УТВЕРЖДАЮ:
Председатель приемной комиссии УлГУ
Б.М. Костишко
5 апреля 2022 г.

ПРОГРАММА

вступительных испытаний по научной специальности

1.2.4. КИБЕРБЕЗОПАСНОСТЬ

для поступающих на обучение по программам подготовки научных и научно-педагогических кадров в аспирантуре Ульяновского государственного университета

Сведения о разработчиках:

ФИО	Аббревиатура кафедры	Ученая степень, звание
Смагин Алексей Аркадьевич	ТТС	д.тех.н., профессор

Ульяновск, 2022

1. Общие положения

1.1. Программа вступительного испытания по специальной дисциплине соответствующей научной специальности программы подготовки научных и научно-педагогических кадров в аспирантуре 1.2.4. Кибербезопасность (далее - Программа), сформирована на основе требований федеральных государственных образовательных стандартов высшего образования к программам магистратуры (специалитета) по соответствующим направлениям (специальностям) подготовки. Программа разработана для поступления на обучение в аспирантуру УлГУ.

Программой устанавливается:

- форма, структура, процедура сдачи вступительного испытания;
- шкала оценивания;
- максимальное и минимальное количество баллов для успешного прохождения вступительного испытания;
- критерии оценки ответов.

Вступительное испытание проводится на русском языке.

1.2. Организация и проведение вступительного испытания осуществляется в соответствии с Правилами приема, утвержденными решением Ученого совета УлГУ, действующими на текущий год поступления.

1.3. По результатам вступительного испытания, поступающий имеет право подать на апелляцию о нарушении, по мнению поступающего, установленного порядка проведения вступительного испытания и (или) о несогласии с полученной оценкой результатов вступительного испытания в порядке, установленном Правилами приема, действующими на текущий год поступления.

2. Форма, структура, процедура, программа вступительного испытания и шкала оценивания ответов

2.1. Вступительное испытание по специальной дисциплине проводится в форме устного экзамена в соответствии с перечнем тем и (или) вопросов, установленных данной Программой.

2.2. Процедура проведения экзамена представляет собой сдачу экзамена в очной форме и (или) с использованием дистанционных технологий (при условии идентификации поступающих при сдаче ими вступительных испытаний):
очно и дистанционно.

2.3. Результаты проведения вступительного испытания оформляются протоколом, в котором фиксируются вопросы экзаменаторов к поступающему. На каждого поступающего ведется отдельный протокол.

2.4. Программа экзамена.

Примерный перечень тем и вопросов для подготовки к сдаче экзамена и

формирования билетов.

1.2.4. КИБЕРБЕЗОПАСНОСТЬ

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 с учетом специфики фаз жизненного цикла.
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, проблемноориентированные 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

Список рекомендуемой литературы:

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.

2.5. Шкала оценивания ответов на экзамене

неудовлетворительно	**удовлетворительно**	**хорошо**	**отлично**
до 39 баллов	40 - 74 баллов	75 - 84 баллов	85 - 100 баллов

Общая продолжительность экзамена составляет 45 минут.

Максимальное количество баллов за экзамен – 100. Минимальное количество баллов для успешного прохождения экзамена - 40. Поступающий, набравший менее 40 баллов за экзамен, не может быть зачислен в аспирантуру.

Таблица критериев оценки устных и письменных ответов (при наличии)

Вид деятельности		
Оценка	Балл	Уровень владения темой
неудовлетворительно	до 39	Ответ на поставленный вопрос не дан или ответ неполный, отсутствует логичность повествования или допущены существенные логические ошибки
удовлетворительно	40-74	Ответ полный, допущены не существенные логические ошибки
хорошо	75-84	Ответ логичный, конкретный, присутствуют незначительные пробелы в знаниях материала программы
отлично	85-100	Ответ полный, логичный, конкретный, без замечаний. Продемонстрированы знания материала программы, умение решать предложенные задачи

Вступительное испытание проводится экзаменационной комиссией, действующей на основании приказа ректора.

Итоговая оценка за экзамен определяется как средний балл, выставленный всеми членами комиссии.