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

ПРОГРАММА КАНДИДАТСКОГО ЭКЗАМЕНА
по научной специальности 1.2.4 «Кибербезопасность»

Ставрополь, 2024

Введение

Программа кандидатского экзамена по научной специальности 1.2.4. Кибербезопасность.

Изучение дисциплины «Кибербезопасность» 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

1. Анализ известных и вновь выявляемых уязвимостей, их систематизация.
2. Разработка методов интеллектуального поиска новых классов уязвимостей.
3. Моделирование политик информационной безопасности, угроз и атак.
4. Методические основы разработки профилей защиты.

5. Методы проектирования, моделирования, анализа, трансформации программ для выявления потенциальных уязвимостей в программных системах.

6. Разработки требований, проектирования архитектуры, разработки программного кода, тестирования, верификации, сертификации и эксплуатации.

7. Методы, алгоритмы и средства пострелизного глубокого анализа защищенности программно-аппаратного обеспечения.

8. Методы интеграции средств защиты на уровне аппаратуры и на уровне программного обеспечения.

9. Методы, алгоритмы и средства обеспечения устойчивого функционирования программно-аппаратных систем в условиях злонамеренного воздействия

10. Методы обфускации и безопасной компиляции программ.

11. Интеллектуальный масштабируемый мониторинг инцидентов безопасности в распределенных программно-аппаратных системах.

12. Методы оперативного реагирования на выявленные угрозы.

13. Масштабируемые средства интеллектуального анализа данных и процессов в распределенных системах, включая социальные сети.

14. Разработка методических основ для создания и развития метрик оценки защищенности,

15. Разработка уровня доверия компьютерных систем и стандартов в области кибербезопасности.

16. Системы и языки программирования.

17. Машинно-ориентированные, проблемно-ориентированные и универсальные языки. Алфавит, синтаксис и семантика.

18. Способы описания языков программирования. Трансляция.

19. Типы данных, способы задания типа. Константы и переменные. Идентификаторы.

20. Структурированные типы данных. Выражения, операции, операторы.

21. Арифметические и логические операции и операторы. Программирование ввода и вывода информации.

22. Подпрограммы, методы передачи параметров при использовании подпрограмм. Основы объектно-ориентированного программирования. Инкапсуляция, наследование, полиморфизм.

23. Шифры замены и перестановки, их свойства, композиции шифров. Криптостойкость шифров, основные требования к шифрам.

24. Теоретическая стойкость шифров, совершенные и идеальные шифры.

25. Блоковые шифры. Потоковые шифры.

26. Криптографические хеш-функции, их свойства и использование в криптографии.

27. Методы получения случайных последовательностей, их использование в криптографии.

28. Системы шифрования с открытыми ключами. Криптографические протоколы.

29. Протоколы распределения ключей. Протоколы идентификации.

30. Парольные системы разграничения доступа. Цифровая подпись. Стойкость систем с открытыми ключами.

Учебно-методическое и информационное обеспечение дисциплины

Основная литература

1. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. - М.: Высшая школа экономики, 2017. – 252с.

2. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях. - М.: ДМК Пресс, 2019. – 325с.

3. Фомичёв, В.М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Юрайт, 2017. – 564с.

4. Фомичёв, В. М. Криптографические методы защиты информации. В 2 ч. Часть 2. Системные и прикладные аспекты: учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников; под ред. В. М. Фомичёва. — М.: Юрайт, 2018. – 346с.

5. Актуальные проблемы информационного права. Учебник для вузов. ФГОС 3+. В.И. Авдийский, Г.О. Крылов и др.; под ред. И.Л. Бачило, М.А. Лапиной, М.: JUSTITIA, 2017.

Дополнительная литература

1. Белоус А., Солодуха В. Кибероружие и кибербезопасность. О сложных вещах простыми словами. – М.: Инфа-Инженерия, – 2023, Цифровая книга.

2. Диогенес Ю. Озкайя Э. Кибербезопасность. Стратегии атак и обороны. – М.: ДМК-Пресс, – 2020, 326с.

3. Ревенков П., Дудка А, Бердюгин А. Кибербезопасность в условиях электронного банкинга. – М.: Прометей, – 2020, 522с.

Интернет-ресурсы

1. Электронная библиотечная система «Университетская библиотека ONLINE». - URL: http://www.biblioclub.ru
2. Электронная библиотечная система издательства «Лань». - URL: http://www.e.lanbook.com
3. Электронная библиотечная система «Юрайт». - URL: http://www.biblioonline.ru
4. Электронная библиотечная система eLIBRARY.RU. - URL: http://www.elibrary.ru
5. Общероссийский портал Math-Net.Ru - это современная информационная система, предоставляющая российским и зарубежным ученым различные возможности в поиске научной информации по математике, физике, информационным технологиям и смежным наукам. - URL: https://www,matlinet.ru/
6. Международная издательская компания, специализирующаяся на

издании академических журналов и книг по естественно-научным направлениям. - URL: https://link.springer.com/

7. Научная библиотека ТГУ. - URL: http://www.lib.tsu.ru/

8. Электронная библиотека диссертаций РГБ. - URL: http://wvvw.diss.rsl,ru.'

9. Научная электронная библиотека. - URL: http://elibrary.ru/