ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ РОССИЙСКИЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАДИО
ИМЕНИ М.И. КРИВОШЕЕВА»

Согласовано

Заместитель генерального директора ФГБУ НИИР по науке, канд. техн. наук, доцент

А.А. Захаров

«22» декабря 2021 г.

Утверждаю

И.о. генерального директора ФГБУ НИИР, канд. воен. наук

О.А. Иванов

«22» декабря 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки:	2.2.15 Системы, сети и устройства телекоммуникаций
Профиль подготовки:	2.2 – Электроника, фотоника, приборостроение и связь
Квалификация выпускника:	исследователь, преподаватель-исследователь
Форма обучения:	очная

Москва, 2022 г.

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ
«ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ РОССИЙСКИЙ
НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИНСТИТУТ РАДИО
ИМЕНИ М.И. КРИВОШЕЕВА»

Согласовано	Утверждаю
Заместитель генерального директора ФГБУ НИИР по науке, канд. техн. наук, доцент	И.о. генерального директора ФГБУ НИИР, канд. воен. наук
А.А. Захаров	О.А. Иванов
«____»_____20__ г.	«____»_____20__ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки:	2.2.15 Системы, сети и устройства телекоммуникаций
Профиль подготовки:	2.2 – Электроника, фотоника, приборостроение и связь
Квалификация выпускника:	исследователь, преподаватель-исследователь
Форма обучения:	очная

Москва, 2022 г.

Программа разработана в соответствии с требованиями Федерального закона Российской Федерации от 29.12.2012 № 273- ФЗ «Об образовании в Российской Федерации», на основании федеральных государственных требований к структуре программ подготовки научных и научно-педагогических кадров в аспирантуре от 20.10.2021.

Одобрена и утверждена на заседании Президиума НТС ФГБУ НИИР. Протокол №4/1-П-2022 от 22.12.2022.

Разработчики:

Веерпалу В.Э., Директор НТЦ А ЭМС ФГБУ НИИР, д.т.н.

Мырова Л.О., ведущий научный сотрудник НТЦ А ЭМС ФГБУ НИИР, д.т.н.

Корж В.А., заместитель директора НТЦ А ЭМС ФГБУ НИИР, к.т.н.

Иванкович М.В., заместитель директора ЦИПБТС ФГБУ НИИР, к.т.н.

Содержание

1. Цели и задачи освоения дисциплины

Цель преподавания дисциплины: обеспечить аспирантов знаниями об архитектуре современных пакетных сетей, включая сети последующих поколений (СПП); ознакомить их с моделями угроз безопасности и с программными и аппаратными средствами защиты в следующих аспектах безопасности: контроль доступа; аутентификация; сохранность данных; конфиденциальность данных; безопасность связи; целостность данных; доступность.

Задачи освоения дисциплины:

1. Овладение методом достижения информационной безопасности при помощи доверенной модели.
2. Овладение методом защиты сети и инфраструктуры поставщика услуг, его активов и ресурсов, таких как элементы сети, системы, компоненты, интерфейсы, а также данные и информацию, его связь, т. е. сигнализацию, управление и трафик данных/канала передачи.
3. Овладение методом защиты голосовых услуг, услуг передачи видео и данных.
4. Овладение методом защиты соединения и информации оконечного пользователя, включая личную информацию.
5. Овладение методом обеспечения безопасности соединений конечных пользователей через административные домены множества сетей.

2. Место дисциплины в структуре образовательной программы высшего образования

Дисциплина относится к вариативной части учебного плана, трудоёмкость дисциплины составляет 5 зачётных единиц, форма итогового контроля – экзамен.

3. Требования к результатам освоения дисциплины

В результате изучения дисциплины аспирант должен обладать следующими компетенциями:

а) универсальными компетенциями (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);

б) общепрофессиональными компетенциями (ОПК):

– владением методологией теоретических и экспериментальных исследований в области профессиональной деятельности (ОПК-1);

в) профессиональными компетенциями (ПК):

– способностью к самостоятельному проведению научно-исследовательской работы и получению научных результатов, удовлетворяющих установленным требованиям к содержанию диссертаций на соискание ученой степени кандидата наук по направлению 2.2.15 Системы, сети и устройства телекоммуникаций (ПК-1);

– способностью ставить и решать прикладные учебно-методические задачи, обосновать выбор методик преподавания специальных дисциплин в ВУЗе (ПК-2).

4. Объём дисциплины и виды учебной работы

Общая трудоёмкость дисциплины составляет 5 зачётных единиц (ЗЕ).

Вид учебной работы		Всего ЗЕ	Курс	
			1	2
Аудиторные занятия (всего)				
В том числе:				
Лекции (Л)		2	1	1
Семинары (С)		1	0,5	0,5
Самостоятельная работа (всего)				
В том числе:				
Подготовка к семинарам		1	0,5	0,5
Подготовка реферата		1		1
Вид аттестации (зачёт, экзамен)				экзамен
Общая трудоёмкость	зач. ед.	5	2	3
	час	180	72	108

5. Содержание дисциплины

5.1 Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Введение	Цели и задачи дисциплины. Терминология. Рекомендации МСЭ-Т по информационной безопасности. Законодательство Российской Федерации в области защиты информации.
2.	Угрозы безопасности	Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности. Виды угроз: уничтожение, повреждение, удаление, раскрытие, прерывание информации. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
3.	Теоретические основы методов защиты информации	Основные положения теории информационной безопасности. Модели безопасности и их применение. Формальные модели безопасности. Доверительная модель. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы. Политика безопасности. Ограничения на области применения формальных моделей.
4.	Защита компьютерных систем	Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от несанкционированного доступа. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.

5.	Основы криптографии	Методы криптографии. Симметричное и асимметричное шифрование. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Сжатие информации. Квантовая криптография.
6.	Архитектура защищенных информационных систем	Основные технологии построения защищенных информационных систем. Функции защиты информации. Классы задач защиты информации. Архитектура систем защиты информации. Ядро и ресурсы средств защиты информации. Стратегии защиты информации.
7.	Защита сети связи	Метод достижения информационной безопасности при помощи доверенной модели. Методы защиты сети и инфраструктуры поставщика услуг, его активов и ресурсов, таких как элементы сети, системы, компоненты, интерфейсы, а также данные и информацию, его связь, т. е. сигнализацию, управление и трафик данных/канала передачи.
8.	Защита услуг связи	Метод защиты голосовых услуг, услуг передачи видео и данных. Метод защиты соединения и информации оконечного пользователя, включая персональную информацию. Метод обеспечения безопасности соединений конечных пользователей через административные домены множества сетей.

5.2 Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	Номера разделов данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин							
		1	2	3	4	5	6	7	8
1.	Системы, сети и устройства телекоммуникаций		v	v	v	v	v	v	v

5.3 Разделы дисциплин и виды занятий

№ п/п	Наименование раздела дисциплины	Часы для видов занятий		
		Лекция	Семинар	Самостоятельная работа
1.	Введение	4		72
2.	Угрозы безопасности	10		
3.	Теоретические основы методов защиты информации	10	2	
4.	Защита компьютерных систем	10	8	
5.	Основы криптографии	8	4	
6.	Архитектура защищенных информационных систем	10	6	
7.	Защита сети связи	10	8	
8.	Защита услуг связи	10	8	
Всего		72	36	72

6. Рекомендуемые образовательные технологии

Активные и интерактивные формы проведения занятий являются основными при реализации образовательной программы. Вовлечение аспирантов в работу действующих исследовательских групп ФГБУ НИИР.

Интерактивные образовательные технологии, используемые в аудиторных занятиях

Номер раздела, темы	Вид занятия: лекция (Л), семинар (С)	Используемая интерактивная образовательная технология	Кол-во часов
3 - 8	С	Семинар	36
Итого:			36

7. Учебно-методическое обеспечение самостоятельной работы аспирантов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

При изучении дисциплины аспирант должен достаточно много работать самостоятельно, особенно при подготовке к семинарам. Для обеспечения эффективного усвоения материалов дисциплины аспирантам передается перечень вопросов для изучения на семинарах, список основной и дополнительной литературы для самостоятельной работы и темы рефератов. Контроль текущего уровня усвоения изученного материала в течение семестра должен осуществляться путём собеседований. Аттестация по дисциплине проводится на 2-м курсе в 4-м семестре в форме экзамена.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Рекомендуемая литература

а) основная литература

1. Sherri Davidoff, Jonathan Ham Network Forensics Tracking Hackers through Cyberspace. –

Upper Saddle River, NJ . – 2012. – 521 p.
2. Christof Paar, Jan Pelzl Understanding Cryptography: A Textbook for Students and Practitioners. – Springer Heidelberg Dordrecht London New York. – 2012. – 367 p.
3. Актуальные проблемы безопасности информационных технологий: материалы III Международной научно-практической конференции / под общей ред. О.Н. Жданова, В. В. Золотарева; Сиб. гос. аэрокосмич. ун-т. – Красноярск, 2009. – 144 с.

б) **Дополнительная литература:**

1. _Мещеряков Р.В., Шелупанов А.А., Белов Е.Б., Лось В.П. Основы информационной безопасности. – М.: Горячая линия – Телеком, 2006. – 540 с.
2. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М: Академический проект; Фонд «Мир», 2003. – 640 с.

в) Интернет-ресурсы

1. Ассоциация безопасности в промышленности (Security Industry Association) – http://www.securitygateway.com
2. About.com Metwork/Internet Security Forum – http://netsecurity.about.com
3. CERIAS (Purdue University) – http://www.cerias.purdue.edu
4. CERT Coordination Center (Carnegie Mellon University) – http://www.cert.org
5. Институт Компьютерной Безопасности – http://www.gocsi.com
6. Институт SANS – http://www.sans.org
7. Информационная безопасность (Information Security) – http://www.infosecuritymag.com
8. Компьютерная защита и разведка – http://www.c4i.org
9. Отделение компьютерных преступлений и интеллектуальной собственности (CCIPS – Computer Crime and Intellectual Property Section) при криминальном управлении департамента юстиции США – http://www.cybercrime.gov
10. Packet Storm – http://www.packetstormsecurity.org

8.2 Программное обеспечение и Internet-ресурсы:

- Каталог по безопасности www.sec.ru.
- Компьютерная безопасность www.bugtraq.ru
- Программные средства MS Office, антивирусные программы.

9. Материально-техническое обеспечение дисциплины

Лекционно-демонстрационный класс.
Проектор.
Компьютеры, с подключением к Интернету.

Аннотация рабочей программы дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки:2.2.15 Системы, сети и устройства телекоммуникаций
Профиль подготовки:2.2 – Электроника, фотоника, приборостроение и связь
Квалификация выпускника: исследователь, преподаватель-исследователь
Форма обучения: очная.

Общая трудоёмкость дисциплины 5 зачетных единиц (180 академических часов). Форма контроля изучения дисциплины – защита реферата и итоговый экзамен на 2-м курсе обучения.

Цели и задачи освоения дисциплины

Цель преподавания дисциплины: обеспечить аспирантов знаниями об архитектуре современных пакетных сетей, включая сети последующих поколений (СПП); ознакомить их с моделями угроз безопасности и с программными и аппаратными средствами защиты в следующих аспектах безопасности: контроль доступа; аутентификация; сохранность данных; конфиденциальность данных; безопасность связи; целостность данных; доступность.

Задачи освоения дисциплины:

1. Овладение методом достижения информационной безопасности при помощи доверенной модели.
2. Овладение методом защиты сети и инфраструктуры поставщика услуг, его активов и ресурсов, таких как элементы сети, системы, компоненты, интерфейсы, а также данные и информацию, его связь, т. е. сигнализацию, управление и трафик данных/канала передачи.
3. Овладение методом защиты голосовых услуг, услуг передачи видео и данных.
4. Овладение методом защиты соединения и информации оконечного пользователя, включая личную информацию.
5. Овладение методом обеспечения безопасности соединений конечных пользователей через административные домены множества сетей.

Требования к результатам освоения дисциплины

В результате изучения дисциплины аспирант должен обладать следующими компетенциями:

а) универсальными компетенциями (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);

б) общепрофессиональными компетенциями (ОПК):

– владением методологией теоретических и экспериментальных исследований в области профессиональной деятельности (ОПК-1);

в) профессиональными компетенциями (ПК):

– способностью к самостоятельному проведению научно-исследовательской работы и получению научных результатов, удовлетворяющих установленным требованиям к содержанию диссертаций на соискание ученой степени кандидата наук по направлению 2.2.15 Системы, сети и устройства телекоммуникаций (ПК-1);

– способностью ставить и решать прикладные учебно-методические задачи, обосновать выбор методик преподавания специальных дисциплин в ВУЗе (ПК-2).

Основные разделы дисциплины

1. Введение
2. Угрозы безопасности
3. Теоретические основы методов защиты информации
4. Защита компьютерных систем
5. Основы криптографии
6. Архитектура защищенных информационных систем
7. Защита сети связи
8. Защита услуг связи

Разработчики: Веерпалу В.Э., Директор НТЦ А ЭМС ФГБУ НИИР, д.т.н.
Мырова Л.О., ведущий научный сотрудник НТЦ А ЭМС ФГБУ НИИР, д.т.н.
Корж В.А., заместитель директора НТЦ А ЭМС ФГБУ НИИР, к.т.н.
Иванкович М.В., заместитель директора ЦИПБТС ФГБУ НИИР, к.т.н.