

ПРАКТИЧЕСКИЕ ВОПРОСЫ РЕАЛИЗАЦИИ ЗАЩИТЫ ИНФОРМАЦИИ В СФЕРЕ ПРЕДПРИНИМАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ

Игнатова Диана Николаевна

магистрант, Тольяттинский государственный университет, РФ, г. Тольятти

Аннотация. В статье автор предлагает исследовать практические вопросы реализации защиты информации в сфере предпринимательской деятельности.

Ключевые слова: защита информации, интернет, защита, телекоммуникационные линии, техническое оборудование.

Основные проблема защиты информации в предпринимательской сфере связаны с государственной политикой Российской Федерации в отношении Интернета и информации находящейся в открытом доступе.

На сегодняшний день, предпринимательское сообщество не обладает средствами и методами, которые могли бы способствовать защите их интересам, в рамках общей системы угроз вмешательства государства в частные интересы корпораций и индивидуальных предпринимателей.

С каждым годом, все больше и больше количества различных данных, в том числе коммерческой и конфиденциальной информации скапливается именно в Интернете. Существующие формы и способы защиты такой информации являются неэффективными для бизнеса.

Новые правила в отношении Интернета в России, большинство из которых вступили в силу 1 ноября 2019 г., а другие должны следовать в январе 2021 г., привлекли международное внимание и были публично названы российским «суверенным законом об Интернете». На самом деле такого нового закона не было, а скорее была серия поправок к существующим федеральным законам «О связи» и «Об информации, информационных технологиях и защите информации».

Официально поправки направлены на защиту Интернета в России от внешних угроз. Фактически, они обеспечивают важнейшую правовую основу для создания централизованной системы управления Интернетом со стороны государственной власти, что теоретически позволяет изолировать российскую сеть от глобального Интернета.

Эти три поправки имеют особенно далеко идущие последствия:

- обязательная установка технических средств противодействия потенциальным угрозам;
- централизованное управление телекоммуникационными сетями в случае угрозы;
- механизм контроля линий связи, пересекающих границу России.

С помощью этих трех ключевых поправок Россия пытается достичь как минимум трех разных

целей. Во-первых, он нацелен на создание механизма эффективного наблюдения за Интернетом в пределах его границ. С этой целью поправка, касающаяся установки «технических средств противодействия угрозам», позволяет усилить государственный контроль над информацией и предотвратить ее распространение в случае необходимости. Следовательно, реализация нового законодательства может дать российскому правительству возможность ограничить активность оппозиции в социальных сетях, помогая ему предотвращать протесты, подобные протестам 2011–2013 годов в преддверии выборов в российский парламент, Государственную Думу, запланированных на 2021 год.

Во-вторых, государство стремится стать ключевым регулятором Интернета в России. Недавняя поправка, позволяющая государству создавать централизованный контроль над интернет-инфраструктурой путем введения трансграничного контроля линий подключения и перенаправления трафика, является попыткой обеспечить изоляцию национальной сети от глобального Интернета, для чего государство может открывать и закрывать «цифровые границы» и определять поток информации внутри них по своему усмотрению. Хотя тотальный государственный контроль над Интернетом в России останется невозможным до тех пор, пока страна подключена к миру через существующую инфраструктуру глобального Интернета, принятие этой поправки режимом Путина было попыткой представить свой контроль над телекоммуникационными линиями, сетями и т. Д. и трафик как свершившийся факт.

В-третьих, Россия намерена расширить государственно-ориентированную модель Интернета на международный уровень. Поправка, направленная на создание инфраструктуры для национальной системы доменных имен (DNS), может, если она будет достигнута в соответствии с планом в январе 2021 года, создаст российский сегмент Интернета - параллельный и, вероятно, несовместимый с существующим. Этим шагом Россия не стремится изолировать себя от остального мира, а скорее создает прецедент, которому могут последовать другие государства, стремящиеся к суверенитету над своими сегментами Интернета. Предположительно, России потребуется еще более тесное сотрудничество с Китаем, чем она уже есть, для разработки технологий для достижения своих целей и координации своей интернет-политики на международном уровне. В долгосрочной перспективе,

Хотя некоторые последствия трех поправок все еще неясны, а некоторые нормативные акты и требования еще не приняты, новое законодательство уже несет в себе конкретные риски, которые касаются не только самой России, но и Германии и других европейских стран, которые сотрудничают с Россией и собственными компаниями. действующий внутри него.

Теперь обязательное «техническое оборудование для противодействия угрозам», например, также сможет определять приоритеты трафика. Он может задерживать поток одних типов сетевых пакетов, отдавая приоритет другим, повышая их производительность. На практике пользователи определенных веб-сайтов и сервисов могут испытывать медленный доступ или недоступность. Такая расстановка приоритетов может поставить под угрозу сетевой нейтралитет и привести к дискриминации компаний, не защищенных российским государством.

Тот факт, что для этого нового оборудования не существует ни технических требований, ни сертификации, также означает, что сбои в сети более вероятны. Компании, работающие в России, в свою очередь, могут понести сопутствующий ущерб, вызванный новым оборудованием, с ограниченными возможностями возмещения убытков.

Кроме того, более вероятная перспектива так называемого «splinternet», когда сегменты Интернета контролируются и регулируются различными государствами и участниками, может привести к несовместимости технических, нормативных и операционных стандартов, что затрудняет трансграничное сотрудничество и совместимость глобального Интернета.

Список литературы:

1. Камалова Г.Г. Сравнительный Информационно-правовой анализ российского и зарубежного

законодательства о коммерческой тайне // Финансовое право и управление. 2017. №1. URL: <https://cyberleninka.ru/article/n/sravnitelnyy-informatsionno-pravovoy-analiz-rossiyskogo-i-zarubezhnogo-zakonodatelstva-o-kommercheskoy-tayne> (дата обращения: 24.06.2021).

2. Нардина О.В. Ограничение конституционного права на доступ к получению и распространению информации в сети "интернет" в связи с противодействием экстремизму и терроризму // Наука. Общество. Государство. 2017. №4 (20). URL: <https://cyberleninka.ru/article/n/ogranichenie-konstitutsionnogo-prava-na-dostup-k-polucheniyu-i-rasprostraneniyu-informatsii-v-seti-internet-v-svyazi-s-protivodeystviem> (дата обращения: 24.06.2021).