МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Российский государственный гуманитарный университет»

(ФГБОУ ВО «РГГУ»)
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

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

ИНФОРМАТИЗАЦИЯ ОБЩЕСТВА И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

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

«Методы и системы защиты информации, информационная безопасность»

Москва 2019

Составитель: Д.А. Митюшин,
кандидат технических наук

Программа утверждена
на заседании кафедры комплексной защиты информации
30 августа 2019 г., протокол № 1

Программа утверждена
на заседании Совета ИИНТБ
30 августа 2019 г., протокол № 1

Программа утверждена
на заседании Научно-методического совета
по аспирантуре и докторантуре
28 ноября 2019 г., протокол № 1

Аннотация

Дисциплина «Информатизация общества и информационная безопасность» является обязательной дисциплиной вариативной части направленности программ подготовки научно-педагогических кадров в аспирантуре «Методы и системы защиты информации, информационная безопасность».

Рабочая программа дисциплины разработана на кафедре комплексной защиты информации Института информационных наук и технологий безопасности.

Содержание дисциплины охватывает круг вопросов, связанных с рассмотрением совокупности проблем, связанных с информатизацией общества, с исследованием, разработкой, совершенствованием и применением моделей, методов, технологий, средств и систем защиты информации, а также обеспечением информационной безопасности объектов и процессов обработки, передачи информации во всех сферах деятельности от внешних и внутренних угроз.

Дисциплина направлена на формирование следующих компетенций выпускника аспирантуры:

универсальные (УК):

способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1);

готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач (УК-3);

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

общепрофессиональные (ОПК):

способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);

готовность к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-2);

профессиональные (ПК):

способность самостоятельно осуществлять научно-исследовательскую деятельность в сфере защиты информации, используя современные научный инструментарий и информационно-коммуникативные практики, принимая во внимание специфику объектов обеспечения информационной безопасности во всех сферах деятельности (ПК-1).

Общая трудоёмкость освоения дисциплины составляет 5 зачётных единиц, 180 часов. Программой дисциплины предусмотрены лекционные занятия (10 часов), самостоятельная работа аспиранта (170 часов).

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

1. Пояснительная записка

Цель дисциплины: сформировать у аспирантов представление об информационной безопасности и об информатизации общества.

Информационная безопасность и защита информации – это научная область, занимающаяся проблемами разработки, совершенствования и применения методов и средств защиты информации в процессе сбора, хранения, обработки, передачи и распространения информации, а также обеспечения информационной безопасности объектов политической, социальной, экономической, оборонной, культурной и других сфер деятельности от внешних и внутренних угроз информации. Значение решения научных и технических проблем в данной области состоит в разработке новых и совершенствовании имеющихся методов и средств защиты информации и обеспечения информационной безопасности.

Задачи дисциплины: показать пути информатизации общества и значение информационной безопасности в развитии современного общества, ее роль в России и в мире, познакомить аспирантов с деятельностью структур, ответственных за формирование и реализацию политики в области информационной безопасности, выявить взаимосвязь в развитии отечественной и зарубежной нормативной базы в области информационной безопасности.

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

Дисциплина «Информатизация общества и информационная безопасность» призвана, прежде всего, помочь аспиранту в его научной деятельности. Данный курс естественным образом связан с курсами «Основы информационной безопасности и методология защиты информации» и «Методы и системы инженерно-технической защиты информации».

Требования к результатам освоения дисциплины:

Дисциплина «Информатизация общества и информационная безопасность» направлена на формирование следующих компетенций выпускника

универсальные (УК):

способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1);

готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач (УК-3);

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

общепрофессиональные (ОПК):

способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность (ОПК-1);

готовность к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-2);

профессиональные (ПК):

способность самостоятельно осуществлять научно-исследовательскую деятельность в сфере защиты информации, используя современные научный инструментарий и информационно-коммуникативные практики, принимая во внимание специфику объектов обеспечения информационной безопасности во всех сферах деятельности (ПК-1).

В результате изучения дисциплины аспирант должен:

знать: нормативно-методическую базу в области информационной безопасности, факторы, определяющие её развитие, механизмы влияния на неё со стороны государства,

знать методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности (УК-1, УК-3, ПК-1).

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 (ОПК-2).

владеть: навыками применения полученных знаний в научно- исследовательской работе и научно-педагогической работе (ОПК-1, УК-4).

2. Структура дисциплины (тематический план)

Общая трудоемкость освоения дисциплины составляет 5 зачётных единиц, 180 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	Введение. Теория и методология обеспечения информационной безопасности и защиты информации	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
2	Методы, аппаратно-программные средства защиты систем формирования и предоставления пользователю информационных ресурсов различного вида	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
3	Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности	1			5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа Лекция с обратной связью
4	Электронные системы документооборота и средства защиты, циркулирующей в них информации	1	1		15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
5	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в	1			15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата Лекция с обратной связью

	открытых компьютерных сетях типа Интернет				5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью
6	Модели и методы формирования комплексов средств противодействия угрозам хищения, разрушения, модификации информации и нарушения информационной безопасности для различных видов объектов защиты вне зависимости от области их функционирования	1	1		15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
7	Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах	1	1		15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата Лекция с обратной связью
8	Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем	1			15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа Лекция с обратной связью
9	Модели и методы оценки защищенности информации и информационной безопасности объекта	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
10	Модели и методы оценки эффективности систем защиты	1			15 Реферирование российской и зарубежной литературы и	Собеседование Лекция с обратной связью

					статей, работа в интернет	
11	Технологии идентификации и аутентификации пользователей и субъектов информационных процессов, системы разграничения доступа	1			10 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью
12	Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
13	Новые принципы и решения (технические, математические, организационные и другие) по созданию и совершенствованию существующих средств защиты	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
14	Модели, методы и средства по обеспечению внутреннего аудита и мониторинга состояний объекта, находящегося под воздействием угроз нарушения его информационной безопасности	1	1		12 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
15	Модели и методы управления информационной безопасностью		1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет Реферат	Собеседование Лекция с обратной связью
16	Подготовка к зачёту с оценкой				18	
	Итого:		**10**		**170**	**Зачет с оценкой**

Структура дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

№ п/п	Раздел дисциплины	Полу-годие обуче-ния	Виды учебной работы, включая самостоятельную работу аспирантов и трудоемкость (в часах)			Формы текущего контроля успеваемости Форма промежуточной аттестации
			Лек-ции	Практ. занятия	Самостоятельная работа	
1	Введение. Теория и методология обеспечения информационной безопасности и защиты информации	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
2	Методы, аппаратно-программные средства защиты систем формирования и предоставления пользователю информационных ресурсов различного вида	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
3	Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности	1			5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа Лекция с обратной связью
4	Электронные системы документооборота и средства защиты, циркулирующей в них информации	1	1		15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
5	Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях типа Интернет	1			15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата Лекция с обратной связью
					5 Реферирование российской и	Лекция с обратной связью

					зарубежной литературы и статей, работа в интернет	
6	Модели и методы формирования комплексов средств противодействия угрозам хищения, разрушения, модификации информации и нарушения информационной безопасности для различных видов объектов защиты вне зависимости от области их функционирования	1	1		15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
7	Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах	1	1		15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Оценка реферата Лекция с обратной связью
8	Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем	1			15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Контрольная работа Лекция с обратной связью
9	Модели и методы оценки защищенности информации и информационной безопасности объекта	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
10	Модели и методы оценки эффективности систем защиты	1			15 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью

11	Технологии идентификации и аутентификации пользователей и субъектов информационных процессов, системы разграничения доступа	1			10 Реферирование российской и зарубежной литературы и статей, работа в интернет	Лекция с обратной связью
12	Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
13	Новые принципы и решения (технические, математические, организационные и другие) по созданию и совершенствованию существующих средств защиты	1	1		5 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
14	Модели, методы и средства по обеспечению внутреннего аудита и мониторинга состояний объекта, находящегося под воздействием угроз нарушения его информационной безопасности	1	2		10 Реферирование российской и зарубежной литературы и статей, работа в интернет	Собеседование Лекция с обратной связью
15	Модели и методы управления информационной безопасностью		2		5 Реферирование российской и зарубежной литературы и статей, работа в интернет Реферат	Собеседование Лекция с обратной связью
16	Подготовка к зачёту с оценкой				18	
	Итого:		**12**		**168**	**Зачет с оценкой**

3. Содержание дисциплины:

Тема 1. Введение. Теория и методология обеспечения информационной безопасности и защиты информации

Во введении даётся обзор информации по начальному уровню подготовки аспирантов по данному курсу. В этом разделе даётся краткое описание стандарта ГОСТ Р ИСО 15408, часть 1. Архитектура безопасности систем коммуникаций компьютерных систем из стандарта ГОСТ Р ИСО 7498, часть 2.

Тема 2. Методы, аппаратно-программные средства защиты систем формирования и предоставления пользователю информационных ресурсов различного вида

Обзор продуктов защиты информации, имеющихся на отечественном рынке, и их основные функции.

Тема 3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности

Обзор уязвимости современных программно-аппаратных систем и методов поиска уязвимости.

Тема 4. Электронные системы документооборота и средства защиты, циркулирующей в них информации

Закон об электронно-цифровой подписи. Стандарты ГОСТы 3410 и 3411. Инфраструктура открытых ключей. Продукты, реализующие электронный документооборот.

Тема 5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях типа Интернет

Межсетевые экраны и их характеристики. РД Гостехкомиссии по межсетевым экранам. Профили защиты для межсетевых экранов. IPsec, VPN. Защита от DoS-атак. Продукты защиты на отечественном рынке.

Тема 6. Модели и методы формирования комплексов средств противодействия угрозам хищения, разрушения, модификации информации и нарушения информационной безопасности для различных видов объектов защиты вне зависимости от области их функционирования

Модель Белла-Лападулла. Модель «невлияния». Модели скрытых каналов.

Тема 7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах

Теоретико-игровая модель вычисления рисков. Вероятностные оценки сбоев и стихийных бедствий. Оценки надёжности систем телекоммуникаций и протоколов связи. Системы реального времени. Схемы деградации для компьютерных систем.

Тема 8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем

Политики безопасности. Формальное обоснование политики безопасности. Гарантированно защищённые информационные системы.

Тема 9. Модели и методы оценки защищённости информации и информационной безопасности объекта

Процедуры сертификации и аттестации и их реализация. ГОСТ Р ИСО 15408, части

2, 3.

Тема 10. Модели и методы оценки эффективности систем защиты

Программные средства моделирования вторжений. Методы анализа аудита. Системы мониторинга больших информационных систем.

Тема 11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов, системы разграничения доступа

Системы идентификации и аутентификации в компьютерных системах. Протокол «RADIUS». Системы с единой точкой входа. Идентификация и аутентификация с помощью протокола LDAPи службы директорий.

Тема 12. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления

Процедуры обследования объектов информатизации. Оценка возможности противника по нанесению ущерба информационным ресурсам. Организационные политики безопасности. Формирование целей безопасности. Формирование профиля безопасности и заданий по безопасности. Разработка автоматизированных систем в защищённом исполнении. Экспертная оценка защищённости и уровня доверия.

Тема 13. Новые принципы и решения (технические, математические, организационные и другие) по созданию и совершенствованию существующих средств защиты

Распределённые системы Grid. Концепция безопасности систем типа Grid. Многоагентные системы. Проблемы информационной безопасности многоагентных систем и пути их решения. Системы обнаружения вторжений и формирование безопасной среды с помощью «событий безопасности».

Тема 14. Модели, методы и средства по обеспечению внутреннего аудита и мониторинга состояний объекта, находящегося под воздействием угроз нарушения его информационной безопасности

Модель мониторинга в продукте HPOpenView. Мониторинг в продуктах IBMTIVOLI.

Тема 15. Модели и методы управления информационной безопасностью

Безопасная конфигурация. Безопасная доставка. Процедуры досертификации и переаттестации. Безопасное администрирование. Взаимодействие администратора и службы безопасности.

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
Отлично	Аспирант способен обобщить материал, сделать собственные выводы, выразить свое мнение, привести иллюстрирующие примеры. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «отлично».
Хорошо	Ответ аспиранта правильный, но неполный. Не приведены иллюстрирующие примеры, обобщающее мнение аспиранта недостаточно четко выражено. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «хорошо».
Удовлетворительно	Ответ правильный в основных моментах, нет иллюстрирующих примеров, отсутствует собственное мнение аспиранта, есть ошибки в деталях. Все предусмотренные рабочей программой дисциплины учебные задания выполнены, качество их выполнения соответствует оценке «удовлетворительно».
Неудовлетворительно	В ответе аспиранта существенные ошибки в основных аспектах темы. Предусмотренные рабочей программой дисциплины учебные задания либо не выполнены, либо выполнены неудовлетворительно.

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

Примерная тематика рефератов

№ пп	Примерная тематика рефератов	Формируемые компетенции
1.	Риски нарушения информационной безопасности.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
2.	Модели противодействия угрозам нарушения информационной безопасности.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
3.	Механизмы формирования политики обеспечения информационной безопасности.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
4.	Новые принципы и технические решения по созданию и совершенствованию существующих средств защиты.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
5.	Проблемы информационной безопасности многоагентных систем и пути их решения.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
6.	Системы обнаружения вторжений и формирование безопасной среды с помощью «событий безопасности».	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
7.	Внутренний аудит и мониторинг состояний объекта, находящегося под воздействием угроз нарушения его информационной безопасности.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
8.	Модели и методы управления информационной безопасностью.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4

Перечень вопросов к зачету с оценкой

№ пп	Перечень вопросов к зачету с оценкой	Формируемые компетенции
1.	Архитектура построения безопасности систем коммуникаций компьютерных систем из стандарта ГОСТ Р ИСО 7498, часть 2.	ОПК-1 УК-3 УК-4
2.	Классификация угроз нарушения информационной безопасности.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
3.	Каковы уязвимости современных программно-аппаратных систем.	ОПК-1 УК-3 УК-4
4.	Продукты, реализующие электронный документооборот.	ОПК-1 УК-3 УК-4
5.	Межсетевые экраны и их характеристики.	ОПК-1 УК-3 УК-4
6.	Профили защиты для межсетевых экранов.	ОПК-1 УК-3 УК-4
7.	Продукты защиты на отечественном рынке.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
8.	Модели скрытых каналов	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
9.	Вероятностные оценки сбоев и стихийных бедствий.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
10.	Оценки надежности систем телекоммуникаций и протоколов связи.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
11.	Процедуры сертификации и аттестации и их реализация.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
12.	Методы анализа аудита. Системы мониторинга больших информационных систем.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4

13.	Процедура обследования объектов информатизации.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
14.	Экспертная оценка защищенности и уровня доверия.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
15.	Системы обнаружения вторжений и формирование безопасной среды с помощью «событий безопасности».	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
16.	Процедуры досертификации и переаттестации.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4
17.	Безопасное администрирование.	ОПК-1 ОПК-2 ПК-1 УК-1 УК-3 УК-4

7. Учебно-методическое и информационное обеспечение дисциплины

Список источников и литературы

Основная

1. Конституция Российской Федерации от 25 декабря 1993 года, с изменениями от 30 декабря 2008 года (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_28399/, свободный. – Загл. с экрана.

2. Указ Президента РФ от 31.12.2015 № 683 "О Стратегии национальной безопасности Российской Федерации" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_191669/, свободный. – Загл. с экрана.

3. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_208191/, свободный. – Загл. с экрана.

4. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_216363/, свободный. – Загл. с экрана.

5. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

6. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ (последняя редакция). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.

7. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9032#011028370269284904, свободный. – Загл. с экрана.

8. ГОСТ Р ИСО/МЭК 27004-2011. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=388#041622976189257066, свободный. – Загл. с экрана.

9. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=666#05511035764404268, свободный. – Загл. с экрана.

10. ГОСТ Р 54989-2012 / ISOTR18492:2005. Обеспечение долговременной сохранности электронных документов" [Электронный ресурс] : Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=2489#0005936991809006864, свободный. – Загл. с экрана.

11. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефиров С.Л., Голованов В.Б. - Москва :ЦИПСиР, 2011. - 373 с. ISBN 978-5-9614-1364-9 - Текст : электронный. - URL: https://new.znanium.com/catalog/product/556539 (дата обращения: 18.08.2019)

12. Грушо А.А. Теоретические основы компьютерной безопасности. – М.: Изд. Центр «Академия», 2009. - 272 с.

13. Малюк, А. А. Защита информации в информационном обществе: Учебное пособие для вузов / Малюк А.А. - Москва : Гор. линия-Телеком, 2015. - 230 с. ISBN 978-5-9912-0481-1. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/536930 (дата обращения: 18.08.2019).

14. Вестник РГГУ. Серия «Информатика. Информационная безопасность. Математика».

Дополнительная:

1. Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) от 18 февраля 2013 г. N 21 [Электронный ресурс] : Режим доступа : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691, свободный. – Загл. с экрана.

2. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК) от 11 февраля 2013 г. N17 [Электронный ресурс] : Режим доступа : https://fstec.ru/normotvorcheskaya/akty/53-prikazy/702, свободный. – Загл. с экрана.

3. Гришина, Н. В. Основы информационной безопасности предприятия : учеб. пособие / Н.В. Гришина. – Москва : ИНФРА-М, 2019. – 216 с. – (Высшее образование: Бакалавриат). – www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-107616-3. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1017663 (дата обращения: 18.08.2019).

4. Ищейнов В.Я. Защита конфиденциальной информации : учебное пособие для студентов вузов, обучающихся по специальности 090103 "Организация и технология защиты информации" и 090104 "Комплексная защита объектов информатизации" / В. Я. Ищейнов, М. В. Мецатунян. - Москва : Форум, 2013. - 254 с. : рис., табл. ; 22 см. - Библиогр.: с. 249-252. - ISBN 978-5-91134-336-1 : 230.00..

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

Периодические и сериальные издания

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

Ресурсы Интернет:

1. Совет безопасности Российской Федерации [офиц. сайт]. http://www.scrf.gov.ru/
2. Федеральная служба по техническому и экспортному контролю [офиц. сайт], http://fstec.ru

3. Управление «К» МВД России [офиц. сайт]. https://мвд.рф/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii

4. Институт информационных наук и технологий безопасности РГГУ [офиц. сайт], http://www.rsuh.ru/iint

5. Методические пособия, рекомендации, перечни [офиц. сайт Федерального архивного агентства], http://archives.ru/documents/methodics.shtml.

6. Информационная безопасность организаций банковской системы Российской Федерации [офиц. сайт Центрального банка Российской Федерации], http://www.cbr.ru/credit/gubzi_docs

8. Материально-техническое обеспечение дисциплины

Освоение дисциплины предполагает использование академической аудитории для проведения лекционных занятий и самостоятельной работы:

Компьютерный класс

12 компьютеров (Процессор: Celeron 2,6GHz. Оперативная память: 256Mb. Объем жесткого диска: 40Gb. Дисковод CD), проектор.

ПО: Windows 7, MS Office 2010, Microsoft Visual Studio 2012

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

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

- с нарушениями зрения:
  - устройство для сканирования и чтения с камерой SARA CE;
  - дисплей Брайля PAC Mate 20;
  - принтер Брайля EmBraille ViewPlus;
- с нарушениями слуха:
  - автоматизированное рабочее место для людей с нарушением слуха и слабослышащих;
  - акустический усилитель и колонки;
- с нарушениями опорно-двигательного аппарата:
  - передвижные, регулируемые эргономические парты СИ-1;
  - компьютерная техника со специальным программным обеспечением.

9. Рекомендации по организации самостоятельной работы аспирантов

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

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

В ходе самостоятельной деятельности необходимо принимать во внимание векторы развития информатизации и глобализации общества, новые технологии и угрозы информационной безопасности личности, обществу, государству.

Организация самостоятельной работы аспирантов направлена на осуществление

научно-исследовательской работы, подготовку научных статей, диссертационной работы, подготовку к преподавательской деятельности.

Информатизация общества и информационная безопасность

Составитель Д.А. Митюшин,
кандидат технических наук

_____

подпись расшифровка подписи

Лист изменений
в рабочей программе дисциплины

Информатизация общества и информационная безопасность
(Название дисциплины)

№ п/п	Дата внесения изменений	Дата и № протокола заседания кафедры	Содержание изменения	Подпись
1.	08.05.2020	Приказ РГГУ от 08.05.2020 г. № 01-229/осн	Зачет проводится в дистанционной форме устно в утвержденные даты и время согласно расписанию промежуточной аттестации. Перед началом зачета аспирант устанавливает с доступного ему устройства видеоконференцсвязь с преподавателем посредством ПО. До начала зачета аспирант демонстрирует через камеру преподавателю отсутствие посторонних лиц в помещении, где он находится, и посторонних предметов перед монитором (экраном) и камерой своего устройства. Преподаватель передает аспиранту в рамках конференцсвязи содержание вопросов, на которые ему необходимо ответить и дает время для подготовки ответа.	Управление аспирантурой и докторантурой

			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 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.	