Российское законодательство в сфере национальной безопасности, а в частности Закон РФ от 5 марта 1992 г. N 2446-I "О безопасности" под безопасностью понимает состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Причем жизненно важные интересы понимаются как совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

Естественно, что такие потребности есть у личности общества и государства в информационной сфере. Их совокупность составляет понятие информационной безопасности, под которой, в соответствии с Доктриной информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895) понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. Законодательство определяет подобные интересы следующим образом:

1. Интересы личности в информационной сфере заключаются в 1) реализации конституционных прав человека и гражданина на доступ к информации, 2) на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.
2. Интересы общества в информационной сфере заключаются в 1) обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в 1) создании условий для гармоничного развития российской информационной инфраструктуры, 2) для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества. Анализ положений законодательства говорит о том, что центральным звеном в обеспечении информационной безопасности являются интересы личности, ее конституционные права.

В частности представляют интерес проблемы правового регулирования защищенности указанных интересов при обмене данными в сети «Интернет».

Во – первых, законодательством Российской Федерации не дано даже само определение ключевых объектов, в кругу которых возникают интересующие нас правоотношения. Это такие понятия как доменное имя, Интернет, протокол и прочие. А если они и представлены где-либо, то сделано это не систематизировано и взаимосвязано. К примеру, вместо понятия «Интернет» Российское законодательство используются такие определения как "компьютерная сеть", "телекоммуникационные сети", а законодательные акты об информатизации оперируют словосочетанием "информационная сеть". При этом не даны признаки, по которым можно было бы уяснить различие этих понятий, и это приводит к избыточному терминологическому многообразию, пересечению предметов регулирования отдельных законов и подзаконных нормативных актов. Российская Федерация ратифицировала Федеральным законом от 30 марта 1995г № 37-ФЗ Устав и Конвенцию Международного союза электросвязи, подписанную в Женеве 22 декабря 1992 года. Осуществление связи с помощью Интернета и других телекоммуникационных сетей подпадает под определение электросвязи, данное в Уставе Международного союза электросвязи. В его пункте 1012 зафиксировано, что электросвязь это "… любая передача, излучение или прием знаков, сигналов письменного текста, изображений и звуков или сообщений любого рода по проводной, радио-, оптической или другим электромагнитным системам".В статье 37 Устава сказано об обязанности принимать меры для сохранения тайны международных сообщений, с резервированием за государством права передавать эти сообщения компетентным властям во исполнение внутреннего законодательства либо международных соглашений

## Проект Федерального закон "О правовом регулировании оказания Интернет-услуг" определяет Интернет как сеть электросвязи общего пользования, обеспечивающая передачу данных между компьютерными устройствами. В данную сеть входят все взаимоувязанные сети электросвязи, осуществляющие передачу компьютерных данных, за исключением выделенных и ведомственных сетей связи. Также даны в данном проекте и иные определения. Однако это всего лишь проект.

Общие методы обеспечения информационной безопасности Российской Федерации в соответствии с Концепцией ИБ разделяются на правовые, организационно-технические и экономические.

Технологические меры защиты информации предлагают все более и более совершенные средства защиты, но всегда находятся в гонке с методами обхода защиты, идя на пути длящейся тысячелетиями состязанию «замка и отмычки». Меня, как юриста, больше интересуют правовые способы защиты информации..

В уголовно-правовом направлении заслуживает внимания Конвенция Совета Европы о преступности в сфере компьютерной информации ETS N 185, которая была подписана 23 ноября 2001 г. в Будапеште. Она открыта для подписания как государствами - членами Совета Европы, так и не являющимися его членами государствами, которые участвовали в ее разработке. В частности, ее подписали Россия, США и Япония. Конвенция Совета Европы о киберпреступности подразделяет преступления в киберпространстве на четыре группы.

В первую группу преступлений указанных данной конвенцией входят преступления, направленные против конфиденциальности, целостности и доступности компьютерных данных и систем, входят: незаконный доступ (ст. 2), незаконный перехват (ст. 3), воздействие на компьютерные данные (противоправное преднамеренное повреждение, удаление, ухудшение качества, изменение или блокирование компьютерных данных) (ст. 4) или системы (ст. 5). Также в эту группу преступлений входит противозаконное использование специальных технических устройств (ст. 6) - компьютерных программ, разработанных или адаптированные на совершение преступлений, предусмотренных в ст. 2 - 5, а также компьютерных паролей, кодов доступа, их аналогов, посредством которых может быть получен доступ к компьютерной системе в целом или любой ее части). Нормы ст. 6 применимы только в том случае, если использование (распространение) специальных технических устройств направлено на совершение противоправных деяний.

* Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог и мошенничество с использованием компьютерных технологий (ст. 7 - 8). Подлог с использованием компьютерных технологий включает в себя злонамеренные и противоправные ввод, изменение, удаление или блокирование компьютерных данных, влекущие за собой нарушение аутентичности данных, с намерением, чтобы они рассматривались или использовались в юридических целях в качестве аутентичных.
* Третью группу составляет производство (с целью распространения через компьютерную систему), предложение и (или) предоставление в пользование, распространение и приобретение детской порнографии, а также владении детской порнографией, находящейся в памяти компьютера (ст. 9).
* Четвертую группу составляют преступления, связанные с нарушением авторского права и смежных прав.

Согласно Конвенции каждое государство-участник обязано создать необходимые правовые условия для предоставления следующих прав и обязанностей компетентным органам по борьбе с киберпреступностью: выемка компьютерной системы, ее части или носителей; изготовление и конфискация копий компьютерных данных; обеспечение целостности и сохранности хранимых компьютерных данных, относящихся к делу; уничтожение или блокирование компьютерных данных, находящихся в компьютерной системе.

Конвенция также требует создать необходимые правовые условия для обязания Интернет-провайдеров проводить сбор и фиксацию или перехват необходимой информации с помощью имеющихся технических средств, а также способствовать в этом правоохранительным органам. При этом рекомендуется обязать провайдеров сохранять полную конфиденциальность о фактах подобного сотрудничества.

В начале 2002 г. был принят Протокол N 1 к Конвенции о киберпреступности, добавляющий в перечень преступлений распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающегося на расовой, национальной, религиозной или этнической принадлежности.

В рамках СНГ можно выделить Федеральный закон от 1 октября 2008 г. N 164-ФЗ "О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации"., Соглашение об обмене экономической информацией от 26 июня 1992 г., Соглашение о межгосударственном обмене научно-технической информацией от 26 июня 1992 г., Соглашение об обмене правовой информацией от 21 октября 1994 г. и др.

Кроме этого, сотрудничество по развитию трансграничных коммуникаций предусматривается двухсторонними договорами Российской Федерации. Среди них Соглашения о сотрудничестве в области информации и вычислительной техники с Правительством Французской Республики от 15 февраля 1996 г., Правительством Республики Беларусь от 27 февраля 1996 г.,

Внутренне законодательство Российской Федерации не столь насыщено.

Ч 2. ст. 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" гласит: «Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации».

Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных" возлагает ответственность за сохранение конфиденциальности данных на операторов (провайдеров) сети.

«Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных, за исключением случаев, предусмотренных частью 2 настоящей статьи. 1. Если субъект персональных данных считает, что оператор осуществляет обработку его персональных данных с нарушением требований настоящего Федерального закона или иным образом нарушает его права и свободы, субъект персональных данных вправе обжаловать действия или бездействие оператора в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке. Статья 12. данного закона посвящена трансграничной передаче данных. «До начала осуществления трансграничной передачи персональных данных оператор обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных.»

Учитывая вышесказанное можно предложить следующие направления защиты конфиденциальности данных при их передаче:

* Дальнейшее развитие нормативно-правовой базы, устранение внутренних противоречий и коллизий
* Изучение, анализ и заимствование положительного опыта зарубежных стран в вопросах сохранения конфиденциальности данных при их передачи
* Развитие дальнейшего международного сотрудничества в сфере защиты информации
* Повышение информационной культуры общества и граждан
* Развитие и законодательное оформление системы технических средств защиты
* Совершенствование правоприменительной деятельности

информационный правовой интернет государство