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 комплексной защиты информации

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

НАУЧНАЯ ПРАКТИКА

Рабочая программа научной практики 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

НАУЧНАЯ ПРАКТИКА

Рабочая программа научной практики для подготовки аспирантов.
Направление подготовки 10.06.01 «Информационная безопасность»
Направленность программ подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность»

Автор (составитель):

Митюшин Д.А. к.т.н., и.о зав. кафедры

Программа утверждена
на заседании кафедры комплексной защиты информации
30 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

© Российский государственный
гуманитарный университет, 2019

Аннотация

Проведение научной практики направлено на приобретение умений и опыта научной деятельности, в частности опыта участия, организации и проведения научных мероприятий (конференций, круглых столов и др.). Научная практика проводится *в* подразделениях факультета информационных систем и безопасности Института информационных наук и технологий безопасности РГГУ.

Рабочая программа научной практики разработана кафедрой комплексной защиты информации *ИИНТБ РГГУ*.

Научная практика 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),

способность следовать этическим нормам в профессиональной деятельности (УК-5),

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),

способность организовать работу коллектива по проведению научных исследований в области информационной безопасности (ОПК-4),

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 научной практики составляет 3 зачётные единицы, 108 часов. Программой научной практики предусмотрены следующие виды контроля: текущий контроль в форме собеседования, промежуточный контроль в форме зачета с оценкой в 5-м полугодии.

1. Пояснительная записка

Цель научной практики: дать аспиранту возможность освоить принципы организации, проведения и участия в научных мероприятиях в области информационной безопасности.

Задачи научной практики: дать аспирантам представление о современных методах проведения, презентации и обсуждения научных исследований в области информационной безопасности, в частности, в области современных методов и моделей защиты информации.

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

Научная практика является обязательной.

Общая трудоёмкость научной практики составляет 3 зачётные единицы, 108 часов. Научная практика проводится в 5-м полугодии 3-го года обучения. Научная практика непосредственно связана с научными исследованиями аспирантов: в ходе практики аспиранты учатся представлять собственные научные достижения, новые научные результаты и положения, выдвигаемые для публичной защиты, и свидетельствовать о личном вкладе автора в науку.

Программой научной практики предусмотрены следующие виды контроля: текущий контроль в форме собеседования, промежуточный контроль в форме зачета с оценкой в 5-м полугодии.

Вид, способ и форма проведения практики:

вид – научная;

способ проведения – стационарная;

форма проведения – дискретная[1].

Требования к результатам прохождения научной практики:

Научная практика 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),

способность следовать этическим нормам в профессиональной деятельности (УК-5),

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

[1] В календарном учебном графике указывается непрерывный период учебного времени для проведения практики.

информационной безопасности (ОПК-3),

способность организовать работу коллектива по проведению научных исследований в области информационной безопасности (ОПК-4),

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 прохождения научной практики аспирант должен:

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 (УК-1, ОПК-1, ОПК-3, ПК-1);

– методы анализа и оценки современных научных достижений в области информационной безопасности, а также принципы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1, УК-2, ОПК-1, ОПК-2, ОПК-3, ПК-1);

– методы научно-исследовательской деятельности (УК-2, ОПК-1, ОПК-2, ПК-1);

– особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах (УК-3, УК-5, УК-6, ОПК-1, ОПК-2, ОПК-3, ПК-1);

– методику и технологии научной коммуникации на государственном и иностранном языках (УК-3, УК-5, УК-6);

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, ОПК-1, ОПК-3);

– участвовать в дискуссиях, а также в выработке коллективных решений (УК-1, УК-3, УК-5, ОПК-1, ОПК-4);

– анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные возможности реализации этих вариантов (УК-1, УК-6, ОПК-3, ПК-1);

– следовать нормам научного общения при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач (УК-3, УК-5, ОПК-4);

владеть:

– навыками анализа мировоззренческих, методологических и специальных проблем, возникающих при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-2);

– методиками и технологиями планирования профессиональной деятельности в сфере научных исследований (УК-3, УК-6, ОПК-2, ОПК-4, ПК-1);

– методиками и технологиями планирования коллективной деятельности по решению научных задач (УК-3, ОПК-4);

– методиками и технологиями оценки результатов коллективной деятельности по решению научных задач (УК-3, ОПК-4);

– различными типами коммуникаций при осуществлении организационной и научной работы в коллективе (УК-3, ОПК-4);

– навыками применения полученных знаний в научно-педагогической работе (УК-1, УК-2, ОПК-1, ОПК-2, ПК-1).

2. Структура и содержание научной практики

Общая трудоёмкость научной практики составляет 3 зачётные единицы, 108 часов.

№ п/п	Разделы (этапы) практики	Виды учебной работы на практике, включая самостоятельную работу аспирантов и трудоемкость (в часах)					Формы текущего контроля Форма промежуточной аттестации
		сбор и систематизация заявок	подготовка программы	подготовка научного доклада	самостоятельная работа	подготовка и защита отчёта	
1	**Участие в подготовке и проведении международной конференции студентов, аспирантов и молодых учёных «Технологии безопасности»**						Собеседование
1.1	Участие в отборе и систематизации заявок	2					
1.2	Участие в составлении программы конференции		2				
1.3	Организационное участие в проведении конференции				12		
2	**Подготовка молодёжного круглого стола**						Собеседование
2.1	Создание оргкомитета				4		
2.2.	Формирование замысла и формулировка тематики круглого стола				6		
2.3.	Отбор и систематизации заявок	6					
2.4.	Разработка программы круглого стола		6				
2.5.	Информационное и документационное обеспечение круглого стола		10				
2.6.	Подготовка тезисов научного доклада			10			
3	**Проведение круглого стола**						**Собеседование**
3.1.	Ведение заседания, организация дискуссии				6		
3.2	Подготовка доклада и выступление			16	2		
3.3	Подведение итогов круглого стола				2		
3.	Подготовка материалов круглого стола для электронной публикации				12		
4.	Подготовка отчета о научной практике				10		
7	Защита отчета о научной практике					2	
8	**Итого**	**8**	**18**	**26**	**54**	**2**	**Зачет с оценкой**

3. Информационные и образовательные технологии

Образовательные технологии проведения научной практики направлены на активизацию самостоятельной и коллективной научно-исследовательской и научно-организационной работы аспирантов во взаимодействии с коллегами – как опытными учёными (участие в организации и проведении международной конференции студентов, аспирантов и молодых учёных «Технологии безопасности»), так и начинающими (аспиранты и студенты).

В ходе научной практики предполагается активное использование практикантами современных информационных технологий для информационного обеспечения самостоятельно подготавливаемого и проводимого круглого стола, для презентации докладов и публикации итоговых материалов

4. Система текущего контроля успеваемости и промежуточной аттестации по итогам прохождения научной практики

Текущий контроль прохождения научной практики проводится научным руководителем аспиранта.

Промежуточная аттестация аспирантов и по итогам прохождения научной практики в 5-м полугодии обучения проводится на заседании кафедры в форме зачета с оценкой.

Отчет о прохождении научной практики с подписями научного руководителя и заведующего кафедрой, осуществляющей подготовку аспиранта, представляется в Управление аспирантурой и докторантурой в феврале 3-го года обучения.

Критерии оценки по итогам промежуточной аттестации

Оценка	Содержание
Отлично	Ответ аспиранта правильный, аспирант проявил способность к самостоятельному осуществлению научно-исследовательской деятельности, владение современным научным инструментарием и информационно-коммуникативными практиками, 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.

5. Фонд оценочных средств для текущего контроля успеваемости и промежуточной аттестации по итогам прохождения научной практики

Перечень заданий для текущего контроля

№ пп	Задания	Формируемые компетенции
1.	Разработка индивидуальной программы прохождения научной практики аспиранта • Ознакомление с целями и содержанием практики; беседа с руководителем практики. • Разработка и утверждение индивидуального	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-2, УК-3, УК-5, УК-6

	плана научной практики. • Подготовка отчета о прохождении научной практики и защита его на заседании кафедры.	
2.	Участие в подготовке, организации и проведении международной конференции студентов, аспирантов и молодых учёных «Технологии безопасности» • Помощь в сборе и систематизации заявок на участие в конференции. • Помощь в составлении программы конференции. • Участие в решении организационных вопросов проведения конференции. • Активное участие в работе конференции в качестве слушателя.	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-2, УК-3, УК-5, УК-6
3.	Самостоятельная подготовка, организация и проведение научного мероприятия (молодёжного «круглого стола» аспирантов и студентов) • Создание оргкомитета круглого стола. • Формирование замысла и формулировка тематики круглого стола. • Отбор и систематизация заявок на участие в круглом столе. • Разработка программы круглого стола. • Информационное и документационное обеспечение круглого стола. • Ведение заседания, организация дискуссии. • Выступление с докладом. • Подведение итогов круглого стола. • Подготовка материалов круглого стола для электронной публикации.	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-2, УК-3, УК-5, УК-6
4.	Ознакомление с организацией научно-исследовательского процесса в высшей школе • Освоение нормативных документов по организации научных исследований. • Знакомство с организацией научно-исследовательской работы на кафедре. • Изучение традиций и актуального состояния научно-педагогической школы кафедрального коллектива	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-2, УК-3, УК-5, УК-6

Перечень контрольных вопросов

№ пп	Вопросы	Формируемые компетенции
1.	Федеральные государственные требования к организации и эффективности научных исследований.	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-2, УК-3, УК-5, УК-6
2.	Современные представления о научно-педагогических школах в системе высшего образования.	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-

		2, УК-3, УК-5, УК-6
3.	Индекс цитирования и иные современные параметры оценивания результативности научной деятельности.	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-2, УК-3, УК-5, УК-6
4.	Особенности постановки научных исследований на кафедре	ОПК-1, ОПК-2, ОПК-3, ОПК-4, ПК-1, УК-1, УК-2, УК-3, УК-5, УК-6

6. Учебно-методическое и информационное обеспечение научной практики

Список источники и литературы

Основные источники

1. Конституция Российской Федерации от 25 декабря 1993 года, с последними изменениями // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

2. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

3. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

4. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

6. О персональных данных: Федеральный закон от 29 июля 2006 г. № 152- ФЗ // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

7. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. М., 2007. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

8. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. М., 2007. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

9. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. М., 2007. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

10. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2007. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

11. ГОСТ Р ИСО/МЭК 27003-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования. М., 2007. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

12. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. М., 2012. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

13. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

14. ГОСТ Р 54989-2012 /ISO TR 18492:2005. Обеспечение долговременной сохранности электронных документов. М., 2013. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

15. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационные технологии Методы и

средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. - М.: ИПК Издательство стандартов, 2002. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

16. ГОСТ Р ИСО/МЭК 15408-2-2002. Информационные технологии Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. М., 2002. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

17. ГОСТ Р ИСО/МЭК 15408-3-2002. Информационные технологии Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. - М., 2002. // ИСС «КонсультатнтПлюс» или ИСС «Гарант».

18. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.

19. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

20. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.

21. Руководящий документ. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

22. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114

Дополнительные источники

1. Приказ ФСТЭК России от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214004&

dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#034991095371992622 по рабочим дням с 20-00 до 24-00 (время московское), в выходные и праздничные дни в любое время. – Загл. с экрана.

2. Приказ ФСТЭК России от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=215976&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#08164959407738432 свободный. – Загл. с экран [Методический документ]. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена приказом ФСТЭК России 14 февраля 2008 г. http://fstec.ru/component/attachments/download/290 (дата обращения: 14.04.2019).

3. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2 014). URL : https://fstec.ru/component/attachments/download/675. Дата обращения: 14.05.2019

Основная литература

1. Кукушкина, В. В. Организация научно-исследовательской работы студентов (магистров) : учеб. пособие / В.В. Кукушкина. – Москва : ИНФРА-М, 2019. – 264 с. – (Высшее образование: Магистратура). – ISBN 978-5-16-101630-5. – Текст : электронный. – URL: https://new.znanium.com/catalog/product/982657 (дата обращения: 08.06.2019)

2. Леонова, О.В. Основы научных исследований [Электронный ресурс] : Учебное пособие / О.В. Леонова. – Москва : Альтаир-МГАВТ, 2015. – 72 с. – Текст : электронный. – URL: https://new.znanium.com/catalog/product/537751 (дата обращения: 08.06.2019)

3. Теоретические основы компьютерной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям группы 090100 "Информ. безопасность" / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. - М. : Академия, 2009. - 267 с. : табл. ; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 261-263 (54 назв.). - ISBN 978-5-7695-4242-8 : 289.30.

4. Малюк, А. А. Введение в информационную безопасность: Учебное пособие для вузов / А.А. Малюк, В.И. Королев, В.М. Фомичев; Под ред. В.С. Горбатов. - Москва : Гор. линия-Телеком, 2011. - 288 с.: ил.; . - (Специальность). ISBN 978-5-9912-0160-5, 1000 экз. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/265558 (дата обращения: 08.06.2019).

Дополнительная литература

1. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. – 2-е изд. – Москва : ДМК Пресс, 2017. – 434 с. – ISBN 978-5-97060-435-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/93278 (дата обращения: 08.06.2019). -- Режим доступа: для авториз. пользователей.

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

3. Некраха А.В. Шевцова Г.А. Организация конфиденциального делопроизводства и защита информации. М., 2007.

4. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2018. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-16-106148-0. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/937502 (дата обращения: 08.06.2019).

Периодические и сериальные издания

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

Интернет-источники

1. Информационно-справочная система «КонсультантПлюс». http://www.consultant.ru
2. Информационно-справочная система «Гарант». http://www.garant.ru
3. Совет безопасности Российской Федерации [офиц. сайт]. http://www.scrf.gov.ru/
4. Федеральная служба по техническому и экспортному контролю [офиц. сайт]. http://fstec.ru
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
7. Институт информационных наук и технологий безопасности РГГУ [офиц. сайт], http://www.rsuh.ru/iintb

7. Материально-техническое обеспечение научной практики

Прохождение научной практики предполагает использование специальных аудиторий с необходимыми техническими средствами (компьютер, проектор, доска, компьютерная сеть с выходом в интернет), а также лабораторий со специализированным оборудованием для проведения лабораторных работ.

Мультимедийный компьютерный класс

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

Перечень ПО

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Adobe Master Collection CS4	Adobe	лицензионное
2	Microsoft Office 2010	Microsoft	лицензионное
3	Windows 7 Pro	Microsoft	лицензионное
4	AutoCAD 2010 Student	Autodesk	свободно распространяемое
5	Archicad 21 Rus Student	Graphisoft	свободно распространяемое
6	SPSS Statisctics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statisctics 25	IBM	лицензионное
9	Microsoft Office 2013	Microsoft	лицензионное
11	Microsoft Office 2013	Microsoft	лицензионное
12	Windows 10 Pro	Microsoft	лицензионное
13	Kaspersky Endpoint Security	Kaspersky	лицензионное

14	Microsoft Office 2016	Microsoft	лицензионное
15	Visual Studio 2019	Microsoft	лицензионное
16	Adobe Creative Cloud	Adobe	лицензионное

Лаборатория технических средств охраны

1. Стенды и оборудование для проведения лабораторных и практических занятий по дисциплинам «Технические средства защиты и охраны объектов», «Системы контроля управления доступом».

2. 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 технической защиты информации

1. Комплект оборудования для выполнения практикумов по курсам «Техническая защита информации» и «Инженерно-техническая защита информации», в т.ч. приборы:

- Пиранья - 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 приёмник; акустический приёмник; проводной акустический приёмник.

- 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 – комплексное устройство защиты информации в телефонных линиях.

- Крона - комплекс обнаружения радиоизлучающих средств и радиомониторинга для обнаружения и локализации средств негласного съёма 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 - 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 (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.

Сведения об авторах (составителях) рабочей программы научной практики

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

Авторы (составители):
И.о. зав. каф. КЗИ, к.т.н.
_____Д.А. Митюшин._____
(Должность, уч. степень, уч. звание подпись расшифровка подписи)

Лист изменений
в рабочей программе научной практики

___ Направление подготовки 10.06.01 Информационная безопасность _____ ____

Направленность подготовки «Методы и системы защиты информации, информационная безопасность»

№ 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	Задания научно-методического характера и проведение научного круглого стола в соответствии с программой научной практики проводятся с использованием дистанционных технологий. Зачет проводится в дистанционной форме устно в утвержденные даты и время согласно расписанию промежуточной аттестации. Информация о проведении зачета должна быть получена каждым аспирантом не позднее чем за 3 дня до зачета.	Управление аспирантурой и докторантурой