

ИНГОССТРАХ

Просто быть уверенным

Возможные направления страхования рисков применения технологий искусственного интеллекта

Дмитрий Чугунов

Калуга, 2025

Страхование рисков применения технологий искусственного интеллекта

Ответственность за вред, причинённый ИИ, может распределяться между несколькими сторонами

Разработчик ИИ-системы несёт ответственность за недостатки в алгоритмах, обучении модели, обеспечении безопасности

Интегратор, внедряющий ИИ-систему, отвечает за правильность её настройки и эксплуатации

Пользователь должен обеспечивать соблюдение требований безопасности, контроль за работой системы

Федеральный закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации» № 258-ФЗ от 31 июля 2020 года

В 2025 вступило в силу положение о том, что

Программа экспериментального правового режима должна содержать:

положения о страховании гражданской ответственности участников экспериментального правового режима за причинение вреда жизни, здоровью или имуществу других лиц при реализации экспериментального правового режима, в том числе в результате использования решений, разработанных с применением технологий искусственного интеллекта, требования к условиям такого страхования, в том числе минимальному размеру страховой суммы, перечню страховых рисков и страховых случаев

Страхование ответственности разработчиков ПО ИИ

в результате непреднамеренных ошибок и/или упущений, допущенных при осуществлении
Застрахованной деятельности:

- Проектирование, разработка и внедрение решений искусственного интеллекта
- Консультирование по дизайну аппаратных/ программных систем/ их приобретению
- Инсталляция программного обеспечения
- Поддержка программного обеспечения
- Тестирование, установка, сопровождение, адаптация и модификация программного обеспечения и баз данных
- Построение интеллектуальных систем, способных обрабатывать данные, обучаться и принимать решения

Разработчик ПО ИИ

Требование наличия страхования
ответственности разработчика
Предъявление требований о возмещении
вреда в результате ошибок ПО ИИ



Пользователи ПО ИИ

Возмещение вреда в результате
ошибок допущенных при разработке
ПО ИИ

Выплата страхового возмещения

Страхование рисков применения технологий искусственного интеллекта

Страхование рисков лиц, применяющих технологии ИИ

Ошибки и упущения работников
на которых возложен функционал
применения технологий ИИ, в т.ч.
постановка задач для ИИ и др.

Внезапные и непредвиденные
технические сбои в работе программного
обеспечения ИИ

Непреднамеренные ошибки Работников,
которые привели к таким сбоям

Ошибки и упущения директоров
принятие решений на основе данных ИИ

Для решения о принятии риска на страхование необходимо сообщить
Список ПО ИИ и функционал применения технологий ИИ

Возможные риски применения технологий ИИ

В финансовой сфере:

- технические сбои и ошибки, которые могут привести к приостановке деятельности
- ошибки, которые могут привести к совершению ненадлежащих операций
- угроза утечки данных в результате хакерских атак на ИИ
- финансовые потери из-за ошибок, используемых для принятия важных управленческих решений
- нарушение прав интеллектуальной собственности
- утечка конфиденциальной информации и репутационные риски

В промышленности:

- нанесение вреда жизни и здоровью людей (работников предприятия, потребителей продукции) в результате ошибок или сбоев в работе ИИ-систем
- имущественный ущерб (например, в случае выхода из строя оборудования или брака продукции)

Аналитики изучили произошедшие в мире инциденты с участием генеративного ИИ и выделили пять самых релевантных рисков, связанных с развитием этой технологии:

- потенциальный вред от ложных ответов ИИ
- рост объёма некачественно сгенерированного контента
- негативное влияние на рынок труда
- цифровое мошенничество
- нарушение этических норм.

Инциденты, связанные с причинением ущерба от применения ИИ

в 2022 году на одном из российских нефтеперерабатывающих заводов ошибка в системе предиктивного обслуживания привела к незапланированной остановке производства и финансовым потерям

в 2023 году на металлургическом заводе в Магнитогорске произошёл сбой в работе ИИ-системы, отвечающей за контроль качества продукции.

В результате были выпущены партии некачественной стали, что привело к поломке оборудования на предприятиях потребителей. Общий ущерб составил около 50 млн рублей. После разбирательства комиссия возложила ответственность на интегратора, который был признан виновным в некорректной настройке алгоритмов

В 2024 году на химическом заводе в Казани ИИ-система, управляющая технологическим процессом, допустила ошибку, что вызвало выброс вредных веществ. В результате пострадали 12 рабочих, двое из них получили тяжёлые травмы. Экспертиза показала, что причиной стали недостатки в обучении нейронной сети, допущенные разработчиком. Страховая компания выплатила пострадавшим около 15 млн рублей.

Страхование рисков Операторов инвестиционных платформ (ОИП) и информационных систем (ИС), в которых осуществляется выпуск ЦФА (ОИС)



Страхование рисков Операторов инвестиционных платформ (ОИП) и информационных систем (ИС), в которых осуществляется выпуск ЦФА (ОИС)



Отличия объемов покрытия по страхованию профессиональной ответственности и кибер-рисков

Действующее покрытие профессиональной ответственности регистраторов и спецдепов, несмотря на наличие покрытия рисков технических сбоев и компьютерных вирусов, нацелено на возмещение убытков клиентов и третьих лиц, но при этом не покрывает риски:

- DDoS атак
- не возмещает собственные убытки
- расходы от поломки и повреждения оборудования и ПО
- расходы на восстановление информации
- убытки от приостановки деятельности
- расходы на диагностику и восстановление информационной системы
- ответственность за нарушение конфиденциальности, включая ответственность за разглашение персональных данных
- хищение денежных средств со счетов
- убытки от кибер-вымогательства
- расходы на восстановление репутации и другие расходы, связанные с кибер-инцидентами

Все перечисленные убытки покрываются кибер-страхованием.

Программа по страхованию кибер-рисков регистраторов и спецдепозитариев

Возможность подготовки типового предварительного предложения с тремя вариантами покрытия и различными размерами страховых сумм от 15 до 200 млн.руб.

Стоимость полиса от 90 тыс. руб.

Тарифы от 0,5 до 1,5% в зависимости от объема покрытия и результатов оценки степени риска.

Возможность тестовой DDoS атаки и аудита информационной безопасности (услуга предоставляется сторонними IT компаниями) до заключения договора, результаты влияют на стоимость полиса

ИНГОССТРАХ

Предварительные условия по страхованию информационных (кибер-) рисков				
Страхователь				
Условия страхования	В соответствии с Правилами страхования информационных рисков СПАО «Ингосстрах» от «30» апреля 2019 г.			
Период страхования	1 (Один) год с согласованной даты			
Территория страхования	Российская Федерация			
Страховой случай	неполучение Страхователем доходов, возникновение непредвиденных расходов, гибель или повреждение имущества, наступление ответственности за причинение вреда Третьим лицам в результате наступления событий, указанных в разделе «Застрахованные риски»			
Вариант страхового покрытия	1	2	3	
Застрахованные риски:				
а) Целенаправленная (таргетированная) компьютерная атака, целью которой является захват контроля (повышение прав) над Информационной системой Страхователя, либо ее дестабилизация, либо отказ в обслуживании, неправомерно совершенные Третьими лицами (хакерская атака);	✓	✓	✓	
б) Внедрение Вредоносных компьютерных программ (вирусов), разработанных Третьими лицами, в Информационную систему Страхователя;	✓	✓	✓	
в) Внезапные и непредвиденные технические сбои в работе программного обеспечения и/или вычислительной техники, входящих в Информационную систему Страхователя, непреднамеренные ошибки Работников Страхователя, которые привели к таким сбоям;	-	✓	✓	
которые привели к следующим негативным последствиям:				
1. Неправомерное использование вычислительных ресурсов Страхователя Третьими лицами (спам-рассылки, участие в botnet-сети от имени Страхователя, майнинг и другие)	✓	✓	✓	
2. Хищение Денежных средств и/или акций в электронной форме со счетов Страхователя Третьими лицами путем: - неправомерного (несанкционированного) получения доступа к системе интернет-банкинга или неправомерного введения в его Информационную систему электронных команд, подготовленных или модифицированных Третьими лицами без ведома или согласия Страхователя; - компрометации ключа электронно-цифровой подписи (ЭЦП) Страхователя или его должностного лица.	✓	✓	✓	
3. Требования о возмещении вреда в связи с наступлением ответственности перед Третьими лицами за вред, причиненный в результате нарушения конфиденциальности, включая ответственность за разглашение персональных данных	✓	✓	✓	
4. Утрата Электронных данных и/или Компьютерных программ	-	✓	✓	
5. Хищение интеллектуальной собственности Страхователя в	-	✓	✓	

ИНГОССТРАХ

электронной форме			
6. Требования о возмещении вреда в связи с причинением вреда имущественным интересам Третьих лиц (кроме указанных в п.3. и п.8) в результате реализации застрахованных рисков	-	✓	✓
7. Кибер-вымогательство в отношении Страхователя	-	✓	✓
8. Ущерб деловой репутации Страхователя вследствие событий, перечисленных в пунктах 1 - 7	-	✓	✓
9. Требования о возмещении вреда в связи с причинением вреда жизни и здоровью Третьих лиц в результате любого из застрахованных рисков	-	-	✓
10. Перерыв в коммерческой (производственной) деятельности Страхователя из-за недоступности, значительного снижения производительности, нарушений в работе Информационной системы и/или частичной или полной недоступности Компьютерной системы Страхователя, недоступности Электронных данных*	-	-	✓
11. Гибель или повреждение Компьютерного оборудования Страхователя в результате реализации любого из застрахованных рисков, которые привели к последующему пожару, взрыву или поломке Компьютерного оборудования, а также перерыву в коммерческой (производственной) деятельности Страхователя	-	-	✓
Страховая сумма, руб.*	Страховая премия, руб.**		
50 000 000	285 000	355 000	885 000
100 000 000	590 000	700 000	1 770 000
200 000 000	1 170 000	1 390 000	3 460 000
Безусловная франшиза	1% от Лимита ответственности		

В отношении следующих видов расходов устанавливается лимит ответственности (единый на все указанные расходы) в размере 10% от Страховой суммы (данный лимит ответственности не увеличивает страховую сумму, а является ее частью):

- по возмещению расходов на диагностику информационной системы и устранение/минимизацию негативных последствий страхового случая;
- по возмещению расходов на юридические консультации в связи с кибер-инцидентом;
- по возмещению расходов на консультации в области репутации в связи с нарушением конфиденциальности;
- по возмещению расходов на защиту.

* Недополученная прибыль и текущие расходы возмещаются за период времени, прошедший по истечению временной франшизы (84), но не более, чем 7 календарных дней с даты возникновения нарушения Информационной безопасности.

**Настоящее предложение является предварительным и действительно 30 дней. Итоговая страховая премия будет определена после предоставления заполненного вопросника.

КОНТАКТНАЯ ИНФОРМАЦИЯ:

Дмитрий Чугунов
Главный консультант по страхованию
финансовых и профессиональных рисков
ИНГОССТРАХ
тел: +7 903 208 16 28
chugunov@97.ingos.ru
www.ingos.ru

СПАО «Ингосстрах»
JSC Ingosstrakh

06/07/2024

06/07/2024

ИНГОССТРАХ

Просто быть уверенным