Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Проректор по науке
_____ А.В. Германенко
«___» _____ 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Перечень сведений о программе аспирантуры	Учетные данные
Программа аспирантуры Методы и системы защиты информации, информационная безопасность	**Код ПА 2.3.6.**
Группа специальностей Информационные технологии и телекоммуникации	**Код 2.3.**
Федеральные государственные требования (ФГТ)	Приказ Министерства науки и высшего образования Российской Федерации от 20 октября 2021 г. № 951
Самостоятельно утвержденные требования (СУТ)	Приказ «О введении в действие «Требований к разработке и реализации программ подготовки научных и научно-педагогических кадров в аспирантуре УрФУ» №315/03 от 31.03.2022

Екатеринбург
2022 г.

Рабочая программа дисциплины составлена авторами:

№	ФИО	Ученая степень, ученое звание	Должность	Структурное подразделение
1	Поршнев Сергей Владимирович	Д.т.н.	Директор	Учебно-научный центр «Информационная безопасность»
2	Баранский Виталий Анатольевич	Доктор физ.-мат. наук, профессор	профессор	Алгебры и фундаментальной информатики
3	Синадский Николай Игоревич	Кандидат тех. наук, доцент	доцент	Учебно-научный центр «Информационная безопасность»
4	Пономарева Ольга Алексеевна	Кандидат тех. наук	Старший преподаватель	Учебно-научный центр «Информационная безопасность»

Рекомендовано:
Учебно-методическим советом института
радиоэлектроники и информационных технологий -РТФ
Протокол № 62 от 17.05.2022

Председатель УМС института Т.И. Алферьева

Согласовано:

Начальник ОПНПК Е.А. Бутрина

1. ОБЩАЯ ХАРАКТЕРИСТИКА ДИСЦИПЛИНЫ

1.1. Аннотация содержания дисциплины

Дисциплина «Методы и системы защиты информации, информационная безопасность» (МиСЗИ, ИБ) относится к базовой части программы аспирантуры.

Целью дисциплины «Методы и системы защиты информации, информационная безопасность» является изучение:

- основных направлений информационной защиты, взгляда на информацию, как объект защиты с выделением характерных свойств защищаемой информации, качественные модели информационной защиты, информационных преступлений и информационных войнам;
- технических средств и методов защиты информации;
- администрирования компьютерных систем и обеспечения защиты информации в компьютерных сетях под управлением ОС Windows NT/2000;
- организационных, технологических и программно-аппаратных мер защиты от опасной компьютерной информации, в первую очередь – от вредоносных программ для ЭВМ.

1.2. Язык реализации дисциплины – русский.

1.3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины аспирант должен:

Знать:

- модели информационной защиты,
- методы обнаружения и нейтрализации средств технической разведки,
- знать основные способы защиты компьютерных систем, построенных на базе ОС Windows NT/2000,
- основные приемы и способы несанкционированного распространения, внедрения и запуска вредоносных программ,

Уметь:

- определить уголовно-правовую характеристику некоторых информационных преступных деяний,
- организовать инженерную защиту и техническую охрану объектов информатизации,
- обеспечивать защиту информации в компьютерных сетях под управлением ОС Windows NT/2000,
- применять на практике методы и технологии антивирусной защиты.

Владеть (демонстрировать навыки и опыт деятельности):

- определить уголовно-правовую характеристику некоторых информационных преступных деяний,
- организовать инженерную защиту и техническую охрану объектов информатизации,
- обеспечивать защиту информации в компьютерных сетях под управлением ОС Windows NT/2000,
- применять на практике методы и технологии антивирусной защиты.

1.4. Объем дисциплины

№ п/п	Виды учебной работы	Объем дисциплины		Распределение объема дисциплины в 4 семестре (час.)
		Всего часов	В т.ч. контактная работа (час.)*	
1.	**Аудиторные занятия**	**4**		**4**
2.	Лекции	4	4	4
3.	**Самостоятельная работа аспирантов, включая все виды текущей аттестации**	**104**	**1**	**104**
4.	**Промежуточная аттестация**	**104**	**1**	**Э**
5.	**Общий объем по учебному плану, час.**	**108**		**108**
6.	**Общий объем по учебному плану, з.е.**	**3**		**3**

*Контактная работа составляет:

в п/п 2,3, - количество часов, равное объему соответствующего вида занятий;

в п.4 – количество часов, равное сумме объема времени, выделенного преподавателю на консультации в группе (15% от объема аудиторных занятий).

в п.5 – количество часов, равное сумме объема времени, выделенного преподавателю на проведение соответствующего вида промежуточной аттестации одного аспиранта.

2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Код раздела	Раздел дисциплины	Содержание
Р1	**Основы информационной безопасности**	Свойства информации как объекта защиты. Содержание и анализ исторически сложившихся направлений информационной защиты. Принципы, стратегии и модели информационной защиты. Информационные и компьютерные преступления.
Р2	**Технические средства и методы защиты информации**	Защита информации от утечки по техническим каналам. Обнаружение и нейтрализация средств. технической разведки. Инженерная защита и техническая охрана объектов информатизации.
Р3	**Безопасность сетевых технологий**	Принципы построения составных сетей. Стек протоколов TCP/IP. Общая характеристика угроз безопасности в компьютерных сетях. Типовые задачи администрирования сетевых служб в ОС Windows 2000-XP. Обеспечение безопасности информации в компьютерных сетях. Протоколы аутентификации в компьютерных сетях. Виртуальные частные сети. Системы обнаружения сетевых атак.

Р4	**Защита от вредоносных программ**	Понятие об опасной компьютерной информации. Классификация вредоносных программ. Уязвимые места программного обеспечения ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ. Изучение функциональных возможностей вредоносных программ.

3. ОРГАНИЗАЦИЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ, САМОСТОЯТЕЛЬНОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ

3.1. Практические занятия

Не предусмотрено.

3.2. Примерная тематика самостоятельной работы

3.2.1. Примерный перечень тем рефератов

Тематика рефератов должна рассматривать аналитический обзор научно-технической литературы.

1. Содержание и анализ исторически сложившихся направлений информационной защиты.
2. Принципы, стратегии и модели информационной защиты.
3. Информационные и компьютерные преступления.
4. Информационные войны и информационное оружие.
5. Защита информации от утечки по техническим каналам.
6. Обнаружение и нейтрализация средств технической разведки.
7. Инженерная защита и техническая охрана объектов информатизации.
8. Принципы построения составных сетей. Адресация в IP-сетях. Стек протоколов TCP/IP.
9. Общая характеристика угроз безопасности в компьютерных сетях. Типовые задачи администрирования сетевых служб в ОС Windows 2000-XP. Обеспечение безопасности информации в компьютерных сетях.
10. Системы обнаружения сетевых атак. Аудит безопасности компьютерных систем и сетей.
11. Классификация и технические возможности вредоносных программ.
12. Уязвимые места программного обеспечения ЭВМ, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ.

Объем реферата 20-25 страниц машинописного текста формата А-4.

3.2.2. Примерная тематика *индивидуальных* или групповых проектов

Не предусмотрено.

4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (Приложение 1)

4.1. Критерии оценивания результатов контрольно-оценочных мероприятий текущей и промежуточной аттестации по дисциплине

Применяются критерии оценивания достижений аспирантов по каждому контрольно-оценочному мероприятию. Система критериев оценивания опирается на три уровня освоения компонентов компетенций: пороговый, повышенный, высокий.

Компоненты компетенций	**Признаки уровня освоения компонентов компетенций**		
	пороговый	**повышенный**	**высокий**

Знания	Аспирант демонстрирует знание-знакомство, знание-копию: узнает объекты, явления и понятия, находит в них различия, проявляет знание источников получения информации, может осуществлять самостоятельно репродуктивные действия над знаниями путем самостоятельного воспроизведения и применения информации.	Аспирант демонстрирует аналитические знания: уверенно воспроизводит и понимает полученные знания, относит их к той или иной классификационной группе, самостоятельно систематизирует их, устанавливает взаимосвязи между ними, продуктивно применяет в знакомых ситуациях.	Аспирант может самостоятельно извлекать новые знания из окружающего мира, творчески их использовать для принятия решений в новых и нестандартных ситуациях.
Умения	Аспирант умеет корректно выполнять предписанные действия по инструкции, алгоритму в известной ситуации, самостоятельно выполняет действия по решению типовых задач, требующих выбора из числа известных методов, в предсказуемо изменяющейся ситуации	Аспирант умеет самостоятельно выполнять действия (приемы, операции) по решению нестандартных задач, требующих выбора на основе комбинации известных методов, в непредсказуемо изменяющейся ситуации	Аспирант умеет самостоятельно выполнять действия, связанные с решением исследовательских задач, демонстрирует творческое использование умений (технологий)
Личностные качества	Аспирант имеет низкую мотивацию учебной деятельности, проявляет безразличное, безответственное отношение к учебе, порученному делу	Аспирант имеет выраженную мотивацию учебной деятельности, демонстрирует позитивное отношение к обучению и будущей трудовой деятельности, проявляет активность.	Аспирант имеет развитую мотивацию учебной и трудовой деятельности, проявляет настойчивость и увлеченность, трудолюбие, самостоятельность, творческий подход.

4.2. Оценочные средства для проведения текущей и промежуточной аттестации

4.2.1. Перечень примерных вопросов для зачета

Не предусмотрено.

4.2.2. Перечень примерных вопросов для экзамена

1. Вредная и опасная информация в Интернет.
2. Атаки на информационные системы путем перегрузки каналов связи и входных буферов памяти. Использование «протоколов вежливости» для реализации сетевых атак.
3. Формы незаконного использования информации. Законодательные меры против незаконного использования информации.
4. Виды и формы применения информационно-технологического оружия.
5. Доктрина информационной безопасности России и реальности ее осуществления.
6. Государственная система защиты граждан и общества от опасной информации (законодательство и практика).
7. Модель комплексной информационной защиты и ее элементы.

8. Модель информационной защиты каналов связи.
9. Угрозы скрытого информационного воздействия на пользователей Интернет.
10. Формы и методы защиты признаковой информации.
11. Угрозы конфиденциальности и формы их реализации.
12. Модель информационного нарушителя, посягающего на конфиденциальную информацию методами несанкционированного доступа.
13. Организационно-распорядительные меры информационной защиты.
14. Характеристики технических каналов утечки информации.
15. Защита линий связи от взаимного влияния.
16. Механизмы побочного электромагнитного излучения радиоэлектронной аппаратуры.
17. Спектры побочных излучений.
18. Оборудование заземляющих устройств.
19. Утечка информационных сигналов через источники питания.
20. Электромагнитное экранирование.
21. Сигналы и помехи, генераторы шума.
22. ЭВМ как источник утечки компьютерной информации.
23. Каналы утечки информации из компьютерных мониторов.
24. Иностранная техническая разведка, классификация по типу используемой аппаратуры.
25. Классификация акустических каналов утечки информации.
26. Электроакустические преобразователи.
27. Средства перехвата и противодействию перехвату речевой инфорсмации по воздушному каналу.
28. Программно-аппаратные методы и средства выделения речевого сигнала и акустического шума.
29. Обнаружение электронных средств подслушивания.
30. Защита акустической информации путем зашумления и экранирования.
31. Электромагнитное экранирование помещений.
32. Аналоговое и цифровое скремблирование.
33. Визуальный и инструментальный досмотр помещений.
34. Безопасность проводных телефонных коммуникаций.
35. Протоколы передачи данных и протоколы обмена маршрутной информацией.
36. Структура стека TCP/IP. Характеристика протоколов. Адресация в IP-сетях.
37. Протокол межсетевого взаимодействия IP.
38. Протокол доставки пользовательских дейтаграмм UDP.
39. Протокол надежной доставки сообщений TCP.
40. Протокол обмена управляющими сообщениями ICMP.
41. Протоколы обмена маршрутной информацией стека TCP/IP.
42. Угрозы безопасности информации, ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию».
43. Классификация и характеристика основных видов атак на компьютерные системы и сети.
44. Настройка базовых сетевых служб и протоколов.
45. Управление рабочей средой пользователя.
46. Организация почтового, DNS и Web-серверов.
47. Межсетевые экраны.
48. Фильтрации пакетов.
49. Атаки на протоколы и службы Интернет.
50. Безопасная настройка клиентского программного обеспечения.
51. Анализатор сетевого трафика MS Network Monitor.
52. Протоколы аутентификации в компьютерных сетях.
53. Схема VPN. Варианты построения VPN.

54. Протоколы PPTP, L2TP. Шифрование в PPTP.
55. Протокол SKIP.
56. Протокол IPSec.
57. Инфраструктура открытых ключей.
58. Защита сетевого трафика с использованием протокола IPSec в Windows 2000-XP.
59. Принципы обнаружения атак. Сигнатуры атак.
60. Аудит безопасности. Средства активного аудита.
61. Методология обеспечения безопасности информационных технологий с применением ГОСТ Р ИСО/МЭК 15408-1-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».
62. Применение программных средств аудита информационной безопасности.
63. Вредоносный программный код документов офисных приложений и его возможности. Методы вирусного копирования.
64. Реализация защиты от вредоносного программного кода в приложениях офисного пакета. Нейтрализация вредоносных макросов с целью их исследования.
65. Механизм сетевых атак на Интернет-браузеры (на примере Microsoft Internet Explorer). Механизмы статического скрытия вредоносного программного кода.
66. Механизмы скрытности вредоносных программ на этапе их выполнения.
67. Механизмы скрытия, используемые современными макровирусами.
68. Классификация и основные особенности различных видов вредоносных программ.
69. Способы подготовки вредоносных программ к безусловному запуску. Несанкционированный характер запуска вредоносных программ.
70. Внедрение и запуск вредоносных программ на этапах самотестирования компьютера и загрузки операционной системы. Способы автоматического запуска вредоносных программ.
71. Возможности программных закладок. Виды и способы программного перехвата компьютерной информации.
72. Виды компьютерных инфекций. Сущность вирусного заражения и жизненный цикл компьютерного вируса.
73. Возможности и особенности сетевых вредоносных программ.
74. Понятие о «троянских» программах и их функциях. Программы-«джойнеры».
75. Виды несанкционированного копирования компьютерной информации.
76. Виды нарушений работы ЭВМ со стороны вредоносных программ.
77. Виды несанкционированного блокирования и модификации компьютерной информации вредоносными программами.
78. Традиционные способы антивирусной защиты и сравнительная оценка их эффективности.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Рекомендуемая литература

1. Бакланов В.В. Введение в информационную безопасность. Модели и стратегии информационной защиты : учеб. пособие. Екатеринбург: изд-во ФГАОУ ВПО УрФУ, 2013. 236 с.
2. Зайцев А. П. Технические средства и методы защиты информации: Учебное пособие для вузов / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков и др.; под ред. А. П. Зайцева и А. А. Шелупанова. – 4-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2009. – 616 с.
3. Андрончик А. Н. и др. Защита информации в компьютерных сетях. Практический курс: Учебное пособие /А. Н. Андрончик, В. В. Богданов, Н. А. Домуховский, А. С.

Коллеров, Н. И. Синадский, Д. А. Хорьков, М. Ю. Щербаков; Под ред. Н. И. Синадского. — Екатеринбург: ФГАОУ ВПО УрФУ, 2012. — 248 с.
4. Бакланов В.В. Защита компьютерной информации в клиентских приложениях: учебное пособие / В.В. Бакланов. Екатеринбург: ГОУ ВПО УрФУ 2013. – 84 с.
5. Бакланов В.В., Пономарев М.Э. Опасная компьютерная информация: учеб. пособие. — Екатеринбург: ФГАОУ ВПО УрФУ, 2012. — 146 с.
6. Андрончик А.Н., Бакланов В.В., Необутов С.А., Пономарев М.Э., Синадский Н.И., Соболев О.Н. Основы компьютерной и информационной безопасности. Часть 3. Проблемы защиты информации в компьютерных системах. Учебно-наглядное пособие. — Екатеринбург: УрГУ, 2002. — 124 с.
7. Бакланов В.В., Духан Е.И., Необутов С.А., Пономарев М.Э., Синадский Н.И. Основы компьютерной и информационной безопасности. Часть 4. Программно-аппаратные средства защиты компьютерных систем. Учебно-наглядное пособие. — Екатеринбург: УрГУ, 2002. — 76 с.
8. Расторгуев С. П. Основы информационной безопасности: Учебное пособие для студентов высших учебных заведений / С. П. Расторгуев. – М.: Академия, 2007. – 192 с.
9. Расторгуев С.П. Философия информационной войны. М.: 2000 г. – 446 с.
10. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: Учебно-практическое пособие. — М.: «Палеотип», «Логос», 2002. — 148 с.
11. Хорев А. А. Техническая защита информации: учеб. пособие для студентов вузов : в 3 т. / А. А. Хорев – М.: НПЦ «Аналитика», 2008.
12. Торокин А. А. Основы инженерно-технической защиты информации. М: «Ось-89», 365 с.
13. Хорев А. А. Защита информации от утечки по техническим каналам утечки информации. Часть 1. Технические каналы утечки информации. М.: Гостехкомиссия России, 1998, 320 с.
14. Люцарев В.С., Ермаков К.В., Рудный Е.Б., Ермаков И.В. Безопасность компьютерных сетей на основе Windows NT. – М.: Издательский отдел «Русская Редакция» ТОО «Channel Trading Ltd.», 1998. – 304 с.
15. Проскурин В.Г., Крутов С.В., Мацкевич И.В. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов. – М.: Радио и связь, 2000. – 168 с.
16. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться. – М.: СК Пресс, 1998. – 288 с., ил.
17. Касперский К. Техника и философия хакерских атак. - М.: «Солон - Р», 1999, 272с.
18. Крис Касперски. Укрощение Интернета. –М.: СОЛОН-Р, 2002. –288 с.
19. Скэмбрей Джоел, Мак-Клар Стюарт. Секреты хакеров. Безопасность Windows 2000 – готовые решения. Пер. с англ. –М.: Издательский дом «Вильямс», 2002. –464 с.
20. Стюарт Мак-Клар, Джоел Скембрей, Джордж Курц. Секреты хакеров. Безопасность сетей - готовые решения, 2-е изд.: Пер. с англ. - М.: Издательский дом "Вильямс", 2001. -656 с.
21.

5.2. Методические разработки

1. Синадский Н.И. Безопасность операционных систем. УМК, 2007. Метаданные ресурса №7029.
2. Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1

электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.

3. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.

.

5.3. Программное обеспечение

1. Microsoft office (Word, Excel, Power point);
2. Adobe Reader.

5.4. Базы данных, информационно-справочные и поисковые системы

1. ScienceDirect: http://www.sciencedirect.com;
2. Web of Science: http://apps.webofknowledge.com;
3. Scopus: http://www.scopus.com;
4. Reaxys: http://reaxys.com;
5. Поисковая система EBSCO Discovery Service http://lib.urfu.ru/course/view.php?id=141;
6. Федеральный институт промышленной собственности http://www1.fips.ru;
7. Интеллектуальная поисковая система Нигма.РФ . режим доступа: http://www.nigma.ru.

5.5. Электронные образовательные ресурсы

1. Зональная научная библиотека http://lib.urfu.ru;
2. Каталоги библиотеки http://lib.urfu.ru/course/view.php?id=76;
3. Электронный каталог http://opac.urfu.ru;
4. Электронно-библиотечные системы http://lib.urfu.ru/mod/resource/view.php?id=2330;
5. Электронные ресурсы свободного доступа http://lib.urfu.ru/course/view.php?id=75;
6. Электронные ресурсы по подписке http://lib.urfu.ru/mod/data/view.php?id=1379.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием

Уральский федеральный университет имеет специальные помещения для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания оборудования.