НЕГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКАЯ АКАДЕМИЯ АДВОКАТУРЫ И НОТАРИАТА»

Творческое задание

на тему: «Информационная безопасность. Актуальные проблемы правового регулирования»

Выполнил:
Магистрант 1 курса
Коноплин Сергей Юрьевич

Проверил:
д-р юрид.наук, проф. Шагиева Р.В.

Москва, 2017

Содержание

Введение

Актуальность темы «Правовое обеспечение информационной безопасности в Российской Федерации» обусловлена фактором вхождения общества в его информационную фазу развития, основанную на новейших наукоёмких технологиях. Реальность 21 века такова, что «информационное воздействие становится главным рычагом управления людьми. Оно все больше заменяет физическое воздействие, тысячелетиями считавшееся единственным и непременным средством управления». В связи с активным внедрением в нашу жизнь информационных технологий и развитием коммуникации в сфере международной жизни возникли отношения, требующие адекватного реагирования и правового регулирования.

Предметом исследования является понятие « информационная безопасность» и анализ существующего правового механизма обеспечения информационной безопасности в Российской Федерации.

1. Современная концепция информационной безопасности

Единой универсальной дефиниции понятия «информационная безопасность» в настоящее время не выработано.

Так, А.А. Стрельцов полагает, что «информационная безопасность определяется защищенностью от угроз информации, информационной инфраструктуры, правового статуса субъектов информационной сферы, определяемого совокупностью их прав и обязанностей, а также деятельности по реализации национальных интересов в информационной сфере».

В.А. Тихонов, В.В. Райх под информационной безопасностью в широком смысле понимают «такую ситуацию в информационной сфере, которая гарантирует выявление, предупреждение, нейтрализацию и устранение всех негативных событий, явлений и процессов, возникающих в ходе информатизации, и обеспечивает дальнейшее развитие рассматриваемого объекта защиты (личности, общества, государства, предприятия и т.д».

Конкретизируя термин «информационная сфера», Л. К. Терещенко формулирует понятие «информационная безопасность», как состояние защищенности национальных интересов Российской Федерации в информационной сфере, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений».

Некоторые авторы обосновывают данное явление через наличие угрозы, т.е. определяют информационную безопасность как состояние защищенности национальных интересов в информационной сфере от внутренних и внешних угроз. Один из подходов нашел свое отражение в работах ученых технического профиля. Они сводят информационную безопасность в основном к деятельности по защите свойств информации и информационной инфраструктуры техническими и организационными мерами, основываясь на положениях государственных стандартов.

В международной практике также не существует единства во взглядах на информационную безопасность. Выработано две принципиально несовместимых позиции. Сторонники первой из них (США) настаивают на том, что информационная безопасность – это, прежде всего, безопасность технических систем связи, защита информации и данных, в особенности результатов научных исследований, интеллектуальной собственности, сведений частного характера, противодействие криминальной и террористической деятельности. Противоположную позицию занимают те, кто рассматривает как принципиально важные военные аспекты информационной безопасности (основные сторонники - Россия и Китай).

Легальное значение данного понятия содержится в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской Федерации 09.09.2000 г. № Пр-1895, согласно которой под информационной безопасностью Российской Федерации понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

В настоящее время возрастает роль и значение информационной безопасности в рамках обеспечения национальной безопасности Российской Федерации по следующим основаниям.

Во-первых, одной из главных причин необходимости поддержания на высоком уровне информационной безопасности, является развитие информатизации общества. Исследования показывают, что развитие окружающей информационной среды оказывает значительное воздействие на общественный прогресс и развитие каждого человека. Поэтому, информационная среда нуждается в надежной защите, в том числе правовой.

Во-вторых, в условиях глобализации роль информации возрастает. Она вполне обоснованно может считаться объектом и продуктом труда, одним из основных богатств страны, а также стратегическим национальным ресурсом.

В-третьих, в политической сфере все большее значение приобретают не столько силовые, сколько информационные факторы. Например, возможности эксплуатировать интеллектуальный потенциал других стран, распространять и внедрять свои духовные, идейные ценности, свою культуру, язык, возможности тормозить духовно-культурное развитие других стран, трансформировать и даже подрывать их духовно-нравственные устои.

Также нельзя не учесть тот факт, что между научно-техническим прогрессом и информационной безопасностью личности, общества и государства прослеживается прямо пропорциональная связь. По мере развития науки и техники возрастает роль и значение информационной безопасности.

Стоит отметить, что информация и информационная инфраструктура для развитых стран стали критическими компонентами, воздействие на которые способно вызвать крупномасштабные аварии, дезорганизовать государственное и военное управление, финансовую систему, научные центры, вызвать военные конфликты и поражения в них.

Многие сферы жизнедеятельности человека, общества и государства трудно представить без последних достижений научно-технического прогресса, которые за последние годы проникли в них настолько, что сделали их зависимыми.

Возросшая роль информации в XXI в., который называют веком информационным, как никогда актуализирует вопрос об обеспечении информационной безопасности. Помимо организационно-технической составляющей обеспечения информационной безопасности значительную роль в этом механизме должно выполнять и право.

2. Объекты и субъекты информационных правоотношений

Правовое регулирование информационной безопасности формируется на базе информационных правоотношений, охватывающих все направления деятельности субъектов информационной сферы. Они охватывают все области информационной сферы, всех субъектов и объектов правоотношений.

Объекты правоотношений в области информационной безопасности - это духовность, нравственность и интеллектуальность личности и общества, права и свободы личности в информационной сфере; демократический строй, знания и духовные ценности общества; конституционный строй, суверенитет и территориальная целостность государства.

Субъектами правоотношений в области информационной безопасности выступают личность, государство, органы законодательной, исполнительной и судебных властей, система обеспечения безопасности, Совет Безопасности РФ, граждане.

Поведение субъектов в данной области определяются предписаниями законов и других нормативных правовых актов в порядке осуществления их прав и обязанностей, направленных на обеспечение защищенности объектов правоотношений.

Права и обязанности субъектов задаются нормами законов и иных нормативных правовых актов, устанавливающих правила поведения субъектов в порядке защиты объектов правоотношений, контроля и надзора за обеспечением информационной безопасности. Здесь же вводятся ограничения информационных прав и свобод в порядке защиты интересов граждан, общества, государства. При формировании норм права, установления прав и обязанностей применяются методы конституционного, административного и гражданского права.

Ответственность за правонарушения в информационной сфере устанавливается в порядке: защиты нравственности и духовности личности, общества, государства от воздействия недоброкачественной, ложной

информации и дезинформации; защиты личности в условиях информатизации; защиты информации и информационных ресурсов от несанкционированного доступа (гражданско-правовая, административно-правовая, уголовно-правовая ответственность). Особенности установления ответственности за правонарушения в среде трансграничных информационных сетей, в том числе в Интернет основываются на особенностях и юридических свойствах информации, информационных технологий и средств их обеспечения.

3. Актуальные проблемы правого регулирования

В настоящее время в мире насчитывается 2,5 миллиарда пользователей Интернет, то есть более трети населения планеты, является частью всемирной паутины. Каждые 30 секунд в сети появляется новый сайт, предлагающий товары и услуги. Мир физически осязаемый уже не может существовать обособленно от мира виртуального. Интернет стал не только многомиллиардной индустрией, но и жизненно важной инфраструктурой для мировой экономики.

Сегодня нет сферы человеческой деятельности, в которой в том или ином виде не присутствовали бы информационные технологии. На международном и национальном уровнях мы говорим об информатизации, компьютеризации, информационных сетях, внедрении и развитии информационных систем. «Перед всеми нами открываются огромные возможности», - отмечает Окинавская Хартия глобального информационного общества.

Вместе с этим оборотной стороной информатизации стала проблема обеспечения информационной безопасности в сети Интернет. Причем угрозы информационной безопасности потенциально опасны для отдельного человека, для государства и для всего мирового сообщества. Более того, на межгосударственном уровне существует возможность использования информационного потенциала одними странами для подчинения и подавления других государств. Многие государства, как, впрочем, и международные организации стали использовать информационные технологии в целях, несовместимых с задачами поддержания международной стабильности и безопасности, соблюдения принципов отказа от применения силы, невмешательства во внутренние дела государств, уважения прав и свобод человека. Угроза Интернет-безопасности может исходить и от частных лиц. Пример этого был продемонстрирован в апреле 2013 года на технологическом форуме в Голландии, где хакер при помощи смартфона

взламывал бортовой компьютер обычного самолета и добивался полной управляемости воздушным судном, работающим в режиме «автопилот».

В формировании стабильных отношений в глобальной сети и обеспечения информационной безопасности решающую роль должно сыграть правовое регулирование. Интернет в силу своей специфики (наднациональный характер, трансграничность, открытый и всеобщий доступ, отсутствие единого владельца) требует особого подхода в регулировании.

Применительно к Интернет-пространству отмечается очевидная сложность разработки такого режима, поскольку международное сообщество сталкивается с задачей кодификации не только новой и сложной с технической точки зрения области деятельности, но и крайне чувствительной для их безопасности сферы.

В качестве нормативно-регулятивной меры обеспечения безопасности в сети Интернет можно рассматривать сетевые кодексы поведения. Эта идея впервые была выдвинута вскоре после появления самой сети – тогда появились первые кодексы. Однако они не были эффективны. Причина в том, что нормы внутрисетевого поведения распространяются только на отдельные, связные сообщества пользователей Интернет. Внутри такого сообщества применяемые нормы саморегулирования эффективны и могут быть легко донесены до каждого пользователя. Вне устойчивого круга общения эти нормы, также могут применяться, но их регулятивные качества резко снижаются. Проблему обеспечения информационной безопасности в сети Интернет не удастся решить только с помощью саморегулирования. Это может быть хорошим дополнением к системе правового регулирования.

К следующей группе мер относятся меры по контролю. Они применяются на всех уровнях регулирования информационной безопасности. Говоря о контроле в глобальной сети в целях обеспечения информационной безопасности все мероприятия необходимо оценивать с точки зрения баланса интересов личности, общества, государства и мирового сообщества. В

нормативных актах различного уровня декларируется стремление обеспечить доступ к информационным ресурсам для максимального числа пользователей. В этих документах речь идет об открытости и доступности Интернета как информационного ресурса и как неотъемлемой части инфраструктуры мировой экономики. Таким образом, по общему правилу, закрепленному в международных, региональных и национальных актах, Интернет должен быть доступным и открытым источником. Однако документы содержат и положения, позволяющие контролировать возможность использования сети Интернет посредством ограничений или запретов.

В России были приняты меры по контролю за информационным наполнением сети Интернет. В 2012 году был принят закон о реестре запрещенных сайтов, предполагающий блокировку страниц и сайтов, содержащих запрещенную в РФ информацию. Принятие этого закона вызвало большой общественный резонанс. В традиционных СМИ и на различных Интернет-площадках были развернуты дискуссии на эту тему. Практически все поддерживали положения, касающиеся защиты детей. Противники закона опасались, что благие намерения защитить российское общество от пагубного влияния негативного сетевого контента обернутся Интернет-цензурой и блокировкой оппозиционных, неугодных власти сайтов. По поводу принятия данного закона Совет при Президенте РФ по развитию гражданского общества и правам человека выступил с заявлением, в котором отмечалось: «Мы считаем крайне важным остановить введение цензуры в русскоязычном сегменте сети Интернет и, в частности, на территории России – это приведёт к появлению нового «электронного занавеса», что губительно скажется на правах и возможностях граждан России, на развитии общества в целом и становлении всей экономики». Против принятия закона (в части введения фильтрации рунета – российского Интернета) выступили такие сетевые ресурсы как Google, LiveJournal, ВКонтакте, Яндекс. В знак протеста русская Википедия объявила забастовку,

и ресурс был недоступен в течение суток. Федеральный закон № 139-ФЗ был принят и вступил в силу 1 ноября 2012 года. Недостатком механизма контроля сети Интернет, прописанном в указанном Федеральном законе, является то, что на официальном сайте www.zapret-info.gov.ru невозможно увидеть полный перечень запрещенных сайтов, что представляется неверным с позиции открытости информации и с точки зрения требований, предъявляемых к правовому национальному закону международным правом.

Конвенция о защите прав человека и основных свобод 1950 г. в ч. 2 ст. 10 предусматривает возможность ограничения свободы выражения мнения в определенных целях. Европейский Суд по правам человека определил критерии такого ограничения. Любое ограничение свободы выражение мнения, закрепленное в национальном законодательстве, должно соответствовать двум требованиям – точности и доступности. Это означает, что право должно быть в адекватной мере доступным: граждане должны иметь возможность ориентироваться в том, какие правовые нормы применяются к данному случаю. Норма не может считаться законом, пока она не будет сформулирована с достаточной степенью точности, позволяющей гражданину сообразовывать с ней свое поведение, предвидеть в разумной степени, применительно к обстоятельствам, последствия, которые может повлечь за собой то или иное действие. Таким образом, ограничивая доступ граждан к информации в виде реестра сайтов, которые были признаны запрещенными в России, государство лишает возможности ориентироваться в информационной среде и определять свое поведение в сети Интернет на будущее. Граждане не могут опираться исключительно на критерии отнесения электронного ресурса к запрещенным, закрепленные в законе, поскольку последние не всегда четко сформулированы. Необходимо основывать свое поведение и на практике применения законодательства.

О стремлении государства усилить контроль в сети свидетельствуют попытки разработать и принять Федеральный закон «О регулировании сегмента Российской Федерации сети Интернет». Существовало несколько

проектов этого документа. В настоящее время идея принятия закона вновь обсуждается, разработана его очередная концепция. Согласно концепции, информационная безопасность в сети Интернет обеспечивается посредством защиты участников взаимодействия в сети от информации, распространение которой в РФ запрещено; защитой авторских и интеллектуальных прав в сегменте РФ в сети; защитой персональных данных и иной информации ограниченного доступа. По словам его инициаторов, закон о регулировании Интернета в России нужен для того, чтобы «преступления, совершаемые с использованием современных технологий под прикрытием анонимности, также расследовались, виновные устанавливались и наказывались. Новый закон необходим для того, чтобы вооружить правоохранительные органы инструментом, необходимым для борьбы со злом в сети». По замыслу разработчиков, все противоправные деяния, совершенные в сети, должны подпадать под действие УК РФ или КоАП РФ.

По оценкам экспертов ежесекундно жертвами киберпреступников становятся 12 человек в мире, и это количество с каждым годом растет.

Начальник Управления «К» МВД России Мошков Алексей Николаевич на XVII Национальном форуме информационной безопасности «Инфофорум-2015» сообщил, что «по данным ведомства в 2014 году на территории Российской Федерации было зарегистрировано 11 тысяч преступлений, связанных с мошенничеством в Интернете и информационной среде. Как и в прежние годы, основным мотивом киберпреступлений является извлечение материальной выгоды. Именно поэтому чуть менее половины (около 41%) из всех зарегистрированных преступлений это мошенничество и кражи».

Таким образом, за год, в период с 2013 по 2014 года, количество преступлений в информационной среде увеличилось на 4,5 тысячи (на 59 %).

По мнению специалистов крупнейшего производителя антивирусного программного обеспечения в России «Лаборатория Касперского», в ближайшие 10 лет киберпреступность будет развиваться в направлении кибершпионажа. Эксперты считают, что кибершпионаж будет

специализироваться в атаках на бизнес, причем в большей степени по заказам. Коммерческий шпионаж, кражи баз данных, информационные атаки с целью подрыва репутации будут особенно востребованы в условиях информационной экономики. В лаборатории считают, что грядет настоящая война хакеров и противостоящих им компьютерных специалистов больших корпораций.

Таким образом, можно говорить о формировании нового сегмента теневой экономики – «черного» киберрынка, отрицательно влияющего на экономическую безопасность всего государства. Кроме того, это свидетельствует о появлении новых видов институциональных ловушек, что также угрожает экономической безопасности государства.

Развитие кибершпионажа в масштабах всей экономики имеет далеко идущие последствия. Наиболее богатые корпорации, способные закупать дорогостоящие IT-системы, получают возможность добывать финансовые, технологические и иные данные, недоступные для более бедных конкурентов. Тем самым нарушается естественная информационная структура рынков, создаются условия для проведения крупных спекулятивных сделок, для нарушения правил проведения открытых торгов на товарных, фондовых и валютных биржах. Кроме того, новейшие электронные технологии используются для формирования ложного имиджа компаний, завышения кредитных рейтингов и даже шантажа.

Правовое регулирование противодействия киберпреступности в Российской Федерации как таковое отсутствует. До сих пор нигде законодательно не закреплены и не раскрыты такие понятия как «киберпространство», «киберпреступность», «кибертерроризм», «кибершпионаж» и прочие, отсутствуют критерии разграничения компьютерной преступности и киберпреступности.

Контролировать киберпреступность и бороться с ней на уровне отдельного государства практически невозможно. Поэтому для борьбы с угрозой киберпреступности, которая, безусловно, будет расти с дальнейшим

расширением сферы использования информационных технологий, предоставляя всё большие возможности для противоправной деятельности, как отдельным лицам, так и преступным группам, необходимо постоянное международное сотрудничество.

Проблемы информационной безопасности нуждаются в дальнейшем развитии системного правового регулирования на основе тщательного анализа международных правовых норм, зарубежного законодательства, действующего законодательства Российской Федерации и правоприменительной практики.

Выводы

В заключении необходимо сказать, что информационная безопасность России является базовой составляющей национальной безопасности России. Она напрямую влияет на эффективную работу органов государственной власти, является неотъемлемым фактором в борьбе с организованной преступностью и мировым терроризмом.

Излишняя открытость России в 90-х годах в период так называемой «демократизации» общества привела к крупным потерям, как в экономической, так и в политической составляющей Российской Федерации.

Внедрение современных технологий и законодательная основа защиты информации, должна стать мощным звеном в укреплении вертикали власти в России и ее становлении как экономически и политически сильного государства на мировой арене.

Список нормативных актов и литературы

1. Доктрина информационной безопасности Российской Федерации: утверждена Президентом Российской Федерации 09.09.2000 № Пр-1895 // Российская газета. – № 187. – 28.09.2000.

2. Стратегия развития информационного общества в Российской Федерации: утверждена Президентом Российской Федерации 07.02.2008 № Пр-212 // Российская газета. – № 34. – 16.02.2008.

3. Всеобщая декларация прав человека: принята Генеральной Ассамблеей ООН 10.12.1948 // Российская газета. – № 67. – 05.04.1995.

4. Окинавская хартия глобального информационного общества: принята на о. Окинава 22.07.2000 // Дипломатический вестник. – № 8. – 2000.

5. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин. – СПб.: СПбНИУИТМО. – 2014. – 173 с.

6. Козориз Н.Л. Информационная безопасность в системе противодействия опасности / Н.Л. Козориз // Информационное право. – 2013. – № 1. – С. 28-31.