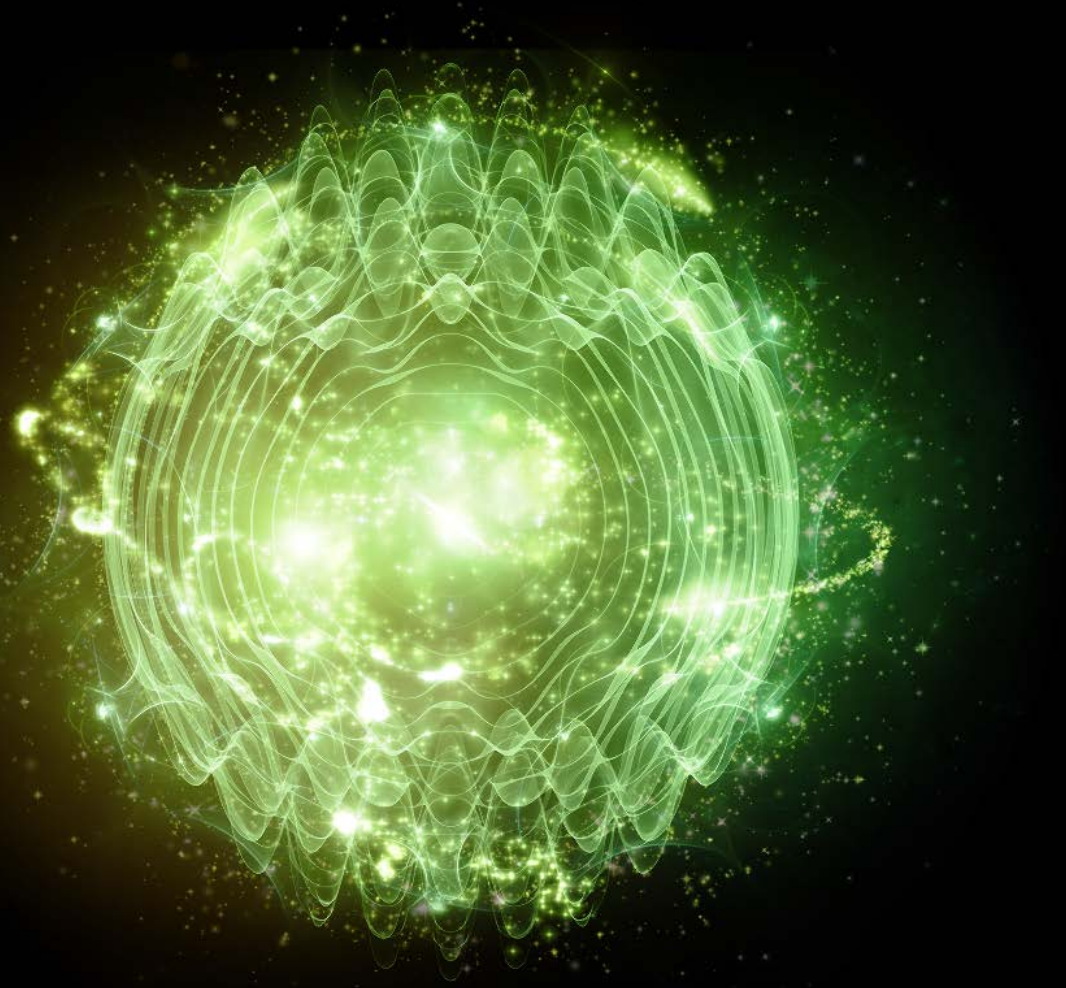
Deloitte.
Legal



Суверенный Интернет: как новый закон может повлиять на бизнес-процессы компании

Карточки Deloitte Legal

11 октября 2019

Закон о суверенном интернете: основные изменения

С 1 ноября 2019 года вступают в силу изменения, целью которых является обеспечение автономности российского сегмента Интернета («Закон о суверенном Интернете»). Положения закона в основном направлены на операторов связи (например, сотовой связи, Интернет-провайдеров и т.д.), но он может сказаться и на рядовых пользователей российского сегмента Интернета.

Обратите внимание, что данная справка не является юридической консультацией. Для получения более полной информации о законе и его юридических последствиях, пожалуйста, обратитесь к специалистам Deloitte Legal, указанным на слайде 10.

Идентификация и учёт «точек обмена трафиком»
Устанавливается требование использовать лишь внесённые в соответствующий реестр Роскомнадзора точки обмена трафиком

Отчетность о трансграничных сетях
Вводится необходимость сообщения о наличии у операторов связи пересекающих границу каналов связи

Установка «технических средств противодействия угрозам»
Средства предназначены для централизованного управления маршрутами интернет-трафика, а также блокировки информации

Обязательные учения
Учения проводятся для приобретения участниками навыков обеспечения устойчивого, безопасного и целостного функционирования Интернета

Возможность введения централизованного управления Интернетом
В случае высокого риска возникновения угроз устойчивости, безопасности и целостности Интернета Роскомнадзор возьмет на себя управление без уведомления операторов связи

Влияние на пользователей Интернета

Каковы возможные последствия вступления закона в силу для рядовых пользователей (компаний)?

1. **Ограниченность** в выборе интернет-сервисов/серверных мощностей

2. **Возможный отзыв лицензии** у оператора связи или оператора электронного документооборота

3. **Увеличение затрат** на использование услуг более крупного и дорогого оператора связи

4. **Необходимость дублирования** баз данных для размещение на серверах на территории РФ

5. **Потенциальное замедление** скорости доступа в Интернет/к западным интернет-сервисам

6. **Потенциальная недоступность** западных интернет-сервисов и корпоративных ресурсов

7. **Потенциальное увеличение затрат** на использование иных средств связи

8. **Потенциальная необходимость закупки** собственных серверных мощностей и их обеспечения

Может ли быть отключен Интернет в России?

Вероятность целенаправленного отключения Интернета на территории всей России невысока.

На данный момент невозможно точно указать на длительность и территориальную распространённость возможного отключения Интернета (сбоев). Возможны временные отключения (сбои) на конкретных территориях.

Подобные отключения (сбои) могут быть связаны с:

- несовершенством предоставляемых операторам связи технических средств противодействия угрозам;
- несовершенством программной составляющей технических средств;
- их недостаточной пропускной способностью.

Проектом Постановления Правительства «Об утверждении Порядка централизованного управления сетью связи общего пользования» устанавливаются виды угроз, которые могут стать основанием для передачи управления маршрутами трафика Центру мониторинга и управления сетью связи общего пользования.

Для целей реализации Закона о суверенном Интернете должен быть создан Центр мониторинга и управления сетью связи общего пользования (на данный момент соответствующий подзаконный акт не подготовлен). Ограничение доступа к информации будет осуществляться посредством направления Центром мониторинга и управления сетью связи общего пользования программных команд на технические средства.

Будет ли отключаться Интернет во время проведения учений?

Временные отключения (сбои) возможны на территории проведения учений.

Согласно Проекту Постановления Правительства «Об утверждении положения о проведении учений по обеспечению устойчивого, безопасного и целостного функционирования информационно-телекоммуникационной сети Интернет и сети связи общего пользования на территории Российской Федерации», участниками проведения учений являются:

- операторы связи;
- собственники или иные владельцы технологических сетей связи;
- собственники или иные владельцы точек обмена трафиком;
- собственники или иные владельцы линий связи, пересекающих государственную границу Российской Федерации;
- организаторы распространения информации в Интернете;
- иные лица, которые могут быть привлечены к участию в учениях с их согласия.

В связи с потенциальным привлечением значительного количества лиц к участию в учениях масштаб и длительность сбоев может значительно варьироваться.

Могут ли произойти сбои в предоставлении доступа к Интернету?

Это возможно.

На данный момент невозможно точно указать на длительность возможных сбоев и их территориальную распространённость: существует вероятность, что сбои могут продлиться от нескольких часов до нескольких дней.

При этом операторов связи к ответственности привлечь будет нельзя: согласно новой редакции п. 5 ст. 46 Федерального закона «О связи», технические средства противодействия угрозам подлежат установке у предоставляющих доступ в Интернет операторов связи и иных аналогичных лиц, а в силу п. 5.1. ст. 46 Федерального закона «О связи», операторы связи не могут быть привлечены к ответственности, и к ним не могут быть применены меры реагирования за нарушения обязательных требований и лицензионных условий, если такие нарушения вызваны сбоями в сетях связи в результате функционирования технических средств противодействия угрозам.

Зачем нужно оборудование, которое обяжут установить операторов связи?

На оборудовании в первую очередь магистральных операторов связи будут бесплатно установлены предоставленные государством технические средства противодействия угрозам. С использованием данного оборудования будет анализироваться весь проходящий трафик.

Также Закон о суверенном Интернете обеспечивает возможность осуществления блокировок с помощью технологии DPI (Deep packet inspection – «глубокий анализ пакетов»). Оборудование будет определять источник передаваемого трафика и, при необходимости, ограничивать доступ к ресурсам с запрещенной информацией не только по сетевым адресам, но и путем запрета пропуска проходящего трафика.

По Закону о суверенном Интернете оператор связи, оказывающий услуги по предоставлению доступа в Интернет, не обязан самостоятельно ограничивать доступ к информации, если доступ ограничивается с помощью технических средств противодействия угрозам в порядке централизованного управления.

Имеется ли возможность обхода блокировок (с использованием DNS серверов, VPN-протоколов и аналогичных технологий)?

Да, но возможность обхода блокировок будет зависеть от технических и программных характеристик используемых технологий блокирования и поддержания ограничения доступа к ресурсам.

Использование корпоративных DNS-серверов, хранящих информацию о соответствии с конкретных доменов IP-адресам, может быть недостаточным для обеспечения доступа к заблокированным ресурсам и сервисам, в связи с тем, что данная мера не позволяет изменять содержимое передаваемых сетевых пакетов. Связано это с реализацией функций DPI в технических средствах противодействия угрозам. С использованием технических средств будут осуществляться проверка и фильтрация сетевых пакетов на основании анализа их содержимого.

Использование корпоративных VPN-серверов, по умолчанию осуществляющих шифрование передаваемых пакетов, в совокупности с иными техническими и программными средствами позволяет получить доступ к заблокированным ресурсам, в связи с чем блокирование доступа с использованием DPI потенциально будет менее эффективным.

Использование инструментов обхода блокировок сайтов не является нарушением закона, однако не является рекомендованным способом минимизации рисков.

Какие действия необходимо предпринять пользователем на случай сбоев?

Для всех компаний, использующих информационные системы через интернет, для минимизации рисков рекомендуется проведение следующих мероприятий:

1. *Разработка плана аварийного восстановления* (Disaster recovery plan, DRP). С использованием DRP компания определяет порядок и очередность действий по восстановлению информационных систем. В частности DRP может включать положения о резервном копировании данных и применении резервирования замещением.
2. *Дублирование каналов связи* может быть эффективно в случае сбоя, вызванного отказом оборудования конкретного оператора связи.
3. *Использование альтернативных каналов связи.* В связи с возможными сбоями в разработанный DRP необходимо включение положений и чек-листов об использовании альтернативных каналов связи.
4. *Построение устойчивых локальных сетей* связано с уменьшением ущерба, вызванного сбоями доступа к сети Интернет. При этом при построении подобных сетей необходимо проведение оценки стоимости и предлагаемой для построения топологии локальной сети.

Для всех производственных и торговых компаний, использующих информационные системы, может быть рекомендовано увеличение запасов продукции в совокупности с применением иных средств передачи информации. Данные мероприятия могут позволить в краткосрочной перспективе решить проблему отсутствия должного уровня координации между сотрудниками или структурными подразделениями.

Наша команда

Анна Костыра

Управляющий Партнер

Делойт Лигал СНГ

+7 (495) 787 06 00 доб. 1481

akostyra@deloitte.ru

Екатерина Портман

Директор

Делойт Лигал СНГ

+7 (495) 787 06 00 доб.1517

eportman@deloitte.ru

Алина Давлетшина

Старший юрист

Делойт Лигал СНГ

+7 (495) 787 06 00 доб. 1783

adavletshina@deloitte.ru

Deloitte.
Legal