

**федеральное государственное автономное образовательное
учреждение высшего образования
«Национальный исследовательский университет ИТМО»
(Университет ИТМО)**

УТВЕРЖДАЮ
Проректор по научной работе
_____ В.О. Никифоров
« ____ » _____ 2022 г.
м.п.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность научных исследований

Группа научной специальности: все группы научных специальностей

Научной специальности: все научные специальности

Форма обучения: Очная

Санкт-Петербург
2022 г.

Рабочая программа составлена на основании Требований к программам подготовки научных и научно-педагогических кадров в аспирантуре, самостоятельно устанавливаемых федеральным государственным автономным образовательным учреждением высшего образования «Национальный исследовательский университет ИТМО»:

Код и наименование группы научной специальности	Реквизиты приказа об утверждении Требований Университета ИТМО
1.1.Математика и механика 1.2.Компьютерные науки и информатика 1.3.Физические науки 1.4.Химические науки 1.5.Биологические науки 1.6.Науки о Земле и окружающей среде 2.1.Строительство и архитектура 2.2.Электроника, фотоника, приборостроение и связь 2.3.Информационные технологии и телекоммуникации 2.4.Энергетика и электротехника 2.5.Машиностроение 2.6.Химические технологии, науки о материалах, металлургия 2.7.Биотехнологии 4.3.Агроинженерия и пищевые технологии 5.2.Экономика 5.5.Политические науки 5.7.Философия	Приказ ректора №325-од от 31.03.2022 Решение Научно-Технического совета №12 от 28.03.2022

Программу разработал: Комаров И.И., к.ф.-м.н., доцент

Программа одобрена на заседании НТС Университета ИТМО протокол №12 от 28 марта 2022 года.

Место дисциплины в структуре учебного плана:

Блок 2, Образовательный компонент

Форма обучения: очная

Год обучения: 1

Семестр: 2

Форма аттестации: зачёт

Вид деятельности	Семестр
	2
Занятий в контактной форме, час.	18
из них лекции, час.	2
из них научно-практических занятий, час.	14
из них промежуточной аттестации (включая консультации), час.	2
Самостоятельная работа, час.	54
Всего часов	72
Всего зачётных единиц	2

Аннотация к рабочей программе дисциплины «Информационная безопасность научных исследований»

Дисциплина «Информационная безопасность научных исследований» реализуется в рамках образовательных программ высшего образования – программ подготовки научно-педагогических кадров в аспирантуре по очной форме обучения на русском языке.

Разделы рабочей программы

1. Место дисциплины в структуре программы аспирантуры.
2. Планируемые результаты обучения по дисциплине.
3. Структура и содержание дисциплины.
4. Текущий контроль и промежуточная аттестация.
5. Учебно-методическое и информационное обеспечение дисциплины.
6. Материально-техническое обеспечение дисциплины.
7. Фонды оценочных средств текущего контроля и промежуточной аттестации.

1. Место дисциплины в структуре программы аспирантуры

Дисциплина «Информационная безопасность научных исследований» реализуется во втором семестре в рамках Образовательного компонента Блока 2 и является основной для освоения программы подготовки в аспирантуре. Дисциплина «Информационная безопасность научных исследований» акцентирует внимание на концептуальных проблемах, современных вызовах и путях их преодоления в области информационной безопасности процессов научного исследования и внедрения его результатов в практику. Дисциплина обеспечивает подготовку аспирантов к комплексному пониманию процессов обеспечения информационной безопасности и практическому обеспечению информационной безопасности производственного и личного информационного пространства.

2. Планируемые результаты обучения по дисциплине

Дисциплина «Информационная безопасность научных исследований» направлена на формирование

универсальных компетенций:

УК-1 - 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-4 - Готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках;

общепрофессиональных компетенций:

ОПК-1 - Способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий;

ОПК-2 - Готовность к преподавательской деятельности по основным образовательным программам высшего образования *в части следующих результатов обучения:*

Формируемые компетенции (код компетенции)	Планируемые результаты обучения по дисциплине (модулю)
---	--

УК-1	<p>Знать: ЗЗ (УК-1) основные проблемы внедрения научных разработок в практическую деятельность.</p> <p>Уметь: УЗ (УК-1) формулировать альтернативные варианты решения исследовательских и практических задач.</p> <p>Владеть (иметь опыт): В1 (УК-1) навыками сбора, обработки, анализа и систематизации информации по теме исследования. В2 (УК-1) навыками выбора методов и средств решения задач исследования.</p>
УК-4	<p>Знать: З1 (УК-4) методы и технологии научной коммуникации на государственном и иностранном языках.</p> <p>Владеть: ВЗ (УК-4) различными методами, технологиями и типами коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках.</p>
ОПК-1	<p>Уметь: У1 (ОПК-1) выбирать и применять в научно-исследовательской деятельности современные информационно-коммуникационные технологии.</p> <p>УЗ (ОПК-1) формировать предложения по масштабированию информационно-коммуникационных технологий, применяемых в ходе научного исследования, для решения задач реального сектора экономики.</p> <p>Владеть: В1 (ОПК-1) навыками использования информационно-коммуникационных технологий при поиске и анализе информации, в том числе по тематике проводимых научных исследований.</p>
ОПК-2	<p>Уметь: У5 (ОПК-2) применять электронные образовательные и информационные ресурсы, необходимые для реализации учебных курсов, дисциплин (модулей), организации исследовательской, проектной и иной деятельности обучающихся.</p>

Способы формирования планируемых результатов обучения

Результаты изучения дисциплины по уровням освоения (знать, уметь, владеть)	Формы организации занятий		
	Лекции	Научно-практические занятия	Самостоятельная работа
УК-1 - Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях			
ЗЗ (УК-1) основные проблемы внедрения научных разработок в практическую деятельность.	+		+
УЗ (УК-1) формулировать альтернативные варианты решения исследовательских и практических задач.		+	+
В1 (УК-1) навыками сбора, обработки, анализа и систематизации информации по теме исследования.		+	+
В2 (УК-1) навыками выбора методов и средств решения задач исследования.		+	+
УК-4 - Готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках			
З1 (УК-4) методы и технологии научной коммуникации на государственном и иностранном языках.	+		+
ВЗ (УК-4) различными методами, технологиями и типами коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках.		+	+
ОПК-1 - Способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий			
У1 (ОПК-1) выбирать и применять в научно-исследовательской деятельности современные информационно-коммуникационные технологии.	+	+	+
УЗ (ОПК-1) формировать предложения по масштабированию информационно-коммуникационных технологий, применяемых в ходе научного исследования,		+	+

для решения задач реального сектора экономики.			
В1 (ОПК-1) навыками использования информационно-коммуникационных технологий при поиске и анализе информации, в том числе по тематике проводимых научных исследований.		+	+
ОПК-2 - Готовность к преподавательской деятельности по основным образовательным программам высшего образования			
У5 (ОПК-2) применять электронные образовательные и информационные ресурсы, необходимые для реализации учебных курсов, дисциплин (модулей), организации исследовательской, проектной и иной деятельности обучающихся.	+	+	+

3. Структура и содержание дисциплины

Изучение курса «Информационная безопасность научных исследований» включает в себя лекции, на которых рассматривается теоретическое содержание курса. научно-практические занятия, предусматривающие углублённое изучение и обсуждение вопросов, обозначенных в темах дисциплины. самостоятельную работу, заключающуюся в подготовке к лекционным и научно-практическим занятиям. Темы, рассматриваемые на лекциях и изучаемые самостоятельно, закрепляются на научно-практических занятиях, по вопросам, вызывающим затруднения, проводятся консультации.

Структура дисциплины:

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоёмкость, часы					Форма текущего контроля успеваемости, промежуточной аттестации
		Всего часов	Лекции	Научно-практические занятия	Зачёт	Самостоятельная работа	
1.	Концептуальные проблемы информационной безопасности	10,5	0,5	2		8	Опрос, собеседование, представление и защита промежуточных результатов итоговой
2	Правовые основы информационной безопасности	8,5	0,5	2		6	

3	Технологии защиты информации	24,5	0,5	8		16	письменной работы
4	Перспективные технологии информационной безопасности.	10,5	0,5	2		8	
5	Промежуточная аттестация	2			2	16	Зачёт в письменной форме с последующим собеседованием
ИТОГО:		72	2	14	2	54	

Содержание дисциплины:

№ п/п	Наименование раздела дисциплины	Содержание	Ссылки на результаты обучения
1	Концептуальные проблемы информационной безопасности	Понятия «информационная безопасность» и «защита информации». Базовые понятия информационной безопасности и их взаимосвязь. Варианты трактовок. Эволюция терминов. Формы и виды защищаемой информации.	33 (УК-1) У3 (УК-1) В1 (УК-1) В2 (УК-1) 31 (УК-4) В3 (УК-4) У1 (ОПК-1) У3 (ОПК-1) В1 (ОПК-1) У5 (ОПК-2)
		Взаимосвязи основных этапов научного исследования и задач обеспечения информационной безопасности.	
		Концептуальные проблемы информационной безопасности	
		Проблемы и задачи информационной безопасности в предметной области диссертационного исследования	
2	Правовые основы информационной безопасности	Правовые и экономические аспекты отношений, связанных с ИБ.	
		Уполномоченные государственные и международные органы (организации), выполняющие функции, связанные с урегулированием отношений в области информационной безопасности.	
		Иерархия организационно-правовых актов в области информационной безопасности	

		Основные этапы деятельности по обеспечению информационной безопасности организации.	
3	Технологии защиты информации	Виды обеспечения информационной безопасности. Защита компьютерной информации.	
		Научно-методические основы защиты информации.	
		Принципы и технологии защиты информации.	
		Модель угроз и модель нарушителя ИБ. Понятие политики безопасности.	
		Программные средства защиты информации.	
		Аппаратные средства защиты информации	
		Комплексные системы защиты информации	
		Особенности обеспечения ИБ распределённых систем.	
4	Перспективные технологии информационной безопасности.	Специфика перспективных информационных систем. «Мягкая» информационная безопасность.	
		Обеспечение ИБ мультиагентных систем.	
		Обеспечение информационной безопасности киберфизических систем.	
		Информационная безопасность систем искусственного интеллекта.	
		Информационная безопасность постквантовой криптографии	

Виды учебной и самостоятельной работы

Виды учебной работы	Ссылки на результаты обучения	Часы
На основе изучения литературы по теме лекционных и научно-практических занятия готовится к ответу с места на предложенные вопросы, к участию в дискуссиях, к тестированию по изученному материалу	33 (УК-1) У3 (УК-1) В1 (УК-1) В2 (УК-1) 31 (УК-4) В3 (УК-4) У1 (ОПК-1) У3 (ОПК-1) В1 (ОПК-1) У5 (ОПК-2)	18
Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение
Самостоятельная подготовка к лекционным и научно-практическим занятиям	33 (УК-1) У3 (УК-1) В1 (УК-1) В2 (УК-1) 31 (УК-4) В3 (УК-4) У1 (ОПК-1) У3 (ОПК-1) В1 (ОПК-1) У5 (ОПК-2)	54
Успешное освоение материала, изучаемого в ходе лекционных и научно-практических занятия, требует дополнительного самостоятельного изучения. По каждому разделу учебной дисциплины предусмотрено изучение теоретического материала с использованием компьютерных технологий. самостоятельное изучение теоретического материала дисциплины с использованием Internet-ресурсов, информационных баз, методических разработок, специальной учебной и научной литературы.		

4. Текущий контроль и промежуточная аттестация

Текущая аттестация по дисциплине «Информационная безопасность научных исследований» осуществляется на лекциях и научно-практических занятиях и заключается в оценке качества предоставляемого промежуточного материала, степени его применимости для диссертационного исследования аспиранта, обоснованности и аргументированности позиции его представления. В ходе текущего контроля также оценивается активность участия в опросах и собеседованиях по проблемам, изучаемых в рамках тем лекционных и научно-практических занятий.

Промежуточная аттестация по дисциплине «Информационная безопасность научных исследований» проводится во втором семестре в форме итоговой письменной работы с последующем её представлением (собеседованием). Оценка по результатам

собеседования выставляется в формате «зачтено» - «не зачтено». Оценка «зачтено» подразумевает удовлетворительное освоение дисциплины и выставляется аспиранту в случае, если он в результате собеседования демонстрирует сформированность общих представлений о проблемах и вызовах обеспечения информационной безопасности своей предметной области, методах и средствах технической защиты информации. демонстрирует наличие базовых представлений о нормативно-правовых и программно-технических аспектах защиты информации.

В качестве итоговой письменной работы аспиранту могут быть зачтены следующие результаты, **соответствующие содержанию дисциплины:**

- публикация в изданиях, входящих в «ПЕРЕЧЕНЬ рецензируемых научных изданий, в которых должны быть опубликованы основные научные результаты диссертаций на соискание учёной степени кандидата наук, на соискание учёной степени доктора наук».

- публикация в рецензируемых изданиях, индексируемых наукометрическими базами Web of Science и/или Scopus.

- РИД, подтверждаемые следующими охранными документами: патентами, свидетельствами о регистрации полезной модели, заявками на получение патента или свидетельства о регистрации полезной модели, прошедших формальную экспертизу.

В любом случае аспирантом готовится итоговая письменная работа с обоснованием соответствия представляемого материала содержанию дисциплины и описанием роли и доли личного участия в результатах, полученных коллективом авторов.

5. Учебно-методическое и информационное обеспечение дисциплины

Учебно-методическое и программное обеспечение дисциплины размещено на образовательном портале Университета ИТМО.

Профессиональные базы данных, интернет-ресурсы, электронные библиотеки и информационные справочные системы:

№	Ссылка на информационный ресурс	Наименование разработки в электронной форме	Доступность
1.	https://digital.gov.ru/ru/documents/	Официальный портал документов Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации	Индивидуальный неограниченный доступ
2.	http://www.fsb.ru/fsb/npd.htm	Нормативные правовые акты Федеральной службы безопасности РФ	Индивидуальный неограниченный доступ
3.	https://fstec.ru/ekspornyj-kontrol/zakonodatelstvo#	Федеральная служба по техническому и экспортному контролю. Законодательство в области экспортного контроля	Индивидуальный неограниченный доступ

4.	https://bdu.fstec.ru/	Банк данных угроз безопасности информации ФСТЭК РФ	Индивидуальный неограниченный доступ
5.	https://habr.com/ru/post/432466/	Авторский справочник законодательства РФ в области информационной безопасности	Индивидуальный неограниченный доступ
6.	http://www.iso27000.ru/	Портал профессионального сообщества в области информационной безопасности	Индивидуальный неограниченный доступ
7.	https://attack.mitre.org/	Открытая международная база данных по техникам и тактикам компьютерных атак	Индивидуальный неограниченный доступ
8.	https://owasp.org/	Открытый международный проект по обеспечению информационной безопасности Web-приложений.	Индивидуальный неограниченный доступ
9.	http://e.lanbook.com/	ЭБС на платформе «Лань». Учебники и учебные пособия для университетов издательства «Лань»	Индивидуальный неограниченный доступ
10.	http://lib.ifmo.ru/	Электронная библиотека НИУ ИТМО.	Индивидуальный неограниченный доступ
11.	http://elibrary.ru/	Научная электронная библиотека (РИНЦ)	Индивидуальный неограниченный доступ
12.	http://window.edu.ru/	Библиотека. Единое окно доступа к информационным ресурсам	Индивидуальный неограниченный доступ
13.	http://elbib.ru/	Российская электронная библиотека	Индивидуальный неограниченный доступ
14.	http://public.ru/	Публичная Интернет-библиотека	Индивидуальный неограниченный доступ

Основная литература:

1. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование: учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Издательство Юрайт, 2018. — 220 с. — (Серия: Университеты России). — ISBN 978-5-9916-9244-1. — Режим доступа: URL: www.biblio-online.ru/book/6946C235-8650-4A29-B75B-68E0EF829422.

2. Зенков А. Информационная безопасность и защита информации. Учебное пособие для вузов. — Litres, 2022, URL: <https://urait.ru/book/E629B901-41C2-44E3-B43F-603C50FAF668>

3. Малюк, А. А. Защита информации в информационном обществе: учебное пособие / А. А. Малюк. — Москва: Горячая линия-Телеком, 2017. — 230 с. — ISBN 978-5-9912-0481-1. — Текст: электронный// Лань: электронно-библиотечная система. — URL: <https://e.lanbook.com/book/111078>

4. Организационное и правовое обеспечение информационной безопасности. Учебник и практикум для вузов - Yurayt, 2022, URL: <https://urait.ru/book/FE30EC8C-081B-428D-A896-BE5081525F24>

5. Суворова Г. М. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Учебное пособие для вузов – Yurayt, 2022, URL: <https://urait.ru/book/C82E0F9F-10D5-4392-B35D-60A4F0D6DCCF>

6. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие / В.Ф. Шаньгин. — Москва: ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1189327>

7. Щеглов А. Ю., Щеглов К. А. Защита информации: основы теории. Учебник для вузов - Yurayt, 2022, URL: <https://urait.ru/book/9350B7A2-D18F-4A90-A15C-A5502EFB9995>

8. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — М.: Издательство Юрайт, 2018. — 309 с. — (Серия: Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Режим доступа: URL:www.biblio-online.ru/book/9CD7BE3A-F9DC-4F6D-8EC6-6A90CB9A4E0E.

Дополнительная литература:

1. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва: ДМК Пресс, 2017. — 434 с. — Режим доступа: <https://e.lanbook.com/book/93278>. — Загл. с экрана.

2. Гуманитарные аспекты информационной безопасности: основные понятия, логические основы и операции [Электронный ресурс]: учеб. пособие / Э.П. Теплов [и др.]. — Электрон. дан. — Санкт-Петербург: НИУ ИТМО, 2016. — 122 с. — Режим доступа: <https://e.lanbook.com/book/91401>. — Загл. с экрана.

3. Девянин, П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками [Электронный ресурс]: учеб. пособие — Электрон. дан. — Москва: Горячая линия-Телеком, 2013. — 338 с. — Режим доступа: <https://e.lanbook.com/book/63235>. — Загл. с экрана.

4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — М.: Издательство Юрайт, 2018. — 312 с. — (Серия: Специалист). — ISBN 978-5-9916-9043-0. — Режим доступа : www.biblio-online.ru/book/E458AFCD-826E-4A1F-9BAB-68BB83EA616F.

5. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности [Электронный ресурс]: учеб. пособие / Н.С. Кармановский, О.В. Михайличенко, Н.Н. Прохожев. — Электрон. дан. — Санкт-Петербург: НИУ ИТМО, 2016. — 168 с. — Режим доступа: <https://e.lanbook.com/book/91449>. — Загл. с экрана.

6. Каторин Ю. Ф. и др. Большая энциклопедия промышленного шпионажа. – Полигон, 2000.

7. Семь безопасных информационных технологий [Электронный ресурс]: учеб. / А.В. Барабанов [и др.]. — Электрон. дан. — Москва: ДМК Пресс, 2017. — 224 с. — Режим доступа: <https://e.lanbook.com/book/97352>. — Загл. с экрана.

8. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников. под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2018. — 209 с. —

(Серия: Бакалавр. Академический курс). — ISBN 978-5-9916-7088-3. — Режим доступа: www.biblio-online.ru/book/C0328DC2-2A46-4945-994F-04F661095B83.

9. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников. под ред. В. М. Фомичёва. — М.: Издательство Юрайт, 2018. — 245 с. — (Серия: Бакалавр. Академический курс). — ISBN 978-5-9916-7090-6. — Режим доступа: www.biblio-online.ru/book/AF99BBDE-AF3A-43A9-A90F-B99806553C25.

10. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс]: учеб. пособие — Электрон. дан. — Москва: ДМК Пресс, 2014. — 702 с. — Режим доступа: <https://e.lanbook.com/book/50578>. — Загл. с экрана

Аспиранту настоятельно рекомендуется использовать дополнительные актуальные источники информации (прежде всего научные статьи, обзоры, материалы производителей и интеграторов информационных систем и систем защиты информации), отражающие специфику материала дисциплины применительно к тематике собственного научного исследования.

Средства, обеспечивающие адаптацию электронных и печатных образовательных ресурсов для обучающихся из числа лиц с инвалидностью и ограниченными возможностями здоровья:

1) Доступ к изданиям электронно-библиотечной системы «Издательство «Лань» (<https://e.lanbook.com>), в адаптированных форматах для лиц с инвалидностью и ОВЗ.

2) Специальные технические средства обучения коллективного и индивидуального пользования для лиц с инвалидностью и ОВЗ:

а) В библиотеке по адресам Кронверкский пр., д.49 и ул. Ломоносова, д.9 обучающимся, имеющим нарушения зрения, предоставляется компьютерное место с клавиатурой, маркированной шрифтом Брайля, и увеличительные лупы нового поколения с подсветкой и семикратным увеличением (лупы настольные с подсветкой PowerLux).

3) Услуги по адаптации учебно-методического материала для лиц с инвалидностью и ОВЗ:

а) обучающиеся с нарушениями зрения по запросу могут получить специальную учебную, научную литературу и периодические издания на основании действующего договора о сотрудничестве между Университетом ИТМО и Государственной библиотекой для слепых и слабовидящих. для обучающихся с нарушениями зрения учебные материалы могут быть предложены на шрифте Брайля.

б) обучающимся с нарушениями слуха по запросу предоставляются услуги сурдопереводчика на основании договора между Университетом ИТМО и «Всероссийским обществом глухих» (СПб РО ООИ ВОГ).

6. Материально-техническое обеспечение дисциплины

Программное обеспечение:

Для обеспечения реализации дисциплины используется стандартный комплект программного обеспечения (ПО), включающий регулярно обновляемое лицензионное ПО Windows и MS Office.

Использование специализированного программного обеспечения для изучения дисциплины не требуется.

Наименование специальных помещений и помещений для самостоятельной работы	Оснащённость специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения.
Занятия лекционного типа:		
мультимедийный класс	аудитория, оснащённая презентационной техникой (проектор, экран, компьютер/ноутбук)	Операционная система Windows Professional 8 Russian Upgrade OLP Academic Edition
Занятия практического типа:		
мультимедийный класс, компьютерный класс	аудитория, оснащённая презентационной техникой (проектор, экран, компьютер/ноутбук)	Операционная система Windows Professional 8 Russian Upgrade OLP Academic Edition
Самостоятельная работа:		
компьютерный класс	15 персональных компьютеров в составе локальной вычислительной сети, подключённой к Internet (30 Мбит/с).	Операционная система Windows Professional 8 Russian Upgrade OLP Academic Edition

7. Фонды оценочных средств текущего контроля и промежуточной аттестации

Требования к структуре и содержанию фонда оценочных средств текущего контроля и промежуточной аттестации по дисциплине

Перечень оценочных средств, применяемых на каждом этапе проведения текущего контроля и промежуточной аттестации по дисциплине, представлены в таблице

Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
Оценочные средства текущего контроля		
Проблемная дискуссия	Средство контроля, организованное как общая беседа по наиболее сложным и неоднозначным вопросам теории и практики обеспечения информационной безопасности процесса научных исследований, рассчитанное на выяснение	Формы и виды защищаемой информации. Правовые и экономические аспекты отношений, связанных с ИБ. Взаимосвязи основных этапов научного исследования и задач обеспечения информационной безопасности. Концептуальные проблемы

	<p>объёма и качества знаний, и понимание концептуальных вопросов обеспечения информационной безопасности.</p>	<p>информационной безопасности. Проблемы и задачи информационной безопасности в предметной области диссертационного исследования. Специфика перспективных информационных систем. «Мягкая» информационная безопасность. Обеспечение ИБ мультиагентных систем. Обеспечение информационной безопасности киберфизических систем. Информационная безопасность систем искусственного интеллекта. Информационная безопасность постквантовой криптографии</p>
<p>Представление и защита промежуточного материала итоговой письменной работы</p>	<p>Средство контроля, используемое на научно-практических занятиях и организованное как представление и защита документированных промежуточных материалов итоговой письменной работы, последовательно реализующей этапы:</p> <ul style="list-style-type: none"> - описание и формализация объекта защиты. - определение организационно-правового поля обеспечения информационной безопасности объекта защиты. - определение актуальных угроз информационной безопасности объекта защиты. - обоснование перечня мер по обеспечению информационной безопасности объекта защиты. - элементы технико-экономического анализа (или оценки эффективности) предлагаемого комплекса мероприятий по обеспечению информационной безопасности объекта защиты. <p>Контроль рассчитан на выявление степени владения материалом, связанным с обеспечением информационной безопасности научных исследований, уровня обоснованности и аргументированности собственной позиции.</p>	<p>Базовые понятия информационной безопасности и их взаимосвязь. Правовые и экономические аспекты отношений, связанных с ИБ. Содержание защищаемой информации. Научно-методические основы защиты информации. Принципы и технологии защиты информации. Модель угроз и модель нарушителя ИБ. Понятие политики безопасности. Программные средства защиты информации. Аппаратные средства защиты информации. Комплексные системы защиты информации. Особенности обеспечения ИБ распределённых систем.</p>

Оценочные средства промежуточной аттестации

Итоговая письменная работа	Средство, позволяющее оценить сформированность систематических знаний, умений и навыков владения в области обеспечения информационной безопасности научных исследований	Типовые тематики и требования к структуре и содержанию итоговой письменной работы
Собеседование	Средство, позволяющее получить экспертную оценку знаний, умений и навыков в области обеспечения информационной безопасности научных исследований	Требования к порядку проведения собеседования

Критерии сформированности компетенций

Код формируемой компетенции	Планируемые результаты обучения по дисциплине	Не сформировано	Сформировано
УК-1	ЗЗ (УК-1) основные проблемы внедрения научных разработок в практическую деятельность	Отсутствие знаний об основных проблемах внедрения научных разработок в практическую деятельность с точки зрения информационной безопасности.	Сформированные знания об основных проблемах внедрения научных разработок в практическую деятельность с точки зрения информационной безопасности.
	УЗ (УК-1) формулировать альтернативные варианты решения исследовательских и практических задач	Отсутствие умения формулировать альтернативные варианты решения исследовательских и практических задач для преодоления проблем информационной безопасности и/или выполнения нормативных требований органов-регуляторов.	Наличие умения формулировать альтернативные варианты решения исследовательских и практических задач для преодоления проблем информационной безопасности и/или выполнения нормативных требований органов-регуляторов.
	В1 (УК-1) навыками сбора, обработки, анализа и систематизации информации по теме исследования	Отсутствие навыков сбора, обработки, анализа и систематизации информации по теме исследования с учётом выполнения требований по обеспечению информационной безопасности научных исследований.	Наличие навыков сбора, обработки, анализа и систематизации информации по теме исследования с учётом выполнения требований по обеспечению информационной безопасности научных исследований.
	В2 (УК-1) навыками выбора методов и средств решения задач исследования	Отсутствие навыков выбора методов и средств решения задач исследования с учётом требований обеспечения информационной безопасности научных исследований.	Наличие навыков выбора методов и средств решения задач исследования с учётом требований обеспечения информационной безопасности научных исследований.
ОПК-1	У1 (ОПК-1) выбирать и применять в научно-исследовательской деятельности современные информационно-коммуникационные технологии	Отсутствие умения выбирать и применять в научно-исследовательской деятельности современные информационно-коммуникационные технологии с учётом требований обеспечения информационной безопасности научных исследований.	Сформированные умения выбирать и применять в научно-исследовательской деятельности современные информационно-коммуникационные технологии с учётом требований обеспечения информационной безопасности научных исследований.
	УЗ (ОПК-1) формировать предложения по масштабированию информационно-коммуникационных технологий, применяемых в ходе научного исследования, для решения задач реального сектора экономики	Отсутствие умения формировать предложения по масштабированию информационно-коммуникационных технологий, применяемых в ходе научного исследования, для решения задач реального сектора экономики с учётом требований обеспечения информационной безопасности.	Сформированные умения формировать предложения по масштабированию информационно-коммуникационных технологий, применяемых в ходе научного исследования, для решения задач реального сектора экономики с учётом требований обеспечения информационной безопасности.

	В1 (ОПК-1) навыками использования информационно-коммуникационных технологий при поиске и анализе информации, в том числе по тематике проводимых научных исследований	Отсутствие навыков использования информационно-коммуникационных технологий при поиске и анализе информации, в том числе по тематике проводимых научных исследований, а также вопросам обеспечения информационной безопасности.	Наличие навыков использования информационно-коммуникационных технологий при поиске и анализе информации, в том числе по тематике проводимых научных исследований, а также вопросам обеспечения информационной безопасности.
ОПК-2	У5 (ОПК-2) применять электронные образовательные и информационные ресурсы, необходимые для реализации учебных курсов, дисциплин (модулей), организации исследовательской, проектной и иной деятельности обучающихся	Отсутствие умения применять электронные образовательные и информационные ресурсы, необходимые для реализации учебных курсов, дисциплин (модулей), организации исследовательской, проектной и иной деятельности обучающихся с соблюдением требований по информационной безопасности.	Сформированные умения применять электронные образовательные и информационные ресурсы, необходимые для реализации учебных курсов, дисциплин (модулей), организации исследовательской, проектной и иной деятельности обучающихся с соблюдением требований по информационной безопасности.

Требования к структуре и содержанию оценочных средств

Требования к порядку проведения зачёта в виде итоговой письменной работы:

Зачёт проводится в форме предоставления и защиты итоговой письменной работы, выполняемой в ходе освоения дисциплины.

Время на выполнения итоговой письменной работы предусмотрено в СРО. Промежуточные результаты работы представляются и аргументируются аспирантом на научно-практических занятиях согласно расписанию занятия и типовому плану выполнения итоговой письменной работы, утверждаемом преподавателем на первом научно-практическом занятии в группе.

Защита итоговой письменной работы состоит в кратком (5-7 минут) публичном докладе, освещающем задачи итоговой письменной работы, ключевые этапы их решения и результаты. Аспиранту могут быть заданы дополнительные вопросы как в рамках итоговой письменной работы, так и в рамках изученного курса.

Критерии выставления оценки:

Знания, умения и навыки обучающихся при промежуточном контроле в форме зачёта определяются оценками «зачтено» и «незачтено».

Оценка «зачтено» подразумевает удовлетворительное освоение дисциплины и выставляется аспиранту в случае, если он:

- своевременно представил материал итоговой письменной работы, соответствующий предъявляемым требованиям по структуре, содержанию, авторскому наполнению и оформлению на оценку не ниже «удовлетворительно» согласно критериям, представленным в таблице. **Работы, имеющие признаки некорректного заимствования (плагиата) не рассматриваются и до защиты не допускаются.**

- в результате доклада по итоговой письменной работе и ответа на вопросы преподавателя аспирант демонстрирует усвоение программного материала, способен грамотно изложить его, может правильно применять теоретические положения и владеет специальной терминологией, продемонстрировал необходимые умения и навыки при выполнении заданий по дисциплине.

Оценка «незачтено» подразумевает неудовлетворительное освоение дисциплины и выставляется аспиранту в любом из случаев:

- если он получил неудовлетворительную оценку за итоговую письменную работу.
- в результате собеседования допускает существенные ошибки.
- демонстрирует отсутствие навыков при выполнении заданий по дисциплине.

Требования к итоговой письменной работе		Оценка			
		Отл.	Хор.	Удовл.	Неуд.
1. Новизна итоговой письменной работы	<ul style="list-style-type: none">актуальность проблемы и темы.новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы.наличие авторской позиции, самостоятельность суждений.	5-4	5-4	5-3	наличие хотя бы одной неудовлетворительной оценки
2. Степень раскрытия сущности проблемы	<ul style="list-style-type: none">соответствие плана теме итоговой письменной работы.соответствие содержания теме и плану итоговой письменной работы.	5	5-4	5-3	

Требования к итоговой письменной работе		Оценка			
		Отл.	Хор.	Удовл.	Неуд.
	<ul style="list-style-type: none"> полнота и глубина раскрытия основных понятий проблемы. обоснованность способов и методов работы с материалом. умение работать с литературой, систематизировать и структурировать материал. умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы. 				
3. Обоснованность выбора источников	<ul style="list-style-type: none"> круг, полнота использования литературных источников по проблеме. привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.). 	5-4	5-3	5-3	
4. Соблюдение требований к оформлению	<ul style="list-style-type: none"> правильное оформление ссылок на используемые источники. грамотность и культура изложения. владение терминологией и понятийным аппаратом проблемы. соблюдение требований к объёму итоговой письменной работы. культура оформления: выделение абзацев. 	5	5	5-4	
5. Грамотность	<ul style="list-style-type: none"> отсутствие орфографических и синтаксических ошибок, стилистических погрешностей. отсутствие опечаток, сокращений слов, кроме общепринятых. литературный стиль. 	5	5-4	5-3	
6. Качество презентации	<ul style="list-style-type: none"> наличие презентации логичность и последовательность подачи материала. использование мнемосхем, и средств визуализации сложных вопросов, данных, зависимостей. соблюдение корпоративного стиля. 	5-3	5-3	не оценивается	
8 Соблюдение графика работ	Своевременность представления и защиты отчёта	в срок	Опозд. до след-го занятия	Опозд. более 2-х занятий	

Темы итоговой письменной работы аспиранта должны адаптироваться к конкретным условиям и требованиям, определяемым тематикой его диссертационного исследования.

Перечень примерных тем итоговой письменной работы:

- Обоснование комплекса мероприятий по обеспечению информационной безопасности процесса научных исследований.
- Концептуальные противоречия информационной безопасности в (отрасли знаний аспиранта) и пути их разрешения.
- Прогнозирование рисков и угроз информационной безопасности (согласно отрасли исследований аспиранта).

- Модели и методы управления информационной безопасностью производства (согласно отрасли исследований аспиранта).
- Применение программного/аппаратного/программно-аппаратного средства обеспечения информационной безопасности процесса научных исследований.
- Разработка организационных документов в области защиты информации производства (согласно отрасли исследований аспиранта).
- Выбор и обоснование технологии научной коммуникации с учётом требований по обеспечению информационной безопасности.
- Выбор и обоснование технологии реализации учебных курсов/дисциплин/модулей/исследовательской/ проектной деятельности обучающихся с учётом требований по обеспечению информационной безопасности.
- Перспективные методы/средства обеспечения информационной безопасности (в отрасли исследований аспиранта).
- Прототип ТЗ на разработку компонента системы защиты информации.
- План масштабирования информационно-коммуникационных технологий, применяемых в ходе научного исследования, для решения задач реального сектора экономики с учётом требований по обеспечению информационной безопасности.

Перечень вопросов для самостоятельной работы:

- 1 Алгоритм работы комбинированной системы криптографической защиты информации.
- 2 Архивация и резервное копирование данных.
- 3 Базовые понятия и определения в области информационной безопасности.
- 4 Гаммирование. Принципы получения гаммы.
- 5 Идентификация и аутентификация
- 6 Компьютерные вирусы
- 7 Компьютерные вирусы. Классификация компьютерных вирусов
- 8 Криптографическая защита информации. Основные методы шифрования
- 9 Криптографические системы с открытым ключом. Упрощённый алгоритм проверки подлинности ЭП
- 10 Криптографические системы с открытым ключом. Упрощённый алгоритм заверения электронного документа с помощью ЭП.
- 11 Метод компрометации открытого ключа “men-in-middle”
- 12 Методы архивации данных
- 13 Методы сжатия данных
- 14 Модель нарушителя.
- 15 Несанкционированный доступ к информации
- 16 Организационные меры защиты информации
- 17 Основные каналы реализации угроз безопасности информации и методы противодействия им.
- 18 Основные угрозы безопасности информации в автоматизированных системах.
- 19 Понятие защищённости информационной системы.
- 20 Понятие политики безопасности. Уровни политики безопасности и их содержание.
- 21 Понятия уязвимости, угрозы, атаки на информационную систему
- 22 Правила формирования паролей. Сгенерировать пароли с использованием различных правил.
- 23 Применимость классических задач оптимального управления для обеспечения информационной безопасности

- 24 Проблема постановки задачи управления комплексной системой защиты информации. Подходы к синтезу целевой функции управления комплексной системой защиты информации.
- 25 Резервное копирование данных: принципы, методы, средства.
- 26 Содержание понятий: параметр, критерий, продуктивность, рациональность, эффективность.
- 27 Сравнительная характеристика методов перестановки и гаммирования. Методы атак на них.
- 28 Сравнительная характеристика программных и аппаратных средств идентификации и аутентификации.
- 29 Сравнительная характеристика систем криптографической защиты информации с закрытым и открытым ключом. Области применимости и особенности использования.
- 30 Стандарты и методологии оценки информационной безопасности.
- 31 Характеристика аппаратных средств вычислительной техники с позиции обеспечения безопасности информации.