Утвержден
решением Совета СРО НАСФП
Протокол №70 от 24 декабря 2025 г.

КОДЕКС ЭТИКИ
В СФЕРЕ ПРИМЕНЕНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА
НА РЫНКЕ ФИНАНСОВОГО КОНСАЛТИНГА

Москва, 2025

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Целями настоящего Кодекса являются:

1) повышение доверия физических и юридических лиц (далее – клиенты) к индустрии финансового консалтинга, в том числе при использовании членами СРО НАСФП искусственного интеллекта (далее – ИИ) при оказании клиентам услуг;

2) минимизация рисков, связанных с использованием членами СРО НАСФП искусственного интеллекта (далее – риски искусственного интеллекта).

3) минимизация рисков, возникающих вследствие цифровых атак и несанкционированного доступа к данным

1.2. В тексте настоящего Кодекса под понятием «искусственный интеллект» подразумевается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые с результатами интеллектуальной деятельности человека или превосходящие их. Указанный комплекс технологических решений включает в себя информационно-коммуникационную инфраструктуру, программное обеспечение (в том числе в котором используются методы машинного обучения и нейронные сети), процессы и сервисы по обработке данных и поиску решений;

1.3. Для достижения указанных целей при использовании искусственного интеллекта членам СРО НАСФП рекомендуется соблюдать следующие принципы:

1) принцип приоритета интересов клиента над интересами советника

2) принцип прозрачности;

3) принципы безопасности, надежности и эффективности;

4) принцип ответственного управления рисками.

1.4. Членам СРО НАСФП рекомендуется обмениваться опытом, а также участвовать в разработке совместных документов и аналитических материалов, содействующих достижению целей настоящего Кодекса.

1.5. В случае привлечения членами СРО НАСФП для работ, связанных с использованием искусственного интеллекта, третьих лиц, членам СРО НАСФП рекомендуется обеспечивать соблюдение такими лицами положений настоящего Кодекса. Также рекомендуется тестировать полученные результаты с привлечением других членов СРО НАСФП.

1.6. В настоящем Кодексе используются следующие термины:

- Большие генеративные модели – модели искусственного интеллекта, способные создавать текст, изображения, аудиоматериалы и другие данные на основе обучающих выборок.

- Данные ограниченного доступа – персональные данные и иная конфиденциальная информация, раскрытие которой может нанести ущерб клиенту или члену СРО НАСФП.

2. ПРИНЦИП ПРОЗРАЧНОСТИ

2.1. членам СРО НАСФП рекомендуется:

1) информировать клиентов о применении искусственного интеллекта при оказании консалтинговых услуг;

2) раскрывать информацию о том, какой именно ИИ используется при оказании консалтинговых услуг;

3) маркировать информацию, созданную с применением больших генеративных моделей, в том числе изображения, аудио- и видеоматериалы, за исключением следующих случаев:

- большие генеративные модели применяются только для редактирования информации, в процессе которого не происходит существенного изменения содержания указанной информации;

- применение больших генеративных моделей очевидно из обстоятельств;

- отсутствует риск причинения вреда клиентам.

2.2. В рамках раскрытия информации об искусственном интеллекте членам СРО НАСФП рекомендуется предоставлять клиентам полную и достоверную информацию о рисках использования ИИ и способах применения членом СРО НАСФП искусственного интеллекта.

2.3. Членам СРО НАСФП рекомендуется объяснять клиентам:

- какие задачи выполняет искусственный интеллект в рамках оказания услуги (формирует основные элементы результата, проверяет и анализирует данные или иное);

- какие ограничения, возможные ошибки и риски связаны с использованием ИИ;

- какие данные используются в работе ИИ, и почему использование этих данных необходимо;

3. ПРИНЦИП приоритета интересов клиента над интересами советника:

3.1. Членам СРО НАСФП рекомендуется руководствоваться следующим:

1) использование ИИ должно вести к повышению качества оказания услуг. В целях повышения качества услуг членам СРО НАСФП рекомендуется осуществлять оценку удовлетворенности клиентов, которым оказаны услуги с применением ИИ, а также осуществлять контроль качества оказания таких услуг;

2) у клиентов должна оставаться возможность отказаться от оказания услуг с применением искусственного интеллекта. Членам СРО НАСФП рекомендуется предоставлять клиентам возможность получить услугу без использования ИИ;

3) клиенты должны иметь возможность пересмотра решений, принятых с применением искусственного интеллекта;

4) следует прилагать усилия для повышения осведомленности клиентов о принятии решений

с применением искусственного интеллекта. Членам СРО НАСФП рекомендуется разъяснять каким образом ИИ помогает вырабатывать решения, предлагаемые клиенту, а также разъяснять какие конкретно данные нужны ИИ для выработки этих решений;

5) Искусственный интеллект не может быть единственным источником рекомендаций или выводов, имеющих существенное значение.

3.2. Искусственный интеллект не должен использоваться для:

- манипулирования клиентом или навязывания ему услуг;

- ограничения выбора клиента;

- дискриминации клиентов по любым признакам.

4. ПРИНЦИП Конфиденциальности и объективности

4.1. Членам СРО НАСФП при работе с ИИ использовать персональные данные клиентов только в случаях, когда их использование требуется для существенного повышения эффективности применения искусственного интеллекта при оказании услуг. При этом клиент должен дать явное согласие на использование его персональных данных для работы с ИИ. Под персональными данными в данном случае понимаются любые данные, которые позволяют идентифицировать клиента, в том числе средствами анализа больших данных.

5. ПРИНЦИП БЕЗОПАСНОСТИ, НАДЕЖНОСТИ И ЭФФЕКТИВНОСТИ

5.1. Членам СРО НАСФП рекомендуется принимать следующие меры:

1) проверка качества искусственного интеллекта. Членам СРО НАСФП рекомендуется установить показатели качества работы искусственного интеллекта и проверять при использовании ИИ соответствие результатов, полученных с использованием ИИ, установленным организацией показателям качества, в том числе посредством валидации, добровольной сертификации;

2) мониторинг качества искусственного интеллекта. Членам СРО НАСФП рекомендуется регулярно осуществлять проверку результатов, полученных с применением ИИ, на предмет соответствия установленным членом СРО НАСФП показателям качества, включая выявление ухудшения показателей (model drift) и иных отклонений;

3) обеспечение информационной безопасности. СРО НАСФП рекомендуется учитывать риски, возникающие при использовании ИИ, связанные с нарушением информационной безопасности, и осуществлять оценку достаточности имеющихся и планируемых к реализации мер противодействия угрозам информационной безопасности при применении ИИ;

4) обеспечение конфиденциальности информации. Членам СРО НАСФП рекомендуется разработать систему технологических и организационных мер по обеспечению безопасности данных ограниченного доступа, используемых при применении

искусственного интеллекта, в том числе меры, связанные с обезличиванием таких данных и противодействием их несанкционированному распространению при применении больших генеративных моделей членом СРО НАСФП и его сотрудниками, а также и его клиентами;

5) проверка качества наборов данных. Членам СРО НАСФП рекомендуется проверять используемые и получаемые от ИИ наборы данных, в том числе на предмет их достоверности, точности и полноты, собирать и хранить информацию об источниках наборов данных, исправлять неточности в наборах данных и осуществлять их актуализацию.

6) назначение сотрудника, несущего ответственность за качество и корректность рекомендаций, подготовленных с помощью ИИ.

6. ПРИНЦИП ОТВЕТСТВЕННОГО УПРАВЛЕНИЯ РИСКАМИ

6.1. Членам СРО НАСФП рекомендуется организовать и осуществлять управление рисками при применении искусственного интеллекта.

6.2. Членам СРО НАСФП рекомендуется при управлении рисками при применении искусственного интеллекта обеспечить следующие процессы:

1) выявление рисков искусственного интеллекта;

2) оценка и присвоение уровня риска искусственного интеллекта;

3) мониторинг и контроль рисков искусственного интеллекта;

4) минимизация выявленных рисков искусственного интеллекта;

5) реагирование на реализовавшиеся риски искусственного интеллекта (далее – риск-события);

6) ведение базы риск-событий.

6.3. Членам СРО НАСФП рекомендуется документировать информацию о процессе и результатах применения искусственного интеллекта, о лицах, ответственных за применение искусственного интеллекта, а также анализировать указанную информацию на предмет наличия рисков, связанных с применением ИИ.

6.4.Членам СРО НАСФП рекомендуется сформировать систему факторов риска и уровней риска, присваивать уровни риска различным способам применения ИИ с учетом установленных факторов риска.

При присвоении уровня риска, возникающего при применении ИИ, рекомендуется учитывать следующие факторы риска:

1) сфера применения искусственного интеллекта (например, применение искусственного интеллекта при оказании услуг клиентам, в системах управления рисками, при управлении активами);

2) использование при применении ИИ данных ограниченного доступа;

3) размер убытков или ущерб деловой репутации, которые могут быть причинены организации в случае реализации риска;

4) количество клиентов, при оказании услуг которым применяется искусственный интеллект;

5) объяснимость решений, принимаемых с использованием ИИ;

6) использование наборов данных, полученных от третьих лиц, или наборов данных, находящихся в открытом доступе в информационно-телекоммуникационной сети «Интернет»;

7) наличие реализовавшихся риск-событий, связанных с применением ИИ;

8) возможность отказа от используемого сервиса без потери данных.

6.5. Членам СРО НАСФП рекомендуется регулярно проверять процессы, связанные с применением искусственного интеллекта на предмет наличия рисков, а также осуществлять предварительный, текущий, последующий контроль рисков с учетом специфики конкретного случая применения искусственного интеллекта.

6.6. Членам СРО НАСФП рекомендуется определять меры, направленные на снижение уровня риска, связанного с применением ИИ, а также обеспечивать контроль за процессами применения ИИ, которым присвоен высокий уровень риска.

6.7. Членам СРО НАСФП рекомендуется определять типы риск-событий и принимать меры, направленные на минимизацию последствий риск-событий, а также обеспечить своим сотрудникам и клиентам возможность направления жалоб и сообщений о риск-событиях.

6.8. Членам СРО НАСФП рекомендуется выявлять риск-события и осуществлять их регистрацию с описанием риск-события, обстоятельств, повлекших наступление риск-события, а также приведением сведений о мероприятиях, направленных на минимизацию последствий риск-события, и статусе исполнения таких мероприятий.

6.9. Член СРО НАСФП, узнавший об уязвимости используемого им программного обеспечения, должен принять меры по скоординированному раскрытию уязвимости, сотрудничая с заинтересованными сторонами, чтобы устранить уязвимость безопасности и минимизировать вред, связанный с раскрытием конфиденциальной информации. Заинтересованные стороны включают производителя программного обеспечения, иных поставщиков программных решений, партнеров члена СРО НАСФП и иных пользователей указанного программного обеспечения.

6.10. К основным рискам, связанным с использованием ИИ, относятся:

1) предоставление клиенту некорректных или искажённых рекомендаций;

2) использование при выработке решений и рекомендаций некачественных или устаревших данных;

3) риск утечки информации;

4) риск возникновения чрезмерной зависимости от автоматизированных решений.

7. Кодекс этики в сфере предупреждения несанкционированного доступа к данным.

7.1. Хранение и передача конфиденциальной информации

7.1.1. Все устройства (а также облачные хранилища, почтовые аккаунты, аккаунты в мессенджерах), на которых хранятся конфиденциальные данные, должны быть защищены паролем. Замена пароля должна производиться не реже, чем один раз в год.

7.1.2. Пароли к устройствам, указанным в п.7.1.1. не должны храниться на самих устройствах.

7.1.3. Членам СРО НАСФП рекомендуется применять двухфакторную аутентификацию везде, где это возможно.

7.1.4. Членам СРО НАСФП рекомендуется обеспечивать регулярное резервное копирование данных с отдельным хранением резервных копий на внешних носителях.

7.1.5. Рекомендуется защищать устройства, указанные в п.7.1.1. антивирусным программным обеспечением с регулярным обновлением указанного программного обеспечения.

7.1.6. Членам СРО НАСФП не рекомендуется подключать к сети Интернет устройства, указанные в п.7.1.1., через виртуальные частные сети (VPN), кроме сетей напрямую принадлежащих члену СРО НАСФП. Также не рекомендуется передавать посредством виртуальных частных сетей (VPN) персональные данные клиентов и иную конфиденциальную информацию в незашифрованном виде.

7.1.7. Членам СРО НАСФП рекомендуется воздерживаться от передачи персональных данных клиентов или иной конфиденциальной информации посредством доступа в сеть Интернет с использованием публичных каналов Wi-Fi (публичные сети Wi-Fi в кафе, библиотеках, транспорте и т.д.).

7.1.8. Членам СРО НАСФП рекомендуется воздерживаться от передачи персональных данных клиентов или иной конфиденциальной информации (данные о личных финансах, платежная информация, сведения о счетах и вкладах и т.д.) посредством программ мгновенного обмена сообщениями через сеть Интернет (мессенджеры), особенно принадлежащих зарубежным компаниям.

7.1.9. Членам СРО НАСФП рекомендуется изучать информацию о передаче и хранении данных в используемых ими программах мгновенного обмена сообщениями через сеть Интернет (мессенджерах). В случае, если у члена СРО НАСФП нет уверенности в безопасности передачи и хранения данных в указанных программах, рекомендуется в явном виде согласовать с клиентом возможность передачи данных посредством указанных программ.

7.1.10. Персональные данные клиентов и иная конфиденциальная информация может храниться с использованием облачных решений исключительно российских компаний с размещением серверов на территории Российской Федерации.

7.2. Обезличивание данных клиентов.

7.2.1. Членам СРО НАСФП рекомендуется запрашивать и использовать данные клиентов исключительно в необходимом для оказания услуг объеме.

7.2.2. Членам СРО НАСФП рекомендуется обезличивать данные клиентов в случаях, когда нет прямой необходимости в использовании исходных персональных данных.

7.2.3. Обезличивание персональных данных должно быть выполнено таким образом, чтобы было невозможно восстановить личность субъекта персональных данных без дополнительной информации, но с сохранением применимости данных для обработки (например, в статистических целях)

7.2.4. Исходный массив персональных данных и обезличенный набор данных должны храниться отдельно друг от друга для предотвращения возможности сопоставления и восстановления исходных данных.

7.2.5. Членам СРО НАСФП рекомендуется выбирать методы обезличивания персональных данных, которые подходят для конкретных целей обработки данных и обеспечивают надежное сокрытие личности. Например:

- Псевдонимизация: Замена идентификаторов на уникальные коды, при этом таблица соответствия хранится отдельно и в секрете.

- Обобщение: Изменение состава данных, например, замена точной даты рождения на год рождения или точной суммы дохода на диапазон.

- Декомпозиция: Разбиение данных на части и хранение их раздельно (например, имена в одной базе, контакты в другой, связанные через ID).

7.2.6. Простое удаление части данных без комплексного подхода не является надлежащим обезличиванием персональных данных в случае, если личность все еще можно установить по оставшимся деталям.

7.3. Членам СРО НАСФП рекомендуется обучать сотрудников правилам безопасного и корректного использования ИИ и правилам предупреждения несанкционированного доступа к данным, включая:

1) правила работы с конфиденциальной информацией и правила передачи данных в публичные системы, работающие на основе различных моделей ИИ;

2) обучение принципам функционирования ИИ с обязательным акцентом на понимание ограничений ИИ и возможных ошибок, возникающих при работе с использованием ИИ;

3) порядок действий при выявлении инцидентов, связанных с ИИ и с несанкционированным доступом к данным.