**Политика использования искусственного интеллекта**

**Последнее обновление:** *Обновлено в январе 2024 года*

**Отказ от свободного использования:** *Эта политика была создана Институтом SANS для интернет-сообщества. Все или отдельные части этой политики могут быть свободно использованы в вашей организации. Предварительное разрешение не требуется. Если вы хотите предложить новую или обновленную версию этой политики, пожалуйста, отправьте письмо по адресу policy-resources@sans.org.*

**ПОЛИТИКА ИСПОЛЬЗОВАНИЯ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

**I. Введение**.

YourCompanyName обязуется полностью соблюдать действующее законодательство, связанное с использованием искусственного интеллекта в странах, в которых YourCompanyName предоставляет продукты и услуги. Кроме того, YourCompanyName стремится к этичному использованию искусственного интеллекта. Настоящая Политика использования искусственного интеллекта ("Политика") описывает требования YourCompanyName в отношении использования всех форм искусственного интеллекта в YourCompanyName. Такое применение искусственного интеллекта включает в себя использование для повышения эффективности бизнеса, операций и включения в продукты и услуги YourCompanyName.

Эта политика распространяется на всех директоров, должностных лиц, членов совета директоров, сотрудников, подрядчиков, представителей, аффилированных лиц, агентов и любых физических или юридических лиц, выполняющих услуги для или от имени YourCompanyName. Ответственный сотрудник компании YourCompanyName отвечает за соблюдение данной Политики.

**II. Определения**.

"Искусственный интеллект" или "ИИ" означает использование технологий машинного обучения, программного обеспечения, автоматизации и алгоритмов для выполнения задач и составления правил или прогнозов на основе имеющихся наборов данных и инструкций.

"Комитет по искусственному интеллекту" или "Комитет по ИИ" - это внутренний комитет компании YourCompanyName, которому поручено рассматривать и утверждать использование ИИ в компании YourCompanyName.

"Система искусственного интеллекта" или "система ИИ" означает программное обеспечение, разработанное с использованием одного или нескольких методов и подходов, перечисленных в Приложении I, и способное для заданного набора целей, определяемых человеком, генерировать выходные данные, такие как контент, прогнозы, рекомендации или решения, влияющие на среду, с которой они взаимодействуют.

"Закрытая система ИИ" означает систему ИИ, в которой для обучения модели ИИ используются данные, предоставленные одним пользователем. Входные данные пользователя изолированы от других пользователей, и такие данные считаются более безопасными.

"Встроенные инструменты ИИ" означают инструменты ИИ, встроенные в существующие программные средства, одобренные и используемые в компании YourCompanyName, и не требующие одобрения Комитета по ИИ для использования.

"Правительство" означает правительство страны или его подразделение.

"Государственная организация" означает любую организацию, полностью или частично контролируемую правительством. Сюда входят принадлежащие правительству или контролируемые им (полностью или частично) коммерческие предприятия, учреждения, агентства, департаменты, ведомства и другие государственные организации, включая научно-исследовательские институты и университеты.

"Государственное должностное лицо" означает любое должностное лицо или сотрудника государственной организации, должностное лицо политической партии, кандидата на политическую должность, должностных лиц и сотрудников неправительственных международных организаций, а также любое лицо, имеющее полномочия распределять государственные средства или влиять на их расходование. Сюда входят специалисты по изучению данных и исследователи, работающие в правительстве или государственной организации. Сотрудники государственных организаций считаются государственными служащими независимо от титула или должности.

"Непубличные данные YourCompanyName" означает любую информацию, которая в случае раскрытия может нарушить неприкосновенность частной жизни, правительственные постановления или законы, поставить под угрозу финансовое положение YourCompanyName, нанести ущерб ее репутации или снизить ее конкурентные преимущества.

"Открытая система ИИ" означает систему ИИ, в которой для обучения модели ИИ используются входные данные, предоставляемые всеми пользователями. Входные данные от всех пользователей не являются закрытыми и могут быть открыты другим пользователям.

"Личная информация" означает информацию, которая идентифицирует, относится к, описывает, может быть связана или может быть обоснованно связана, прямо или косвенно, с конкретным человеком или семьей.

"Представители YourCompanyName" означает всех директоров, должностных лиц, членов правления, сотрудников, подрядчиков, представителей, торговых посредников и субторговцев, дистрибьюторов и субдистрибьюторов, филиалов, агентов, а также любых физических или юридических лиц, выполняющих услуги для YourCompanyName или от ее имени.

**III. Руководящие принципы.**

Цель данной политики - предоставить общие рекомендации по использованию искусственного интеллекта в YourCompanyName, чтобы YourCompanyName могла использовать его в качестве инструмента, обеспечивая при этом выполнение юридических обязательств и соблюдение этических норм. Использование искусственного интеллекта в компании YourCompanyName не должно наносить ущерб основным ценностям YourCompanyName или создавать неоправданный риск для организации. Напротив, использование ИИ в YourCompanyName должно быть направлено на повышение эффективности бизнеса и расширение возможностей YourCompanyName по выполнению своей миссии.

Важно помнить, что YourCompanyName - это глобальная организация. YourCompanyName имеет подразделения и сотрудников по всему миру и предоставляет свои продукты и услуги клиентам также по всему миру. Соответственно, данная политика представляет собой общее руководство, основанное на глобальных стандартах использования ИИ. Представителям YourCompanyName при использовании искусственного интеллекта в YourCompanyName следует подумать о глобальном влиянии их решения об использовании искусственного интеллекта, поскольку использование искусственного интеллекта в одних странах может быть не разрешено в других.

Эта политика не предназначена для рассмотрения всех случаев использования искусственного интеллекта в YourCompanyName представителем YourCompanyName. Существуют определенные подразделения и функции YourCompanyName, которые требуют более внимательного отношения и потенциальных рисков. Прежде чем использовать любой ИИ в YourCompanyName - будь то для решения личных задач, таких как написание электронного письма, или для более сложных бизнес-процессов, таких как анализ массивов данных, - вам следует проконсультироваться с руководителем и получить рекомендации. Кроме того, см. раздел "Запрещенные виды использования" в разделе IV ниже о ситуациях, в которых ИИ не может использоваться в YourCompanyName, и раздел "Использование систем ИИ с высоким риском" в разделе VI ниже о ситуациях, в которых необходимо проявлять особую осторожность при использовании ИИ.

Кроме того, существуют определенные встроенные средства искусственного интеллекта, используемые в существующем утвержденном программном обеспечении YourCompanyName, которые не требуют дополнительного одобрения для использования. Например, использование Microsoft Word, в который встроен инструмент искусственного интеллекта для проверки орфографии или грамматики. Использование встроенных средств искусственного интеллекта в утвержденном программном обеспечении YourCompanyName разрешено при условии, что эти программные средства соответствуют предыдущему общему использованию в бизнесе. Список существующих программных средств со встроенными средствами искусственного интеллекта, одобренных в YourCompanyName, можно найти здесь [ВСТАВЬТЕ ССЫЛКУ].

При использовании программного обеспечения, услуг или подрядчиков третьих сторон, любое использование ИИ в программном обеспечении, используемом этими сторонами или услугами, должно быть отмечено и тщательно оценено. Услуги по контракту, в которых используются технологии ИИ, должны рассматриваться в том же свете, что и использование ИИ отдельными лицами. Проконсультируйтесь с юридическим отделом о включении в соглашения с поставщиками или подрядчиками пункта, касающегося ИИ.

При рассмотрении возможности использования системы искусственного интеллекта в компании YourCompanyName необходимо придерживаться следующих принципов:

* Использование системы искусственного интеллекта должно быть направлено в первую очередь на выполнение задач отдела по указанию руководства компании. За исключением использования встроенного инструмента ИИ в программной системе, одобренной для использования в YourCompanyName, любое использование новой системы ИИ в YourCompanyName должно быть одобрено Комитетом по ИИ. Процесс получения одобрения системы ИИ см. в Стандартной операционной процедуре [ВСТАВЬТЕ ССЫЛКУ]. Также смотрите Общие стандарты использования ИИ и утверждение использования в разделе IV ниже.
* Лица, использующие систему ИИ, должны обладать знаниями в той области, для которой используется ИИ. ИИ должен использоваться как инструмент и не заменять собой знания. Например, если ИИ используется для кодирования, человек, внедряющий ИИ, должен обладать знаниями в области кодирования.
* Весь контент, созданный ИИ (тексты, наборы данных, графики, изображения и т. д.), должен быть тщательно проверен человеком, обладающим опытом оценки такого контента на предмет точности, а также общей корректуры и редактирования. Контент, созданный искусственным интеллектом, следует рассматривать как отправную точку, а не как готовый продукт. Как и любой другой контент на YourCompanyName, созданный искусственным интеллектом контент должен соответствовать внешнему виду бренда YourCompanyName.
* Любое использование системы искусственного интеллекта должно иметь четкие цели применения ИИ в качестве инструмента и приемлемые для бизнеса наборы данных, из которых ИИ черпает информацию. Если наборы данных, которые использует ИИ, не точны, то и информация, которую предоставляет ИИ, не будет точной.
* Системы искусственного интеллекта обучаются на данных, которые могут содержать предвзятость. Пользователи этих систем несут ответственность за проверку любого контента, созданного ИИ, на предмет предвзятости и его исправление в случае необходимости.
* Непубличная информация YourCompanyName никогда не должна попадать в открытую систему искусственного интеллекта.
* Представители компании YourCompanyName должны документировать все системы искусственного интеллекта, которые они используют и для каких функций. Отслеживание использования ИИ не является факультативным и входит в ваши обязанности. Документирование конкретных встроенных средств искусственного интеллекта в утвержденном существующем программном обеспечении при использовании этого средства по назначению не требуется. Обсудите процесс отслеживания использования систем искусственного интеллекта с руководителем отдела.
* Использование системы искусственного интеллекта должно быть задокументировано, чтобы зафиксировать институциональные знания. Например, если ИИ используется для создания кода и включается в более крупный раздел кода, должна быть документация о том, какой раздел кода был создан на основе ИИ и кто его рассматривал.
* Использование системы искусственного интеллекта должно соответствовать любым условиям использования или договорным ограничениям. Договорные ограничения или условия использования могут ограничить использование системой искусственного интеллекта компанией YourCompanyName, которое в противном случае было бы юридически корректным и этически обоснованным. Например, условия использования системы искусственного интеллекта могут требовать использования определенных отказов от ответственности в определенных ситуациях или запрещать использование системы искусственного интеллекта для выполнения определенных задач. Представителям YourCompanyName следует, чтобы все условия использования или контракты на использование систем искусственного интеллекта рассматривались юридическим отделом для обеспечения соблюдения договорных обязательств при использовании системы искусственного интеллекта.
* Утверждение системы искусственного интеллекта не отменяет необходимости других внутренних согласований, необходимых в YourCompanyName для использования технологий, таких как проверка безопасности, проверка конфиденциальности, проверка затрат и утверждение расходов, юридическая проверка, проверка кадровых ресурсов и т. д. Система искусственного интеллекта должна проходить тот же процесс проверки и утверждения, что и другое программное обеспечение или услуги в YourCompanyName. Кроме того, вы должны убедиться, что руководитель вашего подразделения осведомлен об использовании системы искусственного интеллекта и одобрил любое ее использование, особенно в отношении генерируемого искусственным интеллектом контента, который будет передаваться вовне.

**IV. Запрещенные виды использования**.

Существуют определенные виды использования ИИ, которые запрещены. Если иное не одобрено комитетом по ИИ и руководителями соответствующих отделов, представителям YourCompanyName запрещено использовать системы ИИ для любых из следующих действий в любое время:

* Проведение политических лоббистских мероприятий запрещено. Под лоббированием понимается любое действие, направленное на оказание влияния на правительство, правительственное должностное лицо или государственную организацию по любой причине.
* Использование систем искусственного интеллекта для идентификации или категоризации студентов, кандидатов, сотрудников, подрядчиков или других аффилированных лиц на основе статуса защищенного класса запрещено.
* Вносить в открытую систему искусственного интеллекта коммерческие тайны, конфиденциальную информацию или персональные данные о любом человеке.
* Ввод любой конфиденциальной информации о человеке в любую систему искусственного интеллекта. К "конфиденциальной информации" относятся медицинские, финансовые, политические, расовые или этнические данные, религиозные убеждения, пол, сексуальная ориентация, статус инвалида или любая другая часть жизни человека, которую человек хотел бы сохранить в тайне.
* Использование системы искусственного интеллекта для получения юридических консультаций, включая, в частности, создание политик для внутреннего использования или для предоставления третьим лицам.
* Создание интеллектуальной собственности, которую YourCompanyName желает зарегистрировать и/или которая имеет значительную ценность для организации.

**V. Этические принципы.**

YourCompanyName желает действовать этично при использовании ИИ. Соответственно, могут быть случаи использования ИИ, которые допустимы с юридической точки зрения, но не отвечают этическим требованиям. Любое использование системы искусственного интеллекта в компании YourCompanyName должно соответствовать следующим этическим принципам:

* **Информированное согласие:** Перед вводом личной информации в закрытую систему искусственного интеллекта убедитесь, что вы получили информированное согласие от человека (людей), чья личная информация будет вводиться.
* **Честность в использовании**: Все пользователи систем ИИ должны честно рассказывать о том, как ИИ помог выполнить работу. Даже если вы используете систему ИИ, одобренную Комитетом по ИИ для разрешенного использования, вы должны убедиться, что ваш руководитель или отдел, запрашивающий задание, для которого вы используете систему ИИ, знает о вашем использовании системы ИИ. Не выдавайте работу, сгенерированную ИИ, за выполненную исключительно вами. Кроме того, если вы хотите использовать инструмент системы искусственного интеллекта для выполнения задания, вам следует спросить разрешения. Например, вам следует спросить у своего руководителя и представителя отдела кадров, можно ли использовать систему искусственного интеллекта для составления оценки работы.
* **Соответствующий контент**: Не используйте время или ресурсы компании для создания с помощью системы искусственного интеллекта контента, который будет считаться незаконным, неуместным, вредным для бренда или репутации YourCompanyName или неуважительным по отношению к другим.
* **Несанкционированное использование:** Не используйте время или ресурсы компании для создания контента с помощью системы искусственного интеллекта в личных целях без предварительного разрешения руководителя соответствующего отдела.

**VI. Использование систем искусственного интеллекта с высокой степенью риска.**

Некоторые виды использования систем искусственного интеллекта связаны с большим риском, чем другие. Будучи международной компанией, YourCompanyName обязуется соблюдать все законодательные требования и рекомендации по ИИ в странах, в которых она работает. Европейский союз ("ЕС") классифицировал следующие потенциальные виды использования ИИ как представляющие высокий риск для здоровья и безопасности или основных прав физических лиц. Поэтому к использованию систем искусственного интеллекта в таких случаях предъявляется ряд дополнительных требований. Эти требования перечислены в Приложении II, а некоторые функции выделены ниже:

* **Персональные данные в системах ИИ:** ИИ следует использовать с особой осторожностью при вводе любых личных данных человека в закрытую систему ИИ (запрещено вводить любые личные данные в открытую систему ИИ).
* **Отбор кандидатов на работу:** ИИ следует использовать с осторожностью при отборе кандидатов на работу, чтобы убедиться, что он не оказывает негативного воздействия на представителей защищенных классов и не вносит предвзятости. Вопросы равенства и инклюзивности, связанные с использованием ИИ при отборе кандидатов на работу, являются потенциальным источником судебных разбирательств.
* **Кадровые решения:** ИИ следует использовать с осторожностью при принятии решений о повышении, удержании или аналогичных кадровых решений. Следует проявлять крайнюю осторожность, чтобы не допустить предвзятости (в том числе предвзятости, содержащейся в существующих наборах данных).
* **Решения о зачислении:** Следует проявлять крайнюю осторожность при использовании искусственного интеллекта для оценки потенциальных кандидатов на поступление в университет, академию, программу стажировки или ученичества или любую другую программу YourCompanyName.
* **Оценка учащихся:** Любая оценка учащихся в учебных заведениях или учреждениях профессионального образования считается высокорискованной. Соответственно, следует проявлять крайнюю осторожность при использовании любой системы искусственного интеллекта, предназначенной для оценки или анализа любого студента, участвующего в курсе, сдающего экзамен или другой анализ или оценку.

1. **Общие стандарты использования системы ИИ и разрешение на использование**

За исключением встроенных средств ИИ в утвержденное программное обеспечение, все виды использования систем ИИ должны быть одобрены Комитетом по ИИ до начала использования, чтобы убедиться, что использование системы ИИ соответствует следующим принципам:

* **Законно:** Использование систем искусственного интеллекта должно соответствовать всем применимым законам и нормам, а также любым договорным обязательствам, ограничениям и запретам.
* **Этика:** использование систем искусственного интеллекта должно соответствовать этическим принципам, быть справедливым и не допускать предвзятости.
* **Прозрачность:** должны существовать четкие цели использования системы ИИ и документированный надзор за таким использованием, который фиксируется и сохраняется для институциональных знаний. Информация об использовании ИИ при создании контента с помощью ИИ должна быть раскрыта, если этого требует закон или контракт, или если этого требует YourCompanyName.
* **Необходимость:** Использование систем искусственного интеллекта должно преследовать действительные деловые цели, направленные на повышение эффективности бизнеса YourCompanyName и поддержку миссии организации. Использование искусственного интеллекта не заменяет критическое мышление или опыт человека и не должно требовать от YourCompanyName ненужных расходов без какой-либо реальной выгоды.

Прежде чем направить в Комитет по искусственному интеллекту запрос на использование системы искусственного интеллекта, заявитель должен сначала получить одобрение своего руководителя. Кроме того, при рассмотрении вопроса о том, стоит ли подавать запрос, заявитель должен убедиться, что использование системы искусственного интеллекта, если оно будет одобрено, будет соответствовать руководящим принципам данной политики, прежде чем подавать такой запрос. Запросы на использование системы искусственного интеллекта должны соответствовать СОП (стандартная операционная процедура), приведенной здесь [ВСТАВЬТЕ ССЫЛКУ].

1. **Обучение**

Все представители YourCompanyName, взаимодействующие с системами искусственного интеллекта, должны пройти обучение по данной Политике. Кроме того, отдельным отделам или функциям YourCompanyName может потребоваться более специальное обучение по использованию систем искусственного интеллекта для их отдела или функции в случае повышенного риска.

**IX. Сообщение о несоблюдении**.

Директора, менеджеры, сотрудники и агенты YourCompanyName, осведомленные о любом поведении, которое может нарушать настоящую Политику, обязаны сообщить о нем. Людям рекомендуется сообщать об этом через обычные отношения подчинения, начиная со своего руководителя. Все сообщения о предполагаемых нарушениях или несоответствиях будут расследованы Комитетом ИИ, юрисконсультом, отделом кадров или другими соответствующими сторонами. Если сотрудники YourCompanyName не действуют недобросовестно, они не будут подвергаться репрессиям за сообщение о возможных нарушениях.

Если по результатам расследования YourCompanyName установит, что Представитель YourCompanyName не соблюдал настоящую Политику, то к Представителю YourCompanyName будут применены дисциплинарные меры, вплоть до увольнения.

**ПРИЛОЖЕНИЕ I**

**ТЕХНИКИ И ПОДХОДЫ**

* Подходы к машинному обучению, включая контролируемое, неконтролируемое и обучение с подкреплением, с использованием широкого спектра методов, включая глубокое обучение.
* Логические и основанные на знаниях подходы, включая представление знаний, индуктивное (логическое) программирование, базы знаний, выводы, дедуктивные механизмы, (символические) рассуждения и экспертные системы.
* Статистические подходы, байесовское оценивание, методы поиска и оптимизации.

**ПРИЛОЖЕНИЕ II**

**Требования ЕС к системам высокого риска**

К системам ИИ с высоким уровнем риска должны применяться требования к качеству используемых наборов данных, технической документации и ведению учета, прозрачности, предоставлению информации пользователям, человеческому надзору, надежности, точности и кибербезопасности. Эти требования необходимы для эффективного снижения рисков для здоровья, безопасности и основных прав, если это применимо в свете предполагаемого назначения системы, и не существует других менее ограничивающих торговлю мер, что позволяет избежать необоснованных ограничений торговли.

Высокое качество данных необходимо для работы многих систем искусственного интеллекта, особенно когда используются методы обучения моделей, чтобы система искусственного интеллекта с высокой степенью риска работала по назначению и безопасно, а также не стала источником дискриминации, запрещенной законодательством Союза. Качественные наборы данных для обучения, проверки и тестирования требуют применения соответствующих методов управления данными. Наборы данных для обучения, проверки и тестирования должны быть релевантными, репрезентативными, не содержать ошибок и быть полными с точки зрения предназначения системы. Они также должны обладать соответствующими статистическими свойствами, в том числе в отношении лиц или групп лиц, на которых предполагается использовать систему ИИ с высоким уровнем риска. Наборы данных для обучения, проверки и тестирования должны учитывать, в той мере, в какой это необходимо с учетом их предназначения, особенности, характеристики или элементы, характерные для конкретной географической, поведенческой или функциональной среды или контекста, в которых предполагается использовать систему ИИ. Для защиты прав других лиц от дискриминации, которая может быть результатом предвзятости систем ИИ, поставщики должны иметь возможность обрабатывать также специальные категории персональных данных в качестве вопроса, представляющего значительный общественный интерес, для обеспечения мониторинга, выявления и исправления предвзятости в отношении систем ИИ с высоким риском.

Для разработки систем ИИ с высоким уровнем риска определенные субъекты, такие как поставщики, нотифицированные органы и другие соответствующие организации, например, центры цифровых инноваций, испытательные экспериментальные центры и исследователи, должны иметь возможность доступа и использования высококачественных наборов данных в соответствующих областях деятельности, связанных с настоящим Постановлением. Европейские общие пространства данных, созданные Комиссией, и содействие обмену данными между предприятиями и с правительством в общественных интересах будут способствовать обеспечению надежного, подотчетного и недискриминационного доступа к высококачественным данным для обучения, проверки и тестирования систем ИИ. Например, в здравоохранении европейское пространство данных о здоровье будет способствовать недискриминационному доступу к данным о здоровье и обучению алгоритмов искусственного интеллекта на этих наборах данных, с сохранением конфиденциальности, безопасно, своевременно, прозрачно и надежно, а также при надлежащем институциональном управлении. Соответствующие компетентные органы, в том числе отраслевые, предоставляющие или поддерживающие доступ к данным, могут также поддерживать предоставление высококачественных данных для обучения, проверки и тестирования систем искусственного интеллекта.

Для проверки соответствия требованиям настоящих Правил необходимо иметь информацию о том, как разрабатывались системы искусственного интеллекта высокого риска и как они функционируют на протяжении всего жизненного цикла. Для этого необходимо вести учет и техническую документацию, содержащую информацию, необходимую для оценки соответствия системы ИИ соответствующим требованиям. Такая информация должна включать типичные характеристики, возможности и ограничения системы, алгоритмы, данные, используемые процессы обучения, тестирования и проверки, а также документацию по соответствующей системе управления рисками. Техническая документация должна поддерживаться в актуальном состоянии.

Чтобы устранить непрозрачность, которая может сделать некоторые системы ИИ непонятными или слишком сложными для физических лиц, следует требовать определенной степени прозрачности для систем ИИ с высоким уровнем риска. Пользователи должны иметь возможность интерпретировать результаты работы системы и использовать их надлежащим образом. Поэтому системы ИИ с высокой степенью риска должны сопровождаться соответствующей документацией и инструкциями по использованию и содержать краткую и четкую информацию, в том числе в отношении рисков для основных прав и дискриминации, где это необходимо.

Системы ИИ с высоким уровнем риска должны быть спроектированы и разработаны таким образом, чтобы физические лица могли осуществлять надзор за их функционированием. Для этого поставщик системы должен определить соответствующие меры по надзору со стороны человека до ее выхода на рынок или ввода в эксплуатацию. В соответствующих случаях такие меры должны гарантировать, что система имеет встроенные операционные ограничения, которые не могут быть отменены самой системой, и реагирует на действия человека-оператора, а также что физические лица, на которых возложен надзор, обладают необходимой компетенцией, подготовкой и полномочиями для выполнения этой роли.

Системы ИИ с высоким уровнем риска должны стабильно работать на протяжении всего жизненного цикла и обеспечивать соответствующий уровень точности, надежности и кибербезопасности в соответствии с признанным уровнем техники. Уровень точности и показатели точности должны быть доведены до сведения пользователей.

Техническая устойчивость - одно из ключевых требований к системам ИИ с высоким уровнем риска. Они должны быть устойчивы к рискам, связанным с ограничениями системы (например, ошибкам, сбоям, несоответствиям, неожиданным ситуациям), а также к злонамеренным действиям, которые могут поставить под угрозу безопасность системы ИИ и привести к вредному или иному нежелательному поведению. Невозможность защиты от этих рисков может привести к последствиям для безопасности или негативно повлиять на основные права, например, из-за ошибочных решений или неправильных или предвзятых выводов, генерируемых системой ИИ.

Кибербезопасность играет важнейшую роль в обеспечении устойчивости систем ИИ к попыткам изменить их использование, поведение и производительность или скомпрометировать их защитные свойства с помощью злоумышленников, использующих уязвимости системы. Кибератаки на системы ИИ могут использовать специфические для ИИ активы, такие как наборы обучающих данных (например, отравление данных) или обученные модели (например, атаки противника), или использовать уязвимости цифровых активов системы ИИ или базовой ИКТ-инфраструктуры. Поэтому для обеспечения уровня кибербезопасности, соответствующего рискам, поставщики систем ИИ, подверженных высокому риску, должны принимать соответствующие меры, учитывая при этом базовую инфраструктуру ИКТ.

Источник: Закон ЕС об искусственном интеллекте, п. 43-51

**ПРИЛОЖЕНИЕ III**

**Потенциально применимые типы систем ЕС с высоким уровнем риска**

* Системы удаленной биометрической идентификации в режиме реального времени и "после". К обоим типам должны предъявляться особые требования по возможностям регистрации и человеческому контролю.
* Системы искусственного интеллекта, используемые в сфере образования или профессионального обучения, в частности, для определения доступа или распределения людей в учебные заведения и учреждения профессионального обучения или для оценки людей по тестам в рамках или в качестве предварительного условия для получения ими образования.
* Системы искусственного интеллекта, используемые в сфере занятости, управления работниками и доступа к самозанятости, в частности, для найма и отбора людей, принятия решений о продвижении по службе и увольнении, а также для распределения задач, контроля или оценки людей, состоящих в трудовых договорных отношениях.
* Доступ и пользование определенными основными частными и государственными услугами и благами, необходимыми людям для полноценного участия в жизни общества или повышения уровня жизни. Системы искусственного интеллекта используются для оценки кредитного балла или кредитоспособности физических лиц.

Источник: Закон ЕС об искусственном интеллекте, параграф. 33-37