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
«__»_____ г.

МЕТОДЫ И СИСТЕМЫ ИНЖЕНЕРНО-ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

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

«Методы и системы защиты информации, информационная безопасность»

Москва 2019

Методы и системы инженерно-технической 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: 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 инженерно-технической защиты информации» 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).

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).

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 трудоёмкость освоения дисциплины составляет 2 зачётные единицы, 72 часа. Программой дисциплины предусмотрены лекционные занятия (10 часов), самостоятельная работа аспиранта (44 часа).

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

1. Пояснительная записка

Цель дисциплины: выработка у слушателя понимания доминирующей роли семантического содержания объекта защиты в определении основных направлений обеспечения защиты, осознания ограниченности эффективности типовых решений, представлений и динамике развития новейших направлений аппаратной и программной базы информационных систем и ее влияния на организацию и технологию защиты информации.

В ходе подготовки специалиста высшей квалификации предлагаемый курс должен развить его представление об общесистемной роли технического направления в деятельности по обеспечению информационной безопасности, углубить понимание подчинённости технических мер защиты организационной структуре информационного процесса, сконцентрировать внимание на проблемных вопросах, связанных с существенными изменениями в физической и технологической базе современной аппаратуры и новейшими направлениями развития в этой области.

Предметом курса является специфика аппаратурного и программного оснащения различных информационных процессов, влияние этой специфики на постановку и решение задач технической защиты информации.

Курс даёт возможность ознакомиться аспирантам по направлению 10.06.01. с областями исследований по этой специальности.

Задачи дисциплины: изучить специфику аппаратурного и программного оснащения различных информационных процессов, влияние этой специфики на постановку и решение задач технической защиты информации с выработкой у обучаемого понимания доминирующей роли семантического содержания объекта защиты в определении основных направлений обеспечения защиты, осознания ограниченности эффективности типовых решений, представлений и динамике развития новейших направлений аппаратной и программной базы информационных систем и ее влияния на организацию и технологию защиты информации.

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

Дисциплина «Методы и системы инженерно-технической защиты информации» принадлежит к специальным дисциплинам. Данная дисциплина призвана, прежде всего, помочь аспиранту в его научной деятельности. Данный курс естественным образом связан с курсами, «Основы информационной безопасности и методология защиты информации» Дисциплина «Методы и системы инженерно-технической защиты информации» направлена на формирование следующих компетенций выпускника

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).

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).

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: Знать: нормативно-методическую базу в области информационной безопасности, факторы, определяющие её развитие, механизмы влияния на неё со стороны государства, знать методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности (ОПК-1, ОПК-2, ПК-1, УК-3).

Уметь: анализировать источники и литературу в области информационной безопасности, соотносить этот анализ с политической стратегией развития России в области информационной безопасности; определять модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем (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. Функциональные особенности объектов	3	2		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью собеседование
2	Локальные особенности объектов	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью собеседование
3	Постановка задач информационной безопасности и защиты информации на объекте	3			2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
4	Защита объекта от видового наблюдения	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью Собеседование
5	Защита информации в форме акустических и вибрационных сигналов	3			4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью реферат
6	Утечка информации за счёт побочных	3	1		2 Реферирование	Собеседование

	электромагнитных полей и наводок				российской и зарубежной литературы и статей, работа в интернет	
7	Утечка информации за счёт функциональных излучений и по каналам связи	3	1		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата
8	Виды контроля защищённости объекта	3			4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
9	Контроль наличия средств их применения и выполнения соответствующих организационных мер	3	1		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
10	Контроль параметров защищаемых систем и средств защиты	3			4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
11	Контроль эффективности системы защиты	3			4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
12	Аттестация объектов защиты	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
13	Нормативные требования по защите объектов, их роль в обеспечении фактической	3	1		2 Реферирование российской и зарубежной литературы и	Собеседование

	защищённости				статей, работа в интернет	
14	Государственная аттестация объектов защиты	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
15	Применение типовых методик контроля при проверке защищённости информации на объекте		1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
16	Подготовка к зачёту с оценкой				18	
	Итого:		**10**		**62**	**Зачёт с оценкой**

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. Функциональные особенности объектов	3	2		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью собеседование
2	Локальные особенности объектов	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью собеседование
3	Постановка задач информационной безопасности и защиты	3			2 Реферирование российской и	Контрольная работа

	информации на объекте				зарубежной литературы и статей, работа в интернет	
4	Защита объекта от видового наблюдения	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью Собеседование
5	Защита информации в форме акустических и вибрационных сигналов	3			4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью реферат
6	Утечка информации за счёт побочных электромагнитных полей и наводок	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
7	Утечка информации за счёт функциональных излучений и по каналам связи	3	1		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата
8	Виды контроля защищённости объекта	3			4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа
9	Контроль наличия средств их применения и выполнения соответствующих организационных мер	3	1		4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
10	Контроль параметров защищаемых систем и средств защиты	3			4 Реферирование российской и зарубежной литературы и статей, работа в	Собеседование

					интернет	
11	Контроль эффективности системы защиты	3			4 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
12	Аттестация объектов защиты	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
13	Нормативные требования по защите объектов, их роль в обеспечении фактической защищённости	3	1		2 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
14	Государственная аттестация объектов защиты	3	2		1 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
15	Применение типовых методик контроля при проверке защищённости информации на объекте		2		1 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование
16	Подготовка к зачёту с оценкой				18	
	Итого:		**12**		**60**	**Зачёт с оценкой**

3. Содержание дисциплины:

Тема 1. Введение. Особенности объектов защиты различного типа

Функциональные особенности объектов. Место инженерно-технической защиты в общей системе обеспечения информационной безопасности объектов. Принадлежность объектов к различным секторам государственной, коммерческой и общественной деятельности. Пространственные и временные масштабы деятельности объектов. Информационное насыщение деятельности объектов. Особенности управленческой, торговой, банковской, посреднической деятельности.

Локальные особенности объектов. Дислокация на местности. Территория, тип зданий и внутреннее размещение. Особенности организации собственного рабочего процесса и взаимодействия с внешней средой. Технические системы жизнеобеспечения, обеспечения функционального процесса, обеспечения информационной подсистемы. Постановка задач информационной безопасности и защиты информации на объекте. Защита информации государственной значимости. Защита информации, отображённой в правовой базе. Защита общих информативных характеристик деятельности предприятия.

Тема 2. Современные методы получения информации и соответствующие методы противодействия

Защита объекта от видового наблюдения. Характеристики процесса наблюдения в видимом диапазоне спектра и особенности аппаратуры наблюдения. Энергетический и спектральный контраст. Пространственная разрешающая способность. Влияние временных факторов, динамики процессов, индивидуальных характеристик объекта наблюдения. Вероятностные параметры обнаружения и распознавания объекта. Отношение сигнал - шум; энергетическая и пространственная интерпретации. Методы создания преград на пути наблюдения в видимом диапазоне спектра. Непрозрачные преграды. Частично прозрачные преграды. Маскирование объекта. Организационные и организационно-технические меры защиты от видового наблюдения в видимом диапазоне спектра. Наблюдения в условиях слабой освещённости, в инфракрасном свете и в тепловом диапазоне. Радиолокационное наблюдение и методы противодействия.

Защита информации в форме акустических и вибрационных сигналов. Виды акустических и вибрационных сигналов и их информативность. Основные характеристики акустического и вибрационного поля. Распространение акустических и вибрационных сигналов в помещениях и конструкциях. Звукоизоляция как физическое явление, субъективная оценка, строительный норматив и параметр защищённости информации. Характеристики восприятия речевого сигнала в технике связи, как показатель комфортности и как оценки информационной защищённости. Применение защитного шума для подавления утечки акустических сигналов. Влияние защитного шума на восприятие сигнала в канале утечки и на комфортность помещения. Оценка различных способов формирования защитного шума. Особенности распространения сигналов в строительных конструкциях и различных сооружениях. Методы защиты. Применение различных способов зондирования для приёма акустических сигналов.

Утечка информации за счёт побочных электромагнитных полей и наводок. Источники электрических, магнитных и электромагнитных полей в современной аппаратуре. Применение защищённой аппаратуры. Защита помещений и оборудования с применением экранирования фильтров и регенераторов. Защита помещений и оборудования с применением защитных шумов. Особенности защиты современной высокоскоростной аппаратуры.

Утечка информации за счёт функциональных излучений и по каналам связи. Проблема подавления функциональных излучений. Снижение информативности, организационные меры защиты. Защита информации в каналах связи. Методы ограничения доступа к каналу связи. Методы физического преобразования сигнала в

канале связи, затрудняющие его перехват. Криптографические методы защиты каналов связи.

Защита от утечки информации за счёт внедрения ретрансляторов и зондирования направленным излучением. Методы выявления внедрённых ретрансляторов. Ограниченность возможностей. Методы подавления внедрённых ретрансляторов. Система организационных и технических мер по защите помещений от внедрения ретрансляторов. Выявление направленных энергетических воздействий. Методы противодействия. Системы охраны объекта и управления доступом как фактор информационной безопасности.

Тема 3. Контроль эффективности мер по защите информации.

Виды контроля защищённости объекта. Контроль наличия средств их применения и выполнения соответствующих организационных мер. Контроль параметров защищаемых систем и средств защиты. Контроль эффективности системы защиты. Аттестация объектов защиты. Нормативные требования по защите объектов, их роль в обеспечении фактической защищённости. Государственная аттестация объектов защиты. Применение типовых методик контроля при проверке защищённости информации на объекте.

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

№ пп	Примерная тематика рефератов	Формируемые компетенции
1.	Место инженерно-технической защиты в общей системе обеспечения информационной безопасности объектов.	ОПК-1, ОПК-2, ПК-1, УК-1, УК-2
2.	Особенности организации собственного рабочего процесса и взаимодействия с внешней средой.	ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
3.	Защита общих информативных характеристик деятельности предприятия.	ОПК-1, ОПК-3, ПК-1, УК-1, УК-2, УК-3
4.	Характеристики процесса наблюдения в видимом диапазоне спектра и особенности аппаратуры наблюдения.	ОПК-2, ОПК-3, УК-1, УК-2
5.	Вероятностные параметры обнаружения и распознавания объекта.	ОПК-2, ОПК-3, УК-1, УК-2

6.	Организационно-технические меры защиты от видового наблюдения в видимом диапазоне спектра.	ОПК-2, ОПК-3, УК-1, УК-2
7.	Основные характеристики акустического и вибрационного поля.	ОПК-2, ОПК-3, УК-1, УК-2
8.	Влияние защитного шума на восприятие сигнала в канале утечки и на комфортность помещения.	ОПК-1, ОПК-2, ПК-1, УК-1, УК-2, УК-3
9.	Особенности распространения сигналов в строительных конструкциях и различных сооружениях.	ОПК-2, ОПК-3, УК-1, УК-2
10.	Защита помещений и оборудования с применением экранирования фильтров и регенераторов.	ОПК-1, ОПК-2, ПК-1, УК-1, УК-2, УК-3
11.	Методы выявления внедрённых ретрансляторов.	ОПК-1, ОПК-2, ПК-1, УК-1, УК-2
12.	Системы охраны объекта и управления доступом как фактор информационной безопасности.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
13.	Применение типовых методик контроля при проверке защищённости информации на объекте.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3

Перечень вопросов к зачёту с оценкой

№ пп	Перечень вопросов к зачету с оценкой	Формируемые компетенции
1.	Функциональные особенности объектов защиты	ОПК-1, ОПК-2, УК-1, УК-2
2.	Локальные особенности объектов защиты	ОПК-1, ОПК-2, УК-1, УК-2
3.	Постановка задач информационной безопасности и защиты информации на объекте.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
4.	Защита объекта информатизации от видового наблюдения.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
5.	Утечка информации за счёт побочных электромагнитных полей и наводок.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
6.	Утечка информации за счёт функциональных излучений и по каналам связи.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
7.	Защита от утечки информации за счёт внедрения ретрансляторов и зондирования направленным излучением.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
8.	Системы охраны объекта и управления доступом как фактор информационной безопасности.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
9.	Виды контроля защищённости объекта.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1, УК-2, УК-3
10.	Аттестация объектов информатизации.	ОПК-1, ОПК-2, ОПК-3, ПК-1, УК-1

7. Учебно-методическое и информационное обеспечение дисциплины

Список источников и литературы

Основная

1. 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.

2. Федеральный закон РФ от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_48699/, свободный. – Загл. с экрана.

3. 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..

4. Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 (последняя редакция) [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_2481/, свободный. – Загл. с экрана.

5. Указ Президента РФ от 30.11.1995 № 1203 (ред. от 08.08.2019) «Об утверждении Перечня сведений, отнесённых к государственной тайне» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_8522/, свободный. – Загл. с экрана.

6. Указ Президента РФ от 06.03.1997 № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_13532/, свободный. – Загл. с экрана.

7. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / А. А. Торокин. - М. : Гелиос АРВ, 2005. - 958 с. : рис.,табл. - Библиогр.: с. 934-949. - ISBN 5-85438-140-0. - ISBN 5-85438-140-0(ошибоч.) : 275.

Дополнительная:

1. Магауенов Р.Г. истемы охранной сигнализации: основы теории и принципы построения : учеб. пособие для студентов вузов, обучающихся по специальности 200700 - "Радиотехника" направления подгот. дипломир. специалистов 654200 - "Радиотехника" / Р. Г. Магауенов. - 2-е изд., перераб. и доп. - М. : Горячая линия-Телеком, 2008. - 493 с. : рис., табл. ; 22 см. - (Учебное пособие для вузов). - Библиогр.: с. 474-486 (237 назв.). - ISBN 978-5-9912-0025-7 : 297.00. а.

2. Гарсиа М.Л. Проектирование и оценка систем физической защиты / М. Гарсиа ; пер. с англ. В.И. Воропаева [и др]. ; под ред. Р.Г. Магауенова. - М. : Мир, 2003 : АСТ. - 386 : рис. - (Технологии безопасности). - Пер.изд.: The design and evaluation of physical protection systems/ M.L.Garcia (Boston etc.: Butterworth Heinemann).- Доп.тит.л.ориг.англ. - Библиогр. в конце гл.- Предм. указ.: с. 384-386. - ISBN 5-17-018758-0. - ISBN 5-03-003522-2. - ISBN 0-7506-7367-2 : 165.

3. Халяпин Д.Б. Защита информации. Вас подслушивают? Защищайтесь!. - [2-е изд., испр. и доп.]. - М. : Баярд, 2004. - 431 с. : рис.,табл. - Библиогр.: с.426-431 (119 назв.). - ISBN 5-948960-17-X : 300.

4. Зайцев, А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - Москва : Гор. линия-Телеком, 2012. - 442с.; - (Уч. для вузов). ISBN 978-5-9912-0233-6. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/390284 (дата обращения: 23.08.2019).

5. Грибунин В.Г. Комплексная система защиты информации на предприятии : учеб. пособие для студентов вузов, обучающихся по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информатизации" направления подготовки "Информационная безопасность" / В. Г. Грибунин, В. В. Чудовский. - М. : Академия, 2009. - 411 с. : рис., табл. ; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 403-406 (52 назв.). - ISBN 978-5-7695-5448-3 : 442.20.

6. Максимов Н.В. Технические средства информатизации : учебник для студентов вузов, обучающихся по специальности 080801 "Прикладная информатика (по областям)" / Н. В. Максимов, Т. Л. Партыка, И. И. Попов. - 3-е изд., перераб. и доп. - М. : Форум, 2010.

- 606 с. : рис., табл. ; 22 см. - Библиогр.: с. 543-544 (31 назв.). - ISBN 978-5-91134-409-2 : 359.00.

7. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи: Учебное пособие для вузов / Портнов Э.Л. - Москва :Гор. линия-Телеком, 2013. - 544 с. (Специальность)ISBN 978-5-9912-0071-4. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/896340 (дата обращения: 23.08.2019)

8. Каганов, В. И. Основы радиоэлектроники и связи: Уч. пос. для вузов / В.И. Каганов, В.К. Битюков. - 2-е изд., стереотип. - Москва : Гор. линия-Телеком, 2012. - 542 с.: ил.; . - (Учебное пос. для высших учеб. завед.). ISBN 978-5-9912-0252-7, 100 экз. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/353668 (дата обращения: 23.08.2019).

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 инженерно-технической защиты информации

Составитель Д.А. Митюшин,
кандидат технических наук

_____

подпись расшифровка подписи

Лист изменений
в рабочей программе дисциплины

Методы и системы инженерно-технической 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. В процессе подготовки ответа аспирант должен находиться перед камерой своего устройства так, чтобы преподаватель мог его видеть все время подготовки к ответу.	Управление аспирантурой и докторантурой

			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.	