

Перечень мер, направленных на предотвращение неправомерного использования служебной информации при осуществлении профессиональной деятельности на рынке ценных бумаг

1. Общие положения

Настоящий Перечень мер, направленных на предотвращение неправомерного использования информации при осуществлении профессиональной деятельности на рынке ценных бумаг, (далее – Перечень) разработан в соответствии с требованиями законодательства Российской Федерации о рынке ценных бумаг, в том числе нормативных правовых актов федерального органа исполнительной власти по рынку ценных бумаг, и имеет целью:

-снижение рисков неправомерного использования информации сотрудниками ОАО АКБ «ЕВРОФИНАНС МОСНАРБАНК» (далее – Банк) при осуществлении профессиональной деятельности на рынке ценных бумаг;

-повышение уровня доверия к Банку со стороны клиентов.

Для целей настоящего документа под служебной информацией понимается 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 его клиентов на рынке ценных бумаг, которая ставит сотрудников Банка, обладающих такой информацией в силу своего служебного положения или трудовых обязанностей, в преимущественное положение по сравнению с другими субъектами рынка ценных бумаг.

2. Меры, препятствующие неправомерному использованию служебной информации

- Ограничение доступа посторонних лиц в помещения подразделений Банка, предназначенные для осуществления профессиональной деятельности на рынке ценных бумаг или эксплуатации информационно-технологических систем предполагает:

-размещение рабочих помещений Банка и оборудования способом, исключающим возможность бесконтрольного проникновения в эти помещения и к этому оборудованию посторонних лиц, включая сотрудников других подразделений:

-сотрудники подразделений, осуществляющих различные виды профессиональной деятельности размещаются в разных помещениях по функциональному признаку. После окончания рабочего дня дверь каждого помещения закрывается на ключ, который сдается работникам Службы безопасности;

-все помещения имеют разные замки;

-в случае ухода из помещения в течение рабочего дня всех сотрудников, дверь помещения закрывается на ключ. Сотрудники каждого подразделения, расположенного в отдельном помещении, не должны покидать своего рабочего места, оставляя в нем без присмотра посторонних лиц, включая сотрудников других подразделений Банка.

-проведение переговоров с клиентами Банка в специально оборудованном помещении;

-обеспечение контроля за входом в помещения Банка:

-пропускной режим доступа в рабочие помещения и в помещения, в которых эксплуатируется информационно-технологическая система;

-ограничение доступа посторонних лиц в помещения после окончания рабочего дня, установленного в Банке;

-доступ сотрудников Банка в помещения Банка по выходным и праздничным дням осуществляется только по предварительному распоряжению уполномоченных лиц.

- Разграничение прав доступа при вводе и обработке данных с целью защиты от несанкционированных действий сотрудников разных подразделений Банка, а также ограничение доступа сотрудников Банка к служебной информации, предусматривает следующие мероприятия:

-четкое разграничение прав и обязанностей сотрудников Банка:

-наличие должностной инструкции для каждого сотрудника Банка, четко определяющей его функции, права и обязанности;

- функции исполнения отделены от контрольного просмотра информации и выдачи разрешения на проведение операции;
- доступ к данным только ограниченного круга лиц, являющихся непосредственными исполнителями, обеспечивающими осуществление конкретного вида профессиональной деятельности Банка. Доступ сотрудников Банка только к сведениям, необходимым им для выполнения своих прямых служебных обязанностей в пределах предоставленных полномочий:
 - наличие внутренних документов (приказов/распоряжений), определяющих круг лиц, имеющих доступ к служебной информации;
 - наличие письменного обязательства о неразглашении служебной информации от сотрудников, имеющих доступ к служебной информации;
 - наличие системы индивидуальных кодов и паролей доступа к данным для каждого сотрудника Банка.
- наличие системы разграничения доступа к разным уровням баз данных и операционной среды используемого программного обеспечения, состоящей из системы разграничения доступа на уровне локальной сети:
 - при осуществлении профессиональной деятельности используются общепринятые системы безопасности операционных систем, позволяющие распределять права отдельным пользователям и группам пользователей, а также контролировать действия пользователя с сетевыми ресурсами (получение доступа, чтение, изменение данных, удаление и т.д.).
 - 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.
- доступ к данным только с определенных автоматизированных рабочих мест:

-ограничение доступа различных категорий пользователей средствами операционной системы и системы управления базами данных.

-своевременное уничтожение всех, не подлежащих хранению документов.

- Защита рабочих мест и мест хранения документов от несанкционированного доступа и наблюдения, защита служебной информации от неправомерного использования, предусматривает:

-размещение рабочих мест сотрудников таким образом, чтобы исключить возможность несанкционированного просмотра документов и информации, отраженной на экранах мониторов:

-расположение мониторов персональных компьютеров сотрудников вне зрительной видимости от других сотрудников;

-использование жалюзи или специальных штор для защиты окон в помещениях зрительно доступных из вне;

-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.

-хранение документов, содержащих служебную информацию, в запираемых шкафах или сейфах:

-наличие шкафов или сейфов, запираемых на ключ, который хранится у ответственных сотрудников Банка.

-размещение документов, касающихся деятельности Банка по каждому виду профессиональной деятельности и содержащих служебную информацию, в отдельных местах хранения, в запираемых шкафах и сейфах.

-в конце каждого рабочего дня документы, содержащие служебную информацию, с рабочих мест сотрудников убираются в шкафы или сейфы.

-защита документов при доставке их клиенту:

-используются все возможные средства для минимизации рисков, связанных с возможным несанкционированным доступом к документам, направляемым клиенту.

- Управление персоналом предполагает:
 - наличие письменного обязательства сотрудников Банка о неразглашении служебной информации внутри Банка и за его пределами;
 - определение состава служебной информации к которой имеют доступ те или иные сотрудники, связанные с осуществлением профессиональной деятельности на рынке ценных бумаг.
- Защита от несанкционированного распространения служебной информации между подразделениями Банка, осуществляющими различные виды профессиональной деятельности на рынке ценных бумаг предусматривает:
 - документооборот между отдельными подразделениями Банка осуществляется в соответствии с утвержденными внутренними банковскими документами (инструкциями), регламентирующими проведение операций на рынке ценных бумаг.
 - состав сведений, относящихся к служебной информации и допущенных к предоставлению подразделениями Банка друг другу, определяется внутренними документами каждого конкретного подразделения.

3. Контроль и ответственность

- Текущий контроль за соблюдением мер, направленных на предотвращение неправомерного использования служебной информации при осуществлении профессиональной деятельности на рынке ценных бумаг осуществляется руководителями соответствующих подразделений Банка и сотрудниками Службы безопасности. За последующий контроль отвечает Контролер профессионального участника рынка ценных бумаг.
- При выявлении нарушений по результатам как внутренних, так и внешних проверок, в Банке проводится работа по увеличению эффективности системы мер снижения рисков, включающая:
 - анализ допущенных ошибок и нарушений;

-разработка механизмов, направленных на предотвращение или минимизацию выявленных рисков;

-включение разработанных механизмов в документы, регламентирующие деятельность подразделений Банка;

-утверждение таких документов.

- Несанкционированное предоставление служебной информации сотрудниками одних подразделений Банка сотрудникам других подразделений Банка и посторонним лицам, а также неправомерное использование служебной информации в личных целях и в интересах третьих лиц, предусматривает применение дисциплинарной ответственности и административных мер (в случаях, предусмотренных действующим законодательством).