21 сентября Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации разместило на портале regulation.gov.ru для общественного обсуждения проект закона “о внесении изменений в статьи 2 и 10 Федерального закона «Об информации, информационных технологиях и о защите информации (ID проекта - 01/05/09-20/00108513”) в части установления запрета использования на территории Российской Федерации протоколов шифрования, позволяющих скрыть имя (идентификатор) Интернет-страницы или сайта в сети «Интернет».

В случае принятия закона, запрет коснется множества современных криптографических протоколов, таких как TLS 1.3, ESNI, DoH и DoT. Как следует из представленного проекта, нарушение запрета повлечет приостановление функционирования Интернет-ресурса.

Роскомсвобода полагает, что указанный законопроект в случае его принятия несет существенные последствия для IT-компаний, предоставляющих услуги в части доступа к интернет-сервисам и веб-контенту, ограничит право граждан на свободу получения информации и защиту своих данных, а также приведет к серьезному технологическому отставанию отечественного IT-сектора.

Шифрование в сети определяется как процесс кодирования содержания любых пакетов данных или голоса с помощью алгоритма и случайно выбранного набора переменных данных, связанных с алгоритмом, известного как «ключ».

Шифрование означает, что информация может быть расшифрована только предполагаемым получателем сообщения, у которого есть ключ. Хотя шифрование обычно защищает конфиденциальность сообщения или данных содержания, оно не обязательно скрывает для третьих лиц IP-адреса отправителя или получателя (метаданные). В этом смысле только лишь использование шифрования не гарантирует анонимности, поскольку пользователи Интернета остаются отслеживаемыми и, следовательно, потенциально идентифицируемый. Шифрование может также использоваться для проверки подлинности и целостности коммуникации, например с помощью цифровых подписей. Цифровая подпись представляет из себя криптографическую гарантию того, что конкретный документ был создан либо передан определенным лицом.

Шифрование - это фундаментальная особенность Интернета. Без надежных протоколов и алгоритмов шифрования, осуществление безопасных онлайн-транзакций будет невозможно. Без применения шифрования коммуникации любого пользователя Интернета, а также любой частной компании и государственного учреждения приведут к утечкам и злоупотреблениям. По этой причине шифрование используется ежедневно, позволяя обмениваться информацией, использовать онлайн-банкинг, защищать адвокатскую, медицинскую, налоговую и коммерческую тайну. Шифрование особенно важно для правозащитников, информаторов, журналистов и активистов, которые часто становятся объектами слежка со стороны спецслужб или правоохранительных органов.

Технологии DoH (DNS поверх HTTPS) и eSNI внедряются сегодня повсеместно для повышения безопасности и приватности пользователей такими гигантами, как Google, Mozilla, Microsoft, Cloudflare. Криптографические протоколы TLS обеспечивают защищенную передачу данных между узлами в интернете, используя в процессе передачи информации сразу несколько видов шифрования. Блокировка веб-сервисов, использующих DoH приведет к массовому нарушению прав на свободу доступа к информации.

В онлайн-пространстве свобода использования технологии шифрования часто является предварительным условием для осуществления права на неприкосновенность частной жизни и выражения мнения.

Право на шифрование охраняется нормами мягкого права и относится к основополагающим цифровым правам человека. В докладе Специального докладчика ООН по свободе самовыражения за 2013 и 2015 г. установил взаимосвязь между свободой выражения, шифрования и анонимного общения. Таким образом, ООН рекомендует всем государствам поощрять распространение и использование гражданами средств шифрования, признавая их важнейшим инструментом защиты базовых прав человека. В 2012 году Комитет министров Совета Европы (СОЕ) рекомендовал государствам-членам Совета Европы взаимодействовать с частным сектором в целях применения наиболее подходящих мер безопасности для защиты персональных данных от неправомерного доступа третьих лиц. Это должно включать меры по сквозному шифрованию коммуникаций между пользователем и веб-сайтами социальных сетей. Согласно отчету Парламентской Ассамблеи Совета Европы 2015 г. о массовом слежении ПАСЕ решительно осудило действия АНБ, связанные с попытками ослабить стандарты шифрования и использование бэкдоров.

Роскомсвобода считает, что ограничение на использование современных протоколов шифрования являются очевидным нарушением права на неприкосновенность частной жизни и свободу выражения мнения, и противоречит международно признанным стандартам в сфере защиты цифровых прав.

Роскомсвобода считает предложенный законопроект регрессивным и необоснованным, подлежащим отклонению в полном объеме.

Надежное шифрование жизненно важно для защиты конфиденциальности сообщений и личных данных. Запрет использования современных протоколов и алгоритмов шифрования, которые используются все бОльшим количеством веб-сервисов и IT-компаний сродни запрету устанавливать надежные замки на двери или непрозрачные занавески на окнах.