

УТВЕРЖДЕНО

Генеральным директором
Общества с ограниченной ответственностью
«КСП Капитал Управление Активами»
Приказ № 85 от «15» сентября 2016 г.

ПЕРЕЧЕНЬ

мер по снижению рисков, связанных с деятельностью на рынке ценных бумаг (деятельностью по управлению ценными бумагами и деятельностью управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов) Общества с ограниченной ответственностью «КСП Капитал Управление Активами»

г. Москва
2016г.

1. Общие положения

Настоящий документ определяет единые принципы организации системы мер по снижению рисков, связанных с осуществлением Обществом с ограниченной ответственностью «КСП Капитал Управление Активами» (далее по тексту – Организация) при условии совмещения различных видов деятельности на рынке ценных бумаг (деятельности по управлению ценными бумагами и деятельности управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов).

Система мер по снижению рисков при осуществлении Организацией различных видов деятельности на рынке ценных бумаг (деятельности по управлению ценными бумагами и деятельности управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов) включает в себя:

- ✓ выработку рекомендаций по управлению рисками;
- ✓ выделение рисков, наиболее существенных для Организации, которые поддаются управляющему воздействию; в том числе риска возникновения конфликта интересов между Организацией и клиентом;
- ✓ разработку базовых принципов управления рисками в Организации;
- ✓ идентификацию потенциальных источников рисков (групп и типов), характерных для деятельности Организации на рынке ценных бумаг;
- ✓ оценку вероятности возникновения тех или иных негативных событий (явлений);
- ✓ выработку политики в отношении пределов допустимого для Организации риска;
- ✓ анализ причин возникновения рисков;
- ✓ анализ документации (включая внутренние документы Организации) и выработка заключений на предмет соответствия положений документов допустимому риску, определенному политикой Организации;
- ✓ оценку способности Организации компенсировать воздействие нежелательных (негативных) событий (явлений);
- ✓ разработку и принятие методики оценки рисков, выработка индикаторов рисков;
- ✓ мониторинг участков повышенного риска;
- ✓ оценку эффективности существующей в Организации системы внутреннего контроля, предусмотренного для снижения конкретных типов рисков.

2. Процедуры, составляющие систему мер снижения рисков при осуществлении различных видов профессиональной деятельности на рынке ценных бумаг

2.1. Наличие системы ответственности за несанкционированное предоставление сотрудниками подразделений Организации конфиденциальной информации сотрудникам других подразделений Организации.

2.2. Ограничение доступа посторонних лиц в помещения подразделений Организации, предназначенные для осуществления деятельности или эксплуатации информационно-технологических систем, обеспечиваемое следующими мероприятиями:

- ✓ оборудование помещений Организации охранной сигнализацией;
- ✓ использованием технологических средств, специального оборудования и/или услуг специальных Организаций для предотвращения доступа посторонних лиц в помещение Организации;
- ✓ проведением переговоров с клиентами Организации в специально оборудованном помещении (переговорной комнате);
- ✓ обеспечение контроля за входом в помещения Организации;
- ✓ обеспечение постоянного контроля за посторонними лицами в течение всего времени нахождения в помещениях Организации;
- ✓ установлена пропускная система и охрана, обеспечивающая безопасность и невозможность без предварительной договоренности и оформления пропуска, прохода в помещение Организации.

2.3. Разграничение прав доступа при вводе и обработке данных, имеющее своей целью предохранение от несанкционированных действий сотрудников подразделений Организации, обеспечивается следующими мероприятиями:

- ✓ доступ к данным только ограниченного круга лиц, являющихся непосредственными исполнителями, обеспечивающими осуществление конкретного вида деятельности Организации;
- ✓ доступ к данным только в пределах полномочий, предоставленных непосредственно исполнителям;
- ✓ ведение автоматизированного журнала регистрации пользователей информационной системы;
- ✓ ограничение доступа к служебной информации путем использования возможностей программного обеспечения;
- ✓ размещение документов, касающихся конкретного вида деятельности Организации в отдельных местах хранения, шкафах и (или) сейфах, закрываемых на ключ, не период нерабочего времени;
- ✓ размещение рабочих мест сотрудников таким образом, чтобы исключить возможность несанкционированного просмотра документов и информации, отраженной на экранах мониторов. Данное требование достигается соблюдением следующих правил:
 - расположение мониторов персональных компьютеров сотрудников вне зрительной видимости других сотрудников;
 - использование жалюзи или специальных штор для защиты окон в помещениях.
- ✓ хранение документов в запираемых шкафах или сейфах. Данное требование достигается соблюдением следующих правил:
 - наличие шкафов или сейфов, запираемых на ключ, который хранится у ответственных сотрудников Организации;
 - все документы, содержащие служебную информацию, должны храниться в указанных шкафах и сейфах;
 - в конце рабочего дня, документы, содержащие служебную информацию, не должны оставаться на столах работников, а должны убираться в шкаф или сейфы.
- ✓ Наличие доступа сотрудников Организации только к сведениям, необходимым им для выполнения своих прямых служебных обязанностей;
- ✓ установление паролей доступа к данным, содержащимся в автоматизированной системе;
- ✓ своевременное уничтожение всех, не подлежащих обязательному хранению документов.

2.4. Обособленное подчинение функциональных подразделений Организации, наличие разделения обязанностей в каждом подразделении организации: отделение функций исполнения операций от функций контроля и выдачи разрешения на проведение операций.

2.5. Защита рабочих мест сотрудников Организации и мест хранения от беспрепятственного доступа и наблюдения, обеспечиваемая следующими мероприятиями:

- ✓ размещение рабочих мест сотрудников таким образом, чтобы исключить возможность несанкционированного просмотра документов и информации, отраженной на экранах мониторов. Данное требование достигается соблюдением следующих правил:
 - расположение мониторов персональных компьютеров сотрудников вне зрительной видимости других сотрудников;
 - использование жалюзи или специальных штор для защиты окон в помещениях.
- ✓ хранение документов в запираемых на ключ шкафах или сейфах.

2.6. Ограничение доступа сотрудников Организации к конфиденциальной информации, обеспечиваемое следующими мероприятиями:

- ✓ наличие доступа сотрудников Организации только к сведениям, необходимым им для выполнения своих прямых служебных обязанностей;
- ✓ установлением паролей доступа к данным, содержащимся в автоматизированной системе;
- ✓ своевременным уничтожением всех, не подлежащих хранению документов.

Перечень мер по снижению рисков, связанных с деятельностью на рынке ценных бумаг (деятельностью по управлению ценными бумагами и деятельностью управляющей компании инвестиционных фондов, паевых инвестиционных фондов и негосударственных пенсионных фондов), включающий меры по снижению рисков при совмещении различных видов деятельности на рынке ценных бумаг Общества с ограниченной ответственностью «КСП Капитал Управление Активами»

2.7. Наличие системы разграничения доступа к разным уровням баз данных и операционной среды используемого программного обеспечения, состоящей из системы разграничения доступа на уровне локальной сети.

2.8. На уровне локальной сети разграничение прав пользователей по доступу к тем или иным дисковым ресурсам осуществляется с целью исключения несанкционированного доступа пользователей – сотрудников других подразделений Организации – к файлам баз данных (или иным формам хранения данных), а также к файлам, содержащим другую конфиденциальную информацию (документацию).

2.9. Наличие системы мер снижения технических рисков (рисков незапланированной приостановки деятельности), включающей:

- ✓ наличие автономных источников резервного электропитания, способных поддерживать функционирование систем достаточно длительное время;
- ✓ наличие системы резервного копирования данных; хранение копий в защищенных хранилищах, расположенных в ином месте.

2.14. Наличие системы мер снижения финансовых рисков, включающей:

- ✓ изучение специфики работ с различными группами клиентов;
- ✓ внедрение упорядоченной системы выставления и учета счетов за услуги, контроль за внесением оплаты, анализ дебиторской задолженности.

2.15. Наличие системы мер снижения операционных рисков, включающей:

- ✓ защиту активов от несанкционированного доступа;
- ✓ регулярную сверку учетных записей подразделений организации, осуществляющих ведение учета ценных бумаг и/или денежных средств;
- ✓ регулярную инвентаризацию хранилища;
- ✓ регулярное извещение клиентов о состоянии их активов;
- ✓ систематическую работу с запросами клиентов.

3. Регламент взаимодействия подразделений организации, осуществляющих различные виды деятельности

3.1. Конфиденциальная информация предоставляется подразделениями Организации друг другу по специальному письменному запросу установленной формы. Способ и срок предоставления информации указывается в запросе. Запрос должен быть подписан руководителем структурного подразделения, запрашивающего информацию или руководителем Организации или иным уполномоченным лицом Организации.

3.2. Состав сведений, относящихся к конфиденциальной информации, допущенных к предоставлению подразделениям Организации друг другу определяется внутренними документами каждого конкретного подразделения.

3.3. Ответственность сотрудников подразделений Организации за неправомерное предоставление и за неправомерное использование конфиденциальной информации сотрудниками других подразделений, осуществляющих иные виды деятельности на рынке ценных бумаг, устанавливается приказом руководителя Организации и включает в себя меры административного и дисциплинарного воздействия.

3.4. Перечень сотрудников подразделений Организации, уполномоченных предоставлять конфиденциальную информацию, и сотрудников подразделений Организации, уполномоченных запрашивать и получать такую информацию, определяется руководителем Организации.