УДК 340, 341, 347

Д.В. Сироткин[1]
А.А. Тыртышный[2]
А.А. Тыртышный-мл.[3]
И.С. Рекунков[4]

СОВРЕМЕННЫЕ ПОДХОДЫ К ИССЛЕДОВАНИЮ МЕХАНИЗМОВ ПРАВОВОГО РЕГУЛИРОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной статье авторы анализируют основные угрозы государству, обществу, личности в области информационной безопасности, рассматривают подходы к исследованию механизмов правового регулирования в области информационной безопасности через правовые модели.

Ключевые слова: *информационная безопасность, информационная интеграция, информационное противоборство, модели правового регулирования сферы информационной безопасности и противоборства, Стратегия национальной безопасности РФ, Военная доктрина РФ, механизм правового регулировании.*

D.V. Sirotkin
A.A. Tyrtyshny
A.A. Tyrtyshny-j.
I.S. Rekunkov

MECHANISMS OF LEGAL REGULATION IN THE FIELD OF INFORMATION SECURITY

In this article, the authors analyze the main threats to the state, society and personality in the field of information security, and consider some approaches to the study of mechanisms of legal regulation in the field of information security through legal model.

Keywords: *information security, information integration, information confrontation, models of legal regulation in the field of information security and confrontation, the National Security Strategy, Military Doctrine of the Russian Federation.*

Рассматривая зарождающееся информационное общество как новую цивилизационную реальность, которая должна соединить константы жизни локальных цивилизаций и информационные универсалии, следует отметить, что становление информационного общества имеет не только положительные последствия, но и реальные предпосылки активного информационного противоборства. Более того, в XXI веке эта сфера геополитического противостояния для большинства стран перешла в категорию наиболее приоритетных государственных задач. Она пронизывает в настоящее время все формы борьбы, начиная с дипломатической и экономической и заканчивая вооруженной. К тому же, несмотря на существование целого ряда международных соглашений в области информации и коммуникации, международное право во многом отстает от тех задач, которые встали перед человечеством в результате научно-технического прогресса в этой области.

Важным направлением обеспечения информационной безопасности Российской Федерации является совершенствование ее правового обеспечения.

[1] Магистрант АНО ВО «Российский новый университет».

[2] Кандидат психологических наук, доцент, декан юридического факультета АНО ВО «Российский новый университет», член экспертного совета комитета по образованию Государственной думы Федерального собрания Российской Федерации.

[3] Аспирант АНО ВО «Российский новый университет».

[4] Магистрант АНО ВО «Российский новый университет».

Правовое обеспечение информационной безопасности Российской Федерации представляет собой систему правового регулирования общественных отношений в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере.

Правовое обеспечение информационной безопасности Российской Федерации включает согласованную систему нормативных актов, регулирующих рассматриваемые отношения, а также согласованную деятельность органов государственной власти по их развитию и совершенствованию.

Современное состояние правового регулирования информационной безопасности Российской Федерации характеризуется фрагментарностью выбора объектов правового регулирования в области противодействия угрозам национальной безопасности в информационной сфере, недостаточной согласованностью используемых для этого правовых механизмов, стохастичностью деятельности субъектов законодательной инициативы по развитию и совершенствованию этих механизмов, недостаточной эффективностью, а зачастую и противоречивостью включаемых в эти механизмы правовых норм.

В настоящее время правовое регулирование информационной безопасности Российской Федерации как единая система правового регулирования общественных отношений в области противодействия угрозам национальным интересам Российской Федерации в информационной сфере развито недостаточно.

Это обстоятельство заметно снижает возможности Российской Федерации по противодействию угрозам ее информационной безопасности, не способствует укреплению национальной безопасности России.

Зафиксированные в выделенных нормативных правовых актах правовые механизмы противодействия угрозам национальным интересам Российской Федерации в области обеспечения гарантий прав и свобод человека и гражданина в целом оказывают положительное влияние на состояние защищенности данных интересов [5].

В то же время, отдельные положения нормативных правовых актов российского законодательства, регулирующих отношения в области прав и свобод человека и гражданина, внутренне противоречивы и в ряде случаев не согласуются с нормами международного права. Излишняя декларативность некоторых правовых норм приводит к тому, что нарушение законодательных установлений далеко не всегда влечет за собой наступление соответствующей ответственности. Правовые механизмы защиты отдельных прав и свобод человека и гражданина не определены.

К числу наиболее серьезных недостатков правового регулирования защиты прав и свобод человека и гражданина в информационной сфере следует отнести:

– неопределенность механизмов обеспечения доступа к открытой информации органов государственной власти и органов местного самоуправления, создающая условия для ущемления прав и свобод человека и гражданина, включая право на информацию о состоянии окружающей среды, фактах и обстоятельствах, создающих угрозу для жизни и здоровья людей;

– отсутствие установленных норм ответственности за ограничение или нарушение права на доступ к открытой информации;

– отсутствие правового регулирования общественных отношений в области сбора и использования персональных данных, механизмов их внесудебной защиты, реализации права на личную и семейную тайны, неприкосновенность частной жизни, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, телеграфных и иных сообщений;

– недостаточную согласованность и полноту правовых норм, регулирующих установление режимов ограничения доступа к информации, обязанностей субъектов правоотношений по защите информации с ограниченным доступом, ответственности за нарушения установленных режимов ограничения доступа к информации;

– неурегулированность прав государства на объекты интеллектуальной собственности, полученные в результате выполнения работ, полностью или частично финансируемых за счет средств государственного бюджета, а также недостаточное правовое регулирование общественных отношений в области охраны таких объектов интеллектуальной собственности, как ноу-хау, изобретения, составляющие государственную или служебную тайны, фирменные наименования;

– слабое развитие правового регулирования отношений, связанных с ограничением распространения массовой информации в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства;

– отсутствие правового регулирования распространения информации, предназначенной для неограниченного круга потребителей, в открытых информационно-телекоммуникационных сетях.

Российская Федерация, подписавшая Окинавскую хартию глобального информационного общества и тем самым взявшая на себя обязательства по участию в совместной деятельности международного сообщества по созданию условий для перехода человечества к постиндустриальной фазе своего развития, сформулировала свои интересы в Доктрине информационной безопасности Российской Федерации.

В дополнение к вышесказанному, в 2017 году Президент Российской Федерации издал указ, который ввел новую редакцию «Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы». В статье 17 данной Стратегии определено, что международно-правовые механизмы, позволяющие отстаивать суверенное право государств на регулирование информационного пространства, в том числе в национальном сегменте сети Интернет, не установлены. Большинство государств вынуждено «на ходу» адаптировать государственное регулирование сферы информации и информационных технологий к новым обстоятельствам.

После последних мировых событий, а именно «цветных революций», следует вывод, что существует ряд стран, для которых выполнение норм международного права необязательно. В связи с этим можно сказать, что существуют два вида правовых моделей в области информационной безопасности: однополярная и многополярная. Однополярная модель относится отдельно к США как к стране, предполагающей, что законы и «беззакония» ее страны распространяются на весь мир, и многополярная модель, в которой золотой серединой является международное право, одинаково распространяющееся на все страны.

1. Однополярная правовая модель информационной безопасности (ИБ).

После распада Советского Союза США остались единственной сверхдержавой, которая, по мнению сторонников подобной модели, пытается нести «бремя» мирового лидерства, дабы не допустить «вакуума силы» в международных отношениях и обеспечить распространение демократии по всему миру. Интересно отметить, что не только реалисты, но и неолибералы не отвергают тезиса об оправданности американской гегемонии после окончания холодной войны. Так, ряд российских экспертов ссылается на мнение известного американского политолога Дж. Ная, который считает, что отсутствие лидерства со стороны сверхдержавы плохо и для других стран, ибо в одиночку они не в состоянии справиться со сложными проблемами эпохи глобальной взаимозависимости.

Однополярная модель предполагает усиление системы военно-политических союзов, ведомых США. Так, НАТО, по мнению ряда аналитиков, должна обеспечивать стабильность в трансатлантической подсистеме международных отношений, гармонизировать отношения между США и европейскими государствами в стратегической области, обеспечивать американское военное присутствие в Европе и гарантировать недопущение конфликтов на этом континенте.

США ясно дали понять (и продемонстрировали это на деле в ходе войны на Балканах 1999 г.), что именно НАТО должно стать главным гарантом европейской безопасности.

Другие региональные организации – ЕС, ОБСЕ и пр. – могут лишь играть второстепенную роль в архитектуре европейской безопасности XXI в. В соответствии с новой стратегической концепцией НАТО, принятой весной 1999 г., зона ответственности этого блока расширяется за счет включения в нее сопредельных регионов. Любопытно, что, с точки зрения ряда экспертов, НАТО не только выполняет задачи военно-политического союза, но и всё больше приобретает идентификационно-цивилизационные функции. Членство в НАТО служит своего рода индикатором принадлежности к западной, «демократической» цивилизации. Те же, кто не являются членами НАТО и не имеют шансов войти в эту организацию, относятся к «чужим» и даже враждебным цивилизациям. По выражению одного скандинавского аналитика, по границам НАТО пролегает рубеж между Космосом и Хаосом.

После свержения режима Саддама Хусейна некоторые российские эксперты стали утверждать, что с победой США в Ираке окончательно утвердилась однополярная модель мира, и Вашингтон будет фактически единолично править миром и определять способы решения возникающих перед мировым сообществом проблем (лишь для антуража привлекая другие страны или разрешая этим странам действовать самостоятельно только в тех случаях, когда это не задевает американских интересов). По этой причине, настаивают сторонники этого взгляда, России пора отказаться от претензий на роль самостоятельного центра силы и необходимо побыстрее примкнуть к лидеру, то есть к США. В противном случае попусту будут потрачены силы и средства на ненужную конфронтацию с Вашингтоном.

Необходимо, однако, отметить, что однополярная модель международной безопасности подвергается обоснованной критике как в Рос-

сии, так и в самих США. Российские критики однополюсной модели ссылаются на мнение ряда американских специалистов, которые полагают, что США просто не имеют необходимых ресурсов для выполнения функций мирового лидера. Они также обращают внимание на то, что американское общественное мнение тоже весьма сдержанно относится к этой идее, ибо осознает, что подобная роль требует существенных финансовых затрат.

Другие центры силы – ЕС, Япония, Китай – также высказывают свое неприятие американской гегемонии (в открытой или завуалированной форме). Кроме того, основной инструмент осуществления американского лидерства – военно-политические альянсы – плохо приспособлен для решения современных проблем. Эти союзы были созданы в период холодной войны, и их главным предназначением было предотвращение военных угроз. Многие аналитики – российские и зарубежные – считают, что для адекватного ответа на вызовы из области «мягкой безопасности» (финансово-экономические кризисы, экологические катастрофы, терроризм, наркобизнес, незаконная миграция, информационные войны и пр.) военная машина, унаследованная из прошлого, просто не годится.

Ключевую роль в правовом регулировании информационной безопасности США играет американский «Закон об информационной безопасности». Его цель – реализация минимально достаточных действий по обеспечению безопасности информации в федеральных компьютерных системах, без ограничений всего спектра возможных действий.

Характерно, что уже в первом разделе закона называется конкретный исполнитель – Национальный институт стандартов и технологий (НИСТ), отвечающий за выпуск стандартов и руководств, направленных на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Таким образом, имеется в виду как регламентация действий специалистов, так и повышение информированности всего общества.

Согласно закону, все операторы федеральных информационных систем (ИС), содержащих конфиденциальную информацию, должны сформировать планы обеспечения ИБ. Обязательным является и периодическое обучение всего персонала таких ИС. НИСТ, в свою очередь, обязан проводить исследования природы и масштаба уязвимых мест, вырабатывать экономически оправданные меры защиты. Результаты исследований рассчитаны на применение не только в государственных системах, но и в частном секторе.

Закон обязывает НИСТ координировать свою деятельность с другими министерствами и ведомствами, включая Министерство обороны, Министерство энергетики, Агентство национальной безопасности (АНБ) и т.д., чтобы избежать дублирования и несовместимости.

Помимо регламентации дополнительных функций НИСТ, Закон предписывает создать при Министерстве торговли комиссию по информационной безопасности, которая должна:

– выявлять перспективные управленческие, технические, административные и физические меры, способствующие повышению ИБ;

– выдавать рекомендации Национальному институту стандартов и технологий, доводить их до сведения всех заинтересованных ведомств.

С практической точки зрения, важен раздел 6 Закона, обязывающий все правительственные ведомства сформировать план обеспечения информационной безопасности, направленный на то, чтобы компенсировать риски и предотвратить возможный ущерб от утери, неправильного использования, несанкционированного доступа или модификации информации в федеральных системах. Копии плана направляются в НИСТ и АНБ.

В 1997 году появилось продолжение описанного закона – законопроект «О совершенствовании информационной безопасности» (Computer Security Enhancement Act of 1997), направленный на усиление роли Национального института стандартов и технологий и упрощение операций с криптосредствами.

В законопроекте констатируется, что частный сектор готов предоставить криптосредства для обеспечения конфиденциальности и целостности (в том числе аутентичности) данных, что разработка и использование шифровальных технологий должны происходить на основании требований рынка, а не распоряжений правительства. Кроме того, здесь отмечается, что за пределами США имеются сопоставимые и общедоступные криптографические технологии, и это следует учитывать при выработке экспортных ограничений, чтобы не снижать конкурентоспособности американских производителей аппаратного и программного обеспечения.

Для защиты федеральных информационных систем рекомендуется более широко применять технологические решения, основанные на разработках частного сектора. Кроме того, предлагается оценить возможности общедоступных зарубежных разработок.

Очень важен раздел 3, в котором от НИСТ требуется по запросам частного сектора готовить добровольные стандарты, руководства, средства и методы для инфраструктуры открытых ключей, позволяющие сформировать негосударственную инфраструктуру, пригодную для взаимодействия с федеральными ИС.

Приветствуется разработка правил безопасности, нейтральных по отношению к конкретным техническим решениям, использование в федеральных ИС коммерческих продуктов, участие в реализации шифровальных технологий, позволяющее в конечном итоге сформировать инфраструктуру, которую можно рассматривать как резервную для федеральных ИС.

Важно, что в соответствии с разделами 10 и далее предусматривается выделение конкретных (и немалых) сумм, называются точные сроки реализации программ партнерства и проведения исследований инфраструктуры с открытыми ключами, национальной инфраструктуры цифровых подписей. В частности, предусматривается, что для удостоверяющих центров должны быть разработаны типовые правила и процедуры, порядок лицензирования, стандарты аудита.

На законодательном и других уровнях информационной безопасности США было сделано многое. Смягчены экспортные ограничения на криптосредства, сформирована инфраструктура с открытыми ключами, разработано большое число стандартов (например, новый стандарт электронной цифровой подписи – FIPS 186-2, январь 2000 г.). Всё это позволило не заострять больше внимания на криптографии как таковой, а сосредоточиться на одном из ее важнейших приложений – аутентификации, рассматривая ее по отработанной на криптосредствах методике. На базе этих законов в США сформирована общенациональная инфраструктура электронной аутентификации.

Программа безопасности, предусматривающая экономически оправданные защитные меры и синхронизированная с жизненным циклом ИС, упоминается в законодательстве США неоднократно. Согласно пункту 3534 («Обязанности федеральных ведомств») подглавы II («Информационная безопасность») главы 35 («Координация федеральной информационной политики») рубрики 44 («Общественные издания и документы»), такая программа должна включать:

– периодическую оценку рисков с рассмотрением внутренних и внешних угроз целостности, конфиденциальности и доступности систем, а также данных, ассоциированных с критически важными операциями и ресурсами;

– правила и процедуры, позволяющие, опираясь на проведенный анализ рисков, экономически оправданным образом уменьшить риски до приемлемого уровня;

– обучение персонала с целью информирования о существующих рисках и об обязанностях, выполнение которых необходимо для их (рисков) нейтрализации;

– периодическую проверку и переоценку эффективности правил и процедур;

– действия при внесении существенных изменений в систему;

– процедуры выявления нарушений информационной безопасности и реагирования на них; эти процедуры должны помочь уменьшить риски, избежать крупных потерь, организовать взаимодействие с правоохранительными органами.

Помимо этого в законодательстве США имеются в достаточном количестве и положения ограничительной направленности, и директивы, защищающие интересы таких ведомств, как Министерство обороны, АНБ, ФБР, ЦРУ.

2. Многополярная правовая модель информационного противоборства.

Ряд ученых, по своим убеждениям близких к реализму, считают, что в период после окончания холодной войны на деле сложилась не однополярная, а многополярная система международных отношений.

Лидерство США во многом является мифическим, иллюзорным, ибо такие страны, как страны ЕС, Япония, Китай, Индия, страны АСЕАН, Россия, «признавая мощь США», всё же проводят свой курс в международных делах, часто не совпадающий с американскими интересами. Росту влияния этих центров силы способствует тот факт, что меняется сама природа силы в международных отношениях. На передний план выдвигаются не военные, а экономические, научно-технические, информационные и культурные составляющие этого феномена. А по этим показателям США не всегда являются лидером. Так, по экономическому и научно-техническому потенциалу страны ЕС, Япония и страны АСЕАН вполне сопоставимы с США. Например, по объему помощи развивающимся странам Япония сравнялась с США (10 млрд долл. ежегодно). В военной сфере ЕС также проявляет всё большую строптивость, собираясь регулярно начать формирование европейской армии. Китай, осуществляющий широкомасштабную программу модернизации своих вооруженных сил, по оценкам специалистов, превратится к 2020 г. в одну из ведущих военных держав не только АТР, но и всего мира.

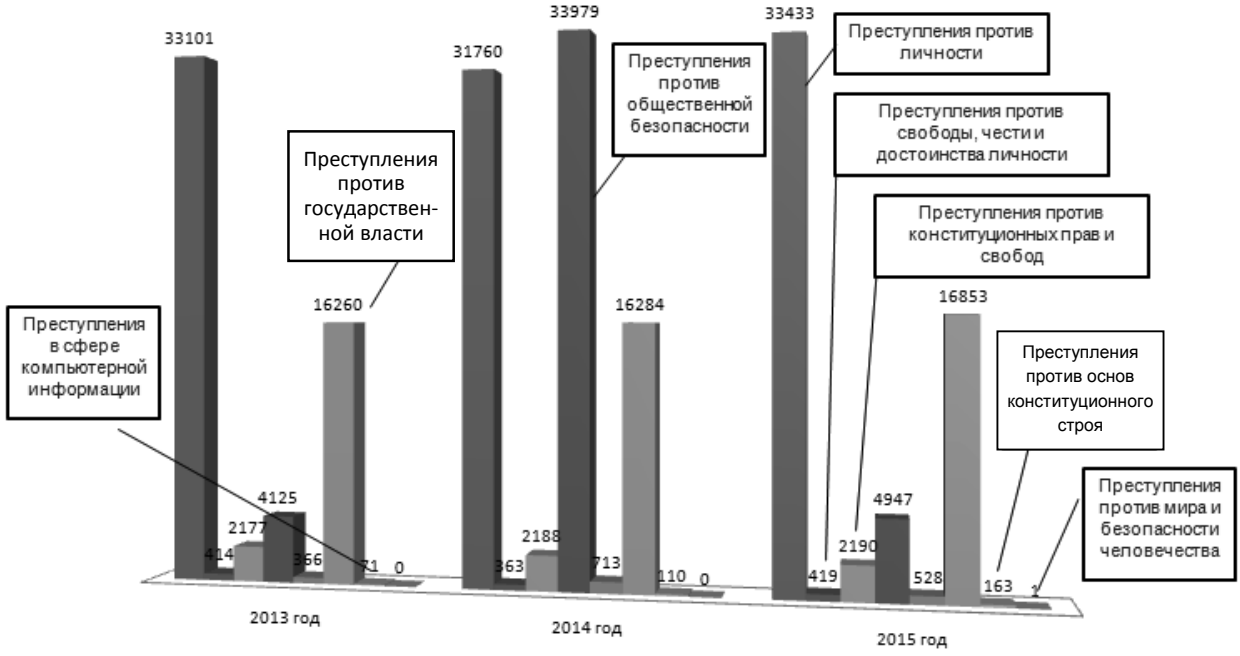

Рис. 1. Анализ состава преступлений
в области информационной безопасности

Сторонники многополярной модели настаивают на том, чтобы США признали необоснованность своих претензий на мировое лидерство и начали партнерский диалог с другими центрами силы.

Идеи равноправности особенно популярны в российском политическом и академическом истеблишменте и даже возведены в ранг официальной внешнеполитической доктрины во всех вариантах КНБ.

Оппоненты многополярности подчеркивают, что подобная модель не принесет стабильности в международных отношениях. Ведь она исходит из видения системы международных отношений как поля вечной конкуренции между «центрами силы». А это, в свою очередь, неизбежно приведет к конфликтам между последними и постоянным переделам сфер влияния.

Из описанных выше моделей в российском внешнеполитическом мышлении доминирует многополярная модель.

В современном мире наметилась тенденция смещения военных опасностей и военных угроз в информационное пространство и внутреннюю сферу Российской Федерации. В соответствии с Военной доктриной Российской Федерации, а это пока единственный открытый нормативный правовой акт в Российской Федерации, где непосредственно упоминается об информационном противоборстве, одной из основных задач является создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности.

Разработанные модели получили свое подтверждение из отчетов Верховного суда Российской Федерации за 2013, 2014, 2015 годы по всем преступлениям против государства, общества, личности. Результаты анализа были классифицированы, объединены и представлены на рис. 1.

Сравнительный анализ состава преступлений в области информационной безопасности за 2013–2015 гг. представлен на рис. 2.

Разработанные модели позволяют исследовать механизм правового регулирования в области информационной безопасности. Статистические данные по преступлениям в сфере информационной безопасности, полученные в ходе анализа, подтверждают практическое применение иностранными государствами в 2014 году информационного воздействия на Российскую Федерацию (государство, общество,

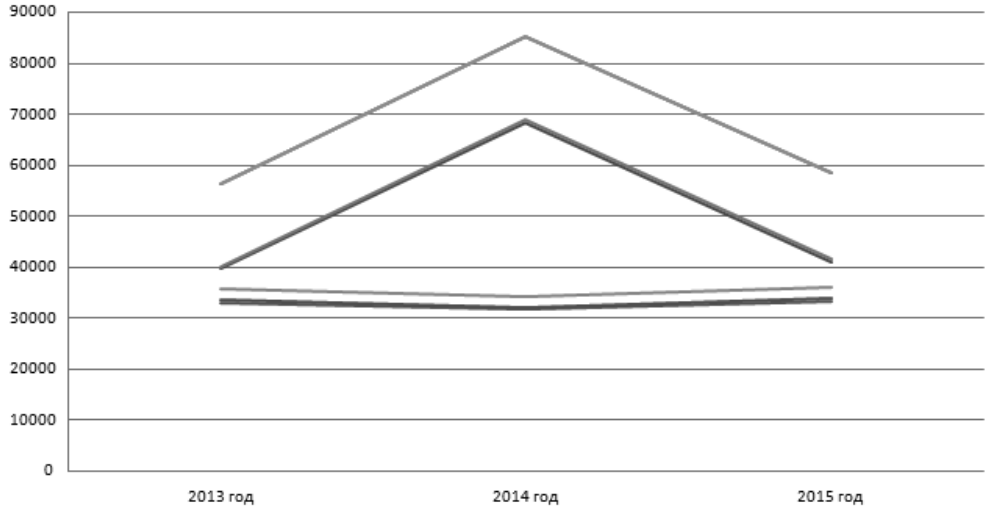

Рис. 2. Сравнительный анализ состава преступлений
в области информационной безопасности за 2013–2015 гг.

личность). Для эффективного построения системы правовой защиты государства, общества и личности необходимо разработать механизм реализации публичных и частно-правовых аспектов информационной безопасности.

Ввиду того что в Украине по указу Президента Петра Порошенко запретили деятельность российских ресурсов, многие из которых пользовались огромной популярностью среди населения, в частности сервисы «Яндекса», «ВКонтакте» и «Mail.ru», ни у общественных организаций, ни у стран ЕС не возникает вопроса о том, что идет прямое нарушение прав человека в получении информации.

Литература

1. Указ Президента Российской Федерации от 1 октября 2017 г. «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

2. О правовом исследовании интеграционных процессов на постсоветском пространстве / А.А. Тыртышный, В.Е. Понаморенко, Д.Г. Коровяковский // Вестник Российского нового университета. – 2010. – № 4. – С. 5–6.

3. Аксёнов С.В., Сироткин Д.В., Тыртышный А.А, Тыртышный-младший А.А. Современное информационное противоборство: публично-правовые и частноправовые аспекты // Цивилизация знаний: российские реалии : труды Семнадцатой Международной конференции (г. Москва, 22–23 апреля 2016 г.). – М. : РосНОУ, 2016. – С. 577–585.

4. http://nvo.ng.ru/concepts/2016-04-22/1_flowers.html

5. https://m.lenta.ru/news/2016/02/04/electronic/