

Необходимо отметить, что исключением киберрисков из страхового покрытия, как правило, исключаются не только риски, связанные с кибератаками (в широком понимании), но и риски, связанные с любыми другими киберинцидентами, под которыми понимается очень широкий круг событий, который может включать в себя, в частности:



- любую ошибку или упущение, или серию ошибок или упущений, относящихся к доступу, обработке, использованию или управлению какой-либо компьютерной системой (это отдельное очень широкое определение, включающее любой компьютер, аппаратное обеспечение, программное обеспечение, коммуникационную систему, электронное устройство и пр.);
- любую частичную или полную недоступность, или отказ, или серию связанных случаев недоступности или отказа, относящиеся к доступу, обработке, использованию или управлению какой-либо компьютерной системой; а также
- перерыв / прерывание деятельности, вызванное случайным, непреднамеренным или неосторожным / небрежным действием или бездействием, ошибкой или упущением сотрудника, независимого подрядчика/консультанта или стороннего поставщика услуг при работе с или обслуживании компьютерной системы, приводящими к полной или частичной недоступности компьютерной системы.

При этом в дополнение к довольно широким формулировкам исключение киберрисков зачастую формулируется с использованием таких обобщающих фраз как: *«прямо или косвенно вызванных»*, *«вытекающих из или каким-либо образом связанных с»*, что дополнительно расширяет сферу применения такого исключения и «размывает» и так неочевидные границы его применения (допуская возможность избыточно расширительного толкования).

Учитывая экспоненциальный рост использования компьютерных систем во всех операционных процессах, начиная от оборудования рабочего места офисного сотрудника и заканчивая строительной или производственной площадкой, вероятность применения исключения киберрисков постоянно возрастает практически для всех видов деятельности и даже для тех, которые, на первый взгляд, защищены от возможных кибератак (так как может оставаться непокрытым риск киберинцидента).

При правильной договорной работе страховщики готовы включать в договоры страхования так называемые исключения из исключений, когда страховое покрытие по некоторым событиям, связанным с киберрисками, все же предоставляется по договорам страхования. Так, например, по договорам страхования имущества можно согласовать покрытие утраты (гибели) или повреждения имущества, вызванных непосредственно киберинцидентом или киберактом (включая кибератаку), которые привели к пожару, или взрыву, или короткому замыканию (короткое замыкание часто забывают добавить).

Формулировки исключения киберрисков могут отличаться в зависимости от страховщика, и даже у одного страховщика в зависимости от договора страхования (конкретного страхового продукта), поэтому страхователям необходимо обращать внимание на формулировки данного исключения не только применительно к конкретному договору страхования, но и учитывать формулировки данного исключения, содержащиеся в других договорах страхования, чтобы обеспечить максимально широкое (с учетом текущего рынка) покрытие. Это особенно актуально в ситуации, когда страхователь принял решение приобрести специальное покрытие киберрисков. В этом случае очень важно проработать условия покрытия по договору страхования киберрисков, чтобы:

1. исключить возможные «разрывы» в покрытии с другими имеющимися у страхователя страховыми продуктами; а также
2. избежать «задвоения» страхового покрытия, когда один и тот же риск покрыт по нескольким договорам страхования. Это позволит (немного) сэкономить на страховой премии, а также избежать возможных дополнительных сложностей при урегулировании страхового случая, если риск застрахован у разных страховщиков.

