Глава НСИС Николай Галушин назвал принципы востребованного страхования киберрисков, на текущий момент в ответ на запрос НСИС на страховом рынке не нашлось предложения с достаточным покрытием и лимитами, уточнил он.

Страхование должно носить добровольный характер, оператор информационной системы должен иметь инструменты возмещения ущерба в связи с требованиями о возмещении ущерба со стороны третьих лиц (владельцев персональных данных), к которым может относиться и договор страхования при достаточном уровне покрытия и по страховой сумме, и набору рисков, считает Н. Галушин.

По его словам, базовым условием наступления ответственности информационной системы является доказательство самого факта утечки персональных данных, учитывая объем данных, которые уже по факту находятся в открытом доступе, в том числе и по причине того, что сами владельцы персональных данных информацию о себе выкладывают свободно в интернет.

После подтверждения факта утечки персональных данных из конкретной системы должна быть доказана причинно-следственная связь между фактом утечки персональных данных и понесенным ущербом (материальным, физическим, моральным) у конкретного владельца персональных данных, чьи данные утекли. При этом ущерб должен быть только в отношении конкретного пострадавшего лица (владельца персональных данных), а не по самому факту утечки данных.

Глава НСИС убежден, что должно действовать освобождение от ответственности в случае выполнения информационной системы всех требований регулирующих и надзорных органов (были приняты все регуляторные, разумные и достаточные меры для охраны персональных данных, защиты информации).

В случае действия страхового покрытия по договору страхования должно быть

предусмотрено только одно исключение, при наступлении которого в случае ущерба конкретному лицу в результате утечки персональных данных не будет производиться страховая выплата — доказанные умышленные действия оператора информационной системы.

Страхование должно быть осуществлено на сумму максимально возможного реального ущерба, который может быть нанесен владельцем персональных данных, при отсутствии достаточной емкости на страховом рынке – на предельную сумму емкости, при этом ущерб сверх этой суммы не возмещается оператором информационной системы.

При этом должна быть предусмотрена субсидиарная ответственность подрядчиков, которые осуществляли работы на инфраструктуре и программного обеспечения в области информационной безопасности (с одинаковым набором рисков и исключений), убежден Николай Галушин.

В условиях ограниченного рынка перестрахования, возможно, помимо емкости РНПК, нужна еще внутренняя пуловая емкость российских страховщиков кибер-рисков. И очень важно, чтобы условия страхования были синхронизированы между страховыми компаниями, заключил глава НСИС.

Википедия страхования