МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА
по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность

Ставрополь, 2022

Введение

Программа кандидатского экзамена по научной специальности 2.3.6 Методы и системы защиты информации, информационная безопасность разработана для аспирантов и соискателей.

Изучение дисциплины «Методы и системы защиты информации, информационная безопасность» и последующая сдача экзамена являются обязательными для каждого соискателя ученой степени кандидата наук, позволяя соблюсти единый минимум требований к уровню знаний в области информационной безопасности.

Аспирант подтверждает степень освоения подготовкой и защитой реферата. Без сдачи рефератов аспирант (соискатель) не допускается к кандидатскому экзамену.

Порядок сдачи кандидатского экзамена

Порядок организации приема кандидатских экзаменов определяется соответствующими нормативными документами и предусматривает обязательное написание реферата по соответствующей научной специальности.

Цель экзамена – установить глубину профессиональных и научных знаний аспиранта или соискателя ученой степени.

В экзаменационный билет включаются 3 вопроса.

Для подготовки по билету отводиться 45 минут. При подготовке к ответу аспиранту или соискателю предоставляется право пользования программой кандидатского экзамена.

Подготовка реферата по научной специальности

Отдельным этапом является подготовка аспирантом или соискателем реферата по научной специальности. Аспирант на базе самостоятельного изучения материала готовит реферат по научной специальности, соответствующей направлению его научного исследования. Проверку подготовленного реферата проводит научный руководитель. При наличии оценки «зачтено» по реферату аспирант или соискатель допускается к сдаче кандидатского экзамена.

Критерии оценивания

Оценка «отлично» выставляется аспиранту, если он глубоко и прочно усвоил материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, использует в

ответе материал монографической литературы, правильно обосновывает принятое решение.

Оценка «хорошо» выставляется аспиранту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения.

Оценка «удовлетворительно» выставляется аспиранту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения в применении теоретических положений на практике.

Оценка «неудовлетворительно» выставляется аспиранту, который не знает значительной части программного материала, допускает существенные ошибки, не может увязывать теорию с практикой.

СОДЕРЖАНИЕ КУРСА

Вопросы для подготовки к кандидатскому экзамену

Современное состояние защиты информации, перспектива и ретроспектива. Информационные системы, средства, каналы, сети и среды. Основные положения теории защиты информации. Определение и основные понятия теории защиты информации. Общеметодологические принципы формирования теории защиты информации. Стратегии защиты информации.

Государственная система защиты информации Российской Федерации. Организационные системы обеспечения безопасности информации. Концептуальные положения организационного обеспечения информационной безопасности. Организация службы безопасности объекта. Структура и деятельность службы безопасности. Организация охраны объектов

Правовые механизмы информационной безопасности Российской Федерации. Правовое регулирование отдельных видов информации. Правовое регулирование деятельности по защите информации. Нарушения правового характера в сфере информационной безопасности. Правовые основы и особенности расследования преступлений в сфере информационной безопасности

Борьба с компьютерными преступлениями. Административная и уголовная ответственность в сфере в сфере информационной безопасности. Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию. Порядок сертификации средств защиты информации.

Электронные вычислительные машины: классификация, принципы построения, основные характеристики. Программное обеспечение ЭВМ – состав и назначение программных средств. Компьютерные сети: классификация, аппаратное, программное и информационное обеспечение, топология.

Информационная безопасность в операционных системах. Угрозы безопасности операционной системы. Административные меры защиты. Архитектура подсистемы защиты операционной системы.

Системы управления базами данных (СУБД) – сравнительный анализ. Архитектура современных сетевых СУБД. Модели безопасности СУБД. Архитектура системы безопасности СУБД.

Модели безопасности. Субъекты, объекты и доступ. Монитор безопасности пересылок. Основные вида политик безопасности.

Дискреционный контроль и управление доступом. Матрица доступа. Модель Харрисона, Руззо и Ульмана. Модель распространения прав доступа TAKE-GRANT. Санкционированное получение прав доступа. Похищение прав доступа. Расширенная модель Take-Grant.

Модели мандатного контроля и управления доступом. Уровни секретности. Модель Белла и Лападула. Критика модели Белла и Лападула.

Модели контроля целостности. Модель Биба. Модель Кларка—Вилсона. Объединение моделей безопасности.

Ролевые модели доступа. Пользователи, роли и операции. Роли и иерархия ролей. Авторизация и активация роли. Операционное разделение обязанностей и доступ к объектам.

Защита информации в компьютерных сетях. Основные типы сетевых атак и методы противодействия им. Обеспечение информационной безопасности сетей. Применение технологии межсетевых экранов в задачах проектирования защищенных ЛВС. Прокси-серверы. Антивирусная защита. Системы обнаружения вторжений. Протоколы защищенного канала. IPSEC.

Технологии безопасности беспроводных сетей. Протоколы и функции, применяемые в межсетевых экранах и интернет-маршрутизаторах. Протоколы IGMP и UPnP. Качество обслуживания и Технология SharePort. Фильтрация трафика и виртуальные сети. Технология преобразования сетевых адресов, механизмы PAT и NAT. Функции IDP, WCF, AV и технология ZoneDefense. Особенности применения межсетевых экранов и маршрутизаторов.

Характеристика компьютерных вирусов: классификация вирусов, файловые вирусы, загрузочные вирусы, вирусы для операционных систем. Методы и средства борьбы с вирусами. Профилактика заражения вирусами компьютерных систем и сетей. Порядок действий пользователя при обнаружении заражения ЭВМ вирусами.

Технические каналы утечки информации. Структура, классификация и основные характеристики. Технические каналы утечки информации при передаче ее по каналам связи. Технические каналы утечки речевой информации. Технические каналы утечки видовой информации.

Демаскирующие признаки объектов. Демаскирующие признаки объектов в видимом диапазоне электромагнитного спектра. Демаскирующие признаки объектов в инфракрасном диапазоне электромагнитного спектра. Демаскирующие признаки радиоэлектронных средств.

Средства выявления каналов утечки информации. Индикаторы электромагнитного поля. Сканирующие радиоприемники. Анализаторы

спектра, радиочастотомеры. Многофункциональные комплекты для выявления каналов утечки информации. Комплексы измерения ПЭМИН. Нелинейные локаторы. Комплексы для измерения характеристик акустических сигналов. Металлодетекторы. Рентгенотелевизионные установки. Досмотровые эндоскопы.

Скрытие и защита информации от утечки по техническим каналам. Концепция и методы инженерно-технической защиты информации. Экранирование электромагнитных волн. Безопасность оптоволоконных кабельных систем. Заземление технических средств и подавление информационных сигналов в цепях заземления. Фильтрация информационных сигналов. Пространственное и линейное зашумление. Способы предотвращения утечки информации через ПЭМИН ПК. Устройства контроля и защиты слаботочных линий и сети. Скрытие и защита от утечки информации по акустическому и виброакустическому каналам. Скрытие речевой информации в телефонных системах с использованием криптографических методов.

Методы и средства инженерной защиты и технической охраны объектов. Категории объектов защиты. Особенности задач охраны различных типов объектов. Общие принципы обеспечения безопасности объектов. Система охранно-тревожной сигнализации. Система контроля и управления доступом. Телевизионные системы. Система пожарной сигнализации. Периметровая охрана.

Технический контроль эффективности мер защиты информации. Цели и задачи технического контроля эффективности мер защиты информации. Порядок проведения контроля защищенности информации на объекте ВТ от утечки по каналу ПЭМИ. Методы испытаний. Порядок проведения контроля защищенности АС от НСД. Методы контроля побочных электромагнитных излучений генераторов технических средств. Порядок проведения контроля защищенности выделенных помещений от утечки акустической речевой информации.

Аттестация объектов информатизации. Мероприятия по выявлению и оценке свойств каналов утечки информации.

Математические основы криптографии. Элементы теории чисел, абстрактной алгебры и алгебраической геометрии. Простые числа и непрерывные дроби. Мультипликативные функции. Сравнение целых чисел по модулю. Решение сравнений первой степени. Группы и их свойства. Кольца и тела в абстрактной алгебре. Конечные поля. Эллиптические кривые над конечными полями.

Нормативно-правовые основы криптографической защиты информации. Действующие стандарты криптографической защиты информации. Федеральный закон об электронной подписи. Нормативно-правовые акты ФСБ по обеспечению безопасности персональных данных с использованием средств криптографической защиты информации (СКЗИ). Нормативно-правовые акты ФСБ по обеспечению функционирования и эксплуатации СКЗИ. Виды работ и услуг, составляющих лицензируемую деятельность с

использованием СКЗИ. Порядок лицензирования деятельности с использованием СКЗИ. Правила сертификации СКЗИ по требованиям ФСБ. Таможенные ограничения на ввоз и вывоз СКЗИ

Основные задачи современной криптографии. Конфиденциальность. Целостность. Аутентификация. Неотслеживаемость. Цифровая подпись. Управление ключами. Общие требования к криптосистемам.

Симметричные криптографические преобразования. Принципы симметричной (одноключевой) криптографии. Практические симметричные криптоалгоритмы. Стандарты симметричных криптосистем

Алгоритмы преобразования сообщений в криптографических системах с открытым ключом. Алгоритм криптографической системы RSA. Алгоритм криптографической системы на основе вычисления дискретных логарифмов в конечном поле — алгоритм Эль Гамаля. Алгоритм функционирования криптографической системы на основе дискретного логарифмирования в метрике эллиптических кривых. Экспериментальное исследование криптографических систем с открытым ключом.

Комплексирование криптосистем с открытым и закрытым ключом. Преимущества и недостатки одно- и двухключевых криптосистем. Преобразование Диффи — Хеллмана в системах криптографии с открытым ключом. Алгоритм автоматического формирования парных симметричных ключей шифрования — дешифрования открытых сообщений на рабочих станциях абонентов информационно-телекоммуникационной системы. Алгоритм Диффи — Хеллмана автоматического формирования парных симметричных ключей шифрования — дешифрования.

Алгоритмы электронной цифровой подписи. Принцип аутентификации сообщений посредством электронной цифровой подписи. Алгоритм RSA формирования и аутентификации электронной цифровой подписи. Алгоритм Эль Гамаля (EGSA) формирования электронной цифровой подписи. Алгоритм DSA формирования электронной цифровой подписи. Алгоритм формирования электронной цифровой подписи на основе разложения на множители больших простых чисел. Алгоритм формирования электронной цифровой подписи по ГОСТ Р34.10–2012.

Стеганографическая защита электронных сообщений. Принципы стеганографии. Алгоритмы стеганографических преобразований.

Методы идентификации объектов информационной инфраструктуры в компьютерных технологиях. Принципы идентификации объектов. Методы аутентификации на основе паролей. Механизмы аутентификации санкционированных пользователей. Протоколы аутентификации с нулевой передачей знаний.

Классификация средств криптографической защиты информации (СКЗИ). Классификация средств криптографической защиты информации по различным признакам. Требования к средствам криптографической защиты информации. Программные СКЗИ. Особенности и примеры. Аппаратные и программно-аппаратные СКЗИ. Критерии выбора СКЗИ. Основные принципы построения СКЗИ. Принципы построения аппаратных СКЗИ. Принципы

построения программных и программно-аппаратных СКЗИ. Основные подходы к обеспечению надежности СКЗИ.

Квантовая криптография. Природа секретности квантового канала связи. Основные направления развития квантовой криптографии. Протоколы квантового обмена информацией. Квантовый криптоанализ. Проблемы практической реализации систем квантовой криптографии.

Биометрическая идентификация личности. Биометрические характеристики личности. Биометрические системы аутентификации. Режимы работы биометрической системы аутентификации. Организация биометрического контроля доступа.

Биометрический контроль доступа по статическим характеристикам. Контроль доступа по папиллярному узору. Контроль доступа по геометрии лица. Контроль доступа по сетчатке. Контроль доступа по радужке. Контроль доступа по геометрии кисти руки. Контроль доступа по термограммам лица и кистей рук.

Биометрический контроль доступа по динамическим характеристикам. Особенности динамических характеристик личности. Контроль доступа по голосу. Контроль доступа по рукописи. Контроль доступа по клавиатурному почерку. Клавиатурный мониторинг. Классификация образов динамической биометрии. Тестирование динамических биометрических систем контроля доступа.

Точность и безопасность биометрических систем контроля доступа. Ошибки биометрических систем. Интеграция данных. Безопасность биометрических систем.

Актуальность проблемы защиты персональных данных в информационных системах. Нормативно-правовое обеспечение защиты персональных данных.

Автоматизированная и неавтоматизированная обработка персональных данных.

Угрозы и уязвимости безопасности персональных данных при их обработке в информационных системах. Модель угроз персональных данных. Организационно-распорядительная документация по защите персональных данных.

Организационные и технические мероприятия по защите персональных данных в информационных системах.

Построение системы защиты персональных данных.

Аттестация, сертификация и лицензирование в области защиты персональных данных.

Этапы создания системы безопасности объекта информатизации. Разработка технического задания на проектирование и эксплуатацию объекта информатизации.

Оценка эффективности функционирования системы безопасности: понятие эффективности, выбор показателей целевой и экономической эффективности функционирования системы, алгоритмы определения значений показателей эффективности. Создание организационной структуры

системы безопасности компьютерных сетей для выполнения организационных мер защиты, эксплуатации аппаратных, программных и криптографических средств защиты, контроля за установленными правилами эксплуатации.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л., Груздева, Ю. С. Нахаева. - 2-е изд., стереотип. - М.: Горячая линия-Телеком, 2012. - 550 с.: ил.

2. Краковский, Ю. М. Методы защиты информации: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург: Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401 (дата обращения: 06.12.2022). — Режим доступа: для авториз. пользователей.

3. Куприянов, А. И. Исследование криптографических методов защиты информации: учебное пособие / А. И. Куприянов, В. Ф. Макаров. — Москва: Московский государственный технический университет имени Н.Э. Баумана, 2019. — 110 с. — ISBN 978-5-7038-5059-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/110633.html

4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва: Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489242 (дата обращения: 18.10.2022).

5. Технические средства и методы защиты информации: учебное пособие / А. П. Зайцев, А. А. Шелупанов, Р. В. Мещеряков, И. В. Голубятников. — Москва: Горячая линия-Телеком, 2012. — 616 с. — ISBN 978-5-9912-0084-4. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/5154 (дата обращения: 18.10.2022).

Дополнительная литература

1. Брюхомицкий, Ю. А. Биометрические технологии идентификации личности: учебное пособие / Ю. А. Брюхомицкий. — Ростов-на-Дону, Таганрог: Издательство Южного федерального университета, 2017. — 263 с.

— ISBN 978-5-9275-2454-9. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/87400.html

2. Бутакова, Н. Г. Криптографические методы и средства защиты информации: учебное пособие / Н. Г. Бутакова, Н. В. Федоров. — Санкт-Петербург: Интермедия, 2020. — 380 с. — ISBN 978-5-4383-0210-0. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/104000.html.

3. В.И. Петренко. Защита персональных данных в информационных системах: Учебное пособие. Курс лекций. – Ставрополь: Изд-во СКФУ, 2016 г. - 210 с.

4. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.

5. Костромитин, К. И. Инженерно-техническая защита информации и технические средства охраны на критически важных объектах: учебное пособие / К. И. Костромитин. — Москва: Ай Пи Ар Медиа, 2022. — 137 с. — ISBN 978-5-4497-1765-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/122647.html.

6. Леонтьев, А. С. Защита информации: учебное пособие/ А. С. Леонтьев. — Москва: РТУ МИРЭА, 2021. — 79 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/182491— Режим доступа: для авториз. пользователей.

7. Масюк, М. А. Основные понятия и правовые основы защиты информации: учебное пособие / М. А. Масюк, А. А. Попов, Е. В. Касьянова. — Красноярск: СибГУ им. академика М. Ф. Решетнёва, 2020. — 82 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/195152

8. Международные и российские акты и стандарты по информационной безопасности: учебное пособие/ А.В. Солодянников. – СПб.: Изд-во СПбГЭУ, 2017. – 87 с. ISBN 978-5-7310-4041-9.

9. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. -М.: Горячая линия - Телеком, 2006. - 544 с.: ил.

10. Основы информационной безопасности: учебное пособие/ В.В. Сухостат, И.Н. Васильева. – СПб: Изд-во СПбГЭУ, 2019. – 103 с. ISBN 978-5-7310-4634-3.

11. Петренко В. И. Теоретические основы защиты информации: учебное пособие. – Ставрополь: Изд-во СКФУ, 2015. – 222 с.

12. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва: Издательство Юрайт, 2022. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8.

13. Программно-аппаратные средства защиты информации: учебное пособие для студентов вузов по направлению подготовки «Информационная безопасность» / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.] ; под редакцией В. К. Головати. — Санкт-Петербург: Интермедия, 2018. — 408 с. — ISBN 978-5-4383-0157-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/73644.html.

14. Программно-аппаратные средства обеспечения информационной безопасности. Учебное пособие для вузов / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов. Под редакцией А. В. Душкина. М.: Горячая линия - Телеком, 2018. - 248 с: ил.

15. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.

16. Технологии защиты информации в компьютерных сетях: учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — 3-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 368 с. — ISBN 978-5-4497-0931-8. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/102069.html.

17. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3 т. Том 1. Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с.: ил.

Интернет-ресурсы

1. Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/ -

3. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/

4. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/

5. Интернет портал Защита-информации.SU http://www.iso27000.ru/

6. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru

7. Консорциум сетевых электронных библиотек ЭБС«Лань» https://e.lanbook.com/

8. ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/

9. ЭБС IPR SMART https://www.iprbookshop.ru/

10. ЭБС Znanium https://znanium.com/

11. ЭБС «Юрайт» http://www.biblio-online.ru

12. Поисковые интернет-системы Яндекс, Rambler, Google и др.

13. Common Vulnerabilities and Exposures/ База данных общеизвестных уязвимостей информационной безопасности https://cve.mitre.org/

14. MITRE ATT&CK® база знаний о тактике и методах противника https://attack.mitre.org/