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

«28» декабря 2022 г.

Утверждаю

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

О.А. Иванов

«21» декабря 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ АСПИРАНТОВ ПО ДИСЦИПЛИНЕ «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

Руководитель аспирантуры

«____» _____ 2022 г.

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.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ КОНТРОЛЯ УСПЕВАЕМОСТИ АСПИРАНТОВ ПО ДИСЦИПЛИНЕ «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

Руководитель аспирантуры

«____»_____2022 г.

Москва, 2022 г.

Контроль успеваемости аспирантов по дисциплине «Информационная безопасность» осуществляется:

при помощи опросов на лекциях по пройденному ранее материалу;

путем публичной защиты рефератов;

по результатам итогового экзамена.

1) Контроль успеваемости аспирантов при помощи опросов на лекциях по пройденному ранее материалу (поверка компетенции УК-1[1])

Опрос аспирантов по пройденному ранее материалу осуществляется на каждой лекции.

Критерий – полное усвоение материала.

При неполном усвоении материала допускается изложение аспирантом материала на следующем занятии.

2) Контроль успеваемости аспирантов при помощи путем публичной защиты реферата (поверка компетенций ОПК-1[2], ПК-1[3], ПК-2[4])

Защита курсового проекта осуществляется на семинаре-конференции с участием аспирантов всех курсов. Защита проводится с участием двух официальных оппонентов старших курсов. Критерий – успешная защита реферата.

При неудачной защите допускается повторная защита переработанного курсового проекта с участием тех же официальных оппонентов.

Темы рефератов приведены в Приложении 1.

3) Контроль по результатам итогового экзамена по программе кандидатского минимума по спецпредмету (поверка компетенций УК-1[5], ОПК-1[6], ПК-1[7], ПК-2[8])

---

[1] способность к критическому анализу и оценке современных научных достижений, к генерированию новых идей при решении исследовательских и практических задач

[2] владение методологией теоретических и экспериментальных исследований в области профессиональной деятельности

[3] способностью к самостоятельному проведению научно-исследовательской работы и получению научных результатов

[4] способностью ставить и решать прикладные учебно-методические задачи, обосновать выбор методик преподавания специальных дисциплин в ВУЗе

[5] См. примечание 1

[6] См. примечание 2

[7] См. примечание 3

[8] См. примечание 4

Экзамен проводится комиссией из трех преподавателей, имеющих ученую степень доктор или кандидат технических наук. Экзамен проводится по вопросам, Приложение 2. Аспирант выбирает билет с 4 вопросами. По каждому из них аспирант должен ответить после 30-минутной подготовки.

Критерий – полный или практически полный ответ по каждому из вопросов.

Оценка по вопросу – полный ответ «отлично», практически полный ответ «хорошо». Итоговая оценка – полные ответы по всем по двум или трем вопросам – «отлично»; практически полные ответ по трем или четырем вопросам – «хорошо».

При неполном ответе хотя бы на один из вопросов экзамен считается не сданным. Допускается повторная сдача экзамена.

Приложение 1

Темы рефератов по дисциплине «Информационная безопасность»

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

Приложение 2

Темы экзаменационных вопросов по дисциплине «Информационная безопасность»

1. Цели и задачи дисциплины. Терминология. Рекомендации МСЭ-Т по информационной безопасности. Законодательство Российской Федерации в области защиты информации.
2. Понятие угрозы. Виды противников или «нарушителей». Классификация угроз информационной безопасности.
3. Виды угроз: уничтожение, повреждение, удаление, раскрытие, прерывание информации. Характер происхождения угроз (умышленные и естественные факторы).
4. Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.
5. Основные положения теории информационной безопасности. Модели безопасности и их применение.
6. Формальные модели безопасности. Доверительная модель.
7. Дискреционная модель Харрисона-Руззо-Ульмана. Типизированная матрица доступа. Модель распространения прав доступа Take-Grant. Мандатная модель Белла-ЛаПадулы.
8. Политика безопасности. Ограничения на области применения формальных моделей.
9. Использование защищенных компьютерных систем. Аппаратные и программные средства для защиты компьютерных систем от несанкционированного доступа.
10. Средства операционной системы. Средства резервирования данных. Проверка целостности. Способы и средства восстановления работоспособности.
11. Методы криптографии. Симметричное и асимметричное шифрование.
12. Алгоритмы шифрования. Электронно-цифровая подпись. Алгоритмы электронно-цифровой подписи.
13. Хеширование. Имитовставки. Криптографические генераторы случайных чисел. Способы распространения ключей.
14. Обеспечиваемая шифром степень защиты. Криптоанализ и атаки на криптосистемы. Сжатие информации. Квантовая криптография.
15. 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.
16. Метод достижения информационной безопасности при помощи доверенной модели.
17. 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.
18. Метод защиты голосовых услуг, услуг передачи видео и данных.
19. Метод защиты соединения и информации оконечного пользователя, включая персональную информацию.
20. Метод обеспечения безопасности соединений конечных пользователей через административные домены множества сетей.