«Утверждаю»
Декан факультета глобальных процессов
МГУ имени М.В.Ломоносова
_____ И.В.Ильин
«___» _____ 2014 г.

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ М.В.ЛОМОНОСОВА

ФАКУЛЬТЕТ ГЛОБАЛЬНЫХ ПРОЦЕССОВ

В.И.Бажуков

ИНФОРМАЦИОННЫЕ ВОЙНЫ: ТЕОРИЯ И ПРАКТИКА

Рабочая программа дисциплины

Рекомендовано Учёным советом факультета глобальных процессов МГУ имени М.В. Ломоносова в качестве учебно-методического пособия по учебному курсу

Москва

2014

Аннотация дисциплины.

Программа дисциплины «Информационные войны: теория и практика» составлена в соответствии с требованиями к обязательному минимуму содержания дисциплины по направлению 41.06.01 «Политические науки и регионоведение».

Данный курс посвящен анализу теоретико-методологических и практических аспектов информационных войн, рассмотрению информационно-технических и информационно-психологических сторон информационного воздействия в современном мире, изучению фактических материалов по основным разделам курса.

Данный курса дает возможностью более глубоко понять сущность информационных войн, исторические этапы их развития, особенностях проявления в начале XXI века, основные угрозы в информационной сфере и задачи в обеспечении информационной безопасности Российской Федерации.

I.Название дисциплины / практики (в соответствии с учебным планом): «Информационные войны: теория и практика».

II.Шифр дисциплины – дисциплина по выбору

III.Цели и задачи дисциплины

А. Цель дисциплины – дать аспирантам целостное представление об информационных войнах, их истории, особенностях проявления в начале XXI века, угрозах в информационной сфере и задачах по обеспечению информационной безопасности Российской Федерации.

Б. Задачи дисциплины:

- изучить теоретико-методологические основы исследования информационных войн;

- рассмотреть концепцию современной российской государственной информационной политики;

- познакомиться с зарубежными и отечественными теоретическими концепциями информационной и информационно-психологической войны, сетевой и кибервойны, информационной безопасности;

- изучить правовые аспекты компьютерных правонарушений и информационных войн;

- выявить исторические этапы развития теории и практики информационных войн, особенности информационного противоборства в годы Первой и Второй мировых войн, в период холодной войны и в начале XXI века;

- рассмотреть особенности информационно-психологических войн, информационно-психологических операций и их место в системе информационных войн;

- познакомиться с деятельностью средств массовой информации в освещении современных событий в мире и их ролью в современных информационных войнах;

- изучить сущность и специфику сетевых и кибервойн;

- выяснить характер угроз национальной безопасности России, связанных с информационными войнами, и определить задачи по созданию системы информационной безопасности страны;

- определить методологию, направления и актуальные проблемы исследований по вопросам информационных войн и информационной безопасности.

IV. Место дисциплины в структуре ООП:

А. Информация о месте дисциплины в образовательном стандарте и учебном плане:

Дисциплина изучается на 2 курсе, в 3 семестре.

Б. Перечень дисциплин, которые должны быть освоены до начала изучения данной дисциплины: всемирная (глобальная) история, геополитика, история международных отношений, теория международных отношений, мировая политика, основы глобалистики, политическое регионоведение, современная внешняя политика Российской Федерации, региональные аспекты международных отношений, актуальные проблемы глобальных исследований, международная конфликтология.

В. *Общая трудоемкость дисциплины* составляет 2 зачетных единицы, 72 часа.

Г. *Формы аттестации.*

Промежуточная аттестация проводится в форме докладов, презентаций, ролевых игр. Аспиранты должны подготовить презентации по результатам самостоятельной работы. Тематика презентаций может варьироваться в зависимости от тематики курса и интересов аспирантов. В презентациях аспирантов отрабатываются прикладные аспекты проблематики курса.

Итоговая аттестация проходит в виде зачета. На зачете учитываются посещения лекций и участие в дискуссиях, выполненные практические работы и презентации. Зачет может проходить в форме письменного тестирования и устного опроса.

V.Формы проведения:

А. Для дисциплин: форма занятий с указанием суммарной трудоемкости по каждой форме:

лекции – 36 часов;

самостоятельная работа – 36 часов;

формы текущего контроля: презентации, рефераты, экспертные заключения, исследовательские проекты, коллоквиумы.

Форма итогового контроля – зачет.

VI.Распределение трудоемкости по разделам и темам, а также формам проведения занятий с указанием форм текущего контроля и промежуточной аттестации:

№ п/п	Наименование разделов и тем дисциплины	Трудоемкость (в ак. часах) по формам занятий			
		Аудиторная работа (с разбивкой по формам занятий)			
		Лекции	Практические занятия (семинары) полевые работы	Лабораторная работа /Камеральная работа	Самостоятельная работа
1	2	3	4	5	6
1	Тема 1. Теоретико-методологические проблемы изучения информационных войн.	2	-	-	2
2	Тема 2. Сущность информационных войн, принципы ведения и средства обеспечения.	4	-	-	4
3	Тема 3. Отечественные и зарубежные исследования по проблемам информационных и информационно-психологических войн: этапы, направления, подходы.	2	-	-	2
4	Тема 4. Исторические этапы формирования теории и практики информационных войн.	4	-	-	4
5	Тема 5. Информационное противоборство в годы	2	-	-	2

	«холодной войны».				
6	Тема 6. Информационное противоборство в начале XXI века.	2	-	-	2
7	Тема 7. Информационно-психологическая война как средство агрессии и достижения политических целей.	4	-	-	4
8	Тема 8. Кибервойна как вид информационных войн. Сетевые войны и их особенности.	4	-	-	4
9	Тема 9. Подготовка США к глобальной информационной войне.	2	-	-	2
10	Тема 10. Правовые аспекты информационных войн.	2	-	-	2
11	Тема 11. Государственная информационная политика в условиях информационной войны.	4	-	-	4
12	Тема 12. Направления деятельности Российского государства в сфере обеспечения информационной безопасности.	4	-	-	4
	Зачет				
	Всего	36	-	-	36

VII.Содержание дисциплины по разделам и темам – аудиторная и самостоятельная работа:

Тема 1. Теоретико-методологические проблемы изучения информационных войн.

1.Информационное общество как среда организации и проведения информационных войн. Зарождение концепции информационного общества. Кисё Курокава и Тадао Умесао об информационном обществе. Развитие теории информационного общества в трудах Мартина Бангемана. Черты информационного общества. Создание глобального информационного пространства. Развитие информационного общества в западных странах и в России. Информационное общество и информационные войны.

2.Политические процессы в современном информационном обществе. Общая характеристика политических процессов в современном информационном обществе. Система политических отношений общества в условиях глобальной информатизации. Изменения в массовом и индивидуальном сознании граждан. Влияние процессов глобализации на информационное общество. Геополитические процессы в современном информационном обществе и информационная политика. Обеспечение информационной безопасности в современном информационном обществе.

Тема 2. Сущность информационных войн, принципы ведения и средства обеспечения.

1.Основные понятия: «информационная война», «информационное противоборство», «информационное воздействие», «идеологическая борьба», «психологическая война», «пропаганда», «кибервойна», «сетевая война», «гибридная война». Характеристики информационной войны. Объекты информационной войны: информационные системы, информационные процессы, массовое сознание, общественное мнение, индивидуальное сознание. Наступательные и оборонительные информационные войны. Виды информационного оружия и способы его применения. Особенности применения информационного оружия.

2.Средства воздействия в информационных войнах: психотронное оружие, Интернет, хакеры, блоггеры, видеоигры, информационный терроризм во всемирной глобальной сети, средства массовой информации.

Тема 3. Отечественные и зарубежные исследования по проблемам информационных и информационно-психологических войн: этапы, направления, подходы.

1.Основные этапы исследований в России информационных и информационно-психологических войн. Разработка проблем идеологической борьбы в СССР. Изучение вопросов психологических войн. Труды Д.А.Волкогонова о психологических войнах и психологических операциях. Переводы зарубежных авторов.

2.Характер современных исследований об информационных и информационно-психологических войнах. Работы В.Г.Крысько, А.В.Манойло, Н.А.Нартова, И.Н.Панарина, А.И.Петренко, Г.Г.Почепцова, П.С.Расторгуева, Д.Б.Фролова, В.М.Щекотихина. Исследование проблем информационной безопасности. Разработка

концепции государственной информационной политики в условиях информационного общества и информационной войны.

Тема 4. Исторические этапы формирования теории и практики информационных войн.

1.Зарождение и развитие форм и способов психологического воздействия на противника. Сунь-Цзы о способах и приемах психологического воздействия на противника. Проблемы информационного противоборства в Средние века и Новое время. Наполеон о роли печатной пропаганды среди своих войск, войск и населения противника. Развитие средств массовой информации в XIX веке и информационное противоборство в период вооруженных конфликтов и войн.

2.Информационное противоборство в годы Первой мировой войны. Формирование органов пропаганды в Германии, Великобритании и России и их деятельность. Развитие средств массовой информации и их роль в пропагандистских операциях. Разработка принципов ведения пропагандистских кампаний. Особенности ведения пропаганды в России.

3.Информационное противоборство в годы Второй мировой войны. Организация тотальной пропаганды в нацистской Германии. Деятельность органов пропаганды Великобритании и США. Направления деятельности органов спецпропаганды СССР в годы Великой Отечественной войны. Роль Совинформбюро в организации деятельности средств массовой информации в стране и за рубежом.

Тема 5. Информационное противоборство в годы «холодной войны».

1.Трансформация информационных войн в новейшее время. Информационно-идеологическое противостояние между СССР и США. Речь У.Черчилля в Фултоне как начало холодной войны. Психологическая война и идеологическая борьбы. Информационное противоборство до начала перестройки. Органы психологической войны США, Великобритании, ФРГ и направления их деятельности в информационном противоборстве с СССР.

2.Информационное противоборство в годы перестройки. Политика СССР на ускорение, гласность и демократизацию. Концепция нового политического мышления и информационное противоборство. Причины краха системы социализма и распада СССР.

Роль руководства СССР в организации и ведении идеологической работы внутри страны и ведении пропаганды за рубежом.

Тема 6. Информационное противоборство в начале XXI века.

1.Особенности информационных войн в начале XXI века. Использование информационных технологий для свержения законных правительств. Информационная война и вооруженное вторжение коалиционных сил во главе с США в Ирак (2003 г.). Роль информационных технологий в «оранжевой» революции (2004-2005 гг.) на Украине. Информационная война и вооруженное вмешательство международных вооруженных сил в гражданскую войну в Ливии. Гражданская война в Сирии и информационная война. Революция «Евромайдана» и противостояние на Украине (2014-2016 гг.).

2.Информационные войны против России. Участники, методы, средства, приемы. Информационное противоборств в связи с агрессией Грузии против Южной Осетии в 2008 г. Информационная война в связи с событиями на Украине (2014-2016 гг.). Борьба против террористической организации «Исламское государство» и информационное противоборство.

Тема 7. Информационно-психологическая война как средство агрессии и достижения политических целей.

1.Понятия информационно-психологической войны. Место психологической войны в системе информационной войны. Основные структурные элементы информационно-психологического воздействия. Дезинформирование, лоббирование, манипулирование, пропаганда, управление кризисами, шантаж. Основные этапы мероприятий и аксиомы психологической войны.

2.Информационно-психологические операции: содержание, классификация, цели и объекты. Методы психологических операций в информационных войнах. Органы психологической войны западных государств. Цели и объекты психологических операций. Восточная модель органов психологического обеспечения. Роль средств массовой информации в информационно-психологических войнах.

Направления противодействия России психологическим операциям западных государств.

Тема 8. Кибервойна как вид информационных войн. Сетевые войны и их особенности.

1.Кибервойна как информационное противоборство в киберпространстве. Зарубежные и отечественные ученые о кибервойнах. Цели кибервойн: дестабилизация компьютерных систем, нарушение доступа к Интернету государственных учреждений и деловых центров, создание беспорядка и хаоса в жизни стран. Формы проявления кибервойн: вандализм, пропаганда, шпионаж, атаки на компьютерные системы и серверы.

2.Направления деятельности различных государств по противодействию кибератакам. Создание Агенства сетевой и информационной безопасности Евросоюза (2005 г.), Киберкомандования в вооруженных силах США и их задачи. Усилия Российской Федерации по обеспечению безопасности в киберпространстве.

3.Сетевые войны и их особенности. Понятия сетевого общества и сети. Особенности сетевого общества. Мануэль Кастельс о сетевом обществе. Сеть как гибкая форма организации взаимодействия различных элементов, предполагающая постоянный обмен информацией. Естественные и искусственные сети. Сети, построенные на основе этнического принципа. Особенности сети: синтез иерархии и энтропии. Клубневая форма существования, легкость проникновения и распространения.

4.Концепция сетецентричной войны. Возможные направления подготовки сетецентричной войны. Принципы ведения сетевых войн. Участие частных военных компаний и неправительственных организаций в сетевых войнах. «Цветные» («бархатные») революции. Роль религиозных организаций в сетевых войнах. Сегменты американской сети в российском обществе.

Тема 9. Подготовка США к глобальной информационной войне.

1.Разработка концепции стратегической информационной войны в США. Основные направления деятельности Пентагона, ЦРУ, ФБР, Агенства национальной безопасности США по подготовке к информационной войне. Директивы министерства обороны США «Информационная война» (1992 г.), «Объединенная доктрина информационных операций» (1998 г.). Стремление США к стратегическому информационному доминированию. Командно-штабные игры и учения в США по проверке безопасности компьютерных систем и сетей, по ведению информационных войн для поражения информационных систем противника.

2.Создание специальных органов информационных войн. Подготовка кадров для ведения информационных войн. Разработка информационного оружия и способов его

применения. Деятельность центров информационных войн сухопутных войск, ВВС, ВМС, разведуправления министерства обороны США. Деятельность США по радиоэлектронному перехвату информации. Разоблачения Э.Сноудена. Деятельность других государств в области подготовки к информационным войнам.

Тема 10. Правовые аспекты информационных войн.

1.Информация и информационные отношения как новый криминалистический объект. Понятие информационных компьютерных преступлений. Законодательство РФ об информационных правоотношениях. Правовая характеристика компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных программ для ЭВМ. Нарушение права эксплуатации ЭВМ или их сети.

2.Виды преступных последствий. Способы совершения преступлений. Свойства личности субъекта преступлений. Предупреждение компьютерных преступлений. Методика и практика расследования преступлений в сфере компьютерной информации. Уголовно-правовая характеристика информационно-психологических операций. Операции информационно-психологической войны в контексте международного права.

Тема 11. Государственная информационная политика в условиях информационной войны.

1.Основные принципы деятельности органов государственной власти в условиях информационно-психологической1 войны. Особенности управления в информационном обществе. Использование информационных технологий в информационном обществе. Роль СМИ в процессах государственного управления. Вовлечение СМИ в психологическое противоборство.

2.Методика оценки враждебных агрессивных действий участников информационно-психологического противоборства. Классификация источников информационно-психологической агрессии. Роль органов государственной власти в разрешении конфликтов и в управлении кризисными ситуациями в информационно-психологической сфере. Деятельность органов государственной власти по отражению информационно-психологической агрессии.

Тема 12. Направления деятельности Российского государства в сфере обеспечения информационной безопасности.

1.Понятие информационной безопасности. Информационная безопасность государства. Две составляющие информационной безопасности: информационно-технологическая и информационно-психологическая. Основные признаки понятия «информационная безопасность»: конфиденциальность, целостность и доступность. Дополнительные признаки понятия. Угрозы информационной безопасности Российской Федерации.

2.Государственная система информационного противоборства. Нормативные документы в области обеспечения информационной безопасности. Органы, обеспечивающие информационную безопасность. Информационно-психологическая защита личности и общества. Развитие технологической основы обеспечения защиты информации в сетях связи специального назначения. Кадровое обеспечение информационной безопасности. Коллективные меры государств ОДКБ в сфере обеспечения информационной безопасности.

VIII.Перечень компетенций, формируемых в результате освоения дисциплины:

- способность анализировать социально значимые проблемы и процессы (ОК-10);

- мотивированность на решение практических задач, нахождение нестандартных интерпретаций международной информации (ОК-22);

- умение работать с материалами средств массовой информации, составлять обзоры прессы по заданным темам, находить, собирать и первично обобщать фактический материал, делая обоснованные выводы (ПК-14);

- умение и навыки слежения за динамикой основных характеристик среды международной безопасности и понимание их влияния на национальную безопасность России (ПДК-3);

- владение основами и базовыми навыками прикладного анализа международных ситуаций (ПДК-10);

- умение профессионально грамотно анализировать и пояснять позиции Российской Федерации по основным международным проблемам (ПДК-12);

IX.Используемые образовательные, научно-исследовательские и научно-производственные технологии:

А.Образовательные технологии:

- активная учебно-познавательная деятельность обучаемых;

- учет направления и профиля подготовки аспирантов, тематики их диссертационных исследований;

- построение учебного процесса с учетом индивидуальных, возрастных, психологических и физиологических особенностей обучаемых;

- формирование готовности у аспирантов к саморазвитию и непрерывному образованию.

Б.Научно-исследовательские технологии:

- придание учебному процессу исследовательского характера;

- вовлечение обучаемых в научно-исследовательскую деятельность;

- совместное выполнение научно-исследовательских работ.

X.Учебно-методическое обеспечение самостоятельной работы обучаемых, оценочные средства контроля успеваемости и промежуточной аттестации:

А.Учебно-методические рекомендации для обеспечения самостоятельной работы аспирантов:

В процессе самостоятельной работы аспирантам рекомендуется выполнять задания творческого, исследовательского характера, осуществлять научный анализ источников и литературы, готовить аналитические материалы с обзором ситуации в информационной обстановке в стране, регионе и в мире, исследовать характер угроз информационной безопасности России и направления противодействия этим угрозам. Учитывать, что важным источником информации в области информационных войн и информационной безопасности являются различные официальные документы: законы, доктрины и

стратегии по проблемам информации, информатизации и информационного сотрудничества, информационной и национальной безопасности.

При подготовке к текущей и промежуточной аттестации рекомендуется обращаться к списку примерных вопросов, к материалам лекций, к основной и дополнительной литературе.

Выполнение презентаций и требования к их оформлению

Презентация представляет собой отчетную форму по самостоятельной работе обучаемых. Подготовка презентации предполагает ориентацию на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учётом интересов обучаемых. Для подготовки презентаций используется программа Microsoft PowerPoint, которая позволяет представить информацию в наглядной форме. На каждом слайде можно разместить текст, рисунки, фотографии, графические объекты, мультимедиа и др.

По своей структуре презентация должна содержать титульный слайд, слайды с основным содержанием и завершающий слайд. На титульном слайде указываются факультет, группа, фамилия, имя и отчество автора, а также тема презентации. Завершающий слайд содержит список используемых источников и литературы. Для обеспечения наглядности следует использовать разные способы размещения информации и разные виды слайдов: с текстом; с иллюстрациями; с текстом и иллюстрациями. Не следует заполнять один слайд слишком большим объемом информации. Размер шрифта должен быть максимально крупным на слайде: самый «мелкий» для презентации – шрифт 24 пт (для текста) и 40 пт (для заголовков).

Выполнение экспертного заключения.

Экспертное заключение – официальный документ, являющийся результатом работы эксперта или экспертной комиссии, отвечающий на поставленные заказчиком вопросы. Экспертное заключение – это результат произведенного исследования, опирающегося на наблюдение, факты и другие возможные методы. Экспертное заключение обычно состоит из нескольких частей: вводной, исследовательской и изложения выводов.

Примерное содержание экспертного заключения по теме: «Сотрудничество государств ОДКБ в сфере информационной безопасности». Первая часть: описательная (общая характеристика сотрудничества в рамках ОДКБ). Вторая часть: исследовательская:

направления сотрудничества в информационной сфере в рамках ОДКБ; особенности сотрудничества в деле обеспечения информационной безопасности; факторы, мешающие успешному сотрудничеству и пути их преодоления. Третья часть: экспертная оценка принятых решений и характера деятельности соответствующих органов государств ОДКБ в информационной сфере; существующие проблемы и перспективы дальнейшего сотрудничества, предложения по повышению эффективности деятельности в обеспечении информационной безопасности стран ОДКБ.

Б.Примерный перечень тем для рефератов и презентаций:

1. Информационная война и психологическая война: общее и особенное.
2. Зарождение и основные этапы развития информационных войн.
3. Информационное противоборство в годы Первой мировой войны.
4. Информационное противоборство в годы Второй мировой войны.
5. Особенности нацистской пропаганды в годы Второй мировой войны.
6. Советская спецпропаганда в годы Великой Отечественной войны.
7. Информационное противоборство в годы холодной войны.
8. Влияние перестройки на ведение информационного противоборства.
9. Информационное противоборство в начале XXI века.
10. Принципы ведения информационных войн западных государств.
11. Психологическая война как вид информационной войны.
12. Психологическое воздействие на массовое и индивидуальной сознание как средство психологической войны.
13. Психологические операции и их типы.
14. Пропаганда в системе психологической войны.
15. Сетевые войны и их особенности.
16. Сетевое общество как предпосылка сетевой войны.
17. Основные принципы сетевых операций.
18. Кибервойна как вид информационной войны.
19. Кибероружие и его особенности.
20. Ассиметричный характер кибервойны.
21. Психологическая война и кибервойна: общие и особенные черты.
22. Разоблачения Эдварда Сноудена.
23. Подготовка к кибервойне ведущих государств мира.
24. Силы и средства США для ведения кибервойны.

25. Американская стратегия ведения кибервойны.

26. Информационная безопасность и национальные интересы России.

27. Угрозы информационной безопасности России и их виды.

28. Состояние информационной безопасности России.

29. Система обеспечения информационной безопасности России.

30. Методы обеспечения информационной безопасности России.

31. Правовые аспекты информационных войн.

32. Государственная информационная политика Российской Федерации в условиях информационной войны.

В.Примерный список вопросов для проведения текущей и промежуточной аттестации

1. Объект и предмет курса «Информационные войны: теория и практика».
2. Основные понятия, применяемые при анализе информационных войн.
3. Степень разработанности проблемы «информационные войны».
4. Соотношение понятий «информационная война» и «идеологическая борьба».
5. Информационная война и психологическая война: общее и особенное.
6. Зарождение и основные этапы развития информационных войн.
7. Идеи Наполеона об информационном противоборстве с противником.
8. Информационное противоборство в годы Первой мировой войны.
9. Ведение пропаганды Германией в годы Первой мировой войны.
10. Органы пропаганды Великобритании и ведение пропагандистских операций в годы Первой мировой войны.
11. Пропагандистские операции России в годы Первой мировой войны.
12. Информационное противоборство в годы Второй мировой войны.
13. Особенности нацистской пропаганды в годы Второй мировой войны.
14. Советская спецпропаганда в годы Великой Отечественной войны.
15. Информационное противоборство в годы холодной войны.
16. Влияние перестройки на ведение информационного противоборства.
17. Информационное противоборство в начале XXI века.
18. Принципы ведения информационных войн западных государств.
19. Психологическая война как вид информационной войны.
20. Психологическое воздействие на массовое и индивидуальной сознание как средство психологической войны.
21. Психологические операции и их типы.

22. Цели и объекты психологических операций.
23. Пропаганда в системе психологической войны.
24. Сетевые войны и их особенности.
25. Сетевое общество как предпосылка сетевой войны.
26. Сущность, структура и функции сетей в сетевом обществе.
27. История создания концепции сетевых войн.
28. Основные принципы сетевых операций.
29. Самосинхронизация и глубокое сенсорное проникновение как принципы сетевых войн.
30. Кибервойна как вид информационной войны.
31. Кибероружие и его особенности.
32. Ассиметричный характер кибервойны.
33. Психологическая война и кибервойна: общие и особенные черты.
34. Разоблачения Эдварда Сноудена.
35. Подготовка к кибервойне ведущих государств мира.
36. Силы и средства США для ведения кибервойны.
37. Американская стратегия ведения кибервойны.
38. Информационная безопасность и национальные интересы России.
39. Угрозы информационной безопасности России и их виды.
40. Состояние информационной безопасности России.
41. Система обеспечения информационной безопасности России.
42. Методы обеспечения информационной безопасности России.
43. Правовые аспекты информационных войн.
44. Государственная информационная политика в условиях информационной войны.

XI.Учебно-методическое и информационное обеспечение дисциплины

А.Основная литература

№ п/п	Автор	Название книги/ статьи	Отв. редактор (для коллективных работ)	Место издания	Издательство	Год издания	Название журнала (сборника	Том (выпуск) журнала/ сборника
1	2	3	4	5	6	7	8	9
1	Барабаш	Государственна		Моск	АИРО-XXI	2015		

	В.В., Бордюгов Г.А., Котеленец Е.А.	я пропаганда и информационные войны. Учебное пособие.		ва				
2	Бубнов А.А. и др.	Основы информационной безопасности: учебное пособие		Москв	Академия	2016		
3	Беликова Ю.В., Крикунов А.В., Королёв А.В.	Сетевые технологии в информационных операциях НАТО и зарубежных неправительственных организаций в ходе цветных революций и военных конфликтов монография		Москва	Акад. ФСО России	2012		
4	Буренок В.М.	Национальная безопасность России в эпоху сетевых войн		Москва	Рос. Акад. рак. и арт. наук	2015		
5	Василенко В.И. и др.	Массмедиа в условиях глобализации: информационно-коммуникационная безопасность: монография.	Василенко В.И.	Москва	Проспект	2015		
6	Демидов О.	Глобальное управление интернетом и безопасность в сфере использования ИКТ		Москва	Альпина Паблишер	2016		
7	Ларина Е.С., Овчинский В.С.	Кибервойны XXI века. О чём умолчал Эдвард Сноуден.		Москва	Книжный мир	2014		
8	Нартов Н.А.	Информационная война: история		Москва	НОУ ВПО	2014		

		и современность: монография.			МИПП			
9	Разиков В.Н.	Информационно-психологическая война как специфический вид боевых действий: монография		Рязань	РВВДКУ	2012		
10	Щекотихин В.М., Королев А.В., Королев В.В. и др.	Информационная война. Информационное противоборство: теория и практика: Монография.	В.М.Щекотихин	Москва	Академия ФСО России, ЦАТУ	2011		

Б.Дополнительная литература

№ п/п	Автор	Название книги/ статьи	Отв. редактор (для коллективных работ)	Место издания	Издательство	Год издания)	Название журнала (сборника	Том (выпуск) журнала/ сборника
1	2	3	4	5	6	7	8	9
1.	Гладкий А.А.	Основы безопасности и анонимности во всемирной сети.		Ростов-на-Дону	Феникс	2012		
2	Дроботенко О.Н.	Информационная безопасность России в условиях глобализации: внешнеполитический аспект: монография		Краснодар	Изд-во Кубанского соц-эконом. ин-та	2016		
3	Дроботушенко Е.В., Днепровский В.В.	Информационное противоборство в региональных конфликтах: безопасность в рамках		Чита	ЗабГГПУ	2012		

		Азиатско-Тихоокеанского региона: учебное пособие.						
4	Лайнбарджер П.Э.	Психологическая война: теория и практика обработки массового сознания		Москва	Центрполиграф	2014		
5	Остапенко Г.А. и др.	Информационные риски в социальных сетях: монография.	Новиков Д.А.	Воронеж	Науч. книга	2013		
6	Смирнов А.А.	Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография.		Москва	ЮНИТИ : Закон и право	2012		

В.Программное обеспечение и Интернет-ресурсы:

Агенство новостей Блумберг http://www.spr.ru/arbat/bloomberg-l-p.html

ТАСС – информационное агенство России http://tass.ru/

«РИА Новости «- Информационное агенство http://ria.ru/

Центр информационных технологий и систем органов исполнительной власти http://www.citis.ru/

Центр информационной безопасности ФСБ России http://www.tadviser.ru/index.php/

Журнал «Информационные войны» http://www.delpress.ru

Журнал «Информационная безопасность» http://www.itsec.ru/subscription.php

Журнал «Проблемы информационной безопасности» http://jisp.ru/

Журнал «Защита информации Inside» http://www.inside-zi.ru/

Сеть безопасности человека http://www.humansecuritynetwork.org/

XII.Материально-техническое обеспечение дисциплины

А.Помещения – лекционные аудитории в первом корпусе гуманитарных факультетов МГУ имени М.В.Ломоносова.

Б.Оборудование – компьютер, диапроектор, экран.

В.Иные материалы: лекции, презентации.

Программу разработал профессор Факультета глобальных процессов, доктор культурологии В.И.Бажуков.