

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации по разработке и утверждению
порядка доступа к инсайдерской информации и правил охраны ее
конфиденциальности

14.09.2018

№ 23-МР

Настоящие Методические рекомендации разработаны в соответствии с пунктом 11 части 1 статьи 14 Федерального закона от 27.07.2010 № 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации» (далее – Федеральный закон) в целях оказания методологической помощи юридическим лицам, указанным в пунктах 1–8, 11 и 12 статьи 4 Федерального закона (далее при совместном упоминании – организации), при разработке и утверждении ими в соответствии с пунктом 1 статьи 11 Федерального закона порядка доступа к инсайдерской информации и правил охраны ее конфиденциальности.

Глава 1. Общие положения

1.1. Организациям рекомендуется в разрабатываемых и утверждаемых ими порядке доступа к инсайдерской информации и правилах охраны ее конфиденциальности предусмотреть следующие положения:

1.1.1. Принципы организации процессов по обеспечению доступа к инсайдерской информации, ее сохранности и защиты, в том числе следующие принципы:

принцип следования этическим стандартам (в случае их наличия);

принцип непрерывности и эффективности процесса обеспечения защиты и сохранности инсайдерской информации;

принцип предотвращения конфликта интересов при обращении инсайдерской информации;

принцип соответствия мер по обеспечению защиты и сохранности инсайдерской информации, в том числе предотвращению, выявлению и пресечению ее неправомерного использования, характеру и масштабу деятельности организации.

1.1.2. Перечень мер по обеспечению доступа, защиты и сохранности инсайдерской информации, принятие которых рекомендуется в соответствии с главой 2 настоящих Методических рекомендаций.

1.1.3. Порядок и сроки принятия мер по предотвращению неправомерного использования инсайдерской информации при наличии информации, поступившей из внутренних и внешних источников, в том числе информации о признаках недобросовестного поведения работников, а также членов органов управления организации.

1.1.4. Перечень мер по обеспечению недопущения незаконного разглашения и (или) использования инсайдерской информации работниками организации и (или) иными лицами, которым стала известна инсайдерская информация, в том числе случайно, в собственных интересах или в интересах третьих лиц, а также последствия, возникающие в результате незаконного разглашения и (или) использования инсайдерской информации.

1.1.5. Порядок информирования работников организации и ее органов управления о требованиях по соблюдению Федерального закона и принятых в соответствии с ним нормативных актов.

1.1.6. Порядок ознакомления работников организации и ее органов управления с действующими редакциями внутренних документов организации, разработанных в соответствии с частью 1 статьи 3, частью 1 статьи 9, статьей 11 и частями 1-3 статьи 12 Федерального закона.

1.1.7. Способы подтверждения факта ознакомления работников, имеющих доступ к инсайдерской информации, а также лиц, указанных в подпункте 1.1.16 настоящего пункта, с действующими перечнем инсайдерской информации, порядком доступа к инсайдерской информации, правилами охраны ее конфиденциальности, требованиями Федерального закона и принятых в соответствии с ним нормативных актов о последствиях неправомерного использования инсайдерской информации, а также порядок хранения документов, подтверждающих такое ознакомление.

1.1.8. Порядок и периодичность проведения обучения работников, в том числе лиц, указанных в подпунктах 1.1.15 - 1.1.17 настоящего пункта, а также в пункте 2.2.14 настоящих Методических рекомендаций, в целях повышения их осведомленности о правилах обращения с инсайдерской информацией и понимания последствий в результате их нарушения.

1.1.9. Права и обязанности лиц, ответственных за обеспечение доступа, защиты и сохранности инсайдерской информации, в том числе должностного лица (работников структурного подразделения), в обязанности которого входит осуществление контроля за соблюдением требований Федерального закона и принятых в соответствии с ним нормативных актов (далее – ОДЛ).

1.1.10. Права и обязанности органов управления организации, утверждающих внутренние документы, разрабатываемые организациями в соответствии с частью 1 статьи 3, пунктом 1 части 1 статьи 9, статьей 11 и частями 1-3 статьи 12 Федерального закона в целях защиты и сохранности инсайдерской информации и реализации мер по предотвращению, выявлению и пресечению ее неправомерного использования.

1.1.11. Порядок формирования и работы рабочих (проектных) групп, создаваемых для оперативного решения задач организации, требующих

обработки инсайдерской информации, в состав которых по решению организации помимо работников организации, которым в целях исполнения ими должностных обязанностей предоставлен доступ к инсайдерской информации, могут входить работники структурных подразделений организации, в должностные обязанности которых не входит получение инсайдерской информации (далее – рабочие (проектные) группы), а также порядок предоставления рабочим (проектным) группам инсайдерской информации.

1.1.12. Порядок уведомления лиц, включенных в список инсайдеров, об их включении в список инсайдеров в соответствии с пунктом 2 части 1 статьи 9 Федерального закона до передачи им инсайдерской информации.

1.1.13. Порядок ведения следующих списков:

списка эмитентов, в отношении которых организацией получена инсайдерская информация и совершение операций в отношении финансовых инструментов которых в собственных интересах организации возможно, а также финансовых инструментов, в отношении которых организацией получена инсайдерская информация и совершение операций с которыми в собственных интересах организации возможно (далее - лист наблюдения),

списка эмитентов, в отношении которых организацией получена инсайдерская информация и совершение операций в отношении финансовых инструментов которых в собственных интересах организацией запрещено, а также финансовых инструментов, в отношении которых организацией получена инсайдерская информация и совершение операций с которыми в собственных интересах организацией запрещено (далее - стоп-лист).

1.1.14. Порядок ознакомления и доступа работников организации к информации, содержащейся в стоп-листе и листе наблюдения, и правила хранения информации, содержащейся в стоп-листе и листе наблюдения.

1.1.15. Права и обязанности в области обеспечения доступа, защиты и сохранности инсайдерской информации работников структурного подразделения (структурных подразделений) организации, должностные

обязанности которых в силу заключаемых с клиентами организации договоров связаны с получением инсайдерской информации от клиентов организации, в том числе, права и обязанности в области обеспечения доступа, защиты и сохранности инсайдерской информации лиц, привлекающих клиентов, и лиц, осуществляющих оценку привлекаемых клиентов в соответствии с требованиями законодательства Российской Федерации и (или) внутренними документами организации.

1.1.16. Права и обязанности в области обеспечения доступа, защиты и сохранности инсайдерской информации работников структурного подразделения организации, в должностные обязанности которых входит совершение операций в собственных интересах организации, в том числе права и обязанности в области обеспечения доступа, защиты и сохранности инсайдерской информации лиц, принимающих решения о совершении операций в собственных интересах организации, и лиц, осуществляющих предварительную оценку условий сделок, заключаемых организацией, в том числе на их соответствие требованиям законодательства Российской Федерации (если такая оценка осуществляется).

1.1.17. Права и обязанности в области обеспечения доступа, защиты и сохранности инсайдерской информации работников структурного подразделения организации, которые предоставляют аналитические материалы лицам, указанным в подпункте 1.1.16 настоящего пункта, и (или) публичную информацию участникам финансового рынка, которая используется при совершении операций с финансовыми инструментами, иностранной валютой и (или) товарами.

1.1.18. Перечень мер, обеспечивающих исключение несанкционированного доступа в помещения структурных подразделений, указанных в подпункте 1.1.15 настоящего пункта, и к рабочим местам работников таких структурных подразделений.

1.1.19. Запрет работникам структурных подразделений, указанных в подпунктах 1.1.16 - 1.1.17 настоящего пункта, на доступ к инсайдерской информации, получаемой от клиентов организации.

1.1.20. Ограничение на использование работниками структурных подразделений, указанных в подпункте 1.1.16 настоящего пункта, личных средств связи, личных компьютеров и личных машинных носителей информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства) при осуществлении своих должностных обязанностей.

1.1.21. Ограничение на передачу работниками организации, имеющими доступ к инсайдерской информации, средств идентификации и аутентификации, используемых ими при работе с инсайдерской информацией, третьим лицам.

1.1.22. Перечень лиц, которым организацией предоставляется доступ к инсайдерской информации, порядок ее передачи указанным лицам инсайдерской информации, в том числе с согласия (без согласия ОДЛ), содержащий форму запроса о предоставлении инсайдерской информации, требования к содержанию запроса, в том числе обоснование необходимости получения инсайдерской информации, сроки рассмотрения запроса, основания для отказа в предоставлении согласия на передачу инсайдерской информации, последствия нарушения порядка использования и хранения инсайдерской информации.

1.1.23. Порядок ведения и хранения журнала передачи инсайдерской информации, включающий указание на фиксацию в нем даты и времени передачи инсайдерской информации, информации о лицах, передающих и получающих инсайдерскую информацию, сути передаваемой инсайдерской информации и способе ее передачи, предоставления ОДЛ, или иным уполномоченным лицом согласия на передачу инсайдерской информации.

Глава 2. Отдельные меры по обеспечению доступа к инсайдерской информации, ее защиты и сохранности

2.1. Организациям рекомендуется включать в разрабатываемые и утверждаемые ими порядок доступа к инсайдерской информации и правила охраны ее конфиденциальности меры, предусмотренные пунктом 2.2 настоящих Методических рекомендаций.

2.2. Организациям рекомендуется принимать следующие меры по обеспечению доступа к инсайдерской информации, ее защиты и сохранности:

2.2.1. Обеспечение недопущения осуществления функций структурными подразделениями, указанными в подпунктах 1.1.15 - 1.1.16 пункта 1.1 настоящих Методических рекомендаций, не входящих в компетенцию таких структурных подразделений.

2.2.2. Установление рабочих мест работников структурных подразделений, имеющих доступ к инсайдерской информации организации, а также работников структурных подразделений, указанных в подпункте 1.1.15 пункта 1.1 настоящих Методических рекомендаций, в помещениях, отделенных друг от друга, а также от помещений, в которых находятся рабочие места работников иных структурных подразделений организации.

При невозможности разделения рабочих мест организациям рекомендуется разработать иные доступные и разумные меры, направленные на защиту и сохранность инсайдерской информации.

2.2.3. Обеспечение расположения мониторов компьютеров работников, имеющих доступ к инсайдерской информации организации, а также работников структурных подразделений, указанных в подпунктах 1.1.15 - пункта 1.1 настоящих Методических рекомендаций, исключающее риски ознакомления с инсайдерской информацией иными лицами, в том числе, в случае если в организации не предусмотрено закрепление компьютеров непосредственно за определенным работником.

2.2.4. Разграничение прав доступа к базам данных работников, осуществляющих ввод инсайдерской информации в базы данных, и работников, осуществляющих последующую обработку инсайдерской информации.

2.2.5. Обеспечение исключения несанкционированного доступа к рабочим местам, компьютерам, машинным носителям информации работников организации, имеющих доступ к инсайдерской информации организации, а также работников структурных подразделений организации, указанных в подпункте 1.1.15 пункта 1.1 настоящих Методических рекомендаций, работниками иных структурных подразделений, в том числе должностными лицами, указанными в абзаце третьем пункта 2.2.12 настоящих Методических рекомендаций, посредством средств идентификации и аутентификации субъектов доступа и объектов доступа, в том числе присвоение субъектам и объектам доступа уникального признака (идентификатора).

2.2.6. Обеспечение контроля за передачей средств идентификации и аутентификации работников организации, имеющих доступ к инсайдерской информации организации, работников (структурного подразделения) структурных подразделений организации, указанных в подпункте 1.1.15 пункта 1.1 настоящих Методических рекомендаций, а также ОДЛ, иным лицам.

Организациям рекомендуется при обеспечении доступа к инсайдерской информации руководствоваться главой 7 национального стандарта Российской Федерации ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» в части процесса 1 «Обеспечение защиты информации при управлении доступом».

2.2.7. Установление копировальных машин, принтеров и аналогичных устройств, используемых работниками организации, имеющими доступ к инсайдерской информации организации, а также работниками структурных

подразделений, указанных в подпункте 1.1.15 пункта 1.1 настоящих Методических рекомендаций, в местах, не доступных иным лицам.

2.2.8. Обеспечение соблюдения ограничений на использование личных средств связи, компьютеров, машинных носителей информации работниками структурных подразделений, указанными в подпункте 1.1.16 пункта 1.1 настоящих Методических рекомендаций, при осуществлении своих должностных обязанностей.

2.2.9. Проведение переговоров, в том числе переговоров с клиентами организации, в отдельных помещениях (комнатах переговоров), обеспечивающих исключение возможности неправомерного распространения информации о факте и содержании указанных переговоров, в случае наличия риска неправомерного использования инсайдерской информации.

2.2.10. Хранение документов, содержащих сведения, составляющие инсайдерскую информацию, в местах, доступ к которым ограничен (для документов на бумажном носителе, машинных носителях информации рекомендуется предусмотреть запираемые места (сейфы, шкафы, помещения и т.п.).

2.2.11. Обеспечение исключения конфликта интересов и получения согласия ОДЛ или иного уполномоченного лица, полученного в порядке и сроки, установленные порядком доступа к инсайдерской информации и правилами охраны ее конфиденциальности, при передаче (в случае возникновения такой необходимости) инсайдерской информации клиентов организации структурным подразделениям, совершающим операции в собственных интересах организации, а также лицам, принимающим решения о совершении таких операций, и лицам, осуществляющим предварительную оценку условий сделок, заключаемых организацией, в том числе на их соответствие требованиям законодательства Российской Федерации (если такая оценка осуществляется).

2.2.12. Обеспечение возможности передачи инсайдерской информации без согласия ОДЛ или иного уполномоченного лица в следующих случаях:

при передаче инсайдерской информации внутри рабочих (проектных) групп;

при передаче инсайдерской информации должностным лицам, определенным организацией;

При передаче инсайдерской информации, полученной рабочей (проектной) группой, лицам, в должностные обязанности которых не входит получение инсайдерской информации, а также при передаче инсайдерской информации рабочей (проектной) группе рекомендуется руководствоваться пунктом 2.2.11 настоящих Методических рекомендаций.

2.2.13. Доведение в уведомительном порядке до сведения ОДЛ или иного уполномоченного лица информацию о создании рабочей (проектной) группы, включая предмет и период деятельности, ее состав.

2.2.14. Определение должностных лиц, инсайдерская информация которым передается без согласия ОДЛ или иного уполномоченного лица, из числа работников осуществляющих следующие функции:

административно-распорядительные функции;

функции внутреннего контроля за деятельностью организации;

функции управления рисками организации;

функции внутреннего аудита организации;

функции правового сопровождения деятельности организации;

функции обеспечения информационной и экономической безопасности деятельности организации.

2.2.15. Обеспечение соблюдения запрета на совершение операций организацией в собственных интересах с финансовыми инструментами, входящими (эмитенты которых входят) в стоп-лист.

2.2.16. Обеспечение своевременного ознакомления работников организации и ее органов управления с порядком доступа к инсайдерской информации и правилами охраны ее конфиденциальности.

2.2.17. Регулярное обучение лиц, указанных в настоящих Методических рекомендациях, в целях повышения уровня их знаний в области обеспечения доступа, защиты и сохранности инсайдерской информации.

Глава 3. Заключительные положения.

Настоящие Методические рекомендации подлежат опубликованию в «Вестнике Банка России».

Первый заместитель
Председателя Банка России

С.А. Швецов