Акопов Григорий Леонидович
(к.п.н., профессор кафедры СЭД
Ростовского филиала ФГОУ ВПО МГТУ ГА)

Политический хактивизм – угроза национальной безопасности.

В статье обозначены основные проблемы и угрозы распространения компьютерных преступлений и информационных атак организованных по политически значимым мотивам. На практических примерах анализируются возможные угрозы применения современных сетевых технологий для организации кибератак.

Ключевые слова: кибертерроризм, хактивизм, хакер, кибервойна, кибератака, информационная безопасность, киберпреступник.

Стремительное развитие и распространение информационных компьютерных сетей общего пользования привело к появлению новых видов преступлений, таких, как киберпреступность (киберпреступник – пользователь компьютера, нарушивший законодательство, используя сеть общего пользования) и кибертерроризм (кибертерроризм– несанкционированное вмешательство в работу компонентов компьютерных сетей общего пользования, вызывающее дезорганизацию работы элементов инфраструктуры политически значимых институтов общества, причинение морального и материального ущерба, а также иных социально опасные последствия). Впервые о компьютерных преступлениях заговорили в 60-х годах прошлого столетия, когда стали выявляться преступления, совершаемые с использованием ЭВМ. Сегодня же о преступлениях в сфере компьютерных технологий говорят многие как отечественные, так и зарубежные ученые. Однако для обозначения данного явления

употребляются различные определения. Назовем лишь наиболее распространенные: компьютерные преступления, коммуникационные преступления, киберпреступления, кибербандитизм, программные злоупотребления, информационные преступления и т.п.

Вот как характеризуются киберугрозы и кибервторжения в материалах Исследовательской службы Конгресса США: «Киберугрозы или кибервторжения – это несанкционированные попытки проникновения в компьютеры, управляемые компьютерами системы или сети. У таких несанкционированных действий могут быть любые цели - от простого проникновения в систему и ее изучения ради риска, острого ощущения или интереса до входа в систему ради мести, кражи информации, внесения замешательства, вымогательства или кражи денег, а также намеренного локализованного повреждения компьютеров или нанесения ущерба значительно большим инфраструктурам, например, системам водоснабжения или энергоснабжения»[1].

В докладе Исследовательской службы Конгресса США за номером RL30735 приводится определение кибертерроризма: «кибертерроризм – это один из многих видов киберугроз, которые вызывают всеобщую озабоченность. Среди других таких угроз - взлом компьютеров, кибервойна и киберпреступность. Кибертерроризм, однако, отличается тем, что в число его целей могут входить политическая или экономическая дестабилизация, саботаж, кража военных или гражданских активов и ресурсов в политических целях». Далее в докладе утверждается: «Кибертеррористы могут работать от имени стран, занимающих враждебную позицию по отношению к интересам США, или действовать вне контроля или влияния других стран. В целом,

[1] Доклад Исследовательской службы Конгресса RL30735. Кибервойна. Стивен А. Хилдрет. Размещено на веб сайте Infousa.ru. 20 февраля 2003. http://www.infousa.ru/information/bt-1028.htm

однако, будет трудно своевременно отличить кибертеррористические нападения от других кибернападений»[2].

Современные политические активисты и кибертеррористы пользуются Интернетом прежде как:

- средство коммуникации и место координации действий;

- место для проведения информационно-пропагандисткой работы;

- место для вербовки сторонников;

- объект для сбора разведывательной информации;

- источник информационно-программного обеспечения;

- и как средство обеспечивающие доставку и внедрение вредоносных компьютерных программ носящих ущерб объектам атаки.

Известный исследователь проблем киберпреступности В. Голубев утверждает, что под кибертерроризмом, следует понимать преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сети, которая создает опасность для жизни и здоровья людей или наступление других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта[3].

Итак, как мы видим, определений кибертерактов и киберпреступлений существует множество, единый понятийный аппарат еще не выработан вследствие новизны проблемы и сложности ее классификации.

По мнению И.М. Рассолова: «Сегодня, как никогда ранее, в интернет-праве актуальна проблема совершенствования законодательства в сфере

---

[2] Там же.

[3]Голубев В.А. Кибертерроризм - угроза национальной безопасности. - http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism/.

борьбы с киберпреступностью»[4]. В современном интернет-сетевом сообществе совершается масса нарушений закона, но в рамках данного исследования нас интересуют профессиональные взломщики компьютерных программ и информационно-коммуникационных систем называемые в обиходе "хакерами". Хакер (от англ. hack — рубить, кромсать, разрубать), в буквальном переводе — рубщик, взломщик. Существуют различные трактовки термина «хакер», наиболее точным нам кажется определение, приведенное на сайте Лаборатории Касперского: «Хакерами называют тех, кто получает или пытается получить незаконный доступ к данным через компьютерные сети (сейчас обычно через Интернет)[5]».

Существует множество других понятий и определений, кто такие хакеры, но мы в своих исследованиях сознательно будем опираться на названное выше определение.

Компьютерные взломщики (хакеры) год от года становятся все более активными и изощренными, что связано прежде всего с массовой компьютеризаций современного общества и с постоянным увеличением числа хакеров. И если раньше говорили о том, что хакеры - это молодые люди, которые путем кибератак пытаются заявить о себе, то сегодня все чаще приходится сталкиваться с появлением хакеров, активно отстаивающих ту или иную позицию, нередко политическую. Более того, появились прецеденты кибертеракторов, проводимых хакерами в связи с определенными политическими заказами. Многие эксперты с опаской говорят о грядущей эпохе кибертеракторов и сращивания криминального мира с виртуальным.

[4] Рассолов И.М. Право и Интернет. Теоретические проблемы. – М.: Издательство НОРМА, 2003. С. 250

[5] http://www.kaspersky.ru/hackers

Интернет предоставляет террористам исключительные возможности. Он служит для них источником легкого (и без привлечения лишнего внимания) получения практически любых необходимых сведений: от предложений потенциальных поставщиков оружия и необходимых технических средств до инструкций по созданию бомб или угону самолета. С помощью Интернета можно перевести необходимые финансовые средства или получить их, собирая пожертвования либо взламывая банки, можно вербовать наемников и осуществлять пропаганду и, наконец, посредством Глобальной сети возможно быстро и с малыми затратами нарушить нормальное функционирование практически любого объекта гражданской или военной инфраструктуры. И все это при исключительно высоком уровне защищенности от вмешательства государства в потоки соответствующей информации, а следовательно, при сохранении анонимности. Пока что террористы используют Интернет в основном как средство передачи информации или пропаганды своих идей, а не как новое оружие. Однако все чаще приходят сообщения о компьютерных атаках на то или иное правительственное учреждение или банк, взламываются не только отдельные сайты, но и целые компьютерные системы.

Не только кибертеррористы, но и сами хакеры в силу своих профессиональных навыков и ментальных характеристик представляют опасность для современного общества. Сегодня уже не являются редкостью ситуации, при которых конфликты в политической среде практически синхронно отзываются в виртуальном пространстве всемирной паутины. Так, например, не успела уладиться ситуация вокруг испанского острова Перехиль, как испанские хакеры атаковали официальный сайт Национального управления по делам туризма Марокко. Его главная страница оказалась залита черным цветом, на котором красовался испанский флаг и надпись: "Вы - Перехиль, мы – ваши сайты". Администраторы сайта были

вынуждены срочно убрать первую страницу с сервера, чтобы устранить последствия хакерской атаки.

Хакеры, поддерживавшие в этом противостоянии Марокко, также не остались в стороне от политического конфликта. Некий компьютерный взломщик, скрывающийся под ником BreaKIce, разместил свои угрозы на электронной странице одной из портовых служб Барселоны. Там появился такой текст: "Война, развязанная Испанией, будет иметь серьезные последствия для нее самой". При этом хакер обещал подпортить и некоторые другие испанские сайты с тем, чтобы высмеять притязания Мадрида на остров Перехиль[6].

За словом последовало дело. Через некоторое время "хакнутыми" оказались сайт барселонской транспортной компании Embarmar, фирмы Lawson и 15 других ресурсов. BreaKIce (ярый националист, как он сам себя назвал) писал на этих страницах промарокканские лозунги, требовал независимости Западной Сахары и призывал арабов к противостоянию с Израилем.

Обозначенный выше пример наглядно показывает, насколько реальна опасность превращения хакеров в политических кибертеррористов, которые в ответ на политические события оказывают виртуальное воздействие. Другой не менее интересный эпизод произошел во время войны в Ираке, когда, в результате действий 24-летнего Джона Вильяма Расина II (John William Racine) все посетители, желавшие попасть на веб-сайт спутникового канала "Аль-Джазира", перенаправлялись на созданную хакером страницу, где был размещен флаг США и патриотический девиз.

---

[6] Подр. см.: Евросоюз озабочен развитием событий вокруг острова Перехиль у берегов Северной Африки. РИА Новости. 17 июля 2002. http://www.rian.ru/politics/20020717/193336.html.

Однако этот взломщик был пойман и окружной суд города Лос-Анджелес приговорил его к 1000 часов общественных работ и штрафу в 2000 долларов. Д. Расина признали виновным в "сетевых махинациях" и незаконном вторжении в процесс обмена электронными данными. В свое оправдание обвиняемый заявил, что действовал "из чувства патриотизма"[7].

Подобные действия «из чувства патриотизма» превращают хакеров в орудие политического противоборства и даже террора. Действия хакеров все чаще наносят не только материальный ущерб, но и моральный урон, показывая уязвимость даже самых серьезных интернет-проектов. Так, например, прямая видеотрансляция в Интернете пресс-конференции Президента Белоруссии Александра Лукашенко на тему белорусско-российских отношений оказалась сорванной. В компании "Белтелеком" сообщили, что президентский сайт "стал недоступен для пользователей". Специалисты объясняют это двумя причинами: перегрузкой канала в связи с большим количеством пользователей, одновременно желающих следить в реальном времени (один из признаков DDoS-атаки) за общением главы государства с журналистами, и возможностями самого сайта. Они также не исключили вероятность атаки хакеров[8].

Атаки хакеров не оставляют в покое и сетевое представительство Президента Российской Федерации. В частности, 19 декабря 2003 г. директор ФСБ Николай Патрушев сообщил журналистам следующие: «В истекшем году только на сайт Президента Российской Федерации было осуществлено около 100 тыс. компьютерных атак. Всего же в 2003 году зарегистрированы свыше 730 тысяч атак на интернет-представительства органов

---

[7] Подр. см.: Хакер, вскрывший сайт Al-Jazeera, был движим патриотизмом. Утро.ру. http://www.utro.ru/news/2003/11/14/250051.shtml

[8] Подр. см.: Интернет-видеоконференция президента Белоруссии сорвана. http://www.newsru.ru/world/24oct2003/lukashenko.html

государственной власти»[9]. Активность хакеров вынуждает ряд стран принимать законы для обеспечения государственной безопасности.

Так, в Грузии на правительственном уровне был одобрен законопроект о внесении изменений и дополнений в Уголовный кодекс, которые ужесточают наказание за терроризм, в том числе и кибертерроризм. Для борьбы с хакерами в грузинском министерстве госбезопасности даже было создано специальное подразделение. Видимо, на грузинские власти повлиял пример противоборства хакеров соседних государств.

В начале 2000 г. агентство ИТАР-ТАСС со ссылкой на национальное телевидение Армении сообщило, что армянские хакеры провели в Интернете "акцию возмездия", выведя из строя ряд азербайджанских сайтов. Среди жертв хакеров оказались сайты посольства Азербайджана в США, Национального телевидения республики, бакинской газеты "Зеркало", а также нескольких провайдеров.

Все попытки пользователей Интернета открыть указанные страницы приводили на страницу, озаглавленную "Не буди лихо, пока оно тихо!" с изображением дьявола. Представитель армянской хакерской группы под названием "Лиазор" ("Уполномоченный") заявил, что эти азербайджанские серверы будут контролироваться по меньшей мере год. "Азербайджан попросту утратил свой Интернет. Однако не мы были инициаторами этой интерактивной войны", - заявил представитель хакеров, выразив сожаление по поводу того, что "Лиазор" была вынуждена пойти на столь радикальные шаги. "Мы достаточно давно обладаем всеми техническими возможностями и необходимыми профессиональными навыками, однако у нас и в мыслях не было проводить такую операцию против азербайджанских сайтов", - заявил хакер. По его словам, акция была предпринята лишь после того, как две

[9] Чекисты отразили около 100 тысяч атак на сайт Президента. 19.12.2003. Страна.Ru

группы азербайджанских хакеров начали кампанию по уничтожению армянских сайтов[10].

Во время захвата одни азербайджанские "оккупанты" заменяли порталы армянских сайтов на другие странички или на гостевые книги (guestbooks), наполняя их уличной бранью. Другие же занялись активной "политической деятельностью". В расположенной на подмененной страничке гостевой книге стали появляться "письма трудящихся", смысл которых сводился к следующему: вся Европа и Америка хвалит азербайджанских "парней" за содеянное.

Нельзя не заметить, что от азербайджанских хакеров пострадали не только сетевые ресурсы зоны «.am»[11], но и сайты армянской тематики зоны «.ru»[12]. Так, например популярный «Армянский сайт» (http://a-arm-a.euro.ru), расположенный на известном российском портале «chat.ru», после ряда успешних атак азербайджанских хакеров на длительный срок прекратил свое существование и создателям сайта не осталось ничего другого, как зарегистрировать новый информационный ресурс www.armiansky.narod.ru для продолжения функционирования веб-сайта.

Успех первой атаки азербайджанцев вызвал эйфорию в интернет-кругах Республики. В форумах и чатах стали появляться призывы "продолжать наступление". Уже не группы профессиональных хакеров, а обычные граждане начали пытаться взламывать армянские сайты.

Терпение армянских хакеров было на пределе и с 11 по 13 февраля 2000 г. хакеры из The Liazor group провели "акцию возмездия", взяв под

[10]См.: «Лента.ру» 15 февраля 2000. http://www.lenta.ru/internet/2000/02/15/az/_Printed.htm .
[11] домен первого уровня «.am» принадлежит Республике Армения.
[12] домен первого уровня «.ru» принадлежит Российской Федерации.

контроль более двух десятков азербайджанских сайтов. В их числе оказались серверы крупных провайдеров и web-версия газеты "Зеркало" (азербайджанский аналог российской "Независимой газеты"). По сути, азербайджанцы на некоторое время утратили свою Интернет-сеть: армяне стерли не только сайты СМИ Азербайджана, но и изменили сайты действующих в Азербайджане международных организаций и зарубежных фирм.

14 февраля 2000 года министр национальной безопасности Азербайджана Намик Аббасов заявил, что "азербайджанские хакеры взяты под контроль Министерством национальной безопасности Республики". Это заявление фактически означало предложение Баку начать мирные переговоры с Ереваном по данной проблеме. Ереван отреагировал мгновенно, распустив группу "Лиазор". Кибервойна, похоже, приостановилась.

Как отмечает корреспондент журнала «Эксперт» С. Петухов, на закавказской кибервойне, как и на всякой другой, не обошлось без диверсионной операции в глубоком тылу противника. Сейчас лиазоровцы говорят, что они хотели просто «показать, что можно делать с Интернетом, если кроме технологий использовать еще и «серое вещество»»[13].

Опыт армяно-азербайджанских виртуальных баталий показал, насколько реальными могут оказаться виртуальные поражения, и позволил понять, как опасны, могут быть их последствия.

Следует отметить, что 2000 год (так называемый - миллениум) явился беспрецедентным с точки зрения распространения хакерских атак и кибервойн. Помимо отмеченного выше противостояния армянских и

[13]Подр. см.: С. Петухов. Карабахские web-баталии.// «Эксперт» № 5, май 2000.

азербайджанских хакеров, в марте 2000 г. в преддверии президентских выборов на Тайване, в мировом виртуальном пространстве шел интенсивный "обмен ударами" между Китаем и Тайванем. За месяц до этого в американском секторе сети Интернет прошли небывалые по своему масштабу атаки, как на второй по популярности в Интернете сайт Yahoo!, так и на сайт телекомпании CNN, а также на десятки других сайтов крупных компаний сетевой торговли и брокерских фирм. Все это вынудило министра юстиции США Джанет Рино обратиться за помощью к ФБР. Билл Клинтон, комментируя сложившуюся ситуацию, отметил, что Интернет предоставляет новые возможности не "для людей с разрушительными устремлениями". Высокопоставленный представитель Пентагона признался, что его ведомство было вынуждено начать проверку собственной сети из десяти тысяч компьютеров.

Обозначенные выше примеры позволяют рассмотреть процесс зарождения хактивизма в киберпространстве. За последнее десятилетие кибервойны стали обыденным явлением и масштабы компьютерных угроз значительно возросли.

27 сентября 2010 года директор Совета информационных технологий министерства промышленности Ирана Махмуд Лиайи заявил, что атаке подверглось около 30.000 компьютеров.

"Компьютерный червь способен передавать информацию о производственных процессах и ходе разработок за границу нашим врагам. Ирану объявили электронную войну", - провозгласил Лийаи[14].

Подобные кибервойны уже не редкость. Многие политические события находят свое развитие в виде хакерских атак, иногда по результатам

[14] 27 сентября – Иран подвергся кибератаке. http://www.cyberpolitics.ru/content/view/406/1/

политических явлений разворачиваются целые информационные баталии с применением хакерских атак.

Большой резонанс во всем мире вызвал арест 7 декабря 2010 года основателя портала WikiLeaks Джулиана Ассанжа. И практически моментально хакеры, сочувствующие ему, атаковали сайты корпораций, которые, по их мнению провинились перед Д. Ассанжем.

По данным NewsInfo[15], портал известной платежной системы MasterCard приостановил свою работу из-за хакерской атаки. Нападение на сайт было совершено в отместку за арест Ассанжа. Кроме того, хакеры обрушились на сайт платежной системы PayPal, отказавшейся принимать пожертвования для WikiLeaks, и на сайт швейцарского банка Swiss Post Office, где были заморожены счета австралийца.

По данным опубликованным на сайте информационного агентства «РИА Новости», атака была проведена группой анонимных активистов, которая называет себя "Anonymous". Ранее эта же группа "Anonymous" создала 208 зеркальных версий сайта WikiLeaks, чтобы максимально облегчить доступ к публикуемой информации и исключить возможность блокирования ресурса.

Сторонники WikiLeaks говорят, что против сайта и его "зеркал" уже давно идет множество онлайновых атак, так что они лишь отвечают на развязанную другими кибервойну.

"Мы считаем, что WikiLeaks перестал быть просто сайтом "утечек". Он превратился в поле битвы между гражданами и правительствами", - сказал

[15]Владельцу WikiLeaks и арест не помеха http://www.newsinfo.ru/articles/2010-12-08/wikileaks/744696/

Би-би-си один из активистов группы, называющий себя Coldblood. Собеседник Би-би-си добавил, что все сайты компаний, которые поддаются давлению правительств, будут атакованы[16].

Следует заметить, что первыми от виртуальных мстителей пострадал сайт шведской прокуратуры, которая инициировала преследование основателя WikiLeaks Джулиана Ассанжа по обвинению в изнасиловании, и финансовый сервис Postfinance швейцарской почтовой службы, заморозившая счета Ассанжа[17].

На наш взгляд, атаки на противников Д. Ассанжа не только носят политический характер, но и демонстрируют объективную угрозу объединения хакерских групп. Виртуальный социум готов к организованным акциям и назревает реальная угроза возникновения кибервойны, если за дело возьмутся организованные группы кибертеррористов, руководимые спецслужбами либо иными профессиональными организациями.

Как известно, наибольшая политическая активность проявляется в период проведения избирательных кампаний. Хакеры не являются исключением. В ночь подведения первых итогов выборов депутатов Государственной Думы четвертого созыва в Сети были осуществлены массовые атаки хакеров на электронную систему Центризбиркома. Говоря о последствиях этих атак, руководивший на тот момент Центризбиркомом А. Вешняков заметил: - «В саму ГАС "Выборы" хакеры проникнуть не могут, так как система работает автономно, без подключения к Интернету. А вот сайт Центризбиркома, на котором оперативно публиковались данные со всех

[16] Подр. см.: Сторонники Ассанжа приступили к "боевым действиям" в Сети. РИА Новости. http://www.rian.ru/world/20101208/306127025.html

[17] Хакеры пошли кибер-войной на обидчиков Ассанжа. Правда.Ру http://www.pravda.ru/news/world/09-12-2010/1060291-hakeri-0/

избирательных участков, взломать пытались более девятисот раз. Причем работали не только любители, но и профессионалы. В том числе и из других государств»[18].

Цель атак, по мнению Александра Вешнякова, очевидна: «разрушить нашу систему обнародования информации. Вспомним ситуацию в Югославии, когда итоги президентских выборов в этой стране местный центризбирком не мог подвести несколько дней. В результате - волнения, беспорядки и смена власти… Но хакерам это оказалось не по зубам. Все предписания закона и взятые на себя обязательства по оперативному обнародованию предварительных итогов голосования мы выполнили. Наш сайт, кстати, за 8 и 9 декабря посетили свыше миллиона пользователей Интернета. Не исключено, что хакеры вновь активизируются ко дню президентских выборов. Мы к этому готовимся»[19].

В своей книге «Информационная война и выборы» И.Н. Панарин, говорит о таком явлении, как «хактивизм», которое он понимает как «бескорыстное» хакерство в целях политического активизма[20]. Там же автор справедливо утверждает, что современное хакерское движение оказалось, втянуто в игры политиков.

В ближайшем будущем масштабы «хактивизма» могут принять угрожающий характер в том случае, если хакеры начнут объединяться в своеобразные сообщества. Судя по сводкам информационных агентств, такие тенденции уже наметились. Так, с 31 мая 2010 года, момента штурма судна "Мави Мармара" спецназом ВМФ ЦАХАЛа, турецкие и исламистские хакеры начали массированную атаку на израильские интернет-сайты. Как

[18] См.: «ЦИК хакерам не по зубам». Российская Газета. 16.01.2004
[19] См.: Там же.
[20]И.Н. Панарин. Информационная война и выборы. М.: ОАО «Издательский Дом «Городец»», 2003. – С. 345

сообщил специализированный портал bubbletech.co.il от действий хакеров пострадали около 1000 сайтов доменной зоны .il, жертвами стали не только израильские сайты, но и еврейские сайты по всему миру. На многих взломанных сайтах оставлена метка "Hackedby IHH". На сайте twitturk.com организована перекличка хакеров, сообщающих о взломе израильских сайтов. Список взломанных израильских сайтов можно найти и в других местах. При этом турецкие хакеры утверждают, что взломали, среди прочего, сайты израильской службы внешней разведки "Мосад" и израильского ВМФ[21].

Другой пример политического хактивизма можно было наблюдать в начале 2011 года представители Еврокомиссии заявили о серьезной распределенной кибератаке на компьютерные системы Еврокомиссии, исполнительного органа ЕС, как сообщило издание Security News Daily, подозреваются в атаке китайские хакеры. Событие произошло накануне двухдневного саммита в Брюсселе, где основной темой дискуссий будет военная операция в Ливии, против которой возражали Россия и Китай[22].

Поскольку компьютерный терроризм - уже реальность сегодняшнего дня, необходимо на государственном уровне разработать меры по обеспечению информационной безопасности и противодействию кибертеррору. Борьбу же с киберрторрористами необходимо вести всем миром, так как в глобальном информационном пространстве не существует границ и мировое сообщество должно объединить усилия для обеспечения

21 Эхо "свободной Газы". Кибер-война против Израиля и исламистов http://newsru.co.il/israel/03jun2010/gaza307.html

22 Еврокомиссия подверглась кибератаке накануне саммита по Ливии. 25.03.2011. {Электронный ресурс} http://www.nazarovo-online.ru/adadym/raznoe/1284-evrokomissiya-podverglas-kiberatake-nakanune-sammita-po-livii.html

информационной безопасности национальных интересов современных государственных образований.

Литература:

1. Акопов Г.Л. Информационное право: учеб. пособие – Ростов н/Д: Феникс, 2008.
2. Акопов Г.Л. Сетевая политика российских партийных элит (проблемы теории и практики). - Ростов-на-Дону: РОСБЛАНК, 2003; Акопов Г.Л. Глобальные проблемы и опасности сетевой политики: Монография. – Ростов-на-Дону: ООО «Ростиздат», 2004.
3. Акопов Г.Л. Правовая информатика: учеб. пособие – Ростов н/Д: Феникс, 2005; Акопов Г.Л. Правовая информатика: учеб. пособие – Москва: Дашков и К, 2008; Акопов Г.Л. Правовая информатика: учеб. пособие издание 2-е – Москва: Дашков и К, 2010.
4. Акопов Г.Л. Кислицын С.А. Политология: учеб. пособие – Ростов н/Д: Феникс, 2010.
5. Копылов В.А. Информационное право: Учебник. – 2-е изд., - М. Юрист, 2003. С. 19-39.
6. Панарин. И.Н. Информационная война и выборы. М.: ОАО «Издательский Дом «Городец»», 2003.
7. Петухов. С. Карабахские web-баталии.// «Эксперт» № 5, май 2000.
8. Рассолов И.М. Право и Интернет. Теоретические проблемы. – М.: Издательство НОРМА, 2003.
9. Серго. А. Интернет и право. – М.: Бестселлер, 2003.
10. Стивен А. Хилдрет. Доклад Исследовательской службы Конгресса RL30735. Кибервойна. Размещено на веб сайте Infousa.ru. 20 февраля 2003. http://www.infousa.ru/information/bt-1028.htm

Сведения об авторе

Акопов Григорий Леонидович, директор Ростовского филиала МГТУ ГА, доцент, кандидат политических наук. В 2000 году окончил Северо-Кавказскую академию государственной службы (менеджер-экономист). Автор пяти десятков научных работ по проблемам информационной политики и права, в том числе нескольких авторских монографий и учебных пособий. Победитель Всероссийского конкурса на лучшую научную книгу 2009 года в области юриспруденции в номинации «Информационные технологии», трижды лауреат Всероссийского конкурса, проводимого Фондом развития отечественного образования на лучшую научную книгу (2008 и 2009 гг.).