# Рекомендации по осуществлению контроля (приложение к Правилам охраны конфиденциальности инсайдерской информации)

Приложение N \_\_\_ к Правилам охраны
конфиденциальности инсайдерской информации
\_\_\_\_\_\_\_\_\_\_\_\_\_ "\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_"
(наименование юридического лица)
от "\_\_\_"\_\_\_\_\_\_\_ \_\_\_\_г.

### Рекомендации по осуществлению контроля

### 1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Рекомендации по контролю инсайдерской информации в \_\_\_\_\_\_\_\_"\_\_\_\_\_\_\_\_\_\_\_\_\_" (далее - ИИ и эмитент) разработаны на основании Федерального закона от 27.07.2010 N 224-ФЗ "О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации" и предназначены органам управления и отдельным сотрудникам, имеющим доступ к ИИ.

1.2. Меры по контролю включают организационные мероприятия и технические способы предупреждения, выявления, пресечения, недопущения в дальнейшем распространение или использования ИИ.

1.3. Вследствие того, что вся ИИ конфиденциальна, но не вся конфиденциальная информация является инсайдерской, часть мер по контролю ИИ принимается при сохранении сведений коммерческой, служебной, государственной (банковской) тайны, тайны связи (в части информации о почтовых переводах денежных средств) и иной охраняемой законом тайны и/или конфиденциальной информации.

1.4. Ответственность за распространение и/или использование ИИ определяется и действующим законодательством Российской Федерации.

### 2. ОРГАНИЗАЦИОННЫЕ МЕРЫ КОНТРОЛЯ

2.1. Организационные меры направлены на своевременное выявление и контроль областей возможного использования ИИ, потенциального конфликта интересов, систематическую проверку исполнения должностных обязанностей лицами, имеющими доступ к ИИ, а также иных сотрудников эмитента, с тем чтобы исключить возможность сокрытия ими противоправных действий.

2.2. Организационные меры включают:

- назначение лица, а при необходимости - структурного подразделения эмитента, ответственного за контроль ИИ;

- разработку и утверждение перечня ИИ;

- определение и постоянное уточнение круга лиц, имеющих доступ к ИИ;

- выработку модели правового поведения лиц, имеющих доступ к ИИ;

- утверждение политики информационной безопасности, включающей раздел относительно ИИ;

- систематизацию и доведение до лиц, имеющих доступ к ИИ, мер ответственности за распространение и/или использование ИИ;

- выработку комплекса организационных мер и технических способов контроля ИИ;

- обеспечение осуществления контроля ИИ.

2.3. Ответственное лицо и/или структурное подразделение (далее - контролер) назначается приказом руководителя эмитента. Требования к контролеру разрабатываются в отдельном локальном нормативном акте эмитента (положении, требованиях и т.п.). Полномочия, ответственность, обеспечение контролера устанавливаются приказом или распоряжением руководителя эмитента. Допускается совмещение функции контроля ИИ с выполнением иных должностных обязанностей. Служба контроля ИИ создана и действует в соответствии с положением о службе контроля ИИ эмитента.

2.4. Перечень ИИ разрабатывается и утверждается в соответствии с 224-ФЗ и внутренними документами эмитента. ИИ маркируется путем проставления на документе или ином носителе, содержащем ИИ, грифа "Коммерческая тайна", "Государственная тайна" и т.д. с указанием даты, фамилии и подписи лица, поставившего гриф. Перечень ИИ эмитента установлен Приложением N \_\_\_\_ к Правилам охраны конфиденциальности ИИ эмитента.

2.5. Круг лиц, имеющих доступ к ИИ, определяется и уточняется в соответствии с 224-ФЗ и внутренними документами эмитента. Список лиц, имеющих доступ к ИИ, установлен приложением к Правилам охраны конфиденциальности ИИ (или к Порядку доступа к ИИ) эмитента.

2.6. Каждое лицо, имеющее доступ к ИИ, под роспись предупреждается об ответственности за распространение и/или использование ИИ.

2.7. Модели правового поведения лиц, имеющих доступ к ИИ, вырабатываются назначенными руководителем эмитента лицами с участием юридической службы, иных структурных подразделений эмитента на основе 224-ФЗ с учетом особенностей деятельности эмитента.

2.8. Политика информационной безопасности разрабатывается на основе ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью (утв. Приказом Ростехрегулирования от 29.12.2005 N 447-ст).

2.9. Систематизацию мер ответственности за распространение и/или использование ИИ проводит и оформляет юридическая служба эмитента.

2.10. Комплекс организационных мер и технических способов контроля ИИ разрабатывается лицами, назначенными руководителем ИИ. Содержание такого комплекса является конфиденциальной информацией. В то же время отдельные его положения закрепляются в общедоступных учредительных и внутренних документах эмитента.

2.11. Осуществление контроля ИИ обеспечивается по смете, утвержденной руководителем эмитента по предложению контролера, согласованному с финансовой и учетной службами эмитента.

2.12. Наряду с указанными выше мерами контролер анализирует:

- состояние конъюнктуры рынков;

- деятельность контрагентов эмитента;

- деятельность руководства самого эмитента;

- изменение уровня доходов лиц и их взаимосвязанных лиц.

### 3. СПОСОБЫ ТЕХНИЧЕСКОГО КОНТРОЛЯ ИИ

3.1. Весь технический контроль проводится для достижения определенной уверенности в том, что аппаратные и программные средства были внедрены правильно, их функционирование обеспечивает безопасность ИИ.

3.2. Перечень способов технического контроля утверждается руководителем эмитента по предложению контролера, согласованному с отделом информационных технологий и службой безопасности. Такой перечень должен соответствовать политике информационной безопасности эмитента.

3.3. Контролер во взаимодействии с другими структурными подразделениями эмитента обеспечивает правильное выполнение всех процедур технического контроля ИИ в пределах их зоны ответственности. Любая техническая проверка должна выполняться только компетентными, авторизованными лицами либо под их наблюдением.

3.4. Контролер регулярно анализирует все сферы деятельности эмитента на предмет обеспечения требований безопасности ИИ.

3.5. С целью обеспечения соответствия систем технического контроля политике безопасности эмитента и стандартам способы технического контроля ИИ по мере необходимости пересматриваются.

3.6. Способы технического контроля включают:

проверка каналов связи на предмет обеспечения защиты передаваемой информации;

контроль процедур управления доступом, аутентификации взаимодействующих информационных систем и проверка подлинности пользователей и целостности передаваемых данных;

контроль обеспечения целостности;

обеспечение предотвращения возможности отрицания пользователем факта отправки персональных данных другому пользователю;

обеспечение предотвращения возможности отрицания пользователем факта получения персональных данных от другого пользователя;

регистрация и учет, документирование фактов несанкционированной передачи и/или получения ИИ;

защита инструментальных средств технического контроля.

### 4. РЕКОМЕНДАЦИИ ОРГАНАМ УПРАВЛЕНИЯ ОРГАНИЗАЦИИ

4.1. Руководители, должностные лица и сотрудники эмитента, участвующие в сборе, хранении, передаче и использовании ИИ, обязаны обеспечить исполнение законодательства Российской Федерации по защите информации (в том числе персональных данных).

4.2. Виновные в нарушении режима защиты информации несут гражданскую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

4.3. Контролер, наряду с изложенным выше:

- участвует в работе по обеспечению информационной безопасности исследований и разработок, соблюдению государственной тайны;

- осуществляет проверку технического состояния, установку, наладку и регулировку аппаратуры и приборов, их профилактические осмотры и текущий ремонт;

- выполняет работы по эксплуатации средств защиты и контроля информации, следит за работой аппаратуры и другого оборудования;

- ведет учет работ и объектов, подлежащих защите, установленных технических средств, журналы нарушений их работы, справочники;

- готовит технические средства для проведения всех видов плановых и внеплановых контрольных проверок, аттестации оборудования, а также в случае необходимости к сдаче в ремонт;

- проводит наблюдения, выполняет работу по оформлению протоколов специальных измерений и другой технической документации, в том числе отчетной, связанной с эксплуатацией средств и контролем информации;

- выполняет необходимые расчеты, анализирует и обобщает результаты, составляет отчеты и оперативные сведения;

- определяет причины отказов в работе технических средств, готовит предложения по их устранению и предупреждению, обеспечению высокого качества и надежности используемого оборудования, повышению эффективности мероприятий по контролю и защите информации;

- участвует во внедрении разработанных технических решений и проектов, оказании технической помощи при изготовлении, монтаже, наладке, испытаниях и эксплуатации проектируемой аппаратуры.

4.4. Отдельные контрольные мероприятия осуществляются органами управления путем запросов отчетов и информации о деятельности структурных подразделений, контрагентов эмитентов, независимых лиц, а также разъяснений экспертов в целях выявления недостатков контроля, нарушений, ошибок, преднамеренного искажения.

4.5. При контроле ИИ особое внимание уделяется проверкам функционирования систем согласования (утверждения) операций (сделок) и распределения полномочий при совершении финансово-хозяйственных операций и других сделок, превышающих установленные лимиты и предусматривающих информирование соответствующих руководителей эмитента (его подразделений).

### 5. РЕКОМЕНДАЦИИ СОТРУДНИКАМ ОРГАНИЗАЦИИ

5.1. Лицам, имеющим или получившим доступ к ИИ, рекомендуется:

1) выполнять установленный эмитентом режим конфиденциальности;

2) принять исчерпывающие меры по сохранению ИИ иными лицами;

3) не предоставлять и не распространять ИИ, информацию, составляющую коммерческую тайну, обладателями которой являются эмитент и его контрагенты, и без их согласия не использовать эту информацию;

4) при утрате статуса лица, имеющего доступ к ИИ, передать эмитенту имеющиеся во владении материальные носители информации, содержащие ИИ;

5) немедленно сообщать своему непосредственному руководителю или лицу, его замещающему, об утрате или недостаче документов, файлов, содержащих конфиденциальную информацию, ключей от сейфов (хранилища), печатей, удостоверений, пропусков, паролей или об обнаружении несанкционированного доступа к ИИ и т.п.

5.2. Лица, по статусу не имеющие доступа к ИИ, но получившие к ней доступ, обязаны:

1) прекратить ознакомление с ней;

2) принять исчерпывающие меры по сохранению конфиденциальности такой ИИ;

3) исключить распространение или предоставление такой ИИ;

4) немедленно доложить непосредственному руководителю о произошедшем ознакомлении с ИИ;

5) действовать в соответствии с указаниями контролера.

Источник - Кабанов О.М.

Сохраните в закладки наш сайт: [Порядокправа.рф](https://порядокправа.рф)

Прямая ссылка на документ: [https://порядокправа.рф/obrazecy/rekomendacii\_po\_osushhestvleniyu\_kontrolya\_prilozhenie\_k\_pravilam\_oxrany\_konfidencialnosti\_insajderskoj.htm](https://порядокправа.рф/rekomendacii_po_osushhestvleniyu_kontrolya_prilozhenie_k_pravilam_oxrany_konfidencialnosti_insajderskoj.htm)