УДК 001:35+004.8

НОВЫЕ УГРОЗЫ НАЦИОНАЛЬНОМУ СУВЕРЕНИТЕТУ РОССИИ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ[1]

Сивоволов Дмитрий Леонидович,
Уральский федеральный университет имени первого Президента РФ Б.Н. Ельцина,
Институт государственного управления и предпринимательства,
кафедра управления общественными отношениями,
доцент, кандидат социологических наук,
г. Екатеринбург, Россия.
E-mail: dioma@inbox.ru

Аннотация
Статья посвящена обоснованию возрастания угроз для информационной безопасности РФ. Приведены доказательства того, что в современной России информационные угрозы рассматриваются как угрозы национальному суверенитету РФ. Особое внимание уделено определению информационной безопасности как информационно-компьютерной безопасности и классификации ее по сферам деятельности.

Ключевые понятия:
информационная безопасность, национальный суверенитет, информационно-компьютерные войны, кибербезопасность, кибервойны.

В сегодняшнем мире тема информационной безопасности приобретает все более острое звучание. Информационная безопасность государства тесно переплетается с темой национального суверенитета. Национальный суверенитет распространяется не только на территорию, государственное устройство, законодательство, экономику, но и на информационные ресурсы государства.

Развитие информационных технологий (IT) порождает новые угрозы информационной безопасности. Суть отличия современных угроз информационной безопасности от традиционных заключается в том, что они «завязаны» на компьютерные технологии. Понимая фундаментальный характер компьютерных технологий сегодня и в будущем, считаем необходимым подчеркнуть, что угрозы информационной безопасности «имеют глубокие исторические корни и прошли долгий путь эволюции» [6, с. 69].

Смещение акцента в терминологии с «информационной безопасности» на «информационный суверенитет» не случайно. В обществе трансграничных информационных потоков информационная безопасность становится атрибутом практически любого вида деятельности.

Это положение, в общих чертах, было сформулировано в Доктрине информационной безопасности РФ, принятой в сентябре 2000 года.[2] Многое за прошедшие пятнадцать лет изменилось, особенно в информационной сфере. И сегодня информационная безопасность требует обновлённого стратегического подхода, учитывающего современную международную ситуацию в сфере IT, современные средства защиты частных и публичных информационных ресурсов.

Многие положения Доктрины информационной безопасности Российской Федерации, принятой на рубеже веков, актуальны и сегодня. Например, ставшая актуальной с 2014 года тема импортозамещения, по отношению к информационной безопасности, была сформулирована в Доктрине информационной безопасности в сентябре 2000 года следующим образом:

[1]Статья подготовлена при финансовой поддержке РГНФ в рамках научно-исследовательского проекта № 14-13-66013/15 «Информационная культура жителей Свердловской области: поселенческий и социально-демографический аспекты».

[2]Доктрина информационной безопасности Российской Федерации: утверждена Указом Президента Российской Федерации № Пр-1895 09.09.2000. Совет безопасности РФ. Официальный сайт. [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/5.html (дата обращения: 18.04.2015).

«развивать производство в Российской Федерации конкурентоспособных средств и систем информатизации, телекоммуникации и связи, расширять участие России в международной кооперации производителей этих средств и систем». Еще пятнадцать лет назад была поставлена амбициозная задача – «Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности».

Нельзя не отметить, что Совет безопасности РФ понимает возрастание информационных рисков, знает о появлении новых информационных угроз. Началась разработка новой Доктрины информационной безопасности РФ, которая должна учесть современные информационные угрозы[3]

Отдавая должное инициаторам разработки новой Доктрины информационной безопасности, нельзя не сказать следующее: тема «информационной безопасности» попала в заложницы эмпирикам, то есть «айтишникам». В их описаниях, прогнозах и рекомендациях технократический подход превалирует над гуманитарным. Социально-философских работ по информационной безопасности крайне мало [1, с. 121].

Разберемся в понятиях: как связаны между собой национальный суверенитет, национальная безопасность и информационная безопасность?

Как указывает в выводах своей статьи Михайленок О. М.: «На сегодняшний момент ни в научном, ни в политико-правовом плане Российская Федерация еще не определилась с пониманием национального суверенитета» [2, с. 8]. Цитируемый автор указывает на многомерность явлений, характеризуемых понятием суверенитет, поскольку оно распадается на государственный суверенитет, народный суверенитет и национальный суверенитет. С точки зрения Михайленка О. М., *независимость* государства во внешней и *верховенство* во внутренней политике – это государственный суверенитет. Но мы считаем, что вмешательство во внутреннюю и внешнюю политику государства выступает и как угроза его *национальному суверенитету*.

В этом контексте национальная безопасность – это состояние защищенности государства от вмешательства в его внутреннюю и внешнюю политику, защита от рисков утраты национального суверенитета. В мире цифровых технологий национальный суверенитет нельзя сохранить без эшелонированной информационной «обороны». Понятие информационной безопасности в Доктрине информационной безопасности РФ раскрывается следующим образом: «Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства».

Обращает на себя внимание тот факт, что уже 15 лет назад использовалась формулировка «национальные интересы в информационной сфере». Защита национальных интересов более объемное понятие, чем защита национальных информационных ресурсов. Национальные интересы пронизывают всю политику государства. Следовательно, укрепление информационной безопасности было задекларировано как один из приоритетов политики национальной безопасности России уже в самом начале этого века.

«Понятие «национальная безопасность» включает в себя безопасность личности, общества, государства от внутренних и внешних угроз. В контексте национальной безопасности первостепенное внимание уделяется проблемам государственной и общественной безопасности, безопасности в социально-экономической сфере, оборонно-промышленной, информационной, военной, международной безопасности».[4]

Необходимо обратить внимание на следующую деталь – в одном ряду с традиционными, устоявшимися сферами государственной и общественной безопасности: социально-экономической, оборонно-промышленной, военной и международной находится информационная сфера безопасности. Очень важно, что такой современный подход присутствует в деятельности Совета безопасности Российской Федерации.

[3] Юлия Воронина. Данные засекречены. В России появится новая Доктрина информационной безопасности // Российская газета – Федеральный выпуск от 10.02.2015. Официальный сайт. [Электронный ресурс]. URL: http://www.rg.ru/2015/02/10/ib.html (дата обращения: 10.10.2015).

[4] Совет безопасности Российской Федерации. Официальный сайт. [Электронный ресурс]. URL: http://www.kremlin.ru/structure/security-council (дата обращения: 19.04.2015).

Вмешательство внешних сил в информационное общественно-политическое и экономическое пространство государства следует понимать как угрозу национальному суверенитету Российской Федерации. На это прямо указывается в «Стратегии национальной безопасности Российской Федерации до 2020 года»: «На обеспечение национальных интересов Российской Федерации негативное влияние будут оказывать вероятные рецидивы односторонних силовых подходов в международных отношениях, противоречия между основными участниками мировой политики, угроза распространения оружия массового уничтожения и его попадания в руки террористов, а также совершенствование форм *противоправной деятельности в кибернетической* и биологической областях, *в сфере высоких технологий. Усилится глобальное информационное противоборство,* возрастут угрозы стабильности индустриальных и развивающихся стран мира, их социально-экономическому развитию и демократическим институтам»[5] (курсив мой. – С. Д. Л.).

В связи с развитием IT, обуславливающих появление новых видов информационных угроз, возникает вопрос: какие виды, группы информационных угроз должны быть учтены в новой Доктрине информационной безопасности Российской Федерации?

В современном информационном пространстве существуют следующие фундаментальные угрозы:

1) *информационные войны;*

2) *киберугрозы*.

Прежде чем раскрыть смысловые и содержательные поля обозначенных угроз, необходимо сделать небольшое пояснение.

До широкого распространения информационно-компьютерных технологий информационная безопасность имела принципиально другой характер. Пропаганда и контрпропаганда, public relations и другие способы информационного воздействия не новы. Такой вид воздействия на массовое сознание изменялся вместе с развитием средств массовой коммуникации. В процессе развития рекламы и public relations в 1986 году появился термин «маркетинговые войны» [4, с. 3], который после трансформировался в «информационные войны» [3, с. 3–5].

С развитием Интернета «традиционные» информационные войны приобрели другое качество. Точнее говоря, сетевой характер. Сетевой характер наиболее ярко проявился в феномене «социальных сетей» (автор считает данный термин некорректным, но его семантический анализ не является предметом данной статьи). «Социальные сети» стали новым видом массовых коммуникаций, переведшим личное общение в публичное пространство. Благодаря своей публичности «социальные сети» стали полем массовых информационных битв. Современные «оранжевые революции» стали возможны благодаря появлению таких атрибутов «социальных сетей», как публичность, трансграничность и глобальность. «Социальные сети» в любой момент могут быть использованы в качестве площадки для виртуальных митингов, содержащих в себе потенциал трансформации в реальные митинги на площадях.

Любой человек сегодня может действовать на поле средств массовой коммуникации в качестве блогера, модератора или еще какого-либо владельца «карманного» mass-media. Таким образом, необходимо отделять информационные войны докомпьютерной эры (можно для терминологического удобства называть их традиционными) от современных информационных войн, имеющих *глобальный масштаб и сетевой характер.*

В информационных войнах XXI века участвуют не только традиционные средства массовой коммуникации, но и диверсанты-одиночки. И невидимые кукловоды, которые скрываются под «никами» одиночек. Современные информационные войны – это воплощение теории Т. Гоббса «войны всех против всех» в современной информационной реальности.

Сутью современных коммуникаций являются компьютерные технологии. Именно компьютерные технологии перевели информационную среду в киберпространство. «Киберпространство» – устойчивая метафора, используемая вместо корректных, но длинных терминов «информационно-компьютер-

[5] Стратегия национальной безопасности Российской Федерации до 2020 года. Утверждена Указом Президента Российской Федерации № 537 от 12.05.2009. Совет безопасности Российской Федерации. Официальный сайт. [Электронный ресурс]. URL: http://www.scrf.gov.ru/documents/1/99.html (дата обращения: 15.05.2015).

ные технологии», или «информационно-компьютерная инфраструктура». Данные значения «киберпространства» понятны практически всем специалистам в сфере IT и ИБ (информационной безопасности), поэтому в дальнейшем мы будем использовать этот термин без кавычек. Если мы соглашаемся с использованием термина *киберпространство*, то вполне уместно тогда использование термина *кибербезопасность* в одном ряду с информационной безопасностью.

Кибербезопасность – это организация защиты от *информационно-компьютерных* угроз, то есть можно сказать: кибербезопасность – это состояние защищенности национальных интересов в киберпространстве. За относительно недолгий период с начала возникновения киберугроз их формы, методы и масштабы существенно изменились. Необходимо подчеркнуть, что в киберпространстве угрозу представляют не только отдельные и малочисленные хакеры-идеалисты начала «компьютерной эры», но и государства с их мощными ресурсами. Кибербезопасность по характеру и целям борьбы с киберугрозами можно разделить на три группы:

1) криминальная – защита от киберпреступности;

2) монетарная – борьба с обращением криптовалют;

3) военная – кибервойны.

Киберпреступность, то есть преступления, совершаемые с использованием IT-технологий. Специалисты классифицируют наличие пяти видов киберпреступности, а именно:

интернет-мошенничество, спам, внутренние сделки, кардинг, кибератаки.

Приведенный список далеко не полон, но оставим обсуждение видов и технических деталей киберпреступности за рамками этой статьи. Финансовая сторона киберпреступности состоит в том, что ее совокупный рынок растет. В России в 2014 году он достиг более 2,5 млд $[6].

Криптовалюты. Специалисты насчитывают уже больше десятка криптовалют, но наиболее известная из них – биткойн. По данным на январь 2014 года мировой рынок оборота только биткойнов равнялся 10,75 миллиарда $. Самая большая опасность криптовалюты заключается в её необеспеченности и «неуправляемости». Это «как бы» деньги, которые не контролиру-



Структура рынка киберпреступности в России в 2014г.

[6] Юлия Воронина. Данные засекречены. В России появится новая Доктрина информационной безопасности // Российская газета – Федеральный выпуск от 10.02.2015. Официальный сайт. [Электронный ресурс]. URL: http://www.rg.ru/2015/02/10/ib.html (дата обращения: 10.10.2015).

ет и не обеспечивает ни один центробанк. Из этого вытекают угрозы национальной валюте и экономическому суверенитету государства. В Российской Федерации политика по отношению к криптовалютам определена – их обращение запрещено[7]. Но на этом угрозы не заканчиваются. Начинается борьба с незаконным оборотом криптовалют, для которой нужны колоссальные ресурсы и, в первую очередь, IT-специалисты соответствующего «монетарного» профиля.

Кибервойны. Кибервойны уже идут. Кибервойска уже атакуют противника. Наиболее известный пример – это кибератака США на ядерные объекты Ирана в 2010 году. В результате проникновения шпионской программы Stuxnet, созданной по заданию Пентагона, были выведены из строя около тысячи центрифуг ядерного исследовательского центра в Натанзе, нанесен ущерб системе управления Бушерской АЭС. Побочным эффектом стало проникновение Stuxnet в сети общего пользования и вывод из строя примерно 60 000 компьютеров на территории Ирана. Нанесен колоссальный экономический, энергетический, оборонный и политический ущерб суверенитету Ирана. Только один этот пример демонстрирует, насколько опасны и масштабны кибервойны. Их последствия, как правило, мультипликативны, то есть ущерб от них распространяется на самые различные сферы жизнедеятельности. Масштаб ущерба от кибервойн может достигать масштаба действия оружия массового поражения. Мир столкнулся с совершенно неизведанным видом войн, в котором оружием стал компьютер.

Автор этой статьи считает, что аттрактором кибервойн будущего выступает киборг – *искусственный интеллект как субъект социальных отношений.* События, созданные в книгах и фильмах, рассказывающих о войне людей с роботами, продвигаются с развитием IT из фантастики в реальную жизнь и реальную политику.

Начало кибервойнам было положено в США в середине 90-х годов XX века принятием новой военной доктрины, получившей название «сетецентрических войн» (Network-centric warfare). Выделение кибервойск в особый род войск произошло в 2009 году, когда в рамках Стратегического командования США был создано Киберкомандование (USCYBERCOM – United States Cyber Command). Как отмечает эксперт Российского совета по международным делам (РСМД) Шариков П. А.: «Исторически Стратком занимался вопросами ядерного сдерживания, поэтому включение в перечень его полномочий вопросов противодействия информационным угрозам может служить доказательством стратегического значения киберпространства для национальной безопасности США» [8].

Сегодня, помимо США, киберкомандование в виде самостоятельных воинских структур работает в Великобритании, Нидерландах, КНДР (Северная Корея), Республике Корея (Южная Корея), КНР, Израиле и России. Названия у «киберштабов» разные, разная численность, различные материальный, технический и организационный потенциал, разные функции, объем полномочий, компетенций и ответственности. Но суть одна – все они занимаются организацией управлением войсками на основе современных информационно-компьютерных систем. Все они создают и развивают новый вид войск – кибервойска.

В Российской Федерации разработкой функций, организационной структуры, подчиненности такого вида военной структуры практически занялись в феврале 2013 года. В итоге была разработана концепция Национального центра управления обороной, который вступил на опытное боевое дежурство 28 марта 2014 года. С 1 декабря 2014 года НЦУО РФ вступил на боевое дежурство. Несмотря на то что, НЦУО стал как бы преемником Центрального командного пункта МО РФ, содержание его деятельности гораздо шире и реализуется с учетом концепции кибервойн[8].

Понимание того, что кибервойны имманентны современным войнам, присутствует в новой военной Доктрине, утвержденной Президентом Российской Федерации 25 декабря 2014 года. В качестве основных внешних военных опасностей закреплено следующее положение: «ис-

[7] Центральный банк РФ. Пресс-служба Центрального банка Российской Федерации. Официальный сайт. [Электронный ресурс]. URL: http://www.cbr.ru/press/PR.aspx?file=27012_1825052.htm (дата обращения: 21.04.2015).

[8] Гаврилов Ю. , Птичкин С. Киборги не прорвутся. Формируются войска информационных операций // РГ от 13.05.2014. Официальный сайт. [Электронный ресурс]. URL: http://www.rg.ru/2014/05/13/kiber.html (дата обращения 13.05.2015).

пользование 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». В качестве основных внутренних опасностей закреплена «деятельность по информационному воздействию на население»[9]. Член Общественного совета при Минобороны РФ, главный редактор журнала «Национальная оборона» И. Ю. Коротченко отмечает новую роль информационных войн: «Также любопытно указание на применение новых нетрадиционных форм ведения боевых действий – использование протестного потенциала местного населения, манипулирование информационными потоками и сознанием – все, что позволит решать прежние военные задачи качественно новыми способами»[10].

В Военной доктрине РФ, в Стратегии национальной безопасности РФ и в Доктрине информационной безопасности РФ сформулированы, в совокупности, положения о защите национального суверенитета России от информационно-компьютерных угроз. Реализация этих положений для России – новая и сложная задача. Это связано с тем, что современная инфосфера – киберпространство – особая, слабо изученная и динамично развивающаяся сфера человеческой деятельности. Борьба государственных интересов мировых держав, экономических интересов влиятельных ТНК в инфосфере, киберпреступность, террористические организации создают новые принципы и формы конкуренции и сотрудничества, войны и мира, новые виды преступлений. И нужно вырабатывать новые меры воздействия, адекватные возникшим вызовам. Необходимо находить эффективные способы борьбы с новыми угрозами нашему национальному суверенитету.

Приведенная выше классификация разделяет информационно-компьютерные угрозы по сферам деятельности, «не мешая все в одну кучу». Такой подход помогает разграничить криминальную, монетарную и оборонную сферы организации информационной безопасности в киберпространстве. Конечно, данная классификация имеет неокончательный вид. Но, по мнению автора, эти угрозы и риски должны быть учтены при разработке новой Доктрины информационной безопасности РФ. Методологически новая доктрина должна основываться на *концепции состояния киберпространства как глобальной, трансграничной сетевой информационно-компьютерной сферы.*

В заключение следует отметить степень возрастания и непредсказуемости информационно-компьютерных угроз. Никто не может себе представить полную картину надвигающихся информационно-компьютерных угроз и последствия их воздействия на человечество. Можно попробовать это сделать, помножив все виды уже известных нам информационных рисков и киберугроз друг на друга. Мы получим коэффициент риска «в десятой степени». Но даже эта угрожающая цифра не даст нам понимания информационно-компьютерной опасности, потому что IT-революция продолжается. Мы не можем ясно спрогнозировать, как и куда она нас приведет. Говоря словами Нассима Талеба, это «Черный Лебедь из Крайнестана» [7, с. 1–3]. «Крайнестан» – это страна, в которой наши прогнозы почти никогда не сбываются. Но мы должны их делать, чтобы не быть безоружными во враждебном нам киберпространстве.

1. Еляков, А.Д. Проблемы информационной безопасности в использовании электронных компьютерных технологий [Текст] / А.Д. Еляков // Социс. 2013. № 10. С. 120–129.

2. Михайленок, О.М. Национальный суверенитет и российский федерализм [Текст] / О.М. Михайленок // Власть. 2010. № 3. С. 4–8.

3. Почепцов, Г.Г. Информационные войны. [Текст] / Г.Г. Почепцов. М.: Рефл-бук, К.: Ваклер, 2000. 586 с.

4. Райс, Э. [Ries A., Trout J.]. Маркетинговые войны. [Электронный ресурс] / Э. Райс, Дж. Траут. URL: http:/bookz.ru/authors/el-rais-djek-traut/trautrise01/1-trautrise01.html (дата обращения: 21.04.2015).

5. Сивоволов, Д.Л. Роль российской дипломатии в построении «электронного государства» в РФ [Электронный ресурс] / Д.Л.

[9] Военная доктрина Российской Федерации. Российская газета от 30.12.2014. Официальный сайт. [Электронный ресурс]. URL: http://www.rg.ru/2014/12/30/doktrina-dok.html (дата обращения: 24.04.2015).

[10] Что доктрина прописала // «Российская газета» – Федеральный выпуск № 6570 от 29.12.2014. Официальный сайт. [Электронный ресурс]. URL: http://www.rg.ru/2014/12/29/doktrina.html (дата обращения: 06.06.2015).

Сивоволов // Вестник МГИМО. 2013. № 5 (32). С. 54–57. Официальное интернет-издание «Вестник МГИМО-Университета». URL: http://www.vestnik.mgimo.ru/razdely/mirovaya-politika/rol-rossiyskoy-diplomatii-v-postroenii-elektronnogo-gosudarstva-v (дата обращения: 08.06.2015).

6. Смирнов, А.А. Эволюция угроз информационной безопасности. [Электронный ресурс] / А.А. Смирнов // Информационная безопасность. 2015. № 2 (34). С. 69–74. URL: http://media.wix.com/ugd/ec9cc2_36deaf967c4942528aae55e354b8c79f.pdf (дата обращения: 15.11.2015).

7. Талеб, Н.Н. [Taleb N.N.] Черный Лебедь. Под знаком непредсказуемости [Электронный ресурс] / Н.Н. Талеб // Сайт С.П. Курдюмова. URL: http://spkurdyumov.ru/what/chernyj-lebed-pod-znakom-nepredskazuemosti-nikolas-taleb/ (дата обращения: 03.05.2015).

8. Шариков, П.А. Информационное сдерживание: трансформация парадигмы стратегической стабильности [Электронный ресурс] / П.А. Шариков // РСМД. Официальный сайт. URL: http://russiancouncil.ru/inner/?id_4=2291&from=oct13rus#top-content (дата обращения: 29.04.2015).

References

1. Elyakov A.D. (2013) Sotsis, no. 10, pp. 120–129 [in Rus].

2. Mihajlenok O.M. (2010) Vlast', no. 3, pp. 4–8 [in Rus].

3. Pocheptsov G.G. (2000) Informatsionnye voyny. Moscow, Refl-buk, K., Vakler, 586 p. [in Rus].

4. Rays E., Traut Dzh. Marketingovye voyny. Available at: http:/bookz.ru/authors/el-rais-djek-traut/trautrise01/1-trautrise01.html (accessed 21.04.2015) [in Rus].

5. Sivovolov D.L. (2013) Rol' rossiyskoy diplomatii v postroenii «elektronnogo gosudarstva» v RF. Vestnik MGIMO, no. 5 (32), pp. 54–57. Ofitsial'noe internet-izdanie «Vestnik MGIMO-Universiteta». Available at: http://www.vestnik.mgimo.ru/razdely/mirovaya-politika/rol-rossiyskoy-diplomatii-v-postroenii-elektronnogo-gosudarstva-v (accessed 08.06.2015) [in Rus].

6. Smirnov A.A. (2015) Jevoljucija ugroz informacionnoj bezopasnosti. Informacionnaja bezopasnost', no. 2 (34), pp. 69–74. Available at: http://media.wix.com/ugd/ec9cc2_36deaf967c4942528aae55e354b8c79f.pdf (accessed 15.11.2015) [in Rus].

7. Taleb N.N. Chernyy lebed'. Pod znakom nepredskazuemosti. Sayt S.P. Kurdyumova. Available at: http://spkurdyumov.ru/what/chernyj-lebed-pod-znakom-nepredskazuemosti-nikolas-taleb/ (accessed 03.05.2015) [in Rus].

8. Sharikov P.A. Informatsionnoe sderzhivanie: transformatsiya paradigmy strategicheskoy stabil'nosti. RSMD. Ofitsial'nyy sayt. Available at: http://russiancouncil.ru/inner/?id_4=2291&from=oct13rus#top-content (accessed 29.04.2015) [in Rus].

UDC 001:35+004.8

NEW THREATS TO THENATIONAL SOVEREIGNTY OF RUSSIA IN THE SPHERE OF INFORMATION SECURITY

Sivovolov Dmitriy Leonidovich,
Ural Federal University named after the first President of Russia B.N. Eltsin, Institute of Public Administration and Entrepreneurship, Department Chair of Management of Social Relations, Associate Professor, Cand. Sc. (Sociology), Yekaterinburg, Russia.
E-mail: dioma@inbox.ru

Annotation
The article deals with justifying the increase of threats to the information security of the Russian Federation. The author provides evidence that in modern Russia information threats are considered as threats to the national sovereignty of Russia. Special attention is given to the definition of information security as an information computer security and its classification according to the spheres of activities.

Key concepts:
information security,
national sovereignty,
information computer wars,
cyber security,
cyber warfare.