МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»

(ФГБОУ ВО «РГГУ»)
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

УТВЕРЖДАЮ
Первый проректор-
проректор по научной работе
_____ О.В. Павленко
28.11.2019 г.

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 10.06.01 Информационная безопасность
Направленность программ подготовки научно-педагогических кадров в аспирантуре:

«Методы и системы защиты информации, информационная безопасность»

Москва 2019

Составитель: Д.А. Митюшин,
кандидат технических наук

Программа утверждена
на заседании кафедры комплексной защиты информации
30 августа 2019 г., протокол № 1

Программа утверждена
на заседании Совета ИИНТБ
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 «Методы и системы защиты информации, информационная безопасность» является обязательной дисциплиной вариативной части направленности программ подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность».

Рабочая программа дисциплины разработана на кафедре комплексной защиты информации Института информационных наук и технологий безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с рассмотрением совокупности проблем, связанных с информатизацией общества, 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 выпускника аспирантуры:

универсальные (УК):

способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1);

способность 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);

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

готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4);

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

общепрофессиональные (ОПК):

способность 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);

способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2);

способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3);

готовность к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-5).

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);

готовность к образовательной деятельности по направлению «информационная безопасность» в рамках направленности «методы и системы защиты информации, информационная безопасность», в том числе с использованием современных мультимедийных и сетевых технологий (ПК-2).

Общая трудоёмкость освоения дисциплины составляет 2 зачётные единицы, 72 часа. Программой дисциплины предусмотрены лекционные занятия (10 часов), самостоятельная работа аспиранта (26 часов).

Программой дисциплины предусмотрены следующие виды контроля освоения: текущий контроль в форме реферата, промежуточный контроль в виде кандидатского экзамена по специальной дисциплине.

1. Пояснительная записка

Цель дисциплины: сформировать у аспирантов представление о методах и системах защиты информации, информационной безопасности.

«Методы и системы защиты информации, информационная безопасность» – это дисциплина, занимающаяся вопросами защищаемых объектов информатизации, автоматизированными системы, информационно-аналитическими системами, информационно-телекоммуникационными сетями и системами и иными информационными системами, а также входящими в них техническими и программными средствами; автоматизированными системами в защищённом исполнении; методами, способами и технологиями обеспечения информационной безопасности объектов информатизации, автоматизированных, информационно-аналитических, информационно-телекоммуникационных и иных информационных систем; методами анализа и проектирования защищённых автоматизированных и информационно-аналитических систем, информационно-телекоммуникационных сетей и систем и иных информационных систем, а также входящих в них технических и программных средств; моделями, методами сбора, обработки, хранения и передачи защищаемой информации, а также методами приёма, обработки и передачи используемых сигналов; моделями, методами и системами управления информационной безопасностью; системами, комплексами и средствами противодействия техническим разведкам, методам их анализа и проектирования; методам, системам и средствам контроля и оценки защищённости информации; образовательным процессом в области информационной безопасности.

Курс даёт возможность ознакомиться аспирантам по направлению 10.06.01. с областями и результатами исследований по этой дисциплине.

Задачи дисциплины: раскрытие сущности и значения методов и систем защиты информации, информационной безопасности 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 «Методы и системы защиты информации, информационная безопасность» принадлежит к специальным дисциплинам.

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

Требования к результатам освоения дисциплины:

Дисциплина «Защита информации от несанкционированного воздействия. Современные проблемы информационно-измерительного обеспечения» направлена на формирование следующих компетенций выпускника

универсальные (УК):

способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1);

способность 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);

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

готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4);

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

общепрофессиональные (ОПК):

способность 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);

способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2);

способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3);

готовность к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-5).

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);

готовность к образовательной деятельности по направлению «информационная безопасность» в рамках направленности «методы и системы защиты информации, информационная безопасность», в том числе с использованием современных мультимедийных и сетевых технологий (ПК-2)..

В результате изучения дисциплины аспирант должен:

знать: законодательные и правовые основы защиты информации и компьютерных технологий, меры по обеспечению сохранности информации, основные задачи обеспечения безопасности информации в информационных системах; принципы построения систем защиты информации и их основы; основные направления создания защищённых информационных систем, определения и свойства математических объектов, используемых в этой области (ОПК-1, ОПК-2, ПК-1, УК-3, УК-4, УК-6).

уметь: решать задачи теоретического характера из различных разделов дисциплины, доказывать утверждения, строить примеры основных объектов и понятий. Владеть: математическим аппаратом, используемым в системах защиты информации, основными алгоритмами, классификацией способов защиты информации; методами защиты информации от несанкционированного доступа и разрушающих программных воздействий процесса хранения и обработки информации (УК-1, УК-2, ОПК-1, ОПК-2, ОПК-3, ПК-1).

владеть: навыками применения полученных знаний в научно- исследовательской работе и научно-педагогической работе (УК-2, ОПК-5, ПК-1, ПК-2).

2. Структура дисциплины (тематический план)

Общая трудоёмкость освоения дисциплины составляет 2 зачётных единицы, 72 часа.

№ п/п	Раздел дисциплины	Полугодие обучения	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
			Лекции	Практ. занятия	Самостоятельная работа	
1	Введение. Основы информационной безопасности и защиты информации	4	3		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
2	Нормативное правовое и организационное обеспечение информационной безопасности и защиты информации	4	2		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
3	Методы и средства технической защиты информации	4	1		3 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
4	Инженерно-технические методы и средства защиты информации	4	1		3 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Реферат
5	Технические средства охраны объектов информатизации	4	1		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	
6	Основы	4	1		4	собеседование

	криптографической защиты информации				Реферирование российской и зарубежной литературы и статей, работа в интернет	
7	Принятие организационно-технических решений по комплексному обеспечению информационной безопасности автоматизированных систем	4	1		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
8	Подготовка к экзамену и индивидуальной дополнительной программы для сдачи кандидатского экзамена	4			36	
	Итого:		**10**		**62**	**Кандидатский экзамен**

Структура дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

№ п/п	**Раздел дисциплины**	**Полу-годие обуче-ния**	**Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)**			**Формы текущего контроля успеваемости** **Форма промежуточной аттестации**
			Лек-ции	**Практ. занятия**	**Самостоятельная работа**	
1	Введение. Основы информационной безопасности и защиты информации	4	3		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
2	Нормативное правовое и организационное обеспечение информационной безопасности и защиты информации	4	2		4 Реферирование российской и зарубежной литературы и статей, работа в	собеседование

					интернет	
3	Методы и средства технической защиты информации	4	1		3 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
4	Инженерно-технические методы и средства защиты информации	4	1		3 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Реферат
5	Технические средства охраны объектов информатизации	4	1		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	
6	Основы криптографической защиты информации	4	2		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
7	Принятие организационно-технических решений по комплексному обеспечению информационной безопасности автоматизированных систем	4	2		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	собеседование
8	Подготовка к экзамену и индивидуальной дополнительной программы для сдачи кандидатского экзамена	4			36	
	Итого:		**12**		**60**	**Кандидатский экзамен**

3. Содержание дисциплины:

Тема 1. Введение. Основы информационной безопасности и защиты информации

Современные условия развития информационного общества и его признаки. Состояние развития информационного общества в России. Причины возникновения и актуальность проблемы обеспечения информационной безопасности. Государственная политика обеспечения информационной безопасности. Ключевые проблемы информационной безопасности государства, общества и личности и пути их решения. Понятийный аппарат в области обеспечения информационной безопасности и защиты информации. Структура информационной безопасности и связанные с ней свойства. Причины нарушения информационной безопасности. Модели нарушения информационной безопасности. Источники и виды угроз. Механизмы реализации угроз. Проблема комплексного обеспечения информационной безопасности и системный подход к её решению. Соотношение понятий информационная безопасность и защита информации.

Тема 2. Нормативное правовое и организационное обеспечение информационной безопасности и защиты информации

Правовой уровень обеспечения безопасности информационных технологий, систем и ресурсов. Роль и место нормативного регулирования при обеспечении информационной безопасности и защите информации.

Задачи нормативного регулирования отношений, возникающих на различных стадиях процесса обеспечения информационной безопасности и защиты информации. Система нормативного обеспечения информационной безопасности. Концептуальные документы федерального уровня. Законодательство Российской Федерации в области обеспечения информационной безопасности и защиты информации, а также в области интеллектуальной собственности. Законодательство о персональных данных, коммерческой и государственной тайне. Руководящие документы ФСТЭК России и применение их требований в практике защиты информации. Нормативное регулирование криптографической защиты информации. Нормативное обеспечение проектирования защищённых информационных систем. Вопросы регулирования деятельности в области обеспечения информационной безопасности организаций. Политики безопасности. Стандарты в области управления информационной безопасностью и особенности их применения. Лицензирование деятельности в области защиты информации. Мировой опыт в области обеспечения информационной безопасности и защиты информации на законодательном уровне. Современные тенденции развития системы нормативного обеспечения информационной безопасности. Организационные системы обеспечения информационной безопасности. Организация объектовых режимов безопасности.

Тема 3. Методы и средства технической защиты информации.

Основные подходы к защите данных от несанкционированного доступа. Разграничение доступа к информации. Идентификация и аутентификация субъектов и объектов компьютерных систем. Методы аутентификации. Подходы к реализации средств идентификации и аутентификации. Средства аутентификации пользователей. Модели управления доступом. Модель Белла-Лападула. Модель Take-Grant. Дискреционная политика. Ролевая политика. Мандатная политика. Политики контроля целостности. Модель Биба. Модель Кларка-Вилсона. Системная классификация средств защиты информации. Аппаратные средства защиты информации. Основные принципы функционирования аппаратных средств защиты информации. Программные средства защиты информации. Основные принципы функционирования программных средств защиты. Методы и средства обеспечения безопасности сетевых информационных

структур. Виртуальные частные сети и их применение. Межсетевое экранирование. Методы и средства обнаружения компьютерных атак.

Тема 4. Инженерно-технические методы и средства защиты информации.

Классификация демаскирующих признаков и их характеристики. Виды каналов утечки, их характеристики. Технические каналы утечки информации, классификация и характеристика. Оптические каналы утечки информации. Способы и средства противодействия наблюдению в оптическом диапазоне. Радиоэлектронные каналы утечки информации. Акустические каналы утечки информации. Материально-вещественные каналы утечки информации. Задачи и принципы инженерно-технической защиты информации. Способы и средства инженерной защиты и технической охраны объектов. Способы и средства противодействия радиолокационному наблюдению. Способы и средства информационного скрытия речевой информации от подслушивания. Энергетическое скрытие акустического сигнала. Основные методы защиты информации техническими средствами.

Тема 5. Технические средства охраны объектов информатизации

Основные параметры системы защиты информации. Классификация способов защиты. Сущность организационных и технических мер защиты. Технические средства охраны. Функциональная схема комплекса ТСО. Структурная схема комплекса охранной сигнализации. Система централизованной охраны. Основные требования к построению системы ТСО. Режим охраны. Датчики, шлейфы охранной сигнализации. Многорубежность построения системы ТСО. Категорирование объектов охраны. Порядок применения классификатора для организации охраны объекта. Модель нарушителя, как основа создания средств ТСО.

Тема 6. Основы криптографической защиты информации

Основные понятия и определения криптологии. Применение симметричных криптосистем для защиты информации в компьютерных системах. Основные режимы работы алгоритма DES. Отечественный стандарт шифрования данных, Режим простой замены. Режим гаммирования. Режим гаммирования с обратной связью. Режим выработки имитовставки. Блочные и поточные шифры. Применение асимметричных криптосистем для защиты информации в компьютерных системах. Концепция криптосистемы с открытым ключом. Однонаправленные функции, криптосистема шифрования данных RSA. Схема шифрования Эль-Гамаля. Методы идентификации и проверки подлинности пользователей компьютерных систем.

Тема 7. Принятие организационно-технических решений по комплексному обеспечению информационной безопасности автоматизированных систем

Существо проблемы комплексного обеспечения информационной безопасности. Комплексное обеспечение информационной безопасности автоматизированных систем как совокупность организационно-технических решений по их защите. Системный подход к решению проблемы. Задачи принятия организационно-технических решений по обеспечению информационной безопасности в различных условиях. Игровые методы принятия решений в условиях информационных конфликтов. Экспертные оценки в системах информационной безопасности. Система комплексного обеспечения информационной безопасности автоматизированных систем. Рубежи защиты автоматизированных систем и связанные с ними задачи. Этапы обеспечения информационной безопасности. Оценка рисков нарушения информационной безопасности. Проектирование автоматизированных систем в защищённом исполнении. Механизмы обеспечения функциональной устойчивости и надёжности защиты информации. Управление информационной безопасностью автоматизированных систем. Оценка эффективности защиты автоматизированных систем.

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 успеваемости аспирантов по дисциплине включает реферат и зачет с оценкой. Оценочные средства включают тематику рефератов, примерные варианты контрольных заданий, вопросы для проведения зачётов и др.

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

Критерии оценки за реферат

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. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «отлично».
Хорошо	Ответ аспиранта правильный, но неполный. Не приведены иллюстрирующие примеры, обобщающее мнение аспиранта недостаточно четко выражено. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке

	«хорошо».
Удовлетворительно	Ответ правильный в основных моментах, нет иллюстрирующих примеров, отсутствует собственное мнение аспиранта, есть ошибки в деталях. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «удовлетворительно».
Неудовлетворительно	В ответе аспиранта существенные ошибки в основных аспектах темы. Предусмотренные рабочей программой дисциплины учебные задания либо не выполнены, либо выполнены неудовлетворительно.

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

Примерная тематика рефератов

№ п п	Примерная тематика рефератов	Формируемые компетенции
1.	Теория и методология обеспечения информационной безопасности и защиты информации.	ОПК-1 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-6
2.	Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вид	ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
3.	Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.	ОПК-1 ОПК-2 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
4.	Системы документооборота и средства защиты циркулирующей в них информации.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
5.	Методы и средства информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
6.	Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
7.	Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
8.	Модели противодействия угрозам нарушения информационной безопасности для любого вида	ОПК-1 ОПК-2 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4

	информационных систем.	УК-6
9.	Модели и методы оценки защищенности информации и информационной безопасности объекта.	ОПК-1 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
10.	Модели и методы оценки эффективности систем обеспечения информационной безопасности объектов защиты.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
11.	Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
12.	Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
13.	Принципы и решения по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
14.	Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.	ОПК-1 ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
15.	Модели и методы управления информационной безопасностью.	ОПК-1 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-3 УК-4 УК-6

Перечень вопросов к экзамену

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

12.	Причины, обстоятельства и условия дестабилизирующего воздействия на информацию.	ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6
13.	Требования к системам защиты информации.	ОПК-2 ОПК-3 ОПК-5 ПК-1 ПК-2 УК-1 УК-2 УК-3 УК-4 УК-6

7. Учебно-методическое и информационное обеспечение дисциплины

Список источников и литературы

Основная

1. Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 года (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_28399/, свободный. – Загл. с экрана.

2. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_191669/, свободный. – Загл. с экрана.

3. Указ Президента РФ от 05.12.2016 № 646 «О Доктрине информационной безопасности Российской Федерации» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_208191/, свободный. – Загл. с экрана.

4. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_216363/, свободный. – Загл. с экрана..

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

6. Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция) [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана..

7. ГОСТы по информационной безопасности и защите информации

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 : 270.00.

9. Коваленко Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учеб. пособие для слушателей, обучающихся по программе доп. проф. образования в области информ. безопасности "Основы лицензирования и сертификации в области защиты информации" / Ю. И. Коваленко. - Москва : Горячая линия-Телеком, 2012. - 138 с. : табл. ; 21 см. - (Учебное пособие для высших учебных заведений). - Библиогр.: с. 134-138. - ISBN 978-5-9912-0261-9 : 341.00.

10. Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика».

Дополнительная:

1. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 [Электронный ресурс] : Режим доступа : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691, свободный. – Загл. с экрана.

2. Об утверждении Требований о защите информации, не составляющей

государственную тайну, содержащейся в государственных информационных системах: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. N 17 [Электронный ресурс] : Режим доступа : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702, свободный. – Загл. с экрана.

3. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. N 17 г. Москва // Российская газета. 2013, 22 мая

4. [Методический документ]. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена приказом ФСТЭ России 14 февраля 2008 г. [Электронный ресурс] Режим доступа : http://fstec.ru/component/attachments/download/290 (дата обращения: 14.08.2019).

5. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014). [Электронный ресурс] Режим доступа : https://fstec.ru/component/attachments/download/675 . Дата обращения: 14.08.2019

6. Малюк, А. А. Теория защиты информации / А.А. Малюк. - Москва : Гор. линия-Телеком, 2012. - 184 с.: ил.; . ISBN 978-5-9912-0246-6, 500 экз. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/367555 (дата обращения: 23.08.2019)

7. Ларин М.В., Янковая В.Ф. Организация хранения электронных документов // Современные технологии делопроизводства и документооборота. – 2013. - № 5. - С. 6-17.

Периодические и сериальные издания

1. Безопасность информационных технологий: научный журнал. - М.
2. Джет Инфо: бюллетень. - М.
3. Защита информации: научный журнал. - М.
4. Информационная безопасность: научный журнал. - СПб.
5. Информационные войны: научный журнал. - М.
6. Открытые Системы. СУБД: научный журнал. - М.

Ресурсы Интернет:

1. Совет безопасности Российской Федерации [офиц. сайт]. http://www.scrf.gov.ru/
2. Федеральная служба по техническому и экспортному контролю [офиц. сайт], http://fstec.ru
3. Управление «К» МВД России [офиц. сайт]. https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii
4. Институт информационных наук и технологий безопасности РГГУ [офиц. сайт], http://www.rsuh.ru/iint
5. Методические пособия, рекомендации, перечни [офиц. сайт Федерального архивного агентства], http://archives.ru/documents/methodics.shtml.
6. Информационная безопасность организаций банковской системы Российской Федерации [офиц. сайт Центрального банка Российской Федерации], http://www.cbr.ru/credit/gubzi_docs

8. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий и самостоятельной работы по дисциплине используются следующие классы и оборудование:

Специальной класс для изучения технической защиты информации

1. Комплект оборудования, в т.ч. приборы:

– «Пиранья» или аналог – прибор для обнаружения и локализации средств негласного съёма информации: состоит из основного блока управления и индикации, комплекта преобразователей и позволяет работать в следующих режимах: высокочастотный детектор-частотомер; сканирующий анализатор проводных линий;

детектор ИК-излучений; детектор низкочастотных магнитных полей; виброакустический приемник; акустический приемник; проводной акустический приемник.

– Нелинейный локатор – устройство для поиска радиозакладных устройств. Частота передатчика 860 МГц, Выходная импульсная мощность >200 Вт, модуляция зондирующего сигнала амплитудно- импульсная, чувствительность не хуже -123 дБ/Вт, принимаемый сигнал - 2 и 3 гармоники, индикация -звуковая с диапазоном 30 дБ.

– «Цикада-М» или аналог – комплексное устройство защиты информации в телефонных линиях.

– «Крона» или аналог – комплекс обнаружения радиоизлучающих средств и радиомониторинга для обнаружения и локализации средств негласного съема информации, передающих данные по радиоканалу (радиозакладок), использующих все известные на сегодняшний день средства маскирования, а также для решения широкого круга задач радиомониторинга. С высоким быстродействием определяет параметры любых радиосредств в диапазоне до 3 ГГц.

Мобильный широкодиапазонный всережимный приёмник

– приёмник AR8600 Мк2 или аналог - Диапазон частот 100 Гц…3000МГц; виды модуляции принимаемых сигналов WFM, NFM, SFM, WAM, AM, NAM, USB, LSB, CW; шаг перестройки программируемый от 50 Гц до 999 кГц; скорость сканирования - 37 шагов перестройки частоты в секунду; количество каналов памяти - 50 каналов х 20 банков = 1000.

– Поисковый приёмник «Скорпион 3.5» или аналог (приёмник-подавитель) – диапазон частот 30…2000 МГц,время просмотра диапазона – не более 10 с, мощность генератора – более 50 мВт.

– Шумомер – прибор для оценки акустической защищённости помещений

2. 2 стенда для изучения защищённости телефонных линий.

Специальной класс для изучения технических средств охраны

Учебно-тематические стенды с элементами систем телевизионного наблюдения, периметровых систем охраны объектов, примеры использования систем охранно-пожарной сигнализации на объектах (всего 12 стендов). Демонстрационная система охранно-пожарной сигнализации, с использованием: приёмно-контрольного прибора «Рубин-6», извещателей: пассивные (Фотон-4) и активные инфракрасные (Вектор-3, Вектор-3), радиоволновые (Фон-1), емкостные (Сет-11М), магнитоконтактные (СМК-1) и электроконтактные (Фольга). Демонстрационная система позволяет изучать физические принципы работы извещателей, условия их эксплуатации и особенности размещения на объекте, определять требования к системам ОПС и осуществлять их выбор.

Лаборатория программно-аппаратных средств обеспечения информационной безопасности

Локальная сеть, 12 компьютеров, подключённых к Интернет (Процессор: Celeron D 2,2, оперативная память: 512Mb, объем жёсткого диска: 40Gb. Дисковод CD, ЭЛТ монитор 15’)

ПО: Windows XP, Microsoft Office, Visual Studio 2005, VMware Player (Open Source), Free BSD (Open Source), Living Disaster Recovery Planning System 10

Мультимедийный компьютерный класс

Локальная сеть, 13 компьютеров, подключённых к Интернет (Процессор Atom 1,6 GHz. Оперативная память: 2Гb. Объем жёсткого 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

Лекционная аудитория

1 компьютер (Процессор: Pentium 4 3GHz. Оперативная память: 512Mb. Объем жёсткого 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.

Методы и системы защиты информации, информационная безопасность

Составитель Д.А. Митюшин,
кандидат технических наук

_____

подпись расшифровка подписи

Лист изменений
в рабочей программе дисциплины

Методы и системы защиты информации, информационная безопасность
(Название дисциплины)

№ п/п	Дата внесения изменений	Дата и № протокола заседания кафедры	Содержание изменения	Подпись
1.	08.05. 2020 г.	Приказ РГГУ от 08 мая 2020 г. № 01-229/осн	Кандидатские экзамены проводятся в дистанционной форме в срок с 15 июня по 28 июня 2020 г. Расписание кандидатских экзаменов составляется в электронной форме Управлением аспирантурой и докторантурой по предложению кафедры. Взаимодействие с обучающимися и проведение кандидатских экзаменов осуществляется с использованием дистанционных технологий. Основной формой деятельности экзаменационных комиссий являются заседания, которые проводятся дистанционно. Решения, принятые экзаменационными комиссиями, оформляются протоколами в электронной форме, которые направляются в Управление аспирантурой и докторантурой.	Управление аспирантурой и докторантурой

			Протоколы на бумажном носителе с установленными подписями предоставляются в Управление аспирантурой и докторантурой после появления такой возможности, но не позднее 20 сентября 2020 г. При проведении кандидатского экзамена обеспечивается идентификация личности обучающегося. В протокол заседания экзаменационной комиссии вносится запись «неявка по неуважительной причине» в связи с невозможностью идентификации обучающегося. Кандидатский экзамен может быть проведен: устно в режиме видеоконференцсвязи (ВКС); письменно с контролем хода проведения кандидатского экзамена в режиме видеосвязи; - в комбинированной форме. Проведение кандидатского экзамена в устной форме в режиме ВКС осуществляется в утвержденные даты и время согласно расписанию. За 15 минут до начала кандидатского экзамена аспирант устанавливает с доступного ему устройства ВКС путем перехода по установленной ссылке. До начала кандидатского	

			экзамена аспирант демонстрирует через камеру экзаменационной комиссии отсутствие посторонних лиц в помещении, где он находится, и посторонних предметов перед монитором (экраном) и камерой своего устройства. Аспиранту в рамках ВКС передается содержание вопросов, на которые ему необходимо ответить, и дается время для подготовки ответа. При этом ВКС не прерывается и аспирант должен в процессе подготовки ответа находиться перед камерой своего устройства так, чтобы члены экзаменационной комиссии могли его видеть все время подготовки к ответу. В случае неполного или некорректного ответа члены экзаменационной комиссии имеют право задавать аспиранту дополнительные вопросы в рамках программы кандидатского экзамена по соответствующей направленности программы аспирантуры. В случае сбоя в работе оборудования, не позволяющего членам экзаменационной комиссии слышать обучающегося, в порядке исключения, допускается подготовка обучающимся ответа в письменной форме, и передача ответа по электронной почте для оценки работы членами экзаменационной комиссии. Данный факт отражается в	

			протоколе заседания экзаменационной комиссии. В случае сбоя в работе оборудования на протяжении более 15 минут допускается перенос кандидатского экзамена на другое время, о чем ставится в известность Управление аспирантурой и докторантурой. Обучающимся предоставляется возможность сдать кандидатский экзамен в другой день в рамках срока, отведенного на промежуточную аттестацию в соответствии с учебным планом подготовки аспиранта и календарным учебным графиком. В случае невыхода обучающегося на связь в течение более чем 15 минут с начала проведения экзамена, он считается неявившимся на кандидатский экзамен. Результаты кандидатского экзамена, проводимого в устной форме, объявляются в день его проведения. Информация о времени, отведенном для выполнения письменного задания, и форме выполнения письменной работы предоставляется обучающемуся не позднее чем за 3 дня до проведения кандидатского экзамена. Результаты кандидатского экзамена, проводимого в письменной форме, объявляются на следующий рабочий день после дня его проведения. В ходе кандидатского экзамена, проводимого	

			в комбинированной форме, обучающийся отвечает на отдельные вопросы устно, на часть вопросов он готовит письменные ответы. Информация о форме проведения кандидатского экзамена должна быть предоставлена обучающемуся не позднее чем за 3 дня до проведения кандидатского экзамена.	