МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

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

Историко-архивный институт
Факультет истории, политологии и права
Кафедра истории и теории исторической науки

УТВЕРЖДАЮ
Первый проректор-
проректор по научной работе
_____О.В. Павленко
_____ 2019 г.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЪЕКТОВ ЗАЩИТЫ В СОВРЕМЕННЫХ УСЛОВИЯХ

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

«Методы и системы защиты информации, информационная безопасность»

Москва 2019

Обеспечение информационной безопасности объектов защиты в современных условиях
Рабочая программа дисциплины для подготовки аспирантов
Направление подготовки 10.06.01. «Информационная безопасность» Направление программ подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность».

Составитель: Г.А. Шевцова,
Кандидат исторических наук, доцент

Программа утверждена
на заседании кафедры информационной безопасности
28 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

Аннотация

Дисциплина «Обеспечение информационной безопасности объектов защиты в современных условиях» является обязательной дисциплиной направленности программы подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность».

Рабочая программа дисциплины разработана кафедрой информационной безопасности Факультет информационных систем и безопасности Института информационных наук и технологий безопасности РГГУ.

Дисциплина направлена на формирование следующих компетенций:

универсальные (УК):

способностью 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);

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

общепрофессиональные (ОПК):

способностью 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);

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

профессиональные (ПК):

способность самостоятельно осуществлять научно- исследовательскую деятельность в сфере науки, техники и технологии, охватывающие совокупность проблем, связанных с исследованием, разработкой, совершенствованием и применением моделей, методов, технологий, средств и систем защиты информации, а также обеспечением информационной безопасности объектов и процессов обработки, передачи информации во всех сферах деятельности от внешних и внутренних угроз (ПК-1).

Общая трудоёмкость освоения дисциплины составляет 1 зачётную единицу, 36 часов. Программой дисциплины предусмотрены лекционные занятия (12 часов), самостоятельная работа аспиранта (24 часа).

Программой дисциплины предусмотрены следующие виды контроля освоения дисциплины: текущий контроль в форме реферата, промежуточный контроль в форме зачета.

1. Пояснительная записка

Цель дисциплины: Формирование представления о месте и роли защиты объектов информации в современных условиях, ознакомление обучаемых с основами построения системы защиты информации в организации, системного подхода к построению системы менеджмента информационной безопасности с использованием риск-ориентированной оценки и базовыми элементами структуры направленности программы аспирантуры «Методы и системы защиты информации, информационная безопасность».
Методы и системы защиты информации, информационная безопасность – направленность, включающая исследования процессов планирования, создания, использования, контроля и совершенствования системы обеспечения информационной безопасности, накопления и обработки информации по событиям информационной безопасности, методов работы со знаниями, методов машинного обучения; исследования принципов создания и функционирования аппаратных и программных средств защиты информации. Курс дает возможность ознакомиться аспирантам по направлению подготовки 10.06.01 с областями исследований по этой направленности.

Задачи дисциплины:

- приобретение теоретических междисциплинарных знаний в области защиты информации;
- освоение методологии обеспечения информационной безопасности;
- ознакомление со структурой и базовыми элементами изучаемой специальности.

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

Дисциплина «Обеспечение информационной безопасности объектов защиты в современных условиях» является обязательной дисциплиной направленности программы подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность».

универсальные (УК):

способностью 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);

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

общепрофессиональные (ОПК):

способностью 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);

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

профессиональные (ПК):

способность самостоятельно осуществлять научно- исследовательскую деятельность в сфере науки, техники и технологии, охватывающие совокупность проблем, связанных с исследованием, разработкой, совершенствованием и применением моделей, методов, технологий, средств и систем защиты информации, а также обеспечением информационной безопасности объектов и процессов обработки, передачи информации во всех сферах деятельности от внешних и внутренних угроз информационной безопасности (ПК-1).

В результате изучения дисциплины аспирант должен:

знать:

- роль и место защиты информации в системе естественнонаучных знаний, предмет и объекты ее деятельности, аксиоматико-терминологический аппарат;
- основы построения систем защиты информации, информационного подхода к моделированию угроз информационной безопасности, оценке рисков информационной безопасности, а также теории их информационного моделирования;
- непосредственные предметные составляющие специальности;
- область исследования (специальности) и смежные специальности;
- систему ограничений на формулу и область исследований специальности (ОПК-1, ОПК-2, ПК-1, УК-1, УК-4);

уметь:

- использовать методологический аппарат объектов защиты информации для оценки характеристик природных и социально-экономических систем;
- использовать аппарат информационного моделирования исследуемых систем защиты информации для строго формального описания и решения задач выбранной предметной области;
- обосновать выбор направления и темы исследований в рамках выбранной специальности;
- использовать методологический аппарат теоретических основ защиты информации для формирования цели, определения объекта и предмета исследования, постановки проблем и задач в изучаемой предметной области, формирования стратегии достижения цели исследования, решения задач и корректной интерпретации в соответствии с формулой специальности достигнутых результатов и положений (УК-1, УК-4, ОПК-1, ПК-1, ПК-2);

владеть:

- навыками применения полученных знаний в научно-исследовательской работе и научно-педагогической работе

2. Структура дисциплины (тематический план)

Общая трудоемкость освоения дисциплины составляет 1 зачетную единицу, 36 часов.

№ п/п	Раздел дисциплины	Полугодие обучения	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
			Лекции	Практ. занятия	Самостоятельная работа	
1	Информация как основной объект защиты.	2	1	-	Реферирование российской и зарубежной литературы и статей	Реферат/доклад
2	Методологические основы построения систем защиты	2	1	-	1 Реферирование литературных источников и	Реферат/доклад

	информации.				работа в интернет	
3	Методологические основы моделирования угроз и оценки рисков информационной безопасности.	2	1	-	1 Реферирование российской и зарубежной литературы и статей	Реферат/доклад
4	Система менеджмента информационной безопасности: основные аспекты и направления.	2	1	-	2 Реферирование литературных источников и работа в интернет	Реферат/доклад
5	Оценка рисков информационной безопасности	2	1	-	2 Реферирование российской и зарубежной литературы и статей	Реферат/доклад
6	Мониторинг информационной безопасности	2	1	-	2 Реферирование литературных источников и работа в интернет	Реферат/доклад
7	Выявление и управление инцидентами информационной безопасности	2	1	-	2 Реферирование российской и зарубежной литературы и статей	Реферат/доклад
8	Организационные и правовые аспекты защиты информации в современных условиях	2	1	-	2 Реферирование литературных источников и работа в интернет	Реферат/доклад
9	Программно-аппаратные и программные средства и системы защиты информации.	2	2	-	2 Реферирование российской и зарубежной литературы и статей	Реферат/доклад
10	Оценка эффективности системы менеджмента информационной безопасности. Используемые методики оценки.	2	2	-	2 Реферирование литературных источников и работа в интернет	Реферат/доклад
	Подготовка к зачету				8	
	Итого:		**12**		**24**	**Зачет**

Структура дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

№ п/п	Раздел дисциплины	Полу-годие обуче-ния	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
			Лек-ции	Практ. занятия	Самостоятельная работа	
1	Информация как основной объект защиты.	2	1	-	Реферирование российской и зарубежной литературы и статей	Собеседование
2	Методологические основы построения систем защиты информации.	2	1	-	1 Реферирование литературных источников и работа в интернет	Собеседование
3	Методологические основы моделирования угроз и оценки рисков информационной безопасности.	2	1	-	1 Реферирование российской и зарубежной литературы и статей	Собеседование
4	Система менеджмента информационной безопасности: основные аспекты и направления.	2	1	-	2 Реферирование литературных источников и работа в интернет	Собеседование
5	Оценка рисков информационной безопасности	2	1	-	2 Реферирование российской и зарубежной литературы и статей	Собеседование
6	Мониторинг информационной безопасности	2	1	-	2 Реферирование литературных источников и работа в интернет	Собеседование
7	Выявление и управление инцидентами информационной безопасности	2	1	-	2 Реферирование российской и зарубежной литературы и статей	Собеседование

8	Организационные и правовые аспекты защиты информации в современных условиях	2	1	-	2 Реферирование литературных источников и работа в интернет	Собеседование
9	Программно-аппаратные и программные средства и системы защиты информации.	2	2	-	2 Реферирование российской и зарубежной литературы и статей	Собеседование
10	Оценка эффективности системы менеджмента информационной безопасности. Используемые методики оценки.	2	2	-	2 Реферирование литературных источников и работа в интернет	Собеседование
	Подготовка к зачету				8	
	Итого:		**12**		**24**	**Зачет**

3. Содержание дисциплины:

Тема 1. Информация как основной объект защиты

Понятие конфиденциальной информации. Виды тайн, служебная информация. Свойства информации, как объекта защиты (конфиденциальность, целостность, доступность).

Тема 2. Методологические основы построения систем защиты информации

Защита информации в информационных системах в современных условиях. Правовая, организационная и техническая защита информации. Использование физических методов защиты информации. Силы и средства обеспечения информационной безопасности. Ресурсное обеспечение системы обеспечения информационной безопасности.

Тема 3. Методологические основы моделирования угроз и оценки рисков информационной безопасности

Моделирование угроз информационной безопасности на основе методики ФСТЭК России. Основные подходы к оценке рисков информационной безопасности. Степень вероятности реализации угроз информационной безопасности, оценка вероятного ущерба. Управление рисками информационной безопасности, основные методы и подходы.

Тема 4. Система менеджмента информационной безопасности: основные аспекты и направления

Построение системы менеджмента информационной безопасности на основе процессного подхода. Модель Деминга-Шухарта. Планирование, внедрение, использование, контроль и совершенствований мероприятий системы менеджмента информационной безопасности.

Тема 5. Оценка рисков информационной безопасности

Риск-ориентированный подход к оценке состояния системы обеспечения информационной безопасности. Основные подходы к оценке рисков информационной безопасности. Допустимые и недопустимые риски информационной безопасности. Минимизация рисков информационной безопасности.

Тема 6. Мониторинг информационной безопасности

Мониторинг информационной безопасности: сбор событий информационной безопасности, их анализ и выявление инцидентов информационной безопасности. Системы и средства мониторинга информационной безопасности. Центры управления информационной безопасностью.

Тема 7. Выявление и управление инцидентами информационной безопасности

Выявление и классификация инцидентов информационной безопасности. Приоритезация и анализ инцидентов информационной безопасности. Управление инцидентами информационной безопасности. Расследование инцидентов информационной безопасности.

Тема 8. Организационные и правовые аспекты защиты информации в современных условиях

Организационные и правовые аспекты защиты информации в современных условиях. Законодательство и нормативные акты регуляторов в области защиты информации. Основные организационные мероприятия, проводимые в организации. Организация доступа к информационным ресурсам организации.

Тема 9. Программно-аппаратные и программные средства и системы защиты информации

Современные программно-аппаратные и программные средства и системы защиты информации. Системы антивирусной защиты, межсетевые экраны, средства защиты сетевого периметра, SIEM-системы, DLP-системы, IDM-системы, системы криптографической защиты информации. Автоматизация управления информационной безопасностью.

Тема 10. Оценка эффективности системы менеджмента информационной безопасности. Используемые методики оценки

Основные подходы к оценке эффективности системы обеспечения информационной безопасности. Модель оценки информационной безопасности. Аудит информационной безопасности. Принципы и критерии аудита. Уровень зрелости системы обеспечения информационной безопасности организации.

4. Информационные и образовательные технологии

Дисциплина включает лекционные занятия, однако из-за небольшого количества аспирантов в группе по сути занятия представляют собой совместную коллективную работу. Главная форма – совместное обсуждение ключевых вопросов, выносимых на занятие и в большинстве случаев опирающихся на предварительную подготовку аспирантами индивидуальных докладов и рефератов. Активно используются электронные ресурсы. Самостоятельная работа аспирантов проводится в виде аннотирования и реферирования научной литературы, статей отечественных и зарубежных авторов.

5. Система текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины

Система текущего и промежуточного контроля успеваемости аспирантов по дисциплине включает реферат и зачет с оценкой.

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

Критерии оценки за реферат

Оценка	Содержание
Отлично	Реферат написан четко и грамотно. Тема реферата хорошо раскрыта. Приведена качественно подобранная российская и зарубежная литература. Ответы на дополнительные вопросы по реферату правильные.
Хорошо	Реферат написан четко и грамотно. Тема реферата раскрыта не полностью. Приведена российская и зарубежная литература. Ответы на дополнительные вопросы по реферату правильные.
Удовлетворительно	Тема реферата раскрыта не полностью. Ответы на дополнительные вопросы по реферату правильные, но неполные.
Неудовлетворительно	Тема реферата не раскрыта. Ответы на дополнительные вопросы по реферату неправильные.

Критерии оценки по итогам промежуточной аттестации

Оценка	Содержание
Зачтено	Аспирант способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «отлично».
	Ответ аспиранта правильный, но неполный. Не приведены иллюстрирующие примеры, обобщающее мнение аспиранта недостаточно четко выражено. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «хорошо».
	Ответ правильный в основных моментах, нет иллюстрирующих примеров, отсутствует собственное мнение аспиранта, есть ошибки в деталях. Все

	предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «удовлетворительно».
Не зачтено	В ответе аспиранта существенные ошибки в основных аспектах темы. Предусмотренные рабочей программой дисциплины учебные задания либо не выполнены, либо выполнены неудовлетворительно.

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

Примерная тематика рефератов

№ пп	Примерная тематика рефератов	Формируемые компетенции
1.	Анализ российского законодательства и нормативных актов регуляторов в области информационной безопасности	УК-1,4, ОПК-1-2, ПК-1
2.	Особенности защиты персональных данных в соответствии с требованиями законодательства и нормативных актов в области защиты персональных данных	УК-1,4, ОПК-1-2, ПК-1
3.	Организация защиты коммерческой тайны на предприятии. Система защиты коммерческой тайны.	УК-1,4, ОПК-1-2, ПК-1
4.	Создание и внедрение системы менеджмента информационной безопасности в соответствии с требованиями ГОСТ 27001 и ГОСТ 27002.	УК-1,4, ОПК-1-2, ПК-1
5.	Особенности оценки угроз и рисков информационной безопасности на основе методики ФСТЭК от 05.02.2021г.	УК-1,4, ОПК-1-2, ПК-1
6.	Силы и средства обеспечения информационной безопасности. Функционирование службы защиты информации.	УК-1,4, ОПК-1-2, ПК-1
7.	Построение системы менеджмента информационной безопасности на основе процессного подхода.	УК-1,4, ОПК-1-2, ПК-1
8.	Основные подходы к оценке рисков информационной безопасности. Модели оценки рисков информационной безопасности.	УК-1,4, ОПК-1-2, ПК-1
9.	Системы и средства мониторинга информационной безопасности. Центры управления информационной безопасностью	УК-1,4, ОПК-1-2, ПК-1
10.	Управление инцидентами информационной безопасности. Расследование инцидентов информационной безопасности.	УК-1,4, ОПК-1-2, ПК-1
11.	Основные организационные мероприятия, проводимые в организации.	УК-1,4, ОПК-1-2, ПК-1
12.	Организация доступа к информационным ресурсам организации	УК-1,4, ОПК-1-2, ПК-1

13.	Анализ современных программно-аппаратных и программных средств и систем защиты информации	УК-1,4, ОПК-1-2, ПК-1
14.	Автоматизация управления информационной безопасностью	УК-1,4, ОПК-1-2, ПК-1
15.	Основные подходы к оценке эффективности системы обеспечения информационной безопасности	УК-1,4, ОПК-1-2, ПК-1
16.	Оценка уровня зрелости системы обеспечения информационной безопасности организации	УК-1,4, ОПК-1-2, ПК-1

Перечень вопросов к зачету

№ пп	Перечень вопросов к зачету с оценкой	Формируемые компетенции
1.	Конфиденциальная информация, виды тайн, служебная информация. Свойства информации, как объекта защиты (конфиденциальность, целостность, доступность)	УК-1,4, ОПК-1-2, ПК-1
2.	Законодательство и нормативные акты регуляторов в области защиты информации.	УК-1,4, ОПК-1-2, ПК-1
3.	Правовая, организационная и техническая защита информации.	УК-1,4, ОПК-1-2, ПК-1
4.	Основные подходы к оценке рисков информационной безопасности.	УК-1,4, ОПК-1-2, ПК-1
5.	Построение системы менеджмента информационной безопасности на основе процессного подхода	УК-1,4, ОПК-1-2, ПК-1
6.	Основные подходы к оценке рисков информационной безопасности.	УК-1,4, ОПК-1-2, ПК-1
7.	Мониторинг информационной безопасности: сбор событий информационной безопасности, их анализ и выявление инцидентов информационной безопасности	УК-1,4, ОПК-1-2, ПК-1
8.	Управление инцидентами информационной безопасности. Расследование инцидентов информационной безопасности	УК-1,4, ОПК-1-2, ПК-1
9.	Организационные и правовые аспекты защиты информации в современных условиях	УК-1,4, ОПК-1-2, ПК-1
10.	Современные программно-аппаратные и программные средства и системы защиты информации. Системы антивирусной защиты, межсетевые экраны, средства защиты сетевого периметра, SIEM-системы, DLP-системы, IDM-системы, системы криптографической защиты информации.	УК-1,4, ОПК-1-2, ПК-1
11.	Использование криптографических методов и средств защиты информации.	УК-1,4, ОПК-1-2, ПК-1
12.	Защита сетевого периметра информационной системы. Особенности использования межсетевых экранов.	УК-1,4, ОПК-1-2, ПК-1

13	Системы обнаружения вторжений (IDS\IPS-системы). Особенности их использования.	
14	Системы антивирусной защиты. Методы выявления вредоносной активности. Организация антивирусной защиты в организации.	
15	Управление доступом к информационным ресурсам организации. Модели доступа. Ресертификация доступа.	
16	Уничтожение конфиденциальной информации. Способы уничтожения информации.	
17	Основные подходы к оценке эффективности системы обеспечения информационной безопасности. Модель оценки информационной безопасности	
18	Аудит информационной безопасности. Принципы и критерии аудита.	
19	Резервное копирование информации. Особенности хранения и восстановления информации с резервных копий.	
20	Служба информационной безопасности. Кадровое и ресурсное обеспечение.	

7. Учебно-методическое и информационное обеспечение дисциплины

Список источников и литературы
Основная:

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Стандарт Банка России СТО БР ИББС 1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», 2014. Принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399.
4. ГОСТ Р ИСО/МЭК 27001:2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», 2006. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 15.11.12 № 813-ст.
5. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. — Москва : ИД «ФОРУМ» ; ИНФРА-М, 2016. — 416 с. - Режим доступа: URL: http://znanium.com/catalog/product/549989
6. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации (учебное пособие). СПб: Национальный исследовательский университет ИТМО, 2018. - 100 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=44449457 https://e.lanbook.com/book/11834 (дата обращения: 21.06.2021). -- Режим доступа: для авториз. пользователей

Дополнительная:

1. Положение Банка России от 08.04.2020 №716-П «О требованиях к системе управления операционным риском в кредитной организации и банковской группы».
2. Методика оценки угроз безопасности информации, Москва: ФСТЭК России, Утвержден 05.02.2021.
3. Защита информации в компьютерных системах / под ред. Е.В. Стельмашонок, И.Н. Васильевой. – СПб: Изд-во СПбГЭУ, 2017. – 163 с. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=32254007
4. Корякин С.В. Разработка концепции построения программно-аппаратного ядра универсальной среды проектирования автоматизированных систем защищенного исполнения // Проблемы автоматики и управления. 2020, №1 (38). - С. 60-69. - Режим доступа: URL: https://www.elibrary.ru/item.asp?id=43980501
5. Белоус, А. И. Кибероружие и кибербезопасность. О сложных вещах простыми словами: монография / А. И. Белоус, В. А. Солодуха. – Москва; Вологда: Инфра-Инженерия, 2020. – 692 с. – ISBN 978-5-9729-0486-0. – Текст: электронный. - URL: https://znanium.com/catalog/product/1167736 (дата обращения: 21.06.2021). – Режим доступа: по подписке

Ресурсы Интернет:

1. http://www.aspirantura.spb.ru/ - портал для аспирантов.
2. https://www.dissercat.com/catalog/tekhnicheskie-nauki – электронная библиотека диссертаций.
3. Официальный сайт Российской государственной библиотеки http://www.rsl.ru/
4. Официальный сайт Российской национальной библиотеки http://www.nlr.ru/

8. Материально-техническое обеспечение дисциплины

Освоение дисциплины предполагает использование классической академической аудитории для проведения лекционных занятий с необходимыми техническими средствами (компьютер, проектор, экран) и доступом к Интернету.
Перечень необходимого программного обеспечения:
Microsoft Office 2010, договор №17/03 от 21.03.2017 с АО «СофтЛайнТрейд»
Microsoft Office 2013, договор №16 от 13..06.17 с ООО «Софтлайн Проекты»
Windows 7 Pro, договор №17/03 от 21.03.2017 с АО «СофтЛайнТрейд»
Windows 10 Pro, договор №16 от 13.06.17 с ООО «Софтлайн Проекты»
Microsoft Share Point 2010, договор №17/03 от 21.03.2017 с АО «Софтлайн Трейд»
Kaspersky Endpoint Security, договор №594-05-44 от 19.12.18 с АО «СофтЛайнТрейд»
Microsoft Office 2016, договор №16 от 13.06.2017 с ООО «Софтлайн Проекты»

Для инвалидов и лиц с ограниченными возможностями здоровья:

обеспечивается возможность беспрепятственного доступа обучающихся инвалидов в аудитории и другие помещения, а также их пребывания в указанных помещениях (наличие пандусов, лифтов, наличие специальных кресел и других приспособлений).

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения для обучающихся с ограниченными возможностями здоровья и обучающихся инвалидов с разными видами ограничений здоровья:

- с нарушениями зрения:
    - устройство для сканирования и чтения с камерой SARA CE;
    - дисплей Брайля PAC Mate 20;
    - принтер Брайля EmBraille ViewPlus;
- с нарушениями слуха:

9. Рекомендации по организации самостоятельной работы аспирантов

Самостоятельная работа аспирантов организуется в форме аннотирования и реферирования научной литературы, статей отечественных и зарубежных авторов. По итогам самостоятельной работы аспиранты готовят рефераты, лучшие из которых заслушиваются на научном семинаре кафедры.

Готовя рефераты, аспиранты должны показать навыки научного поиска, используя литературу и источники, которые не нашли отражения в данной программе.

Очень важно в рамках самостоятельной работы выявлять связующие линии компоненты информационной безопасности как в содержательном плане, так и в контексте исследовательского инструментария, теоретических и методологических разработок направления.

В ходе самостоятельной деятельности необходимо принимать во внимание векторы развития современных технологий, информатизации, особенно в плане использования междисциплинарного инструментария.

Организация самостоятельной работы аспирантов направлена на осуществление научно-исследовательской работы, подготовку научных статей, диссертационной работы, подготовку к преподавательской деятельности.

Автор (составитель):
Составитель: Г.А. Шевцова,
Кандидат исторических наук, доцент

_____

подпись расшифровка подписи

Лист изменений
в рабочей программе дисциплины

Обеспечение информационной безопасности объектов защиты в современных условиях

№ п/п	Дата внесения изменений	Дата и № протокола заседания кафедры	Содержание изменения	Подпись
1.	08.05.2020	Приказ РГГУ от 08.05.2020 г. № 01-229/осн	Зачет проводится в дистанционной форме устно в утвержденные даты и время согласно расписанию промежуточной аттестации. Перед началом зачета аспирант устанавливает с доступного ему устройства видеоконференцсвязь с преподавателем посредством ПО. До начала зачета аспирант демонстрирует через камеру преподавателю отсутствие посторонних лиц в помещении, где он находится, и посторонних предметов перед монитором (экраном) и камерой своего устройства. Преподаватель передает аспиранту в рамках конференцсвязи содержание вопросов, на которые ему необходимо ответить и дает время для подготовки ответа. В процессе подготовки ответа аспирант должен находиться перед камерой своего устройства так, чтобы преподаватель мог его видеть все время подготовки к ответу. В случае неполного или некорректного ответа преподаватель имеет право задавать аспиранту дополнительные вопросы в рамках материалов дисциплины. По окончании ответа преподаватель озвучивает аспиранту итоги зачета и вносит соответствующие сведения в электронную аттестационную ведомость, которую по итогам сдачи зачета передает в Управление аспирантурой и докторантурой в электронном виде. Возможны различные варианты сдачи зачета: устный, письменный или комбинированный (письменно+устно). Для визуальной и голосовой коммуникации возможно использование Zoom, Skype, WhatsApp и.т.п. Для отправки выполненных заданий в письменной форме возможно	Управление аспирантурой и докторантурой

			использование электронной почты, WhatsApp и т.п. Всю необходимую информацию о проведении зачета каждый преподаватель должен довести до аспирантов в письменной форме по электронной почте. Информация о проведении зачета должна быть получена каждым аспирантом не позднее чем за 3 дня до зачета.	