Тип работы: Дипломная работа

Предмет: Международные отношения

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ
Актуальность темы исследования. В современном мире информация становится основой деятельности во всех сферах общественных отношений. В то же время, ценность информации обуславливает существование различного рода правонарушений, объектом которых выступает сама информация. Именно поэтому, вопросы правовой защиты различных видов информации приобретают особую актуальность в условиях жесткой конкуренции на мировой арене и внутри государства.
Повсеместное использование информации оказывает влияние на специфику правового регулирования порядка поведения сторон правоотношений, возникающих при осуществлении поиска, передачи, производства и распространении, и обеспечении защиты информации.
Специфика правового регулирования защиты информации в Российской Федерации заключается в

различной отраслевой принадлежности правовых норм, обусловленной повсеместностью использования информации в общественных отношениях.
Особую разновидность информации представляет собой информация, образующаяся в результате деятельности государственных органов, информация, распространение которой может нанести ущерб безопасности Российской Федерации. К указанной категории относятся сведения, составляющие государственную тайну. Государственная тайна как правовое явления является достаточно сложным, выступающим одновременно и как элемент системы права, и как острый политический инструмент, способный оказать существенное влияние на самые различные сферы государственной и общественной жизни.
1. КОНЦЕПТУАЛЬНЫЕ ОСНОВЫ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ОБОСТРЕНИЯ ГЕОПОЛИТИЧЕСКОЙ КОНКУРЕНЦИИ
1.1. Глобальное информационное противостояние как характеристика современных международных отношений
Символом настоящего времени становится информационная безопасность. В этой связи необходимо отметить значение Интернета, который уже является таким же пространством международной политики. В сети возможно применение различными террористическими и экстремистскими организациями информационных технологий с целью военных угроз, вербовки

террористов 4>, воздействия на атомные и военные объекты, а также кибератаки в сфере коммуникационных сетей и бытовых цифровых технологий. Наметился рост компьютерной преступности в кредитно–финансовой сфере с нарушением конституционных прав и свобод человека и гражданина.
Дезинформация и фальсификация данных становятся прикрытием геноцида, агрессии, атак террористов и начала военных действий. Все «арабские весны» были направлены на разрушение сознания гражданина, носителя тех ценностей гражданских прав и свобод человека, которые позволяют ему чувствовать национальное достоинство, защищать свою страну.
Наблюдаемые процессы интеграции и унификации оказывают заметное влияние на информационные отношения. Под воздействием глобализации информационные потоки выходят за рамки национальных и интегрируются в мировое информационное пространство, чему в значительной степени способствует совершенствование в ходе информационной революции коммуникационных систем и способов использования космического пространства для передачи информации.
Хартия глобального информационного общества (Окинава, 22 июля 2000 г.) прямо утверждает, что «информационно–коммуникационные технологии (ИТ) являются одним из наиболее важных факторов, влияющих на формирование общества XXI века. Их революционное воздействие касается образа жизни людей, их образования и работы, а также взаимодействия правительства и гражданского общества».
Возможности Интернета широко задействовались и задействуются для организации «цветных революций», например, в Ираке, Ливии, Сирии, Украине. Воздействие на массовое сознание граждан осуществляется таким образом, что не просто преподносится недостоверная информация, а используются механизмы влияния на принятие решений личностью, формулирование и восприятие ею оценочных суждений. Зачастую это осуществляется за счет использования эгоистических побуждений, ложного патриотизма, низкой правовой и политической культуры, не говоря уже о ксенофобии и прочих взглядах экстремистской направленности.

Противник использует предпосылки для социальных конфликтов, играет на незащищенности и нереализованности прав и свобод отдельных групп населения, т.е. ищет надломы, противоречия и использует их в своих геополитических интересах. Сегодня, как отмечают ученые, отсутствуют гарантии обеспечения прав и свобод личности в силу социального и экономического кризисов, и именно это может стать причиной снижения авторитета власти, усиления напряженности в обществе и появления экстремистских настроений.
Такие негативные проявления могут быть использованы в качестве условий для разжигания «цветных революций» и прочих деструктивных проявлений, что особенно актуально в условиях планирования акций провокационного характера перед предстоящими выборами 2016 и 2018 гг.
В Стратегии Национальной безопасности США 2015 г. отмечены тенденции противостояния государственного управления и народа в некоторых государствах, подрыва легитимности государственной власти. США рассматривают обязанность по защите своего народа как не заканчивающуюся на своих границах, а также утверждают об укреплении обороны и внутренней безопасности страны, достижении своих геополитических целей не исключительно вооруженными методами, а с помощью повышения активности гражданского общества, развития свободы и объединений групп в сети Интернет и т.д., в том числе среди населения других стран.
1.2. Основные подходы к трактовке понятий «Информационная война» и «Информационная безопасность»
Принцип экстерриториальности Интернета обращает внимание на то, что Интернет может быть оружием в информационной войне как извне, так и снаружи государственных границ. Поэтому первоочередной задачей является обеспечение информационной безопасности и необходимое установление правового регулирования информации в сети Интернет, распространение которой запрещено на территории Российской Федерации.
Сложным, а местами почти невозможным, является нахождение консенсуса между правовым регулированием и принципами цифрового равенства и свободы, которые заложил Тим Бернерс–Ли. Кроме фундаментального принципа, гласящего, что любой человек может делиться информацией с кем угодно и где угодно, и универсальности, существуют принципы, которыми во

избежание нарушения целостности сети Интернет пренебрегать нельзя.
Информационная безопасность есть защита конфиденциальности, целостности и доступности информации. В свою очередь под конфиденциальностью понимается обеспечение доступа к информации только авторизованным пользователям, целостность представляется как обеспечение достоверности и полноты информации и методов ее обработки, а доступность – как обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости. Информационная безопасность не является проблемой, специфичной только для Российской Федерации. Практически все страны с развитой экономикой на уровне государственных органов, предпринимательских структур разрабатывают и применяют комплексные меры, направленные на обеспечение информационной безопасности.
Информационная безопасность направлена прежде всего на безопасность субъектов (личности, общества, государства), при этом в зависимости от группы субъектов ее содержание может различаться. Не случайно в Доктрине информационной безопасности Российской Федерации речь идет о сбалансированных интересах личности, общества и государства в информационной сфере. И даже внутри указанных крупных блоков могут выделяться определенные группы субъектов, применительно к которым установлены особенности их информационной безопасности. С этой

точки зрения можно говорить об информационной безопасности органов исполнительной власти, представляющих собой одну из ветвей власти государства.
По мнению А. Я. Приходько для того, чтобы стать полноценным субъектом информационной войны, необходимо обладать следующими признаками:
– обязательное наличие у субъекта воздействия собственных интересов, которые он и стремится соблюдать в противодействии;
– наличие у субъекта информационной агрессии специальных сил, которые направлены на воздействие на реципиента;
– разработка и использование в деле информационного оружия;
– подконтрольное субъекту информационной агрессии информационное пространство, при помощи которого он оказывает влияние на общество. Чаще всего – это агрессия государства через СМИ или же агрессия других государств через информационные ресурсы;
– существование некоей государственной идеологии, которая позволяет участие субъекта информационной агрессии в информационной войне
– власть над средствами массовой информации – телевидением, радио, Интернет–СМИ .
1.3 Цифровой суверенитет и информационная война в контексте международного права
Возможности сети Интернет почти безграничны, и любая информация, распространяемая профессионалами по спланированному алгоритму, может достигнуть федерального и мирового масштаба в считанные часы.
Современный этап жизни российского общества, связанный с глобализацией информационного пространства, создает новые проблемы для развития личности, общества и государства. В социальном пространстве информация распространяется быстро, преимущественно благодаря техническим возможностям. При этом используемая информация часто носит противоречивый, агрессивный и негативный характер и, как следствие, воздействует на социальные, нравственные и психологические составляющие общественной жизни. Деструктивные изменения духовной сферы общества проявляются в форме искажения нравственных норм и критериев, а также в неадекватных социальных стереотипах и установках, ложных ориентациях и ценностях. В связи с этим целесообразно говорить о проблеме информационной безопасности.
Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе развития технического прогресса, быстрыми темпами растущего использования современных информационных технологий эта зависимость неизбежно возрастает. Значимость информационной безопасности для Российской Федерации обусловлена тем, что информационная сфера обеспечивает функционирование всех остальных сфер жизни общества и государства.
До недавнего времени национальная безопасность рассматривалась как сохранение суверенитета и территориальной целостности государства, его устойчивость перед угрозой применения вооруженной силы со стороны других государств.
Однако в настоящее время национальная безопасность видится как комплексная системная

проблема, учитывающая наличие многообразных факторов и угроз, в том числе информационных.
5
В последние годы в официальных заявлениях Президента РФ и иных высших должностных лиц неоднократно указывается на необходимость обеспечения «цифрового» или «технологического» суверенитета. Однако данные цели пока не получили своего системного решения в российском законодательстве, что обусловлено недостаточной теоретической разработкой концепции информационного суверенитета государства.
Цифровой суверенитет – это право государства самостоятельно определять, что происходит в его цифровой сфере. И самому принимать решения по всем необходимым вопросам регулирования и защиты этой сферы от любого внешнего внимания.
Информация, размещаемая на форумах, в социальных сетях, должна подвергаться верификации, что необходимо в целях пресечения попыток размещения недостоверной и провокационной информации, например, о вводе российских войск на территорию иного государства и пропаганде в целях возбуждения расовой, национальной вражды, например, о выброшенных портретах после шествия «Бессмертного полка».
2. РОССИЙСКАЯ ФЕДЕРАЦИИ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
2.1. Международный аспект деятельности РФ по обеспечению информационной безопасности
Международное позиционирование института информационной безопасности в контексте взаимодействия государств по противодействию международной преступности предметно ориентировано на создание и поддержание универсальной системы информационной безопасности в интересах всего мирового сообщества. Российская Федерация в своем статусном положении великой державы, постоянного члена Совета Безопасности ООН, предметно заявившего о своей приверженности верховенству права (Декларация тысячелетия 2000 г., Итоговый документ Всемирного саммита 2005 г.), занимает важное место в универсальной системе информационной безопасности. Примером систематизации норм в сфере защиты информационной безопасности служит правительственное соглашение между Россией и США, заключенное в 2013 году о сотрудничестве в научных исследованиях и разработках в ядерной и энергетической сферах. В документе в том числе перечислялись меры доверия и способы противодействия кибервойне, а также декларировалось создание общей системы информационной безопасности. Однако в 2016 году действие соглашения приостановили.
Основными направлениями международного сотрудничества, отвечающими интересам РФ, являются:
- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских сетях и в каналах информационного обеспечения мировой торговли, к конфиденциальной информации в международных политических, экономических и военных союзах, блоках и организациях, к информации в международных правоохранительных организациях, ведущих борьбу с международной организованной преступностью, международным терроризмом, распространением наркотиков и незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми;
- запрещение разработки, распространения и применения «информационного оружия»;
- обеспечение безопасности международного информационного обмена, в том числе сохранности информации при её передаче по национальным телекоммуникационным сетям и каналам связи;
- координация деятельности правоохранительных органов государств
- участников международного сотрудничества по предотвращению компьютерных преступлений;
6
- участие в проведении международных конференций и выставок по проблеме безопасности информации;
- контроль обеспечения безопасности информации в ходе международного военно-технического сотрудничества, при проведении международных выставок (салонов) вооружения и военной техники.
Международная значимость включенности Российской Федерации в универсальную систему информационной безопасности по линии борьбы мирового сообщества с международной преступностью обозначена конкретной готовностью Российского государства внести свой собственный (соизмеримый с его местом в современном миропорядке) вклад в дело обеспечения международной законности и правопорядка.

2.2. Национальный аспект деятельности РФ по обеспечению информационной безопасности
В России все аспекты борьбы с ИБ-угрозами национального масштаба рассматриваются на уровне Доктрины информационной безопасности, которая служит основой для принятия нормативных актов.
Среди фундаментальных вопросов доктрины – необходимость самостоятельного информационного присутствия России в международном сообществе и выбор каналов поставки достоверных данных и новостей, что позволит снизить ущерб от дезинформационных атак.
Они нашли отражение в основных принципах Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы, утвержденной Указом Президента РФ от 9 мая 2017 г. N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»:
Как показало исследование Лаборатории Касперского, в 2017 году треть российских компаний (36%) хотя бы раз подверглась DDoS–атакам (в 2016 году – 17%). Среди микропредприятий пострадали 37%, компаний среднего и малого бизнеса – 31%, а больших корпораций – 39%. При этом каждый пятый пострадавший (21%) признался, что атака привела к значительному снижению производительности сервисов компании, а у 8% произошел сбой транзакций и процессов.
Помимо непосредственного ущерба, кибератака может таить в себе и скрытую угрозу. Каждая третья компания (35%) полагает, что атаки были отвлекающим маневром. Почти в половине случаев (47%) кибератака «прикрывала» утечку или кражу данных, 43% случаев – взлом корпоративной сети, а в 41% – включала заражение вредоносным программным обеспечением. У трети пострадавших (31%) произошло еще и прямое хищение денег.
2.3. Проблемы реализации мер обеспечения информационной безопасности
В условиях Интернета зачастую происходят правонарушения, связанные с обработкой персональных данных, не соответствующей целям, заявленным операторами персональных данных (термин в соответствии с российским законодательством) или контролерами данных (термин в соответствии с законодательством Великобритании).
Например, поисковые системы собирают информацию обо всех действиях своих пользователей, осуществляемых в Интернете без их согласия, и в дальнейшем эту информацию используют для рассылки рекламы или предоставления дополнительных услуг.

Свои действия поисковые системы обосновывают тем, что информация о совершаемых действиях пользователей не относится к персональным данным. В 2015 г. в Великобритании рассматривались поправки к дефиниции «персональные данные», в связи с чем предлагалось расширить определение персональных данных так, чтобы в него были включены IP–адреса и cookie.
В поправках к Закону предлагается следующее определение: «Персональные данные – данные, с помощью которых физическое лицо может быть идентифицировано прямо или косвенно на основании средств, которые могут быть использованы контролером данных... в том числе применительно к идентификационным номерам, данным о местоположении, онлайн–идентификаторам...».
В настоящее время остро стоит проблема как правового регулирования собственно оказания услуг в сфере «облачных» технологий в целом , так и обеспечения информационной безопасности при использовании «облачных» технологий в частности.
Однако, по данным исследований European Union Agency for Network and Information Security (ENISA), не существует реальной возможности обеспечить информационную безопасность при оказании облачных сервисов. Несмотря на это, международным сообществом предпринимается ряд мер, направленных на обеспечение безопасности в «облаке», к числу которых можно отнести:
– руководство информационной безопасностью при заключении договоров SLA, что включает в себя разработку ряда сервисных контрактов между клиентами и провайдерами «облачных» услуг;
– анализ критических «облачных сервисов» – выражается в анализе и обсуждении с заинтересованными сторонами последствий сбоя «облачных» служб и обстоятельств, при которых «облачные» технологии следует рассматривать как критические информационные инфраструктуры;
– экспертная оценка «облачной» безопасности и устойчивости – включает в себя работу постоянной экспертной группы ENISA Cloud Security and Resilience Expert Group;

– выработка предложений об эффективной практической деятельности для обеспечения безопасности правительственных облаков;
– отчеты об инцидентах «облачных» вычислений – определяют методику предоставления информации об инцидентах «облачной» безопасности в критических секторах и для государственных органов;
– список схем сертификации «облака» (Cloud Certification Schemes List, CCSL), актуальных для потенциальных клиентов «облачных» вычислений;
– сертификация «облачных» Стратегий Евросоюза.
В рамках технологического решения по обеспечению безопасности информации при оказании «облачных» услуг и иерархии рисков применяется стандарт ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services, который определяет совокупность рисков:

ЗАКЛЮЧЕНИЕ

Информационная безопасность не является проблемой, специфичной только для Российской Федерации. Практически все страны с развитой экономикой на уровне государственных органов,

предпринимательских структур разрабатывают и применяют комплексные меры, направленные на обеспечение информационной безопасности.
Информационная безопасность направлена прежде всего на безопасность субъектов (личности, общества, государства), при этом в зависимости от группы субъектов ее содержание может различаться.До сих пор ни отечественная, ни зарубежная юридическая наука не выработали комплексного и универсального определения понятия киберсуверенитета с включением в него всего многообразия субъектов и видов интернет–правоотношений, возникающих в связи с осуществлением публично–властных полномочий государства в национальном сегменте «всемирной паутины», с установлением четких границ и целевых ориентиров для государственного вмешательства в указанную сферу, являющуюся первопричинно сферой реализации суверенитета личности.Международно–правовое позиционирование института информационной безопасности в контексте взаимодействия государств по противодействию международной преступности предметно ориентировано на создание и поддержание универсальной системы информационной безопасности в интересах всего мирового сообщества.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Нормативные правовые акты

1. «Окинавская хартия глобального информационного общества» (Принята на о. Окинава 22.07.2000)// Дипломатический вестник. 2000. N 8. С. 51 – 56.
2. «Устав Организации Объединенных Наций» (Принят в г. Сан–Франциско 26.06.1945)// «Сборник действующих договоров, соглашений и конвенций, заключенных СССР с иностранными государствами», Вып. XII, – М., 1956, с. 14 – 47
3. «Международный пакт о гражданских и политических правах» (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496–ом пленарном заседании Генеральной Ассамблеи ООН)// «Бюллетень Верховного Суда РФ», N 12, 1994
4. Федеральный закон от 27.07.2006 N 149–ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2018) // «Российская газета», N 132, 31.07.2016
5. Федеральный закон от 26.07.2017 N 187–ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»// «Российская газета», N 167, 31.07.2017
6. Федеральный закон от 27.07.2006 N 149–ФЗ (ред. от 25.11.2017) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2018)// «Парламентская газета», N 126–127, 03.08.2006
7. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»// «Собрание законодательства РФ», 12.12.2016, N 50, ст. 7074
8. Указ Президента РФ от 09.05.2017 N 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы»// «Собрание законодательства РФ»,

15.05.2017, N 20, ст. 2901
Специальная и научная литература
9
9. Баринов С.В. О правовом определении понятия «информационная безопасность личности» // Актуальные проблемы российского права. 2016. N 4. С. 97 – 105.
10. Бородин К.В. Правовое регулирование распространения информации в сети Интернет в условиях информационной войны // Право и кибербезопасность. 2014. N 1. С. 27 –
11. Баранов А.П. Можно ли защитить в «облаке» конфиденциальную информацию / А.П. Баранов // Системы высокой доступности. 2012. N 8. С. 12 – 15.
12. Велиева Г.М. Защита свободы информации в практике Европейского суда по правам человека // Современное право. 2014. N 4. С. 159 – 164.
13. Долинская В.В. Источники права и официальные информационные ресурсы // Законы России: опыт, анализ, практика. 2017. N 10. С. 3 – 10.
14. Ефремова М.А. Информационная безопасность как объект уголовно–правовой охраны // Информационное право. 2014. N 5. С. 21 – 25.
15. Ефремова М.А. Социальная обусловленность уголовно–правовой охраны информационной безопасности Российской Федерации // Вестник Пермского университета. Юридические науки. 2017. N 2. С. 222 – 230.
16. Жигоцкий П.Э., Чесноков Н.А. Проблемы информационной безопасности (защита от информации, распространение которой запрещается) // Российский следователь. 2015. N 4. С. 35 – 42.
17. Жарова А.К. Право и информационные конфликты в информационно–телекоммуникационной сфере: монография. М.: Янус–К, 2016. 248 с.
18. Трунцевский Ю.В. Вербовка в террористические организации: анализ форм и содержания подбора новобранцев // Военно–юридический журнал. 2016. N 6. С. 10 – 14.
19. Тарасов А.М. Киберугрозы, прогнозы, предложения // Информационное право. 2014. N 3. С. 11 – 15.
20. Седых Н.С., Гшиянц Р.Э. Графическая модель социальных репрезентаций терроризма // Национальная безопасность // Nota bene. 2014. N 5(34). С. 712 – 724.
21. Киреев В.В., Майоров В.И. Стратегия конституционного развития современной России (ценности, цели, риски) // Lex russica. 2017. N 6. С. 68 – 74.
22. Курносов Ю. В., Конотопов П. Ю. Аналитика: методология, технология и организация информационно–аналитической работы. – М., 2004. – с. 97
23. Молчанов Н.А., Матевосова Е.К. Доктрина информационной безопасности Российской Федерации (новелла законодательства) // Актуальные проблемы российского права. 2017. N 2. С. 159 – 165.
24. Приходько, А. Я. Информационная безопасность в событиях и фактах / А. Я. Приходько. – М.: СИНТЕГ, 2001. – с. 57
25. Саитов И.А., Миронов А.Е., Королев А.В. Противодействие кибертерроризму – важнейшая задача обеспечения информационной безопасности // Вестник национального антитеррористического комитета. 2012. N 2. С. 78 – 79.
26. Смородина О.С. Исторические особенности развития конституционных идей в России // Проблемы права. 2012. N 1.
10
27. Сухаренко А.Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. N 2. С. 2 – 5.
28. Терещенко Л.К., Тиунов О.И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. N 8. С. 100 – 109.
29. Цибуля А.Н., Гордин В.А. К вопросу о состоянии информационной безопасности государства в условиях современных вызовов и угроз // Военно–юридический журнал. 2014. N 3. С. 20 – 24.
30. Чеботарева А.А. Информационная политика России в обеспечении информационной безопасности личности: история и современность // История государства и права. 2015. N 24. С. 24 – 28.
31. Чеботарева А.А. Правовое обеспечение информационной безопасности личности в

глобальном информационном обществе // Юридический мир. 2016. N 8. С. 63 – 66.
32. Lazarsfeld P. The varied sociology of Paul F. Lazarsfeld / P. Lazarsfeld. – New York: Columbia University Press, 1982. – p. 74
33. Lamb, Ch. J. The Impact of Information Age Technologies on Operations Other than War / G. S. Lamb. – Washington, 1997. – 278 p.
34. Turkay Henkoglu and Ozgur Kulcu Evaluation of Conditions Regarding Cloud Computing Applications in Turkey, EU and the USA // 4th International Symposium on Information Management in a Changing World, IMCW 2013, Limerick, Ireland, September 4 – 6, 2013. Revised Selected Papers.
35. Fu X.W. Analysis of the Security Issues in Cloud Computing Mode. Computer CD / X.W. Fu // Software and Applications 5, 106 – 107 (2012).
36. Cloud computing security risks and opportunities for SMEs // European Union Agency for Network and Information Security. April 2015.
37. Incident Reporting for Cloud Computing Published: December 9, 2013. Authors: Marnix Dekker, ENISA, Dimitra Liveri, ENISA, Matina Lakka, ENISA // URL: https://www.enisa.europa.eu/publications/incident–reporting–for–cloud–computing.
Интернет источники
38. Есть ли войска России на Украине: история с фотографиями. URL: http://www.bbc.co.uk/russian/international/2014/04/140422_ukraine_russian_troops_photos.
39. МИД России. Основные тенденции развития международных отношений и пути формирования новой системы мироустройства // Официальный сайт Министерства иностранных дел Российской Федерации. URL: http://www.mid.ru/foreign_policy/positionwordorder/–/asset_publisher/6S4RuXfeYlKr/content/id/431964
40. Ложь: российские войска не вторгались в Украину (обновлено). URL: http://www.stopfake.org/lozh–rossijskie–vojska–ne–vtorgalis–v–ukrainu/.
41. Российские войска в Украине: война под прикрытием. URL: http://www.golos–ameriki.ru/content/article/2652995.html.
11
42. Наумов В.Б. Интернет и государственный суверенитет // Тезисы доклада на I Всероссийской конференции «Право и Интернет: теория и практика». URL: http://www.ifap.ru/pi/01/r16.htm.
43. Сокерин К.В. Субъекты права на доменное имя // Юридический мир. 2007. N 4. С. 10. URL: https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf
44. Лаборатория Касперского зафиксировала 2–кратный рост DDoS–атак на российский бизнес. // http://safe.cnews.ru/news/line/2017–10–13_laboratoriya_kasperskogo_zafiksirovala_2kratnyj
45. Cloud Security Guide for SMEs // URL: https://www.enisa.europa.eu/activities/Resilience–and–CIIP/cloud–computing/security–for–smes/cloud–security–guide–for–smes.
46. ISO/IEC 27017 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services // URL: https://www.iso.org/standard/43757.html.