Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Ярославский государственный технический университет»

Утверждаю:
Председатель приемной комиссии,
ректор ФГБОУ ВО «ЯГТУ»

_____ Е.О. Степанова

19.01.2026

Программа вступительного испытания в аспирантуру
по научной специальности 2.3.6 «Методы и системы защиты информации, информационная безопасность»

ЯГТУ самостоятельно проводит вступительное испытание при приеме на обучение по программам аспирантуры. Вступительное испытание проводится с каждым поступающим индивидуально. Экзаменационная комиссия в устной форме проводит собеседование по темам, представленным в приложении № 1 к настоящей программе. Цель собеседования – определить готовность поступающего к освоению выбранной программы аспирантуры.

Минимальное количество баллов, подтверждающее успешное прохождение вступительного испытания и необходимое для участия в конкурсе – 70.

Максимальное количество баллов за вступительное испытание – 100.

Критерии оценивания:

Оценка от 81 до 100 баллов	Соответствует высокому уровню подготовленности поступающего (поступающий исчерпывающе и точно ответил на все вопросы, продемонстрировал отличное владение базовыми знаниями в области выбранного направления).
Оценка от 61 до 80 баллов	Соответствует хорошему уровню подготовленности поступающего (поступающий точно и без повторных наводящих вопросов ответил на 60 – 80 % вопросов, продемонстрировал хорошее владение базовыми знаниями в области выбранного направления).
Оценка от 41 до 60 баллов	Соответствует удовлетворительному уровню подготовленности поступающего (поступающий точно и без повторных наводящих вопросов ответил на менее 60 % вопросов, продемонстрировал удовлетворительное владение базовыми знаниями в области выбранного направления).
Оценка от 21 до 40 баллов	Соответствует неудовлетворительному уровню подготовленности поступающего (поступающий не смог в полной мере продемонстрировать владение базовыми знаниями в области выбранного направления, при этом неудовлетворительно отвечал на заданные комиссией вопросы).
Оценка от 1 до 20 баллов	Выставляется за неподготовленность поступающего, проявившуюся в неспособности ответить на большую часть вопросов, заданных комиссией, и/или за грубые ошибки в базовых вопросах.
0 баллов	Оценка не выставляется в случае отсутствия ответа.

Приложение № 1

Перечень тем для подготовки к собеседованию

1. **Теоретические основы обеспечения информационной безопасности и защиты информации**
   1.1. Основные положения Доктрины информационной безопасности Российской Федерации.
   1.2. Информационная безопасность в системе национальной безопасности Российской Федерации. Критическая информационная инфраструктура Российской Федерации. Субъекты и объекты критической информационной инфраструктуры.
   1.3. Основные положения Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».
   1.4. Основные положения Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
   1.5. Классификация методов и средств обеспечения безопасности информации.
   1.6. Определение и принципы построения систем защиты информации.
   1.7. Риски, уязвимости и угрозы безопасности информации, их взаимосвязь. Классификация источников угроз безопасности информации.

2. **Безопасность компьютерных сетей и программно-аппаратные средства защиты информации**
   2.1. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения прав доступа.
   2.2. Основные сетевые атаки. Классическая модель системы обнаружения вторжений (СОВ). Требования к СОВ.
   2.3. Модели защиты от угрозы отказа в обслуживании.
   2.4. Программно-аппаратные средства обеспечения информационной безопасности в вычислительных сетях.
   2.5. Резидентный компонент безопасности. Средства доверенной загрузки.
   2.6. Методы и средства антивирусной защиты.
   2.7. Организация управления доступом и защиты ресурсов ОС. Основные механизмы безопасности: средства и методы аутентификации в ОС.
   2.8. Модели разграничения прав доступа, организация и использование средств аудита.
   2.9. Средства обеспечения безопасности баз данных: средства идентификации и аутентификации объектов баз данных, средства разграничения доступа, концепция и реализация механизма ролей.
   2.10. Организация аудита событий в системах баз данных; средства контроля целостности информации, организация взаимодействия СУБД и базовой ОС, журнализация, средства создания резервных копий и восстановления баз данных.

3. **Методы криптографической защиты информации**
   3.1. Базовые криптографические примитивы. Шифры перестановки и замены.
   3.2. Криптосистемы с секретным ключом.
   3.3. Криптосистемы с открытым ключом.
   3.4. Криптография на эллиптических кривых.
   3.5. Криптографическая стойкость шифров. Активные и пассивные атаки на шифрсистемы. Теоретически стойкие шифры.
   3.6. Криптографические хеш-функции.
   3.7. Понятие и классификация криптографических протоколов.

4. **Основы защиты информации от утечки по техническим каналам**
   - 4.1. Структура, классификация и основные характеристики технических каналов утечки информации. Основные методы и средства защиты информации от утечки по техническим каналам.
   - 4.2. Технические каналы утечки акустической (речевой) информации. Основные методы и средства защиты речевой информации в помещениях.
   - 4.3. Обнаружение и локализация закладных устройств, подавление их сигналов.
   - 4.4. Технические каналы утечки информации за счет побочных электромагнитных излучений и наводок (ПЭМИН). Основные методы и средства защиты информации от утечки за счет ПЭМИН.
   - 4.5. Технические каналы утечки информации при передаче по каналам связи. Основные методы и средства защиты информации в каналах связи.

5. **Управление информационной безопасностью**
   - 5.1. Политики обеспечения информационной безопасности и управление системой обеспечения информационной безопасности.
   - 5.2. Анализ и оценка угроз информационной безопасности объекта управления. Методология оценки ущерба от нарушений безопасности информации.
   - 5.3. Понятие секретного (конфиденциального) делопроизводства. Общие принципы его организации.
   - 5.4. Особенности организации защищенного электронного документооборота. Система удостоверения ЭЦП и удостоверяющие центры.

Рекомендуемая литература

Нормативные акты:

1. Доктрина информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 5 декабря 2016 г. № 646).
2. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
5. ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (идентичен ИСО/МЭК 27001:2013). Приказ руководителя Росстандарта № 1653-ст от 30.11.2021 г. Дата введения в действие с 01.01.2022 г.
6. ГОСТ Р ИСО/МЭК 27004-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание» (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. N 388-ст).
7. ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (идентичен ISO/IEC 27005:2008). Приказ руководителя Росстандарта № 632-СТ от 30.11.2011. Дата введения в действие с 01.12.2011.

Основная:

1. Информационная безопасность и защита информации: Учебное пособие /Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.
2. Фомичёв В. М., Мельников Д.А. Криптографические методы защиты информации в 2 ч.: учебник для вузов / под редакцией В. М. Фомичёва. – Москва: Издательство Юрайт, 2022. – 245 с.
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2011. – 320 с.
4. Защита информации в телекоммуникационных системах / Кохановић Г.Ф. и др. - М.: Пресс, 2005.
5. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. 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.: Машиностроение, 2009. – 508 с.
6. Бузов Г.А. Защита информации ограниченного доступа от утечки по техническим каналам. – М.: Горячая линия – Телеком, 2014. – 594 с.

Дополнительная:

7. Методы и средства защиты информации в компьютерных системах / Хорев П.Б. - М.: Академия, 2006.
8. Комплексная защита информации в корпоративных системах / Шаньгин В.Ф. - М.: ИД Форум: НИЦ Инфра-М, 2012.
9. Мельников Д.А. Организация и обеспечение безопасности информационно-технологических сетей и систем. Учебник. – М: Университетская книга, 2012. – 598 с.

Рекомендуемые для самостоятельного изучения издания и ресурсы информационно-телекоммуникационной сети Интернет:

- ЭБС «Консультант студента» www.studentlibrary.ru;
- СПС КонсультантПлюс URL: http://www.consultant.ru/;
- НЭБ eLibrary http://www.elibrary.ru/.