

МИНОБРНАУКИ РОССИИ



Федеральное государственное автономное образовательное учреждение
высшего образования

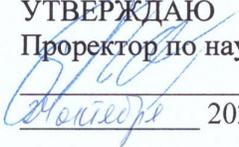
«Российский государственный гуманитарный университет»
(ФГАОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ
БЕЗОПАСНОСТИ

Факультет информационных систем и безопасности
Кафедра комплексной защиты информации

УТВЕРЖДАЮ

Проректор по научной работе
О.В. Павленко


2024 г.

НАУЧНО-ПЕДАГОГИЧЕСКАЯ ПРАКТИКА

Рабочая программа научно-педагогической практики для подготовки
аспирантов

2.3. Информационные технологии и телекоммуникации
(Шифр и наименование группы научных специальностей)

2.3.6. Методы и системы защиты информации, информационная безопасность
(Шифр и наименование научной специальности)

Москва 2024

НАУЧНО-ПЕДАГОГИЧЕСКАЯ ПРАКТИКА

Рабочая программа научно-педагогической практики для подготовки аспирантов

2.3. Информационные технологии и телекоммуникации.

2.3.6. Методы и системы защиты информации, информационная безопасность

Автор (составитель): Д.А. Митюшин,
кандидат технических наук

Программа утверждена
на заседании кафедры комплексной защиты информации
19 сентября 2024 г., протокол № 2

Программа утверждена
на заседании Совета ИИНТБ
17 октября 2024 г., протокол № 3

Программа утверждена
на заседании Научно-методического совета
по аспирантуре и докторантуре
24 октября 2024 г., протокол № 1

Аннотация

Проведение научно-педагогической практики направлено на приобретение умений и опыта профессиональной деятельности, в том числе опыта преподавательской деятельности, организации и проведения научных мероприятий (конференций, круглых столов и др.).

Научно-педагогическая практика проводится в подразделениях факультета информационных систем и безопасности Института информационных наук и технологий безопасности РГГУ.

Рабочая программа научно-педагогической практики разработана кафедрой комплексной защиты информации ИИНТБ РГГУ.

Требования к результатам прохождения научно-педагогической практики:

В результате прохождения научно-педагогической 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;

- 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;

- методы научно-исследовательской деятельности;

- особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах;

- методiku и технологии научной коммуникации на государственном и иностранном языках;

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;

- участвовать в дискуссиях, а также в выработке коллективных решений;

- анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные возможности реализации этих вариантов;

- следовать нормам научного общения при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач;

владеть:

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

- методиками и технологиями планирования профессиональной деятельности в сфере научных исследований;

- методиками и технологиями планирования коллективной деятельности по решению научных задач;

- методиками и технологиями оценки результатов коллективной деятельности по решению научных задач;

- различными типами коммуникаций при осуществлении организационной и научной работы в коллективе;

- навыками применения полученных знаний в научно-педагогической работе.

Общая трудоёмкость научно-педагогической практики составляет 2 зачётные единицы, 72 часа. Программой научно-педагогической практики предусмотрены следующие виды контроля: текущий контроль в форме собеседования; промежуточная аттестация в форме зачета с оценкой в 3-м семестре 2-го курса и в 5-м семестре 3-го курса.

1. Пояснительная записка

Цель научно-педагогической практики: дать аспиранту возможность освоить принципы организации, проведения и участия в научных мероприятиях в области информационной безопасности, применять профессиональные знания аспиранта, приобрести умения работы в студенческой аудитории, сформировать навыки педагогической деятельности.

Задачи научно-педагогической 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;
- ознакомление с современными образовательными технологиями и практическое их применение;
- освоение путей и принципов структурирования и педагогически обоснованного преобразования научного знания в учебный материал;
- овладение спектром целесообразных форм управления учебной деятельностью студентов.

Место научно-педагогической практики в структуре программы подготовки научных и научно-педагогических кадров в аспирантуре:

Научно-педагогическая практика является обязательной.

Общая трудоёмкость научно-педагогической практики составляет 2 зачётные единицы, 72 часа. Научно-педагогическая практика проводится в 3-м семестре 2-го курса (1 зачетная единица – 36 часов) и в 5-м семестре 3-го курса (1 зачетная единица – 36 часов). Научно-педагогическая практика непосредственно связана с научной деятельностью аспирантов: в ходе научно-педагогической практики аспиранты учатся использовать собственные научные достижения в преподавательской деятельности, представлять новые научные результаты и положения, выдвигаемые для публичной защиты, и свидетельствовать о личном вкладе автора науку.

Программой научно-педагогической практики предусмотрены следующие виды контроля: текущий контроль в форме собеседования; промежуточная аттестация в форме зачетов с оценкой в 3-м семестре 2-го курса и 5-м семестре 3-го курса.

Вид и способ проведения научно-педагогической практики:

вид – научно-педагогическая;

способ проведения – стационарная.

Научно-педагогическая практика проводится в подразделениях факультета информационных систем и безопасности Института информационных наук и технологий безопасности РГГУ.

Аспиранты, совмещающие освоение программы аспирантуры с трудовой деятельностью, вправе проходить научно-педагогическую практику по месту трудовой деятельности в случаях, если профессиональная деятельность, осуществляемая ими, соответствует требованиям программы аспирантуры к проведению научно-педагогической практики.

Требования к результатам прохождения научно-педагогической практики:

В результате прохождения научно-педагогической 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;

– 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;

– методы научно-исследовательской деятельности;

– особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах;

– методику и технологии научной коммуникации на государственном и иностранном языках;

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;

– участвовать в дискуссиях, а также в выработке коллективных решений;

– анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные возможности реализации этих вариантов;

– следовать нормам научного общения при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач;

владеть:

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

– методиками и технологиями планирования профессиональной деятельности в сфере научных исследований;

– методиками и технологиями планирования коллективной деятельности по решению научных задач;

– методиками и технологиями оценки результатов коллективной деятельности по решению научных задач;

– различными типами коммуникаций при осуществлении организационной и научной работы в коллективе;

– навыками применения полученных знаний в научно-педагогической работе.

2. Структура и содержание научно-педагогической практики

Общая трудоёмкость научно-педагогической практики составляет 2 зачётные единицы, 72 часа.

2-й курс, 3-й семестр*Рабочий график (план) проведения научно-педагогической практики*

№ п/п	Разделы (этапы) практики	Виды работ по прохождению научно-педагогической практики, включая самостоятельную работу аспирантов и трудоёмкость (в часах)	Формы текущего контроля Форма промежуточной аттестации

1	Подготовительный этап. Организация проведения научного мероприятия (круглого стола, конференции и др.)						Собеседование
1.1.	Разработка плана проведения круглого стола	4	2				
1.2.	Создание оргкомитета		2				
1.3.	Разработка программы круглого стола		2				
1.4.	Информационное и документационное обеспечение проведения круглого стола		6				
1.5.	Подготовка научных докладов и тезисов докладов			10			
2.	Проведение круглого стола						
2.1.	Проведение круглого стола. Участие в дискуссии				4		
3.	Подготовка отчета о проведении круглого стола – отчета о научной практике				4		
4	Защита отчета о научной практике					2	
5	Итого	4	12	10	8	2	Зачет оценкой с

3. Информационные и образовательные технологии

В процессе прохождения научно-педагогической практики используются традиционные технологии (подготовка и проведение лекционных, семинарских, практических занятий), инновационные методы обучения (участие в организации и проведении круглых столов, дискуссий и др.), технологии подготовки и планирования деятельности в рамках работы в коллективе по решению научных и научно-образовательных задач, оценки результатов коллективной деятельности по решению научных и научно-образовательных задач, использования различных типов коммуникаций при осуществлении работы в коллективе по решению научных и научно-образовательных задач.

4. Система текущего контроля успеваемости и промежуточной аттестации по итогам прохождения научно-педагогической практики

Текущий контроль и промежуточная аттестация аспирантов по итогам прохождения научно-педагогической практики проводятся научным руководителем аспиранта и кафедрой.

Промежуточная аттестация проводится в форме зачетов с оценкой по итогам прохождения научно-педагогической практики в 3-м и 5-м семестрах.

Отчеты о прохождении научно-педагогической практики включаются в листы аттестации аспирантов за 3-й и 5-й семестры.

Критерии оценки по итогам промежуточной аттестации

Оценка	Содержание
Отлично	Аспирант проявил готовность к преподавательской деятельности, способность обоснованно выбирать и эффективно использовать образовательные технологии, методы и средства обучения. Аспирант проявил способность к самостоятельному осуществлению научно-

	исследовательской деятельности, владение современным научным инструментарием и информационно-коммуникативными практиками. Аспирант способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры.
Хорошо	Аспирант проявил готовность к преподавательской и научной деятельности. В ходе собеседования по не приведены иллюстрирующие примеры, обобщающее мнение аспиранта недостаточно четко выражено, ответы неполные.
Удовлетворительно	Ответы правильные в основных положениях, отсутствуют иллюстрирующие примеры, собственное мнение аспиранта, имеются 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 научно-педагогической практики

Примерные контрольные вопросы и задания для текущего контроля

№ п/п	Задания
1.	<p>Разработка индивидуальной программы прохождения научной практики аспиранта</p> <ul style="list-style-type: none"> • Ознакомление с целями и содержанием практики; беседа с руководителем практики. • Разработка и утверждение индивидуального плана научной практики. • Подготовка отчета о прохождении научной практики и защита его на заседании кафедры.
2.	<p>Участие в подготовке, организации и проведении международной конференции студентов, аспирантов и молодых учёных «Технологии безопасности»</p> <ul style="list-style-type: none"> • 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.
3.	<p>Самостоятельная подготовка, организация и проведение научного мероприятия (молодёжного «круглого стола» аспирантов и студентов)</p> <ul style="list-style-type: none"> • 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.
4.	<p>Ознакомление с организацией научно-исследовательского процесса в высшей школе</p> <ul style="list-style-type: none"> • 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
5.	Функции, принципы, методы обучения.

6.	Формы учебных занятий.
7.	Особенности преподавания информационно-аналитических дисциплин в вузе.
8.	Учебно-методическое обеспечение учебного процесса.
9.	Порядок разработки рабочей программы курса.
10.	Порядок разработки фондов оценочных средств по дисциплине.
11.	Порядок разработки методических указаний по семинарским занятиям.
12.	Порядок разработки методических указаний по практическим занятиям.
13.	Порядок разработки методических указаний по лабораторным занятиям.
14.	Структура, содержание и организация занятия.

Перечень вопросов к зачету с оценкой

№ п/п	Вопросы
1.	Федеральные государственные требования к организации и эффективности научных исследований.
2.	Современные представления о научно-педагогических школах в системе высшего образования.
3.	Индекс цитирования и иные современные параметры оценивания результативности научной деятельности.
4.	Особенности постановки научных исследований на кафедре
5.	Функции, принципы, методы обучения.
6.	Формы учебных занятий.
7.	Особенности преподавания информационно-аналитических дисциплин в вузе.
8.	Учебно-методическое обеспечение учебного процесса.
9.	Порядок разработки рабочей программы курса.
10.	Порядок разработки фондов оценочных средств по дисциплине.
11.	Структура, содержание и организация занятия.
12.	Методика проведения занятий. Интерактивные методы обучения.
13.	Балльно-рейтинговая система в вузе.
14.	Формы и методы проведения промежуточной аттестации.
15.	Организация самостоятельной работы студентов.
16.	Формы контроля знаний, умений и навыков.
17.	Организация воспитательной работы со студентами.
18.	Организация научной работы студентов.
19.	Обратная связь «студент-преподаватель».

6. Учебно-методическое и информационное обеспечение научно-педагогической практики

Список источников и литературы

Основные источники

1. Конституция Российской Федерации от 25 декабря 1993 года, с последними изменениями // ИСС «КонсультантПлюс» или ИСС «Гарант».
2. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // ИСС «КонсультантПлюс» или ИСС «Гарант».
3. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // ИСС «КонсультантПлюс» 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 «КонсультантПлюс» или ИСС «Гарант».
5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ // ИСС «КонсультантПлюс» 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-predsdatelya-gostekhkommisii-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-predsdatelya-gostekhkommisii-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-gostekhkommisii-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-gostekhkommisii-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 недеklarированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114
23. ГОСТы по информационной безопасности и защите информации

Дополнительные источники

24. Приказ ФСТЭК России от 11.02.2013 № 17 «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.
25. 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>.
26. [Методический документ]. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014). URL : <https://fstec.ru/component/attachments/download/675>.

Основная литература

27. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. — 3-е изд., стер. — Санкт-Петербург : Лань, 2024. — 324 с. — ISBN 978-5-507-49077-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/370967> (дата обращения: 15.09.2024). — Режим доступа: для авториз. пользователей.
28. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/207095> (дата обращения:

- 15.09.2024). — Режим доступа: для авториз. пользователей.
29. Киренберг, А. Г. Защита информации от утечки по техническим каналам : учебное пособие / А. Г. Киренберг, В. О. Коротин. — Кемерово : КузГТУ имени Т.Ф. Горбачева, 2023. — 222 с. — ISBN 978-5-00137-407-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/399665> (дата обращения: 15.09.2024). — Режим доступа: для авториз. пользователей.
 30. 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.znaniium.com/catalog/product/982657> (дата обращения: 16.05.2022)
 31. Леонова, О.В. Основы научных исследований [Электронный ресурс] : Учебное пособие / О.В. Леонова. — Москва : Альтаир-МГАВТ, 2015. — 72 с. — Текст : электронный. — URL: <https://new.znaniium.com/catalog/product/537751> (дата обращения: 16.05.2022)
 32. 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://znaniium.com/catalog/product/265558> (дата обращения: 16.05.2022). — Режим доступа: по подписке
 33. 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://znaniium.com/catalog/product/367555> (дата обращения: 16.05.2022). — Режим доступа: по подписке.
 34. Резник, С. Д. Аспиранты России: отбор, подготовка к самостоятельной научной и педагогической деятельности: Монография / Под общ. ред. С.Д. Резника. — 2-е изд., перераб. и доп. — Москва : ИНФРА-М, 2019. — 236 с. — (Научная мысль). (Обложка. КБС) ISBN 978-5-16-006929-6. — Текст : электронный. — URL: <https://new.znaniium.com/catalog/product/1010473> (дата обращения: 16.05.2022)
 35. Андриади, И.П. Основы педагогического мастерства : учебник / И.П. Андриади. — 2-е изд., испр. и доп. — Москва : ИНФРА-М, 2018. — 209 с. — (Высшее образование: Бакалавриат), — www.dx.doi.org/10.12737/16061. -- ISBN 978-5-16-011222-0 (print); ISBN 978-5-16-103378-4 (online). — Текст : электронный. — URL: <https://new.znaniium.com/catalog/product/959864> (дата обращения: 16.05.2022)

Дополнительная литература

36. Сычев, Ю. Н. Защита информации и информационная безопасность: учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znaniium.ru/catalog/product/1912987> (дата обращения: 15.09.2024). — Режим доступа: по подписке.
37. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В.Я. Ищейнов, М.В. Мещатунян. — Москва : ИНФРА-М, 2024. — 256 с. — (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст : электронный. - URL: <https://znaniium.ru/catalog/product/2139841> (дата обращения: 15.09.2024). — Режим доступа: по подписке.
38. 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: 16.05.2022). -- Режим доступа: для авториз. пользователей.
39. Организация хранения электронных документов[Текст] / М. В. Ларин, В. Ф. Янковая // Современные технологии делопроизводства и документооборота. - 2013. - № 5. - С. 6-17.
40. Некраха А.В. Шевцова Г.А. Организация конфиденциального делопроизводства и защита

- информации. М., 2007.
41. 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: 16.05.2022).
 42. Резник, С. Д. Преподаватель вуза: технологии и организация деятельности : учебник / С.Д. Резник, О.А. Вдовина ; под общ. ред. С.Д. Резника. — 2-е изд., перераб. — Москва : ИНФРА-М, 2019. — 339 с. — (Менеджмент в высшей школе). — www.dx.doi.org/10.12737/textbook_5c21d9297bb760.62805950. - ISBN 978-5-16-107286-8. - Текст : электронный. — URL: <https://new.znanium.com/catalog/product/1003448> (дата обращения: 16.05.2022).
 43. Гальперин П.Я. Введение в психологию : учеб. пособие / П. Я. Гальперин. - 7-е изд. - М. : Кн. дом "Ун-т", 2007. - 327 с. ; 20 см. - Библиогр. : с. 309-314 (98 назв.). - ISBN 978-5-98227-284-3 : 143.00..
 44. Мильситова, С.В. Педагогические теории, системы и технологии : учебное пособие / С.В. Мильситова. — Кемерово : КемГУ, 2011. — 197 с. — ISBN 978-5-8353-1202-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/30018> (дата обращения: 10.04.2022). -- Режим доступа: для авториз. пользователей.

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.

Ресурсы Интернет

1. Информационно-справочная система «КонсультантПлюс». <http://www.consultant.ru>
2. Информационно-справочная система «Гарант». <http://www.garant.ru>
3. Совет безопасности Российской Федерации [официальный сайт]. <http://www.scrf.gov.ru/>
4. Федеральная служба по техническому и экспортному контролю [официальный сайт]. <http://fstec.ru>
5. Методические пособия, рекомендации, перечни [официальный сайт Федерального архивного агентства]. <http://archives.ru/documents/methodics.shtml>.
6. Информационная безопасность организаций банковской системы Российской Федерации [официальный сайт Центрального банка Российской Федерации]. http://www.cbr.ru/credit/gubzi_docs
7. Институт информационных наук и технологий безопасности РГГУ [официальный сайт], <http://www.rsuh.ru/iintb>

7. Материально-техническое обеспечение научно-педагогической 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 Гб. 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 Statistics 22	IBM	лицензионное
7	Microsoft Share Point 2010	Microsoft	лицензионное
8	SPSS Statistics 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:

- Пираня - 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 Mk2 - 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 x 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 научно-педагогической практики

для подготовки аспирантов

2.3. Информационные технологии и телекоммуникации. 2.3.6. Методы и системы защиты информации, информационная безопасность

Автор (составитель):

Д.А. Митюшин, кандидат технических наук
 (Инициалы, фамилия, уч. степень, уч. звание)

_____ (подпись)

Лист изменений
в рабочей программе научно-педагогической практики
2.3. Информационные технологии и телекоммуникации.
2.3.6. Методы и системы защиты информации, информационная безопасность
(Шифр и наименование научной специальности)

№ п/п	Дата внесения изменений	Дата и № протокола заседания кафедры	Содержание изменения	Подпись