Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего сбразования
«Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых» (ВлГУ)

«УТВЕРЖДАЮ»
Проректор
по учебно-методической работе
_____ А.А. Панфилов
«25» февраля 2016 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки – 44.03.05 Педагогическое образование

Профили подготовки – «География. Безопасность жизнедеятельности»

Уровень высшего образования бакалавриат

Форма обучения очная

Семестр	Трудоем-кость зач. ед,час.	Лек-ций, час.	Практич. занятий, час.	Лаборат. работ, час.	СРС, час.	Форма промежуточного контроля (экз./зачет)
X	3, 108	14	0	28	66	зачет
Итого	3,108	14	0	28	66	зачет

Владимир, 2016

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью курса является ознакомление студентов с проблемами информационной безопасности, приобретшими в последнее время особую остроту и имеющими чрезвычайную актуальность. «Информационная безопасность – это состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств» (Закон РФ «Об участии в международном информационном обмене»). Информационная безопасность общества в целом и личности в частности характеризуется степенью защищенности и, следовательно, устойчивостью основных сфер жизнедеятельности (экономики, науки, техники, сферы управления, военного дела, общественного сознания и т.д.) по отношению к опасным, дестабилизирующим, деструктированным, ущемляющим интересы общества и личности информационным воздействиям на уровне, как внедрения, так и получения информации. Информационная безопасность определяется способностью нейтрализовать либо ликвидировать такие последствия.

В задачи курса входит:

- получение студентами знаний об основных составляющих обеспечения информационной безопасности Российской Федерации в условиях современных международных отношений;
- изучение нормативной базы;
- знакомство с формами и методами создания информационной безопасности на международном уровне, в зарубежных странах, в Российской Федерации;
- определить и понять специфику ИБ в России, представлять роль школы, учительства и педвузов в обеспечении грамотности в ИБ;
- представлять ИБ, как научную основу обеспечения национальной безопасности;
- представлять информационное нормирование как теоретические основы обеспечения здоровья человека и безопасности технологий и страны в целом.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Учебная программа по курсу «Информационная безопасность» разработана в соответствии с требованиями ФГОС ВО. Содержание программы позволяет студентам педагогических вузов получить необходимый объем знаний, навыков и умений в области информационная безопасности.

Актуальность изучения проблематики курса обусловлена возрастанием влияния информации на политические, экономические, военные, культурные процессы развития общества, а также ее недостаточной защищенностью как на внешнеполитической арене, так и внутри Российской Федерации. Мировое сообщество признало международную информационную безопасность глобальной проблемой, необходимым условием безопасного существования человеческого сообщества в послеядерный век.

Под информационной безопасностью Российской Федерации понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» (Доктрина информационной безопасности Российской Федерации).

Информационная безопасность (ИБ) - учебный предмет, основанный на знаниях полученных студентами по всем предыдущим изученным курсам, касающихся безопасности жизнедеятельности. Программа рассчитана для повышения культуры безопасности работы с информацией, особенно в сфере информационных технологий, а также направлена на организацию внешкольной работы в сфере информационной безопасности.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

Выпускник должен обладать следующими общекультурными компетенциями (ОК):

- владением культурой мышления, способностью к обобщению, анализу, восприятию информации, постановке цели и выбору путей ее достижения (ОК-1);
- способностью использовать знания о современной естественнонаучной картине мира в образовательной и профессиональной деятельности, применять методы математической обработки информации, теоретического и экспериментального исследования (ОК-4);
- способностью логически верно выстраивать устную и письменную речь (ОК-6);
- осознанием социальной значимости своей будущей профессии, обладанием мотивацией к осуществлению профессиональной деятельности (ОПК-1);
- владением основами речевой профессиональной культуры (ОПК-3);
- способностью к подготовке и редактированию текстов профессионального и социально значимого содержания (ОПК-5);
- готовностью применять современные методики и технологии, методы диагностирования достижений обучающихся для обеспечения качества учебно-воспитательного процесса (ПК-3);
- способностью осуществлять педагогическое сопровождение процессов социализации и профессионального самоопределения обучающихся, подготовки их к сознательному выбору профессии (ПК-4).

Студент, изучивший дисциплину, должен

знать:

- опасности и угрозы в сфере информационных процессов и систем;
- основы государственной политики обеспечения информационной безопасности;
- методы и средства, используемые в информационных войнах;
-международные проблемы обеспечения информационной безопасности.

уметь:

- использовать методы и средства защиты обычной и электронной информации для защиты интеллектуальной собственности;
- прививать умения и навыки учащимся по защите электронной информации при работе на ПК;
- применять правовые, организационные, технические и программные средства защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость дисциплины составляет 3 зачетных единицы, 108 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)								Объем учебной работы с применением интерактивных методов (в часах / %)	Формы текущего контроля успеваемости *(по неделям семестра)* , форма промежуточной аттестации *(по семестрам)*
				Лекции	Консультации	Семинары	Практические занятия	Лабораторные работы	Контрольные работы, коллоквиумы	СРС	КП / КР		
1	Раздел 1. Понятие информационной безопасности. Её место в системе национальной безопасности РФ.			4				8		17		3;25%	
2	Раздел 2. Опасности и угрозы в сфере информационных процессов и систем. Информационные войны, используемые методы и средства.			4				8		17		3; 25%	Рейтинг-контроль
3	Раздел 3. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну.			2				4		15		1,5; 25%	Рейтинг-контроль
4	Раздел 4. Информационные технологии и здоровье. Негативные последствия глобальной информатизации общества.			4				8		17		3; 25%	Рейтинг-контроль
Всего				14				28		66		10,5;25%	3 рейтинга

СОДЕРЖАНИЕ РАЗДЕЛОВ ДИСЦИПЛИНЫ

Раздел 1. Понятие информационной безопасности. Её место в системе национальной безопасности РФ.

Укрепление информационной безопасности как одна из важнейших долгосрочных задач в Концепции национальной безопасности Российской Федерации. Закон РФ «О безопасности».

Информатизация современного общества – активная разработка и внедрение во все сферы человеческой деятельности информационных технологий и средств. Информация и информационные ресурсы как один из решающих факторов развития личности, общества и государства. Широкие возможности компьютеров и информационных технологий в автоматизации процессов мониторинга и управления государственными, экономическими, социальными, оборонными и другими объектами и системами, получении, накапливании, обработке и передачи информации об этих процессах практически с любой требуемой скоростью, в любом количестве.

Основные категории информационной безопасности. Концептуальные и научно-методологические основы информационной безопасности. Формирование понятийного аппарата при создании теории информационной безопасности. Базовые понятия: информационная опасность, информационная угроза и информационная безопасность.

Раздел 2. Опасности и угрозы в сфере информационных процессов и систем. Информационные войны, используемые методы и средства.

Виды опасностей и угроз в сфере информационных процессов и систем. Информационная безопасность государства как состояние защищенности национальных интересов страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз.

Информационная война как действия, предпринимаемые для достижения информационного превосходства путем нанесения ущерба информационной сфере противника и обеспечения собственной информационной безопасности. Используемые методы и средства ведения информационной войны. Государственная информационная политика в условиях угрозы информационно-психологической агрессии (войны).

Раздел 3. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну.

Понятие информационного ресурса как всей накопленной информации об окружающей нас действительности, зафиксированную на материальных носителях и в любой другой форме, обеспечивающей ее передачу во времени и пространстве между различными потребителями для решения различных задач (научных, управленческих, производственных и других). Законодательство РФ об информационных ресурсах, закон «Об информации, информационных технологиях и защите информации».

Информатизация как организационный, социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Основные принципы построения систем защиты информации: принцип системности, принцип комплексности, принцип непрерывности защиты, разумная достаточность, гибкость системы защиты, открытость алгоритмов и механизмов защиты, принцип простоты применения средств защиты.

Раздел 4. Информационные технологии и здоровье. Негативные последствия глобальной информатизации общества.

Влияние информационной среды на здоровье населения. Информационная гигиена и благополучие интеллекта. Электромагнитное поле и его влияние на здоровье человека. Влияние средств массовой информации на уровень агрессивности детей и подростков. Влияние мобильного излучения на состояние здоровья современной молодежи. Психиатрия, средства массовой информации и реклама. Информационная безопасность в духовной сфере жизни. Виртуальная реальность и ее воздействие на нравственное, духовное, эмоциональное здоровье школьников. Проблема информационной безопасности в образовательных сетях.

5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

В соответствии с требованиями ФГОС ВО по направлению подготовки бакалавра реализация компетентностного подхода предусматривает широкое применение в учебном процессе активных и интерактивных форм проведения занятий. В рамках учебного курса по дисциплине «Информационная безопасность» используются следующие образовательные технологии:

- интерактивные формы проведения занятий (компьютерные симуляции, работа с мультимедийными программами и оборудованием);
- технологии коллективного взаимообучения;
- технология проблемного обучения (решение ситуативных задач на лабораторных работах);
- интенсивная внеаудиторная работа (подготовка рефератов и презентаций);
- активные формы проведения практических занятий (работа в парах, симуляционные ролевые игры).

На проведение занятий в интерактивной форме отводится около 25% учебного времени, что соответствует норме согласно ФГОС.

6. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

ЗАДАНИЯ К РЕЙТИНГ-КОНТРОЛЮ

Рейтинг 1

1. В каких единицах измеряется риск? б) а) в стоимостном выражении б) во временном выражении
в) в процентах г) в уровнях.

2. Анализ информационных рисков предназначен для:
а) оценки существующего уровня защищенности информационной системы и формирования оптимального бюджета на информационную безопасность б) оценки технического уровня защищенности информационной системы получения стоимостной оценки вероятного финансового ущерба от реализации угроз, направленных на информационную систему компании и для оценки возможности реализации угроз в)убеждения руководства компании в необходимости вложений в систему обеспечения информационной безопасности и для инструментальной проверки защищенности информационной системы.

3. Политика информационной безопасности прежде всего необходима для: а) успешного прохождения компанией регулярного аудита по ИБ б)обеспечения реального уровня защищенности информационной системы компании в) понимания персоналом важности требований по ИБ
в) обеспечения адекватной защиты наиболее важных ресурсов компании.

4. Политика информационной безопасности в общем случае является : а)руководящим документом для администраторов безопасности и системных администраторов б) руководящим документом для ограниченного использования в) руководящим документом для руководства компании, менеджеров, администраторов безопасности и системных администраторов г)руководящим документом для всех сотрудников компании.

5. Предположим, информационная система компании надежно защищена комплексом средств информационной защиты (межсетевые экраны, антивирусы, системы защиты от НСД, системы обнаружения атак и т.д.). Выберите, как на существующий уровень рисков влияет реализация требований политики безопасности:
а) информационная система сама по себе надежно защищена комплексом средств защиты, поэтому реализация требований политики безопасности не оказывает существенного влияния на уровень рисков
б) политика безопасности, как документ для непосредственного использования, отсутствует, что не оказывает существенного влияния на уровень рисков из-за высокого (технологического) уровня защищенности информационной системы
в) политика безопасности является формальным, не используемым на практике документом, и это не оказывает серьезного влияния на существующий уровень рисков
г) реализация требований политики безопасности существенно влияет на уровень рисков, так как (технологический) фактор защищенности информационной системы является лишь необходимым, но не достаточным условием обеспечения безопасности.

6. Выберите, невыполнение какого из следующих требований политики безопасности, на Ваш взгляд, может наибольшим образом повысить существующие в системе информационные риски:
а) регулярное обновление антивирусных баз
б) создание и поддержание форума по информационной безопасности для всех специалистов, вовлеченных в процесс обеспечения ИБ
в) классификация ресурсов по степени важности с точки зрения ИБ
г) завершение активной сессии пользователя по окончании работы.

7. Международный стандарт управления информационной безопасностью ISO 17799 предъявляет :
а) требования, предъявляемые только для узкого круга крупнейших мировых компаний
б) базовые требования по обеспечению ИБ
в) повышенные требования по обеспечению безопасности информационной системы
г) требования, которые не соответствуют законам стран СНГ в области информационной безопасности.

Рейтинг 2

1. Одной из рекомендаций ISO 17799 является : а) четкая регламентация настроек межсетевых экранов б) применение антивирусных продуктов ведущих производителей в) проведение

анализа рисков и регулярных тестов на проникновение сторонней компанией г) необходимость прохождения руководством компании регулярных тренингов по ИБ.

2. Проведения анализа информационных рисков прежде всего необходимо: а) градация информационных рисков б) построение полной модели информационной системы с точки зрения информационной безопасности в) модель нарушителя г) вероятностные оценки угроз безопасности.

3. Основной задачей теста на проникновение, прежде всего, является : а) оценка возможности обнаружения атаки службой ИБ компании б) проверка времени реакции службы обеспечения информационной безопасности в) оценка возможности осуществления атаки из Интернет на информационную систему компании г) оценка возможных потерь при реализации атаки из Интернет.

4. Тест на проникновение позволяет (выберите наиболее полное и точное определение):
а) убедить руководство компании в реальной опасности вторжения из Интернет и обосновать необходимость инвестиций в ИБ
б) снизить вероятные риски вирусной атаки на корпоративную сеть
в) обеспечить должный уровень отношения руководства компании к проблеме обеспечения ИБ
г) убедиться в способности службы ИБ противостоять возможным атакам злоумышленников из Интернет.

5. Укажите в общем случае возможные типовые пути воздействия при получении удаленного доступа пользователя к информации на сервере а) атака на канал передачи, атака на сервер, атака на пользовательскую группу б) вирусная атака на корпоративную сеть в) атака на станцию пользователя, атака на канал передачи, атака на сервер г) проникновение злоумышленника в сеть компании из Интернет.

6. Какой метод обычно используется профессиональными взломщиками при информационной атаке?
а) атака на наиболее защищенную цель б) атака на промежуточную цель в) атака на наименее защищенную цель г) атака осуществляется без целенаправленного выбора цели.

7. Пользователь осуществляет удаленный доступ к информации на сервере. Пусть условный уровень защищенности информации на сервере - 24 единицы; условный уровень защищенности рабочего места пользователя - 10 единиц. Оцените условный уровень защищенности удаленного доступа пользователя к информации на сервере:
а) 24 единицы б) 34 единицы в) 17 единиц г) 10 единиц.

Рейтинг 3

1. Выберите наиболее оптимальную стратегию управления рисками в следующем случае: Веб-сервер компании находится внутри корпоративной сети и его программное обеспечение, возможно, содержит уязвимости а) уменьшение риска и уклонение от риска б) принятие риска в) изменение характера риска и уклонение от риска г) изменение характера риска и уменьшение риска.

2. Для оценки ущерба по угрозе (целостность) необходимо : а)оценить полную стоимость информации б) оценить какой ущерб понесет компания в случае изменения информации в) оценить какой ущерб понесет компания в случае осуществления несанкционированного доступа к информации

г) оценить возможность осуществления атаки на ресурс, на котором хранится информация .

3. Выберите наиболее полное описание методов, которые применяются при оценке ущерба в случае нарушения конфиденциальности информации а) оценка стоимости затрат на реабилитацию подмоченной репутации, престижа, имени компании б) стоимость упущенной выгоды (потерянный контракт) в) стоимость затрат на поиск новых клиентов, взамен более не доверяющих компании
г) оценка стоимости контрмер по уменьшению ущерба от нарушения конфиденциальности информации; оценка прямого ущерба от нарушения конфиденциальности информации.

4. В случае анализа рисков базового уровня необходимо : а) провести тесты на проникновение
проверить выполнение требований соответствующего стандарта, например ISO 17799
б) провести полный аудит информационной безопасности, включая тесты на проникновение
в) построить полную модель информационной системы с точки зрения информационной безопасности

5. В случае полного анализа рисков обычно на практике используется следующий подход:
а) накопление статистических данных о реально случившихся происшествиях, б) анализ и классификация их причин; в) на выходе метода г)вероятностная оценка рисков на основе статистических данных. г) анализ технологических особенностей информационных систем (например, на основе немецкого стандарта BSI) .

6. Аудит информационной безопасности, в том числе должен включать в себя (выберите наиболее полный ответ из перечисленных):
а) анализ информационных рисков для оценки вероятного ущерба и инструментальную проверку защищенности для определения возможности реализации угроз
б) оценку зависимости компании от внешних связей и тесты на проникновение
в) оценку стоимости ресурсов и информации
г) анализ и классификацию угроз безопасности согласно модели нарушителя.

ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ И ЗАДАНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

1. Опасности и угрозы в сфере информационных процессов и систем. Информационные войны, используемые методы и средства.
2. Понятие информационной безопасности. Её место в системе национальной безопасности РФ.
3. Основы государственной политики обеспечения информационной безопасности. Международные проблемы обеспечения информационной безопасности. Законодательство в области информационной безопасности.
4. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну.
5. Защита интеллектуальной собственности.
6. Методы и средства защиты обычной и электронной информации.
7. Информационные технологии и здоровье.
8. Негативные последствия глобальной информатизации общества, влияния средств массовой информации и рекламы, их дестабилизирующее воздействие на человека.
9. Способы защиты человека от негативного влияния информации.

Контроль знаний осуществляется в форме собеседования, подготовки докладов и рефератов, выполнения тестовых задвний.

ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Исторические аспекты возникновения и развития информационной безопасности.
2. Понятие информационной безопасности. Ее место в системе национальной безопасности РФ.
3. Международные проблемы обеспечения информационной безопасности. Законодательство в области информационной безопасности.
4. Угрозы информационной безопасности России (основные определения и классификации угроз).
5. Основы государственной политики обеспечения информационной безопасности.
6. Опасности и угрозы в сфере информационных процессов и систем.
7. Статистика нарушений информационной безопасности, наиболее характерные случаи.
8. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну.
9. Понятие «информационный ресурс». Классы информационных ресурсов по типам носителей информации.
10. Информационная система. Доступность, целостность, конфиденциальность информации.
11. Классификация каналов утечки информации.
12. Защита интеллектуальной собственности. Методы и средства защиты обычной и электронной информации.
13. Понятие «информационная война» и «информационный терроризм». Концепция информационной войны. Информационное оружие.
14. Информационно-психологическая война.
15. Проблемы защиты информации в Интернете.
16. Криптографические методы защиты информации.
17. Классификация компьютерных вирусов. Обоснование необходимости защиты.
18. Антивирусные программы, их использование.
19. Влияние информационной среды на здоровье населения.
20. Информационная гигиена и благополучие интеллекта.
21. Электромагнитное поле и его влияние на здоровье человека.
22. Влияние средств массовой информации на уровень агрессивности детей и подростков.
23. Влияние мобильного излучения на состояние здоровья современной молодежи.
24. Психиатрия, средства массовой информации и реклама.
25. Информационная безопасность в духовной сфере жизни.
26. Информационная безопасность в сфере обороны.
27. Защита в средах Windows.
28. Виртуальная реальность и ее воздействие на нравственное, духовное, эмоциональное здоровье школьников.
29. Проблема информационной безопасности в образовательных сетях.
30. Информационные технологии и здоровье. Негативные последствия глобальной информатизации общества, влияния средств массовой информации и рекламы, их дестабилизирующее воздействие на человека.
31. Способы защиты человека от негативного влияния информации.

ТЕМАТИКА РЕФЕРАТОВ

1.Опасности и угрозы в сфере информационных процессов и систем.
2. Информационные войны, используемые методы и средства.
3. Понятие информационной безопасности. Её место в системе национальной безопасности РФ.
4. Основы государственной политики обеспечения информационной безопасности.
5. Международные проблемы обеспечения информационной безопасности.

6. Законодательство в области информационной безопасности.
4. Основы защиты деловой информации и сведений, составляющих служебную, коммерческую, государственную тайну.
5. Защита интеллектуальной собственности.
6. Методы и средства защиты обычной и электронной информации.
7. Информационные технологии и здоровье.
8. Негативные последствия глобальной информатизации общества, влияния средств массовой информации и рекламы, их дестабилизирующее воздействие на человека.
9. Способы защиты человека от негативного влияния информации.

Требования и методические рекомендации по написанию рефератов

Объем реферата в пределах 0,5-0,8 печатного листа (10-16 страниц машинописного через 2 интервала текста), возможны компьютерный или рукописный варианты. В реферате, наряду с изложением сведений и материалов, содержащихся в использованных литературных источниках, желательно отразить позицию автора реферата (согласие или несогласие с позициями авторов опубликованных материалов, свое видение вопроса, концепции, предложения, модели его решения).

В конце реферата должен быть приведен список использованных автором источников.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

ЛИТЕРАТУРА

ОСНОВНАЯ:

1.Мельников В.П. Информационная безопасность и защита информации : учебное пособие для вузов по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова .— 2-е изд., стер. — Москва : Академия, 2007,2008,2009.— 331 с. — (Высшее профессиональное образование, Информатика и вычислительная техника) .— Библиогр.: с. 327-328 .— ISBN 978-5-7695-4148-3. (Библ. ВлГУ).
2. Расторгуев С.П. Основы информационной безопасности : учебное пособие для вузов по специальностям "Компьютерная безопасность", "Комплексное обеспечение информационной безопасности автоматизированных систем" и "Информационная безопасность телекоммуникационных систем" / С. П. Расторгуев .— Москва : Академия, 2007,2009.— 187 с. : ил. — (Высшее профессиональное образование, Информационная безопасность) .— Библиогр.: с. 180-181 .— ISBN 978-5-7695-3098-2. (Библ. ВлГУ).
3. Ярочкин В.И. Информационная безопасность : учебник для вузов по гуманитарным и социально-экономическим специальностям / В. И. Ярочкин .— 5-е изд. — Москва : Академический проект, 2008 .— 543 с. : ил., табл. — (Gaudeamus) .— Библиогр.: с. 534-539 .— ISBN 978-5-8291-0987-5.(Библ. ВлГУ).

ДОПОЛНИТЕЛЬНАЯ:

1. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты : учебное пособие для вузов по специальности 090102 "Компьютерная безопасность", 090105 "Комплексное обеспечение информационной безопасности автоматизированных систем" / Ю. А.

Родичев .— Санкт-Петербург : Питер, 2008 .— 272 с. — (Учебное пособие) .— Библиогр.: с. 269-272 .— ISBN 978-5-388-00069-9. (Библ. ВлГУ).
2. Панарин И.Н. Информационная война и мир : [информационное противоборство в современном мире] / Игорь Панарин, Любовь Панарина .— Москва : Олма-Пресс, 2003 .— 383 с. — Библиогр.: с. 377-381 .— ISBN 5-224-04397-2. (Библ. ВлГУ).
3. Расторгуев С.П. Философия информационной войны / С. П. Расторгуев ; Российская академия образования (РАО) ; Московский психолого-социальный институт (МПСИ) .— Москва : Московский психолого-социальный институт (МПСИ) : Прайм, 2003 .— 495 с. : ил., табл. — Библиогр.: с. 481-489 .— ISBN 5-89502-346-0 (МПСИ) .— ISBN 5-902188-07-5 (Прайм) . (Библ. ВлГУ).

ИНТЕРНЕТ-РЕСУРСЫ

1. http://www.bezopasnost.edu66.ru/ Информационный портал ОБЖ и БЖД: всё о безопасности жизнедеятельности
2. Encyclopedia of Law and Economics – http://allserv.rug.ac.be/~gdegeest
3. Международная организация по новой институциональной экономике ISNIE http://www.isnie.org/
4. Библиотечка Либертариума - http://www.libertarium.ru/library
5. Электронный учебный курс: http://econline.edu.ru

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Мультимедийное оборудование, кинофильмы, слайды.

Рабочая программа дисциплины составлена в соответствии с требованиями ФГОС ВО по направлению 44.03.05 Педагогическое образование.
Профиль/программа подготовки «География. Безопасность жизнедеятельности».
Форма обучения очная.

Рабочую программу составил доцент кафедры биологического и географического образования Морев С.Ю._____

Рецензент: заместитель директора по учебно-воспитательной работе МАОУ г.Владимира «Гимназия №35» Плышевская Е.К._____

Программа рассмотрена и одобрена на заседании кафедры биологического и географического образования.
Протокол № 5 от 26.01 2016 года

Заведующий кафедрой: _____ доцент Грачева Е.П.

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 44.03.05 Педагогическое образование.
Протокол № 3 от 29.01 2016 года

Председатель комиссии:_____ директор ПИ ВлГУ Артамонова М.В.

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ (МОДУЛЯ)

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой____

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой____

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой____

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой____

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой____

Рабочая программа одобрена на ___________ учебный год

Протокол заседания кафедры № ______ от _________ года

Заведующий кафедрой____