МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

Институт информационных наук и технологий безопасности
Факультет информационных систем и безопасности
Кафедра информационной безопасности

УТВЕРЖДАЮ
Первый проректор-
проректор по научной работе
_____ О.В. Павленко
«___» _____2019 г.

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Рабочая программа дисциплины для подготовки аспирантов

Направление подготовки 10.06.01 «Информационная безопасность»
Направленность программы подготовки научно-педагогических кадров в аспирантуре
«Методы и системы защиты информации, информационная безопасность»

Москва 2019

Основы информационной безопасности и методология защиты информации
Рабочая программа дисциплины для подготовки аспирантов
Направление подготовки 10.06.01 «Информационная безопасность»
Направленность программы подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность»

Составитель: И.А. Русецкая, к.и.н., доцент

Программа утверждена
на заседании кафедры информационной безопасности
28 августа 2019 г., протокол № 1

Программа утверждена
на заседании Совета института
30 августа 2019 г., протокол № 1

Программа утверждена
на заседании Научно-методического совета
по аспирантуре и докторантуре
28 ноября 2019 г., протокол № 1

АННОТАЦИЯ

Дисциплина «Основы информационной безопасности и методология защиты информации» является дисциплиной по выбору аспиранта вариативной части направленности программы подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность» Рабочая программа дисциплины разработана кафедрой информационной безопасности факультета информационных систем и безопасности ИИНТБ РГГУ.

Содержание дисциплины включает сферы науки, техники и технологии, охватывающие совокупность проблем, связанных с информатизацией общества, а также с исследованием, разработкой, совершенствованием и применением моделей, методов, технологий, средств и систем защиты информации, а также обеспечением информационной безопасности объектов и процессов обработки, передачи информации во всех сферах деятельности от внешних и внутренних угроз.

Дисциплина направлена на формирование следующих компетенций:

универсальные (УК):

способностью проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки (УК-2);

готовностью участвовать в работе российских и международных исследовательских коллективов по решению научных и научно образовательных задач (УК-3);

способностью планировать и решать задачи собственного профессионального и личностного развития (УК-6).

общепрофессиональные (ОПК):

способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1).

профессиональные (ПК):

способность самостоятельно осуществлять научно-исследовательскую деятельность в сфере защиты информации, используя современные научный инструментарий и информационно-коммуникативные практики, принимая во внимание специфику объектов обеспечения информационной безопасности во всех сферах деятельности (ПК-1).

Общая трудоемкость освоения дисциплины по направленности программы подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность» составляет 2 зачетные единицы. Программой предусмотрены лекционные занятия (10 часов) и самостоятельная работа аспирантов (44 часа).

Программой дисциплины предусмотрены следующие виды контроля освоения: текущий контроль в форме реферата, промежуточный контроль в виде зачета с оценкой.

1. Пояснительная записка

Цель дисциплины: сформировать у аспирантов представление об информационной безопасности и методологии защиты информации

Основы информационной безопасности и методология защиты информации - это дисциплина, занимающаяся вопросами сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов. Значение решения научных и технических проблем в данной специальности состоит в разработке новых и совершенствования имеющихся подходов и методов, лежащих в основе информационной безопасности и методологии защиты информации. Курс дает возможность ознакомиться аспирантам по направленности 10.06.01 с областями и результатами исследований по этой дисциплине.

Задачи дисциплины: раскрытие сущности и значения защиты информации, информационной безопасности в системе национальной безопасности, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов.

Место дисциплины в структуре образовательной программы высшего образования – программы подготовки научно-педагогических кадров в аспирантуре:

Дисциплина «Основы информационной безопасности и методология защиты информации» является дисциплиной по выбору аспиранта вариативной части направленности программы подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность».

Данная дисциплина призвана, прежде всего, помочь аспиранту в его научной деятельности. Данный курс естественным образом связан с курсами «Методы и системы защиты информации, информационная безопасность» «Информатизация общества и информационная безопасность», «Методы и системы инженерно-технической защиты информации», «Защита информации от несанкционированного воздействия. Современные проблемы информационно-измерительного обеспечения».

Требования к результатам освоения дисциплины:

универсальные (УК):

способностью проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки (УК-2);

готовностью участвовать в работе российских и международных исследовательских коллективов по решению научных и научно -образовательных задач (УК-3);

способностью планировать и решать задачи собственногопрофессионального и личностного развития (УК-6).

общепрофессиональные (ОПК):

способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1).

профессиональные (ПК):

способность самостоятельно осуществлять научно-исследовательскую деятельность в сфере защиты информации, используя современные научный инструментарий и

информационно-коммуникативные практики, принимая во внимание специфику объектов обеспечения информационной безопасности во всех сферах деятельности (ПК-1).

В результате изучения дисциплины аспирант должен:

Знать: основы информационной безопасности, факторы, определяющие ее развитие. Механизмы влияния на нее со стороны государства, методологию защиты информации, включая существующие концепции информационной безопасности и защиты информации

Базовый понятийный аппарат в области информационной безопасности и защиты информации

Виды и состав угроз информационной безопасности

Принципы и общие методы обеспечения информационной безопасности

Основные положения государственной политики обеспечения информационной безопасности

Критерии, условия и принципы отнесения информации к защищаемой

Современные подходы к классификации информации ограниченного доступа по видам тайны

Виды и типы носителей защищаемой информации

Виды уязвимости защищаемой информации и формы ее проявления

Источники, виды и способы дестабилизирующего воздействия на информацию

Каналы и методы несанкционированного доступа к информации ограниченного доступа

Организационные основы и методологические принципы защиты информации

Состав объектов защиты информации

Классификацию видов методов и средств защиты информации

Состав кадрового, ресурсного и технологического обеспечения защиты информации (ОПК-1, ПК-1).

Уметь: анализировать источники и литературу в области информационной безопасности, соотносить этот анализ с национальной безопасностью России

Использовать методологию защиты информации для любого вида организационных и информационных систем,

Выявлять угрозы информационной безопасности применительно к объектам защиты

Определять состав защищаемой информации применительно к видам тайны

Выявлять причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию со стороны различных источников воздействия

Выявлять применительно к объекту защиты каналы и методы несанкционированного доступа к информации

Определять направления и виды защиты информации с учетом характера информации и задач по ее защите;

Организовывать системное обеспечение защиты информации (УК-2, УК-3, ОПК-1, ПК-1).

Владеть: навыками применения полученных знаний в научно- исследовательской работе и научно-педагогической работе (УК-6, ПК-1).

2. Структура дисциплины (тематический план)

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа

№	Раздел дисциплины	Полу-годие обучения	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма итогового контроля
			Лек-ции	Практические занятая	Самостоятельная работа	
	Введение	3	1			
1	Основы информационной безопасности и защиты информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
2	Сущность и базовые положения защиты информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
3	Состав и классификация защищаемой информации	3			Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
4	Угрозы информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	Реферат Собеседование
5	Компоненты и организация защиты информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата
6	Подготовка к зачету с оценкой	3			18	
	Итого	3	10		62	Зачет с оценкой

Структура дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

№	Раздел дисциплины	Полу-годие обучения	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма итогового контроля
			Лек-ции	Практические занятая	Самостоятельная работа	
	Введение	3	1			
1	Основы информационной безопасности и защиты информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
2	Сущность и базовые положения защиты информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
3	Состав и классификация защищаемой информации	3			Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
4	Угрозы информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	Реферат Собеседование
5	Компоненты и организация защиты информации	3	2		Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата
6	Подготовка к зачету с оценкой	3			18	
	Итого	3	12		60	Зачет с оценкой

3. Содержание дисциплины

Введение

Предмет и задачи курса. Научная и учебная взаимосвязь курса с другими дисциплинами.

Структура курса. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения семинарских занятий. Состав и методика самостоятельной работы слушателей по изучению дисциплины. Формы проверки знаний.

Анализ нормативных источников, научной и учебной литературы.

Знания и умения слушателей, которые должны быть получены в результате изучения курса.

1. Основы информационной безопасности

1.1 Сущность и понятие информационной безопасности. Становление и развитие понятия «информационная безопасность». Современные подходы к определению понятия.

Сущность информационной безопасности. Объекты информационной безопасности. Связь информационной безопасности с информатизацией общества и безопасностью информации. Структура информационной безопасности. Определение понятия “информационная безопасность”.

1.2 Значение информационной безопасности и ее место в системе национальной безопасности.

Значение информационной безопасности для обеспечения прав граждан, удовлетворения информационных потребностей субъектов информационных отношений, предотвращения негативного информационного воздействия, обеспечения безопасности различных сфер деятельности.

Понятие и современная концепция национальной безопасности. Место информационной безопасности в системе национальной безопасности.

1.3 Современная Доктрина информационной безопасности Российской Федерации

Понятие и назначение Доктрины информационной безопасности.

Интересы личности, общества и государства в информационной сфере. Составляющие национальных интересов в информационной сфере, пути их достижения.

Виды и состав угроз информационной безопасности.

Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.

Принципы обеспечения информационной безопасности.

Общие методы обеспечения информационной безопасности. Особенности обеспечения информационной безопасности в различных сферах общественной жизни.

Основные положения государственной политики обеспечения информационной безопасности, мероприятия по их реализации.

Организационная основа системы обеспечения информационной безопасности.

2. Сущность и базовые положения защиты информации

2.1 Сущность и понятие защиты информации

Значение раскрытия сущности и определения понятия защиты информации.

Существующие подходы к содержательной части понятия “защита информации” и способам реализации содержательной части.

Методологическая основа для раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации. Обусловленность статуса информации ее уязвимостью.

Понятие уязвимости информации. Формы проявления уязвимости информации. Виды уязвимости информации. Понятие “утечка информации”.

Соотношение форм и видов уязвимости информации. Содержательная часть понятия “защита информации”.

Способ реализации содержательной части защиты информации. Определение понятия “защита информации”.

2.2 Цели и значение защиты информации

Существующие подходы к определению целей защиты информации.

Понятие целей защиты информации, их отличие от задач защиты информации. Увязка целей защиты информации с защищаемой информацией и субъектами информационных отношений.

Непосредственная цель защиты информации. Опосредованные (конечные) цели защиты информации.

Место защиты информации в системе национальной и информационной безопасности. Значение защиты информации для субъектов информационных отношений: государства, общества, личности. Значение защиты информации в политической, военной, экономической и других областях деятельности. Социальные последствия защиты информации.

2.3 Теоретические и концептуальные основы защиты информации. Понятие и назначение теории защиты информации.

Основные положения теории защиты информации: объективная необходимость и общественная потребность в защите информации, включенность ее в систему общественных отношений; зависимость защиты информации от политико-правовых, социально-экономических, военно-политических реальностей; увязка защиты информации с проблемами информатизации общества, обеспечения баланса интересов личности, общества и государства, правовое регулирование и взаимный контроль субъектов информационных отношений в сфере защиты информации, содействие повышению эффективности соответствующей области деятельности.

Теоретические основы национальной политики в сфере защиты информации.

Понятие и назначение концепции защиты информации. Теория защиты информации как основа концепции защиты информации.

Современные концептуальные походы к защите информации.

Содержание концепции защиты информации, ее значение для разработки стратегии, формирования целевых программ и практических мероприятий по защите информации.

Уровни и виды концепции защиты информации.

Становление и развитие государственной концепции защиты информации. Современная стратегия защиты информации.

3. Состав и классификация защищаемой информации

Критерии, условия и принципы отнесения информации к защищаемой.

Современные подходы к составу защищаемой информации. Основа для отнесения информации к защищаемой, категории информации, подпадающие под эту основу

Критерии отнесения открытой информации к защищаемой, их обусловленность необходимостью защиты информации от утраты. Критерии отнесения информации к информации с ограниченным доступом, их обусловленность необходимостью защиты информации от утраты и утечки.

Условия, необходимые для отнесения информации к защищаемой.

Правовые и организационные принципы отнесения информации к защищаемой.

3.2 Классификация информации ограниченного доступа по видам тайны

Показатели разделения информации ограниченного доступа на виды тайны.

Становление и современное определение понятия «государственная тайна». Основания и организационно-правовые формы отнесения информации к государственной тайне. Перечни сведений, являющихся государственной тайной, их назначение и структура.

Степени секретности сведений, отнесенных к государственной тайне. Критерии отнесения сведений к различным степеням секретности. Грифы секретности носителей информации. Основания для рассекречивания информации.

Становление и современное определение коммерческой тайны. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Функции государства в сфере защиты коммерческой тайны. Тенденции, определяющие факторы развития коммерческой тайны.

Современные подходы к сущности служебной тайны. Понятие служебной тайны, границы и области ее действия.

Понятия «личная тайна». Функции государства и граждан в сфере защиты личной тайны.

Современные подходы к определению сущности профессиональной тайны. Понятие и особенности профессиональной тайны. Сфера действия профессиональной тайны. Соотношение между профессиональной и другими видами тайны. Разновидности профессиональной тайны.

3.3 Классификация носителей защищаемой информации

Понятие «носитель защищаемой информации». Соотношение между носителем и источником информации.

Виды и типы носителей защищаемой информации. Способы фиксирования информации в носителях. Виды отображения информации в носителях. Методы воспроизведения отображенной информации в носителях информации.

Опосредованные носители защищаемой информации.

Свойства различных типов носителей защищаемой информации.

4. Угрозы информации

4.1 Понятие и структура угроз информации

Современные подходы к понятию угрозы информации. Связь угрозы информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы информации.

Структура явлений как сущностных проявлений угрозы информации. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.

4.2 Источники, виды и способы дестабилизирующего воздействия на информацию

Источники дестабилизирующего воздействия на информацию как определяющая структурная часть угрозы. Состав и характеристика источников дестабилизирующего воздействия на информацию.

Виды и способы дестабилизирующего воздействия на информацию со стороны различных источников. Соотношение видов дестабилизирующего воздействия на информацию с формами проявления уязвимости информации.

4.3 Причины, обстоятельства и условия дестабилизирующего воздействия на информацию

Соотношение между причинами, обстоятельствами и условиями дестабилизирующего воздействия на информацию, их обусловленность источниками и видами воздействия.

Причины, вызывающие преднамеренное и непреднамеренное дестабилизирующее воздействие на информацию со стороны людей. Обстоятельства (предпосылки), способствующие появлению этих причин. Условия, создающие возможность для дестабилизирующего воздействия на информацию.

Причины, обстоятельства и условия дестабилизирующего воздействия на информацию со стороны других источников воздействия.

4.4 Каналы и методы несанкционированного доступа к информации. Канал несанкционированного доступа к информации как составная часть угрозы информации.

Современные подходы к понятию канала несанкционированного доступа к информации. Соотношение между каналами несанкционированного доступа и каналами утечки информации, их сущность и понятия.

Состав и характеристика каналов несанкционированного доступа к информации. Специально создаваемые и потенциально существующие каналы.

Методы несанкционированного доступа к информации, применяемые при использовании каждого канала. Зависимость методов и форм их использования от целей и возможностей соперника.

Существующая классификация каналов, ее недостатки.

Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к информации

5. Компоненты и организация защиты информации

5.1 Организационные основы и методологические принципы защиты информации

Организационные основы как необходимые условия для осуществления защиты информации. Основы, обеспечивающие технологию защиты информации. Основы, необходимые для обеспечения сохранности и конфиденциальности информации.

Значение методологических принципов защиты информации. Принципы, обусловленные принадлежностью, ценностью, конфиденциальностью информации, технологией ее защиты.

5.2 Объекты защиты информации

Понятие объекта защиты. Соотношение объекта с рубежом защиты информации.

Носители информации как конечные объекты защиты. Особенности отдельных видов носителей как объектов защиты.

Состав объектов хранения носителей информации, подлежащих защите.

Состав подлежащих защите технических средств отображения, обработки, хранения, воспроизведения и передачи информации.

Другие объекты защиты информации.

Виды и способы дестабилизирующего воздействия на объекты защиты.

5.3 Классификация видов, методов и средств защиты информации. Виды защиты информации, сферы их действия.

Классификация методов защиты информации. Универсальные методы защиты информации, область их применения. Области применения организационных, криптографических и инженерно-технических методов защиты информации.

Понятие и классификация средств защиты информации. Назначение программных, криптографических и технических средств защиты.

5.4 Кадровое, ресурсное и технологическое обеспечение защиты информации

Значение и состав кадрового обеспечения защиты информации.

Полномочия руководства предприятия в области защиты информации.

Полномочия подразделений по защите информации.

Полномочия пользователей защищаемой информации.

Состав и назначение ресурсного обеспечения защиты информации. Значение ресурсного обеспечения для организации и эффективности защиты информации.

Понятие и назначение технологического обеспечения защиты информации.

Классификация организационно-технологических документов по защите информации. Классификация мероприятий по защите информации. Сферы применения организационно-технологических документов и мероприятий.

5.5 Назначение и структура систем защиты информации. Понятие «система защиты информации». Назначение систем.

Классификация систем защиты информации, сферы их действия.

Сущность и значение комплексной системы защиты информации как формы

организации деятельности по защите информации.

Структура системы защиты информации, назначение составных частей системы. Требования к системам защиты информации.

4. Информационные и образовательные технологии

В учебном процессе широко используются активные и интерактивные формы проведения занятий:

традиционные формы подачи лекционного материала;

лекции с использованием мультимедийной техники;

использование локальной сети компьютерного класса с выходом в интернет;

методы сетевого взаимодействия и контроля;

самостоятельная работа аспирантов в виде аннотирования и реферирования научной литературы, статей отечественных и зарубежных авторов, работа в интернет и использованием компьютеров (библиотека РГГУ), личных компьютеров, мобильных устройств.

5. Система текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Система текущего и промежуточного контроля знаний аспирантов по дисциплине включает реферат и зачет с оценкой. Оценочные средства включают тематику рефератов, вопросы для проведения зачета.

Объем реферата по дисциплине - 15-25 страниц печатного текста. При защите реферата аспирант кратко излагает концепцию реферата и основные выводы, отвечает на поставленные вопросы.

Оценка	Содержание
Отлично	Реферат написан четко и грамотно. Тема реферата хорошо раскрыта. Приведена качественно подобранная российская и зарубежная литература. Ответы на дополнительные вопросы по реферату правильные.
Хорошо	Реферат написан четко и грамотно. Тема реферата раскрыта не полностью. Приведена российская и зарубежная литература. Ответы на дополнительные вопросы по реферату правильные.
Удовлетворительно	Тема реферата раскрыта не полностью. Ответы на дополнительные вопросы по реферату правильные, но неполные.
Неудовлетворительно	Тема реферата не раскрыта. Ответы на дополнительные вопросы по реферату неправильные.

Критерии оценки по итогам промежуточной аттестации

Оценка	Содержание
Отлично	Аспирант способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры.
Хорошо	Ответ аспиранта правильный, но неполный. Не приведены иллюстрирующие примеры, обобщающее мнение аспиранта недостаточно четко выражено.
Удовлетворительно	Ответ правильный в основных моментах, нет иллюстрирующих примеров, отсутствует собственное мнение аспиранта, есть ошибки в деталях.
Неудовлетворительно	В ответе аспиранта существенные ошибки в основных аспектах темы.

6. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Примерная тематика рефератов

№ пп	Примерная тематика рефератов	Формируемые компетенции
1.	Модели противодействия угрозам нарушения информационной безопасности.	УК-2, УК-6, ОПК-1, ПК-1
2.	Механизмы формирования политики обеспечения информационной безопасности.	УК-6, ОПК-1, ПК-1
3.	Новые принципы и технические решения по созданию и совершенствованию существующих средств защиты	УК-2, УК-3, УК-6,
4.	Модели и методы управления информационной безопасностью	УК-2, УК-3, ПК-1
5.	Виды и характеристика носителей защищаемой информации.	УК-2, УК-3, УК-6, ОПК-1, ПК-1
6.	Структура и характеристика угроз защищаемой информации.	УК-2, УК-3, УК-6, ПК-1
7.	Соотношение угроз защищаемой информации с видами носителей и формами проявления уязвимости информации.	УК-2, УК-3, ОПК-1, ПК-1
8.	Соотношение видов разведывательной деятельности с каналами и методами несанкционированного доступа к конфиденциальной информации.	УК-3, УК-6, ОПК-1, ПК-1

9.	Классификация и характеристика объектов защиты информации.	УК-2, УК-3, УК-6, ОПК-1
10.	Классификация и характеристика видов, методов и средств защиты информации и их соотношение с объектами защиты.	УК-2, УК-6, ОПК-1, ПК-1
11.	Сущность, назначение и структура систем защиты информации.	УК-2, УК-3, УК-6, ОПК-1, ПК-1

Перечень вопросов к зачету

№ пп	Перечень вопросов для зачета с оценкой	Формируемые компетенции
1.	Сущность и понятие информационной безопасности.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
2.	Значение информационной безопасности и ее место в системе национальной безопасности.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
3.	Современная доктрина информационной безопасности Российской Федерации.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
4.	Сущность и понятие защиты информации	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
5.	Цели и значение защиты информации.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
6.	Теоретические и концептуальные основы защиты информации.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
7.	Критерии, условия и принципы отнесения информации к защищаемой	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
8.	Классификация информации ограниченного доступа по видам тайны.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
9.	Классификация носителей защищаемой информации.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
10.	Понятие и структура угроз информации.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
11.	Источники, виды и способы дестабилизирующего воздействия на информацию.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2
12.	Причины, обстоятельства и условия дестабилизирующего воздействия на информацию.	УК-1, УК-2, УК-3, ОПК-1, ПК-1, ПК-2

7. Учебно-методическое и информационное обеспечение дисциплины

Список источников и литературы

Основные источники

1. Федеральный закон «О безопасности» от 28.12.2010 №390-ФЗ http://www.consultant.ru/document/cons_doc_LAW_108546/

2. Федеральный закон «О государственной тайне» от 21.07.1993 N 5485-1 (ред. от 08.11.2011) http://www.consultant.ru/document/cons_doc_LAW_2481

3. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ http://www.consultant.ru/document/cons_doc_LAW_61798

4. Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ http://www.consultant.ru/document/cons_doc_LAW_48699

5. Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ (ред. от 25.07.2011) http://www.consultant.ru/document/cons_doc_LAW_61801/

6. ГОСТ 50922-2006. Защита информации. Основные термины и определения. http://docs.cntd.ru/document/1200058320

7. Доктрина информационной безопасности Российской Федерации (утв. Президентом Рос. Федерации 05.12.2016 № Пр-646) http://ivo.garant.ru/#/document/71556224/paragraph/1:1

Основная литература

8. Галатенко В. А. Основы информационной безопасности : учеб. пособие : для студентов вузов, обучающихся по специальности 351400 "Прикладная информатика" / В. А. Галатенко; [под ред. В. Б. Бетелина]. - 4-е изд. - М. : Интернет-Ун-т информ. технологий : БИНОМ, Лаб. знаний, 2008. - 205 с. : рис., табл. - (Серия "Основы информационных технологий"). - Библиогр.: с. 200-205. - ISBN 978-5-94774-821-5

9. Гришина Н. В. Информационная безопасность предприятия: Учебное пособие. - 2 ; доп. - Москва ; Москва : Издательство "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2017. - 239 с. - ISBN 978-5-00091-007-8. -Режим доступа: http://new.znanium.com/go.php?id=612572.

10. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации : учеб. пособие для студентов вузов, обучающихся по специальности 075400 - "Комплексная защита объектов информ." / А. А. Малюк. - М. : Горячая линия-Телеком, 2004. - 280 с. : рис.,табл. - Библиогр.: с.276-278 (51 назв.). - ISBN 5-935171-97.

Дополнительная литература

11. Информационная безопасность и защита информации [Электронный ресурс] : учебное пособие / Е. К. Баранова, А. В. Бабаш. - 4-е изд., перераб. и доп. - Москва: РИОР : Инфра-М, 2019. - 336 с. - ВО - Бакалавриат. - ISBN 978-5-369-01761-6. -Режим доступа: http://new.znanium.com/go.php?id=1009606.

12. Словарь терминов и определений по информационной безопасности и защите информации [Электронный ресурс] : учебно-справочное пособие : для бакалавриата по направлению 090900.62 "Информационная безопасность" / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. информац. безопасности ; [сост.: Ищейнов В. Я., Мецатунян М. В.]. - Москва : РГГУ, 2014. - 117 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009502. - ISBN 978-5-7281-1836-7.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет»:
- http://www.consultant.ru/
- http://base.garant.ru/

8.Материально-техническое обеспечение дисциплины

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных занятий с необходимыми техническими средствами (компьютер, проектор, доска):

Мультимедийный компьютерный класс

Локальная сеть, 13 компьютеров, подключенных к Интернет (Процессор Atom 1,6 GHz. Оперативная память: 2Гb. Объем жесткого диска: 160Gb. Дисковод DVD, Web-камера, звуковая гарнитура), проектор.

ПО: Windows XP, MS Office 2003, Visual Studio2005, Matlab R2010a, Autodesk AutoCAD 2010, Autodesk 3DSMAX Design 2010, Adobe Photoshop CS4, Turbo Delphi 2010, Adobe Extend Script Toolkit CS4, Adobe After Effects CS4 , Adobe Dreamweaver CS4.

Проекционная аудитория

1 компьютер (Процессор: Pentium 4 3GHz. Оперативная память: 512Mb. Объем жесткого диска: 80Gb. Дисковод DVD), проектор, звуковые колонки.

ПО: Windows XP, MS Office 2003

Для инвалидов и лиц с ограниченными возможностями здоровья: обеспечивается возможность беспрепятственного доступа обучающихся инвалидов в аудитории и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, лифтов, наличие специальных кресел и других приспособлений).

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения для обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов с разными видами ограничений здоровья:

- с нарушениями зрения:
  - устройство для сканирования и чтения с камерой SARA CE;
  - дисплей Брайля PAC Mate 20;
  - принтер Брайля EmBraille ViewPlus;
- с нарушениями слуха:
  - автоматизированное рабочее место для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- с нарушениями опорно-двигательного аппарата:
  - передвижные, регулируемые эргономические парты СИ-1;
  - компьютерная техника со специальным программным обеспечением.

9.Рекомендации по организации самостоятельной работы аспирантов

Самостоятельная работа аспирантов организуется в форме аннотирования и реферирования научной литературы, статей отечественных и зарубежных авторов. По

итогам самостоятельной работы аспиранты готовят рефераты, лучшие из которых заслушиваются на научном семинаре кафедры, Гуманитарных чтениях РГГУ, профильных конференциях.

Готовя рефераты, аспиранты должны показать навыки научного поиска, используя литературу и источники, которые не нашли отражения в данной программе.

В ходе самостоятельной деятельности необходимо принимать во внимание векторы развития информатизации и глобализации общества, новые технологии и угрозы информационной безопасности личности, обществу, государству.

Организация самостоятельной работы аспирантов направлена на осуществление научно-исследовательской работы, подготовку научных статей, диссертационной работы, подготовку к преподавательской деятельности.

Основы информационной безопасности и методология защиты информации

Составитель: Доцент кафедры информационной безопасности
ИИНТБ РГГУ, к.и.н., доцент И.А. Русецкая

_____

подпись расшифровка подписи

Лист изменений
в рабочей программе дисциплины

Основы информационной безопасности и методология защиты информации
(Название дисциплины)

№ п/п	Дата внесения изменений	Дата и № протокола заседания кафедры	Содержание изменения	Подпись
1.	08.05.2020	Приказ РГГУ от 08.05.2020 г. № 01-229/осн	Зачет проводится в дистанционной форме устно в утвержденные даты и время согласно расписанию промежуточной аттестации. Перед началом зачета аспирант устанавливает с доступного ему устройства видеоконференцсвязь с преподавателем посредством ПО. До начала зачета аспирант демонстрирует через камеру преподавателю отсутствие посторонних лиц в помещении, где он находится, и посторонних предметов перед монитором (экраном) и камерой своего устройства. Преподаватель передает аспиранту в рамках конференцсвязи содержание вопросов, на которые ему необходимо ответить и дает время для подготовки ответа.	Управление аспирантурой и докторантурой

			В процессе подготовки ответа аспирант должен находиться перед камерой своего устройства так, чтобы преподаватель мог его видеть все время подготовки к ответу. В случае неполного или некорректного ответа преподаватель имеет право задавать аспиранту дополнительные вопросы в рамках материалов дисциплины. По окончании ответа преподаватель озвучивает аспиранту итоги зачета и вносит соответствующие сведения в электронную аттестационную ведомость, которую по итогам сдачи зачета передает в Управление аспирантурой и докторантурой в электронном виде. Возможны различные варианты сдачи зачета: устный, письменный или комбинированный (письменно+устно). Для визуальной и голосовой коммуникации возможно использование Zoom, Skype, WhatsApp и.т.п. Для отправки выполненных заданий в письменной форме возможно использование электронной почты,	

			WhatsApp и т.п. Всю необходимую информацию о проведении зачета каждый преподаватель должен довести до аспирантов в письменной форме по электронной почте. Информация о проведении зачета должна быть получена каждым аспирантом не позднее чем за 3 дня до зачета.	