УТВЕРЖДАЮ

Генеральный директор
ООО «Газпром инвестхолдинг»

_____
/Е.Л.Шадрин/

“19” января 2017 года

Перечень мер по снижению рисков при совмещении различных видов профессиональной деятельности на рынке ценных бумаг.

ООО «Газпром инвестхолдинг» (редакция № 2)

г. Москва
2017 г.

Общие положения

Настоящий Перечень мер по снижению рисков при совмещении различных видов профессиональной деятельности на рынке ценных бумаг ООО «Газпром инвестхолдинг» (далее - «Перечень») включается в состав внутренних документов Общества, регулирующих его деятельность как профессионального участника рынка ценных бумаг. Редакция № 2 Переченя вступает в силу с даты ее утверждения Генеральным директором ООО «Газпром инвестхолдинг».

Единые принципы системы управления рисками, возникающих при осуществлении ООО «Газпром инвестхолдинг» (далее – «Общество») профессиональной деятельности на рынке ценных бумаг, регламентируются внутренними документами Общества, а именно:

- Политикой управления рисками ООО «Газпром инвестхолдинг»;
- Регламентом взаимодействия участников системы управления рисками ООО «Газпром инвестхолдинг»;
- иными документами в области управления рисками, которые будут утверждены в Обществе в рамках совершенствования и функционирования системы управления рисками Общества.

Процедуры, составляющие систему мер снижения рисков совмещения различных видов профессиональной деятельности

1. Размещение сотрудников подразделений Общества, осуществляющих различные виды профессиональной деятельности, в отдельных изолированных помещениях.

2. Наличие письменного обязательства каждого сотрудника Общества о не разглашении конфиденциальной информации в том числе, внутри Общества.

3. Наличие системы ответственности за несанкционированное предоставление сотрудниками подразделений Общества конфиденциальной информации сотрудникам других подразделений Общества.

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

- размещением помещений подразделений Общества и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая сотрудников других подразделений;
- оборудованием помещений Общества охранной сигнализацией;
- проведением переговоров с клиентами Общества в специально оборудованном помещении;
- обеспечением контроля за входом в помещения Общества сотрудниками службы охраны;
- обеспечением постоянного контроля со стороны службы охраны Общества за посторонними лицами в течение всего времени их нахождения в помещениях Общества.

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

- доступ к данным только ограниченного круга лиц, являющихся непосредственными исполнителями, обеспечивающими осуществление конкретного вида профессиональной деятельности Общества;
- доступ к данным только с определенных автоматизированных рабочих мест;
- доступ к данным только в пределах полномочий, предоставленных непосредственно исполнителям;
- ведение автоматизированного журнала регистрации пользователей информационной системы и регистрации попыток несанкционированного доступа к данным.

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

7. Размещение документов, касающихся деятельности Общества по каждому виду профессиональной деятельности, в отдельных местах хранения, опечатываемых на период нерабочего времени.

8. Обособленное хранение сданных в архив документов по каждому виду профессиональной деятельности Общества.

9. Защита рабочих мест сотрудников Общества и мест хранения от беспрепятственного доступа и наблюдения, обеспечиваемая следующими мероприятиями:
- размещением рабочих мест сотрудников таким образом, чтобы исключить возможность несанкционированного просмотра документов и информации, отраженной на экранах мониторов;
- хранением документов в запираемых шкафах или сейфах.

10. Ограничение доступа сотрудников Общества к конфиденциальной информации, обеспечиваемое следующими мероприятиями:
- наличие доступа сотрудников Общества 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.

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

12. 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 Общества – к файлам баз данных (или иным формам хранения данных), а также к файлам, содержащим другую конфиденциальную информацию (документацию).