DOI: 10.7256/2073-8560.2014.3.11511
При цитировании этой статьи сноска на doi обязательна

§ 4 ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Владимирова Т.В.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: СОЦИАЛЬНЫЕ ПРАКТИКИ И СТРУКТУРЫ

Аннотация: *Понятие информационной безопасности продолжает находиться в становлении, как в отдельных сферах жизнедеятельности общества, так и в целом — в теоретическом знании. Считаем, что разнообразные направления исследований и подходы к определению информационной безопасности возможно увидеть в едином методологическом ключе, исполненном на языке социально-философской теории. Такая операция, на наш взгляд, поспособствует дальнейшему наполнению и развитию понимания социальной природы понятия. Обеспечение информационной безопасности мы связываем с пониманием и владением особенностями современных социальных практик, которые позволяют сохранять адекватность внешнему миру информационных потоков, как индивиду, так и отдельным социальным системам, а значит, сохранять и индивиду и системе целостность и устойчивость в условиях нарастания девиации/инновации как вариативности коммуникаций, выраженной в росте интенсивности информационных потоков. Теоретико-методологическим основанием исследования явились социологические теории Э. Гидденса, М. Кастельса, Дж. Урри. В работе использовались труды российских ученых в области обеспечения информационной безопасности. Отмечается, что обеспечение информационной безопасности складывается из социальных практик и социальных структур. Предлагаемый подход позволяет развить понимание социальных аспектов информационной безопасности: увидеть особенности практик обеспечения безопасности, зафиксировать противоречие между локальностью структур и потоковым, сетевым характером информационных угроз. Отмечается, что высокая интенсивность коммуникаций практик мобильностей в обеспечении безопасности становится возможной благодаря такой особенности практик как приватизация безопасности.*

Ключевые слова: *информационная безопасность, практики информационной безопасности, структуры информационной безопасности, приватизация безопасности, локальность структур, информационная индустрия, информационная инфраструктура, институты информационного права, новые мобильности, информационные потоки.*

«На полях» саммита G20 в Мексике в 2012 году президенты Владимир Путин и Барак Обама могли подписать двустороннее соглашение о сотрудничестве в киберпространстве и мерах доверия. Однако договоренности сорвались из-за одного слова. Чтобы уйти от спора — «международная информационная безопасность» или «кибербезопасность», — стороны выработали компромиссную формулировку «безопасность в сфере использования информационно-коммуникационных технологий». Однако в последний момент Вашингтон потребовал убрать из этой конструкции слово «использования», делая упор лишь на физической защите своих компьютерных систем. Но для Москвы этот вопрос оказался принципиальным — она-то как раз считает, что дело не только в защите сетей и ресурсов, но и в том, кем, как и с какой целью информационно-коммуникационные технологии могут быть использованы (иными словами, не будут ли они оружием для психологических войн и пропаганды). Консультации по этой теме продолжаются.[1] Судя по всему, понятие информационной безопасности продолжает находиться в становлении, как на практике, так и в теории. Сегодня для осмысления проблемы обеспечения информационной

[1] Черненко Е. В. Холодная война 2.0? Киберпространство как новая арена противостояния // Россия в глобальной политике. 2013. — Том 11, — № 1. — С. 162–170.

DOI: 10.7256/2073-8560.2014.3.11511
При цитировании этой статьи сноска на doi обязательна

безопасности, необходима концептуализация ряда подходов к понятию на уровне социально-философского, гуманитарного дискурса.

Традиционно параметры понятия информационной безопасности принято осмысливать в технических и психологических характеристиках. Информационную безопасность определяют как защиту информации и защиту от информации[2]. С. П. Расторгуев отмечает, что информационная безопасность, являясь составляющей национальной безопасности, имеет два направления: безопасность информации (защита информации) и безопасность от информации (защита от «опасной», «неадекватной картине мира информации»).[3] Оба эти направления взаимосвязано реализуются как в гуманитарной, так и в технической сферах. При этом информационная безопасность в той или иной степени присутствует при обеспечении всех видов безопасности, начиная от экологической и заканчивая информационной. Подобное же видение информационной безопасности излагает Р. М. Юсупов. Он утверждает, что информационная безопасность соответствующего субъекта (личность, общество, государство, любая система) может быть определена как состояние, в котором ему (субъекту) не может быть нанесен существенный ущерб путем воздействия на его информационную сферу[4].

Считаем, что, методологически продуктивным является утверждение об информационной безопасности, как о «снятии информационной неопределенности относительно объективно и субъективно существующих потенциальных и реальных угроз за счет контроля над мировым пространством и наличия возможностей, условий и средств для отражения этих угроз, что в совокупности определяет уровень (степень) информационной безопасности каждого субъекта»[5]. Мы разделяем утверждение, что в содержании информационной безопасности ключевым является контроль за информацией, циркулирующей в мировом пространстве, а также наличие возможностей и средств для отражения возникающих угроз.[6] Подобный подход к определению информационной безопасности актуализируются в понятиях информационной войны, сетецентричной войны и информационного противоборства (М. В. Арсентьев, С. Н. Бухарин, С. П. Расторгуев, В. В. Цыганов, А. И Ивлева и др.) Также пишут о кибернетической безопасности и кибернетической войне (А. Д. Еляков, А. В. Тонконогов и др.)

В целом, существующая литература, посвященная анализу информационной безопасности в обществе, — в большей мере, — это тексты технологического и организационного характера, посвященные систематизации и структурированию организации действий субъектов различного масштаба, обеспечивающих информационную безопасность государства или отдельных организационных структур (С. П. Расторгуев, С. Н. Бухарин, В. В. Цыганов, В. В. Кульба, А. Г. Глушков, А. А. Смирнов и др.). Также рефлексия проблемы обеспечения информационной безопасности представлена в работах нормативно-правового характера (В. Н. Лопатин, И. Л. Бачило, П. У. Кузнецов, С. Н. Соколова, Е. К. Волчинская и др.).

Можно встретить аналитику, различного уровня системного анализа, посвященную: использованию информационных технологий в экстремистской деятельности (И. Ю. Сундиев, С. С. Станчик, Е. О. Кубякин); информационным аспектам экономической безопасности (С. А. Бахтин, А. М. Ельчанинов, А. Зуев, Л. Мясникова, З. Ч. Схаляхо); информационной безопасности в мировом политическом процессе (И. В. Сурма, А. Ф. Федоров) и др. Отдельным направлением, которое имеет прямое отношение к информационной безопасности, является информационное противоборство (С. П. Расторгуев, С. Н. Бухарин, В. В. Кульба, В. В. Цыганов, В. В. Прохватилов), теория информационных, сетецентричных войн (А. Г. Дугин, В. И. Ковалев, Ю. А. Матвиенко).

Считаем, что все вышеназванные направления и подходы к определению информационной безопасности возможно увидеть в едином методологическом ключе, исполненном на языке социально-философской теории. Такая операция, на наш взгляд, поспособствует дальнейшему наполнению и развитию понимания социальной природы понятия. Обеспечение

[2] Илюшенко В. Н. Информационная безопасность общества / Учебное пособие для ВУЗов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 1998. С. 3.

[3] Расторгуев С. П. Основы информационной безопасности / Учеб. пособие для студ. высших учебных заведений. — М.: Издательский центр «Академия», 2009. С. 18.

[4] Юсупов Р. М. Информационное обеспечение национальной безопасности // Национальная безопасность 2010. — № 7/8. — С. 87.

[5] Арсентьев М. В. К вопросу о понятии «Информационной безопасности» // Информационное общество. — 1997. — № 4–6. С. 48–50.

[6] См. там же.

DOI: 10.7256/2073-8560.2014.3.11511
При цитировании этой статьи сноска на doi обязательна

информационной безопасности мы связываем с пониманием и владением особенностями современных социальных практик, которые позволяют сохранять адекватность внешнему миру информационных потоков, как индивиду, так и отдельным социальным системам, а значит, сохранять и индивиду и системе целостность и устойчивость в условиях нарастания девиации/инновации как вариативности коммуникаций (роста интенсивности информационных потоков).

Об обеспечении информационной безопасности можно говорить в широком и узком смысле этого слова: информационная безопасность в условиях современного общества (актуальной социальной реальности потоков и сетей) и информационная безопасность в условиях киберпространства (виртуальной социальной реальности). В первом случае, и в целом, речь идет о социальных практиках, адекватных скорости и многообразию современных коммуникаций.[7] Во втором случае, речь идет о сетевых практиках, адекватных изменчивому виртуальному пространству сетей и потоков. Второй тип практик обеспечения информационной безопасности составляет частный случай первого. И первый тип, и второй тип социальных практик сводятся, к содержанию:

1. защиты субъектом своей информации и защиты от внешней информации;
2. к ориентации в информационном пространстве, поскольку ресурсы в условиях роста устаревания информации должны всякий раз пересматриваться и обновляться.

При рассмотрении информационной безопасности обратимся к возможностям теории структурации Э. Гидденса. Для нас функциональность понятий «социальная практика» и «социальная структура» заключается в их посреднической роли между понятием *коммуникации* (социальным информационным взаимодействием) *как социальной практикой и структурой как некоторой локальной упорядоченностью нормированных практик* (системой социальных ограничений). Подразумевается, что практика — действование, наполняется и структурируется коммуникацией/информацией. Термин указывает на то, что различные социальные деятельности «растягиваются» в широком пространственно-временном диапазоне. Социальные практики считаются источником и основой образования и субъекта, и объекта. В подобном аспекте теория структурации близка теории социальных систем Н. Лумана, где процессность коммуникации исключает дуальность субъекта/объекта.

Можно сказать, что *обеспечение информационной безопасности* общества в целом, и безопасности отдельных социальных субъектов *реализуется социальными практиками и социальными структурами*. С другой стороны, свою информационную безопасность субъект обеспечивает как в условиях актуальной реальности (не виртуальной), так и в условиях потоков и сетей киберпространства. Обращаем внимание на то, что рост интенсивности социального взаимодействия формирует, в целом, такие общие особенности социальных практик как рефлексивность и информационную насыщенность. Современные социальные практики для защиты информации и для защиты от информации в условиях интенсивности и устаревания коммуникации/информации выработали свои техники обеспечения безопасности. На эти особенности современных практик мы не раз указывали ранее[8]. Напомним: такие «особенности-техники» фиксируются в социальной теории в терминах «скорости и временности», «степени проходимости социальных ситуаций» (Э. Тоффлер), «отношения ограниченного участия» (Э. Тоффлер, З. Бауман, С. Леш и др.), «дальнодействия и отвлеченности» (В. Е. Кемеров), «объектуализации отношений или появлении «объектцентрированной социальности» (К. Кнорр Цетина), «делокализации социальных действий, их извлечения из конкретного контекста и свободного перемещения в самых широких пространственно-временных рамках»; «контрфактуальность мышления и калькуляция рисков» (Э. Гидденс), «частично-непрерывное внимание» и «пост-многозадачное поведение, характеризующее стремление индивида быть живым узлом коммуникационной сети» (Л. Стоун). Считаем, что в методологическом плане целесообразно объединить все эти особенности практик термином «новые социальные мобильности», который является основополагающим в социологии мобильностей Дж. Урри.

Важным аспектом новых социальных мобильностей как практик обеспечения безопасности является

[7] См. Владимирова Т.В. Информационная безопасность: к методологическим основаниям анализа вопроса // Информационное общество. — № 5. — 2012. — С. 47–52; Владимирова Т.В. Информационная безопасность: социологическая перспектива понятия // Национальная безопасность. — Nota bene. 2013. № 4 (27). — С. 597– 604. DOI: 10.7256/2073-8560.2013.4.7476.

[8] См. там же.

DOI: 10.7256/2073-8560.2014.3.11511
При цитировании этой статьи сноска на doi обязательна

высокая интенсивность коммуникаций, выраженная в скорости и многообразии взаимодействия. Чем выше уровень интенсивности (скорости и разнообразия) коммуникаций, осуществляемых субъектом, тем в большей безопасности он пребывает в смысле защищенности своих интересов в условиях роста информационных потоков и устаревания информации. *Высокая интенсивность коммуникаций в обеспечении безопасности становится возможной благодаря такому феномену как приватизация безопасности.*

Термин «приватизация безопасности» в своих работах развивает сегодня Ю. А. Полтораков. Он отмечает, что соответствующее «право на применение насилия» (традиционная прерогатива национального государства) присваивают себе уже не только национальные государства или объединения (НАТО и пр.) или их официальные представители («голубые каски» ООН и пр.), а разные неофициальные и неправительственные группы, движения и организации. Объединяя всех тех, кто использует насилие в своих целях, с «террористами», во многих случаях власти не только становятся неспособными адекватно «отразить» сам феномен приватизированного насилия, но и получают удобный повод для расправы с политическими противниками, которые также применяют насилие для достижения своих политических целей. Приобрел достаточно завершенный вид такой феномен как «частные армии».[9]

В современном обществе бурными темпами стал развиваться «негосударственный сектор безопасности». Ю. А. Полтораков отмечает, что косвенным проявлением этой тенденции в «экономической культуре» стало обновление подходов бизнеса к вопросам безопасности. Опираясь на исследования бизнес-обозрения компании Pricewaterhouse Coopers (согласно которому более 42% бизнеса сейчас рассматривает расходы на безопасность как стратегическую инициативу), Ю. А. Полтораков утверждает, что вместо того, чтобы реагировать на атаки и вторжения, компании хотят заранее быть активными в развертывании систем защиты с целью предотвращения возможных неприятностей в будущем. Это, в свою очередь, обозначилось на «качестве» экономической разведки, которая стала откровенно доминировать над политической.[10]

Считаем, что *приватизация безопасности*, которая выражается в росте многообразия частных структур обеспечения безопасности, также является *особенностью современных практик обеспечения информационной безопасности. Мобильность практик обеспечения безопасности и приватизация безопасности связаны тесным образом.*

Приведенные нами «особенности-техники» практик информационной безопасности (социальные мобильности) характеризуют сегодня, прежде всего, практики ведения информационного противоборства — «борьбы в информационной сфере, которая предполагает комплексное деструктивное воздействие на информацию, информационные системы и информационную инфраструктуру от подобного воздействия. Конечной целью информационного противоборства является завоевание и удержание информационного превосходства над противоборствующей стороной»[11]. Информационное противоборство представлено такими формами как информационная война, информационная борьба и борьба с информационной преступностью.

Как социальные практики в обеспечении информационной безопасности можно рассматривать политику государства по информатизации общества и обеспечению независимости информационной инфраструктуры. Важно отметить, что *развитие информационной инфраструктуры общества обеспечивает «инфраструктуру мобильностей» социальных субъектов.* Сама информационная инфраструктура и развитая информационная индустрия общества рассматриваются нами как социальные структуры в обеспечении информационной безопасности государства.

В целом, представление о структурах (отчасти и институтах) обеспечения информационной безопасности сегодня носит системный характер. Основные сегменты этих структур, их нормативный и правовой характер развиваются такой отраслью знания как информационное право.[12]

Российское государство как основной институт обеспечения безопасности общества разрабатывает информационную политику, основные направления

[9] Полтораков Ю. А. Политико-системные аспекты безопасности постиндустриального общества // Национальная безопасность / nota bene. — 2009. — № 2. — С. 19.

[10] Там же. С. 20.

[11] Пирумов В.С. Информационное противоборство. Четвертое измерение противостояния / В.С. Пирумов. — М.: «Оружие и технологии», 2010. — С. 41.

[12] В России проблемы правового обеспечения жизнедеятельности информационного общества сегодня активно ставятся и анализируются авторами ж. Информационное право.

DOI: 10.7256/2073-8560.2014.3.11511
При цитировании этой статьи сноска на doi обязательна

которой, первоначально, были заложены в Доктрине информационной безопасности от 2000 г. Эта политика направлена на поддержание и формирование различного рода систем, институтов, защищающих и развивающих информационную сферу общества. Это и институты информационного права, управленческие государственные структуры в области информационной политики и обеспечения информационной безопасности, и др.

Опосредованно, к структурам обеспечения информационной безопасности можно отнести различные организации по производству экспертного знания. Сегодня — это не только научные и образовательные структуры. Речь идет о беспрецедентном росте аналитических структур различного уровня, занимающихся анализом и прогнозированием экономических и социальных процессов (ВЦИОМ, ФОМ, Левада-Центр и др.). В том числе, отдельно, здесь же можно говорить об институциализации мониторинга общественного мнения.

Идет формирование структур информационной индустрии, уровень развития которой является основным показателем развитости и защищенности общества и государства. В нее входят частные и государственные организации, которые создают информацию различных видов, интеллектуальную собственность, обеспечивают функционирование устройств для распространения информации для потребителей, производят оборудование и программное обеспечение, призванное обрабатывать информацию.

Информационную индустрию можно представить в виде трех ее отраслей, которые создают содержание, его распространяют и обрабатывают. К индустрии содержания относятся организации, которые создают интеллектуальную собственность. В этом им помогают издатели, продюсеры, вещатели и прочие организации, которые придают первоначальному содержанию «товарный вид». Сюда же входят организации, которые сами не создают новой информации, но компилируют ее, производя справочники, базы данных, статистические сборники и т. п. На долю этих поставщиков информации приходится значительная часть доходов, получаемых в индустрии содержания. Индустрия распространения информации связана с созданием и управлением телекоммуникациями и сетями распространения информации. Она включает телекоммуникационные компании, сети кабельного телевидения, системы спутникового вещания, радио и телевизионные станции, компании сотовой связи и т. п. Индустрия обработки содержания охватывает производителей компьютеров, телекоммуникационного оборудования и потребительской электроники.[13]

Перевод информации в цифровую форму приводит к перекодировке значительных массивов информации, которые ранее были представлены на традиционных носителях — бумаге, видеопленке, магнитных лентах. В результате информация может легко копироваться, передаваться, объединяться, что дало толчок интенсивному развитию нового сектора информационной индустрии — мультимедийной промышленности. Происходит конвергенция технологий, связанных с созданием, обработкой и передачей информации.

Развиваются отдельные системы по обеспечению информационной безопасности внутри государственной власти — системы электронного правительства, отдельные подразделения государственных органов по защите критически важной информационной инфраструктуры страны, по защите государственной и коммерческой тайны и др.

Но существует противоречие между локальностью структур обеспечения безопасности и потоковым, сетевым характером угроз, не имеющих территориальную локализацию. Мы понимаем социальную структуру как некоторую *локальную упорядоченность нормированных практик* или условия ограничений в области допускающих соединение операций (Н. Луман). Всякая организационная структура имеет различный спектр ограничений действия — территориальный, нормативный, организационный и др. Большей подвижностью и мобильностью, а соответственно преимуществами в реализации целей, обладает не структура, а сети и потоки (Дж. Урри). Сети и потоки развивают действие экстерриториально, нормы, отрываясь от локальных культур, становятся относительными, ситуационными. *С нарастанием сетей и потоков растет несостоятельность структур обеспечения информационной безопасности в силу их локальности и нормативности.* На наш взгляд, такая фиксация проблемы в обеспечении информационной безопасности является методологически плодотворной в случае ее дальнейшего осмысления и развития.

[13] Мелюхин И. С. Информационное общество и баланс интересов государства и личности // Информационное общество. — 1997. — № 4–6. URL: http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/23d97560ce093100c32575bc002dfc6c (дата обращения 17. 03. 2014)

DOI: 10.7256/2073-8560.2014.3.11511
При цитировании этой статьи сноска на doi обязательна

Выводы

В целом, наш подход к пониманию информационной безопасности задает новый социальный внешний контур представления об обеспечении безопасности субъекта. Этот контур очерчивает традиционное, прежнее определение информационной безопасности, суть которого заключается в «защите конфедициальности, целостности и доступности», «защите информации и защите от информации». Обеспечение информационной безопасности общества в целом, и безопасности отдельных социальных субъектов реализуется социальными практиками и социальными структурами.

Важным аспектом новых социальных мобильностей как практик обеспечения безопасности является высокая интенсивность коммуникаций, выраженная в скорости и многообразии взаимодействия. Высокая интенсивность коммуникаций в обеспечении безопасности становится возможной благодаря такому феномену как приватизация безопасности. Приватизация безопасности является особенностью практик обеспечения информационной безопасности. Она выражается в росте многообразия частных структур обеспечения безопасности. Мобильность практик обеспечения безопасности и приватизация безопасности связаны тесным образом.

Мы предприняли попытку дать краткий обзор структур обеспечения информационной безопасности. Это институты информационного права, управленческие государственные структуры в области информационной политики и обеспечения информационной безопасности, различные государственные и частные структуры обеспечения безопасности в различных сферах и др. Опосредованно, к структурам обеспечения информационной безопасности можно отнести организации по производству экспертного знания. В широком масштабе, как структуры обеспечения информационной безопасности, возможно рассматривать отрасли информационной индустрии и информационную инфраструктуру общества в целом.

Существует противоречие между локальностью структур обеспечения безопасности и потоковым, сетевым характером угроз, не имеющих территориальной локализации. Оно заключается в росте дисфункциональности структур обеспечения информационной безопасности в силу их локальности и нормативности в условиях роста информационных потоков.

Библиография:

1. Черненко Е. В. Холодная война 2.0? Киберпространство как новая арена противостояния // Россия в глобальной политике. 2013. — Том 11, — № 1. — С. 162–170.
2. Илюшенко В. Н. Информационная безопасность общества / Учебное пособие для ВУЗов. — Томск: Томский государственный университет систем управления и радиоэлектроники, 1998.
3. Расторгуев С. П. Основы информационной безопасности / Учеб. пособие для студ. высших учебных заведений. — М.: Издательский центр «Академия», 2009. С. 18.
4. Юсупов Р. М. Информационное обеспечение национальной безопасности // Национальная безопасность 2010. — № 7/8.
5. Арсентьев М. В. К вопросу о понятии «Информационной безопасности» // Информационное общество. — 1997. — № 4 –
6. См. там же.
7. См. Владимирова Т.В. Информационная безопасность: к методологическим основаниям анализа вопроса // Информационное общество. — № 5. — 2012. — С. 47–52; Владимирова Т.В. Информационная безопасность: социологическая перспектива понятия // Национальная безопасность. — Nota bene. 2013. № 4 (27). — С. 597– 604. DOI: 10.7256/2073-8560.2013.4.7476.
8. Полтораков Ю. А. Политико-системные аспекты безопасности постиндустриального общества // Национальная безопасность / nota bene. — 2009. — № 2. — С. 19.
9. Там же. С. 20.
10. Пирумов В.С. Информационное противоборство. Четвертое измерение противостояния / В.С. Пирумов. — М.: «Оружие и технологии», 2010. — С. 41.
11. В России проблемы правового обеспечения жизнедеятельности информационного общества сегодня активно ставятся и анализируются авторами ж. Информационное право.

12. Мелюхин И. С. Информационное общество и баланс интересов государства и личности // Информационное общество. — 1997. — № 4–6.
13. Владимирова Т. В. Интенсивность коммуникаций практик новых мобильностей и информационная безопасность // NB: проблемы общества и политики — 2014. — № 1. — С. 89–111. DOI: 10.7256/2306-0158.2014.1.10918. URL: http://e-notabene.ru/pr/article_10918.html
14. Акопов Г. Л. Политико-правовые угрозы распространения социально ориентированных интернет-технологий // Национальная безопасность / nota bene. — 2012. — 2. — С. 60–67.
15. Владимирова Т.В. К социальной природе понятия «информационная безопасность» // NB: Национальная безопасность. — 2013. — 4. — С. 78–95. DOI: 10.7256/2306-0417.2013.4.596. URL: http://www.e-notabene.ru/nb/article_596.html
16. Акопов Г.Л. Хактивизм в процессе информационно-политических конфликтов // NB: Национальная безопасность. — 2014. — 1. — С. 24–32. DOI: 10.7256/2306-0417.2014.1.11609. URL: http://www.e-notabene.ru/nb/article_11609.html
17. Пономарев Д.Ю. Программная система для распределения нагрузки информационных систем // NB: Кибернетика и программирование. — 2013. — 5. — С. 29–36. DOI: 10.7256/2306-4196.2013.5.9762. URL: http://www.e-notabene.ru/kp/article_9762.html
18. Щупленков О.В., Щупленков Н.О. Проблемы информационно-коммуникационного потенциала современного общества // NB: Проблемы общества и политики. — 2013. — 12. — С. 70–96. DOI: 10.7256/2306-0158.2013.12.10537. URL: http://www.e-notabene.ru/pr/article_10537.html
19. Акопов Г.Л. Интернет-модернизация политической системы-базис для формирования информационного общества // NB: Проблемы общества и политики. — 2012. — 2. — С. 55–63. URL: http://www.e-notabene.ru/pr/article_180.html.

References:

1. Chernenko E. V. Kholodnaya voina 2.0? Kiberprostranstvo kak novaya arena protivostoyaniya // Rossiya v global'noi politike. 2013. — Tom 11, — № 1. — S. 162–170.
2. Ilyushenko V. N. Informatsionnaya bezopasnost' obshchestva / Uchebnoe posobie dlya VUZov. — Tomsk: Tomskii gosudarstvennyi universitet sistem upravleniya i radioelektroniki, 1998.
3. Rastorguev S. P. Osnovy informatsionnoi bezopasnosti / Ucheb. posobie dlya stud. vysshikh uchebnykh zavedenii. — M.: Izdatel'skii tsentr «Akademiya», 2009. S. 18.
4. Yusupov R. M. Informatsionnoe obespechenie natsional'noi bezopasnosti // Natsional'naya bezopasnost' 2010. — № 7/8.
5. Arsent'ev M. V. K voprosu o ponyatii «Informatsionnoi bezopasnosti» // Informatsionnoe obshchestvo. — 1997. — № 4 –
6. Sm. tam zhe.
7. Sm. Vladimirova T.V. Informatsionnaya bezopasnost': k metodologicheskim osnovaniyam analiza voprosa // Informatsionnoe obshchestvo. — № 5. — 2012. — S. 47–52; Vladimirova T.V. Informatsionnaya bezopasnost': sotsiologicheskaya perspektiva ponyatiya // Natsional'naya bezopasnost'. — Nota bene. 2013. № 4 (27). — S. 597– 604. DOI: 10.7256/2073-8560.2013.4.7476.
8. Poltorakov Yu. A. Politiko-sistemnye aspekty bezopasnosti postindustrial'nogo obshchestva // Natsional'naya bezopasnost' / nota bene. — 2009. — № 2. — S. 19.
9. Tam zhe. S. 20.
10. Pirumov V.S. Informatsionnoe protivoborstvo. Chetvertoe izmerenie protivostoyaniya / V.S. Pirumov. — M.: «Oruzhie i tekhnologii», 2010. — S. 41.
11. V Rossii problemy pravovogo obespecheniya zhiznedeyatel'nosti informatsionnogo obshchestva segodnya aktivno stavyatsya i analiziruyutsya avtorami zh. Informatsionnoe pravo.
12. Melyukhin I. S. Informatsionnoe obshchestvo i balans interesov gosudarstva i lichnosti // Informatsionnoe obshchestvo. — 1997. — № 4–6.

13. Vladimirova T. V. Intensivnost' kommunikatsii praktik novykh mobil'nostei i informatsionnaya bezopasnost' // NB: problemy obshchestva i politiki — 2014. — № 1. — S. 89–111. DOI: 10.7256/2306-0158.2014.1.10918. URL: http://e-notabene.ru/pr/article_10918.html
14. Akopov G. L. Politiko-pravovye ugrozy rasprostraneniya sotsial'no orientirovannykh internet-tekhnologii // Natsional'naya bezopasnost' / nota bene. — 2012. — 2. — C. 60–67.
15. Vladimirova T.V. K sotsial'noi prirode ponyatiya «informatsionnaya bezopasnost'» // NB: Natsional'naya bezopasnost'. — 2013. — 4. — C. 78–95. DOI: 10.7256/2306-0417.2013.4.596. URL: http://www.e-notabene.ru/nb/article_596.html
16. Akopov G.L. Khaktivizm v protsesse informatsionno-politicheskikh konfliktov // NB: Natsional'naya bezopasnost'. — 2014. — 1. — C. 24–32. DOI: 10.7256/2306-0417.2014.1.11609. URL: http://www.e-notabene.ru/nb/article_11609.html
17. Ponomarev D.Yu. Programmnaya sistema dlya raspredeleniya nagruzki informatsionnykh sistem // NB: Kibernetika i programmirovanie. — 2013. — 5. — C. 29–36. DOI: 10.7256/2306-4196.2013.5.9762. URL: http://www.e-notabene.ru/kp/article_9762.html
18. Shchuplenkov O.V., Shchuplenkov N.O. Problemy informatsionno-kommunikatsionnogo potentsiala sovremennogo obshchestva // NB: Problemy obshchestva i politiki. — 2013. — 12. — C. 70–96. DOI: 10.7256/2306-0158.2013.12.10537. URL: http://www.e-notabene.ru/pr/article_10537.html
19. Akopov G.L. Internet-modernizatsiya politicheskoi sistemy-bazis dlya formirovaniya informatsionnogo obshchestva // NB: Problemy obshchestva i politiki. — 2012. — 2. — C. 55–63. URL: http://www.e-notabene.ru/pr/article_180.html.