих непосредственных обязанностей и не имеют права предоставлять информацию от имени Банка.

3.5. Должностные лица и сотрудники Банка не имеют права использовать служебную информацию в личных целях.

4. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ И ДОЛЖНОСТНЫХ ЛИЦ БАНКА ЗА НАРУШЕНИЯ РЕЖИМА ОБРАЩЕНИЯ СЛУЖЕБНОЙ ИНФОРМАЦИИ И ПОРЯДОК НАЛОЖЕНИЯ ВЗЫСКАНИЯ

4.1. Виды взысканий, применяемых к сотрудникам и должностным лицам Банка, нарушившим режим обращения служебной информации:

4.1.1. предупреждение;

4.1.2. выговор;

4.1.3. увольнение с работы.

4.2.Взыскание на сотрудника или должностное лицо Банка налагается Председателем Правления Банка.

4.2.1. Взыскание на сотрудника или должностное лицо Банка может быть наложено по представлению начальника службы внутреннего контроля.

4.3. Взыскание на Председателя Правления Банка, Председателя Совета Директоров Банка или членов совета Директоров Банка налагается советом Директоров Банка. Решение о наложении данного взыскания принимается квалифицированным большинством состава совета Директоров банка.

4.3.1. Инициатором рассмотрения советом Директоров Банка вопроса о наложении данного взыскания может выступать:

4.3.1.1. Председатель Правления Банка;

4.3.1.2. Председатель совета Директоров;

4.3.1.3. Член совета Директоров.