МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ

УТВЕРЖДАЮ
Директор Политехнического института
Артамонов Д.В.
«7» 09 2015 г

ПРОГРАММА
ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ ВЫПУСКНИКОВ
И ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ГИА

А.4. Г.1 Подготовка к сдаче и сдача государственного экзамена

Направление подготовки

10.06.01 Информационная безопасность

Направленность (профиль):

Методы и системы защиты информации, информационная безопасность

Квалификация (степень) – Исследователь. Преподаватель-исследователь.

Форма обучения: очная, заочная

Пенза, 2015

Программа государственного экзамена составлена в соответствии с требованиями ФГОС ВО, утвержденного приказом Минобрнауки РФ с изменениями и дополнениями от 30 апреля 2015 г. по направлению подготовки 10.06.01 Информационная безопасность и согласована со следующими представителями работодателей:

Генеральный директор АО „ПНИЭИ" _____ В.А. Рунтиков
(Ф.И.О., должность, подпись, дата)

Генеральный директор АО „ПО „Электроприбор" _____ Ю.С. Почивалов
(Ф.И.О., должность, подпись, дата)

Программу составили:

1. Зефиров С.Л., зав. кафедрой _____
2. Кашаев Е.Д., профессор _____
3. Фатеев А.Г., доцент _____

Программа обсуждена на заседании кафедры «Информационная безопасность систем и технологий»

Протокол № 1 от «3» 09 2015 года

Зав. кафедрой ИБСТ _____ С.Л. Зефиров
(подпись, Ф.И.О.)

Программа согласована с деканом факультета приборостроения, информационных технологий и электроники

Декан факультета ПИТЭ _____ В.Д. Кревчик
(подпись, Ф.И.О., дата)

Программа одобрена методической комиссией факультета ПИТЭ

Протокол № 1 от «7» 09 2015 года

Председатель методической комиссии факультета ПИТЭ _____ А.В. Задера
(подпись, Ф.И.О.)

1 ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Цели государственной итоговой аттестации, виды аттестационных испытаний

Государственная итоговая аттестация проводится государственной экзаменационной комиссией (далее - ГЭК) в целях определения соответствия результатов освоения обучающимися основных профессиональных образовательных программ требованиям ФГОС ВО по направлению подготовки 10.06.01 Информационная безопасность (уровень подготовки кадров высшей квалификации).

Государственная итоговая аттестация по программам подготовки научно-педагогических кадров в аспирантуре проводится в форме (в указанной последовательности):

- подготовки к сдаче и сдачи государственного экзамена (государственного экзамена);
- научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации) (далее - научный доклад, вместе – государственные аттестационные испытания).

Результаты каждого аттестационного испытания определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» и объявляются в день его проведения. Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение аттестационного испытания.

Государственный экзамен, наряду с представлением научного доклада об основных результатах подготовленной научно-квалификационной работы призван установить степень соответствия уровня профессиональной подготовки выпускника требованиям ФГОС ВО по направлению подготовки 10.06.01 Информационная безопасность в части сформированности компетенций, необходимых для осуществления выпускником профессиональной деятельности.

1.2 Виды профессиональной деятельности выпускника

Виды профессиональной деятельности, к которым готовятся выпускники, освоившие программу аспирантуры:

- научно-исследовательская деятельность в области информационной безопасности;
- преподавательская деятельность по образовательным программам высшего образования.

Виды профессиональной деятельности выпускника связаны с решением профессиональных задач в образовательных организациях высшего образования, профильных академических институтах и НИИ.

2 СОДЕРЖАНИЕ ПРОГРАММЫ И ОЦЕНОЧНЫЕ СРЕДСТВА ГОСУДАРСТВЕННОГО ЭКЗАМЕНА

Государственный экзамен (ГЭ) носит комплексный характер и включает проверку теоретических знаний в сфере педагогики и психологии высшей школы, проверку сформированности следующих универсальных, общепрофессиональных и профессиональных компетенций по направлению подготовки ОПК-1, ОПК-3,ОПК-5,ПК-1, ПК-3, ПК-4, ПК-5, ПК-6, ПК-7, ПК-8, УК-5, УК-6. Содержание компетенций отражено в таблице 1.

Таблица 1

Коды компетенции	Наименование компетенции	Структурные элементы компетенции (в результате освоения дисциплины обучающийся должен знать, уметь, владеть)
1	2	3
ОПК-1	Способность формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность	*Знать*: - основные методы и модели обеспечения и управления информационной безопасностью; - методологические основы исследования проблем информационной безопасности объектов
		Уметь: - применять научно-методологический базис для моделирования и исследования объектов защиты; - применять методы и системы защиты информации для обеспечения информационной безопасности объектов
		Владеть: - методологией рискориентированного подхода при анализе и исследовании методов и систем защиты информации
ОПК-3	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности	*Знать*: - действующие нормативные документы в области обеспечения информационной безопасности; - модели оценки информационной безопасности объектов
		Уметь: - выбирать модели и методы измерения и оценивания информационной безопасности объектов
		Владеть: - навыками анализа и синтеза методов и моделей измерения и оценивания информационной безопасности в зависимости от целей и особенностей объекта защиты
ОПК-5	Готовность к преподавательской деятельности по основным образовательным программам высшего образования	*Знать:* основные принципы организации преподавательской деятельности по основным образовательным программам высшего образования.
		Уметь: организовать преподавательскую деятельность по основным образовательным программам высшего образования.
		Владеть: методами организации преподавательской деятельности по

		основным образовательным программам высшего образования.
ПК-1	Способность отбирать, обобщать и адаптировать результаты современных исследований в предметной области информационной безопасности для целей преподавания учебных дисциплин в образовательных организациях высшего образования	*Знать:* подходы к отбору содержания высшего образования.
		Уметь: применять принципы отбора содержания высшего образования.
		Владеть: способами отбора, обобщения и адаптации результатов современных исследований в предметной области информационной безопасности для целей преподавания.
ПК-3	Способность использовать современные программные средства и электронные ресурсы в соответствии со спецификой научно-исследовательской деятельности в предметной области информационной безопасности	*Знать:* – принципы разработки и функционирования программных и программно-аппаратных средств защиты информации (ЗИ); – методы ЗИ, особенности применения, типовую структуру и типовые функции программных и программно-аппаратных средств ЗИ
		Уметь: – проводить сбор, обработку и анализ научно-технической информации, в том числе с использованием электронных ресурсов, в области защиты информации – проводить анализ рынка программных, программно-аппаратных средств и систем ЗИ; – производить выбор программных, программно-аппаратных средств ЗИ в соответствии с требуемым уровнем защищенности информации
		Владеть: – навыками установки программных и программно-аппаратных средств и систем защиты информации; – навыками настройки и проверки функционирования программных, программно-аппаратных средств и систем защиты информации
ПК-4	Способность разрабатывать методы и модели информационной безопасности, проводить анализ защищенности и оценивать информационную безопасность объектов	*Знать*: - основные методы и модели обеспечения и управления информационной безопасностью; - модели оценки информационной безопасности объектов
		Уметь: - применять научно-методологический базис для моделирования и исследования объектов защиты;

		- разрабатывать модели и методы измерения и оценивания информационной безопасности объектов
		Владеть: - методологией построения моделей и методов информационной безопасности объектов
ПК-5	Способность анализировать риски информационной безопасности, разрабатывать и применять современные методы и модели обеспечения информационной безопасности, оценки информационной безопасности автоматизированных систем	*Знать:* методы анализа и оценки рисков информационной безопасности автоматизированных систем
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от целей систем и их особенностей; - определить метод оценки информационной безопасности автоматизированных систем в зависимости от целей оценки и особенностей систем.
		Владеть: методиками оценки информационной безопасности автоматизированных систем
ПК-6	Способность анализировать риски информационной безопасности, разрабатывать и применять современные методы обеспечения информационной безопасности в телекоммуникационных системах специального назначения	*Знать:* тенденции развития средств обеспечения информационной безопасности телекоммуникационных систем специального назначения
		Уметь: разрабатывать модели и алгоритмы защиты информации в телекоммуникационных системах специального назначения; проводить статистические исследования разработанных алгоритмов защиты информации в телекоммуникационных системах специального назначения
		Владеть: навыками планирования и оценки результатов статистических исследований
ПК-7	Способность создавать и исследовать модели систем защиты информации различного назначения, проводить анализ и обосновывать выбор решений по их применению	*Знать* модели управления информационной безопасностью систем различного назначения
		Уметь: - разрабатывать модели информационной безопасности автоматизированных систем в зависимости от назначения
		Владеть: методиками анализа и оценки информационной безопасности автоматизированных систем
ПК-8	Способность анализировать проблемы обеспечения безопасности информации ограниченного доступа и применять методы защиты	*Знать*: – основные методы защиты информации, применяемые для информационных систем, находящихся в состоянии информационного противоборства;

	информации при ее обработке в информационных системах	– программные, программно-аппаратные средства и системы защиты информации и технические характеристики соответствующего оборудования и программного обеспечения
		Уметь: - анализировать проблемы информационной безопасности и применять методы и средства защиты информации ограниченного доступа в информационных системах
		Владеть: - навыками применения методов и средств защиты информации ограниченного доступа в информационных системах
УК-5	Способность следовать этическим нормам в профессиональной деятельности	*Знать:* основные понятия и категории реализации этических норм в профессиональной деятельности.
		Уметь: реализовать этические нормы в профессиональной деятельности.
		Владеть: технологиями реализации этических норм в профессиональной деятельности.
УК-6	Способность планировать и решать задачи собственного профессионального и личностного развития	*Знать:* основы планирования и решения задач собственного профессионального и личностного развития.
		Уметь: планировать и решать задачи собственного профессионального и личностного развития.
		Владеть: основами планирования и решения задач собственного профессионального и личностного развития.

Трудоемкость программы подготовки к государственному экзамену и время подготовки определяются требованиями ФГОС ВО по направлению подготовки: учебным планом и календарным учебным графиком (3 з.е. в 8 семестре для очной формы обучения и в 10 семестре для заочной формы обучения).

2.1 Содержание программы государственного экзамена

Раздел 1. Педагогика и психология высшей школы

Цивилизационно-культурное значение высшего образования в современном мире и России.

Университет как основной фактор развития профессионального образования в современном мире. Структура, функции, образовательные задачи современного университета.

Нормативно-правовые основы высшего образования в РФ

Предмет и основные категории педагогики. Специфика педагогики высшей школы. Система педагогических наук и связь педагогики с другими науками.

Формы, средства и методы обучения студентов в образовательном процессе

современного университета

Формы, средства и методы воспитания и социализации студентов в образовательном процессе современного университета

Формирование устойчивой мотивации и ценностного отношения студентов к образовательной деятельности в вузе. Личностное и профессиональное самоопределение и самореализация студентов в образовательном процессе вуза.

Содержание деятельности и профессиональная культура вузовского преподавателя

Информатизация образовательного пространства, ее влияние на содержание и организацию образовательного процесса в современном вузе

Современные образовательные технологии и специфика их использования в образовательном процессе вуза.

Традиционные и инновационные формы и способы педагогического контроля в высшей школе. Критерии и показатели сформированности профессиональных компетенций.

Учебно-исследовательская и проектная деятельность студентов как фактор их профессионального становления и совершенствования

Содержание и формы организации производственной практики студентов университета. Связь высшего профессионального образования с социально-экономическими потребностями современного общества.

Инклюзивное образование: проблемы и перспективы развития в системе высшей школы.

Технологии профессионально направленного смыслообразующего акмеологического взаимодействия преподавателей и студентов.

Психологические особенности развития образования в современном обществе.

Раздел 2. Методы и средства защиты информации в условиях информационного противоборства

Основы теории информационного противоборства. Концепции и цели информационного противоборства. Модели и методы информационного противоборства. Информационная война. Информационное оружие. Средства, применяемые в качестве информационного оружия в информационном противоборстве.

Методы защиты информации (ЗИ), реализуемые специальными средствами защиты информации (СЗИ). Методы ЗИ, реализуемые СЗИ от НСД. Методы ЗИ, реализуемые средствами защиты от вредоносного ПО. Методы ЗИ, реализуемые СЗИ, обеспечивающими безопасное межсетевое взаимодействие. Методы ЗИ, реализуемые средствами контроля и предотвращения утечек информации. Методы и средства, применяемые для контроля и оценки эффективности функционирования СЗИ

Защита информации в виртуальных инфраструктурах (ВИ). Технологии виртуализации. Методы и средства ЗИ, применяемые для защиты ВИ

Методы ЗИ, реализуемые в операционных системах. Механизмы обеспечения ИБ, реализованные в ОС общего назначения: идентификация и аутентификация, парольные системы, управление доступом, политики безопасности. Сертифицированные защищенные ОС. Механизмы обеспечения ИБ, реализованные в защищенных ОС.

Раздел 3. Информационная безопасность бизнеса и деятельности организации

Информационные характеристики бизнеса (деятельности) организации

Модель информационной безопасности бизнеса. Общая структура информационной сферы. Связь с материальным миром

Модель информационной безопасности бизнеса. Риски, рисковые события, ущербы и уязвимости

Основные источники рисков в информационной сфере организации. Сложность информационной сферы. Отображение материального мира. Конфликт интересов

Основные модели и методы управления информационной безопасностью.

Процессы управления информационной безопасностью бизнеса (деятельности) в зависимости от целей бизнеса в информационной сфере.

Модели и методы измерения и оценивания информационной безопасности

Раздел 4. Проблемы и методы защиты информации в телекоммуникационных системах специального назначения

Проблемы защиты информации в развернутых и перспективных телекоммуникационных системах специального назначения.

Методические, научно-технические и организационные проблемы защиты информации.

Информационный конфликт.

Обеспечение взаимоувязанности задач управления функциями передачи информации и функциями обеспечения информационной безопасности.

Проблемы разработки методов защиты информации в перспективных телекоммуникационных системах специального назначения. Тенденции развития имеющихся методов и средств защиты информации.

Синтез интегрированных систем телекоммуникационных систем и обеспечение их информационной безопасности.

Разработка устройств защищенных телекоммуникационных систем специального назначения на базе отечественных сигнальных процессоров.

Методология исследований методов, моделей и алгоритмов защиты информации в телекоммуникационных системах специального назначения.

Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами.

Необходимость построения математических имитационных моделей исследуемых систем, средств и устройств, учитывающих условия пассивного и активного информационного противодействия угрозам нарушения информационной безопасности.

Требования к методикам статистических исследований моделей, обеспечивающих полноту, точность и достоверность полученных результатов.

2.2. Оценочные средства ГЭ

Примерные вопросы к государственному экзамену:

Раздел 1

1. Цели и содержание высшего образования в современном обществе. Структура, функции, образовательные задачи современного университета.
2. Нормативно-правовые основы высшего образования в РФ.
3. Предмет и основные категории педагогики. Специфика педагогики высшей школы.
4. Формы, средства и методы обучения студентов в вузе.
5. Формы, средства и методы воспитания студентов в вузе.
6. Формирование мотивации и ценностного отношения студентов к обучению в вузе.
7. Профессионально-педагогическая культура преподавателя вуза.
8. Информатизация образовательного пространства, ее влияние на содержание и организацию образовательного процесса в современном вузе.
9. Современные образовательные технологии и специфика их использования в образовательном процессе вуза.
10. Критерии и показатели сформированности профессиональных компетенций.
11. Учебно-исследовательская и проектная деятельность студентов как фактор их

профессионального становления.

12. Содержание и формы организации производственной практики студентов вуза.

13. Инклюзивное образование: проблемы и перспективы развития в системе высшей школы.

14. Конфликты. Конфликты в студенческой среде: проблемы диагностики и урегулирования.

15. Предмет, задачи и методы психологии высшей школы. Профориентация и профессиональный отбор в высшую школу.

Раздел 2

1. Основные принципы создания средств защиты информации
2. Концепция построения программно–аппаратных средств обеспечения информационной безопасности
3. Методы ограничения доступа и управления доступом. Идентификация и аутентификация. Парольные системы
4. Методы ограничения доступа и управления доступом. Дискреционное управление доступом
5. Методы ограничения доступа и управления доступом. Мандатное управление доступом
6. Методы ограничения доступа и управления доступом. Ролевое управление доступом
7. Структура и функции программно–аппаратных средств обеспечения информационной безопасности
8. Жизненный цикл компьютерных вирусов
9. Основные методы и средства защиты от вредоносных программ
10. Основные классы программных закладок
11. Требования к СЗИ, обеспечивающим безопасное межсетевое взаимодействие. Типовые функции
12. СЗИ, обеспечивающие безопасное межсетевое взаимодействие
13. Общая характеристика систем контроля и предотвращения утечек информации. Контролируемые каналы утечки информации
14. Типовые функциональные возможности. Поиск защищаемой информации в ИС. Контроль действий пользователей. Мониторинг и защита агентов. Реакция на инциденты. Режимы функционирования
15. Типовые функциональные возможности. Интеграция со сторонними сервисами и средствами. Обеспечение производительности и отказоустойчивости. Хранение, ретроспективный анализ и отчётность
16. Типовые функциональные возможности. Анализ информации при контроле каналов передачи. Применяемые технологии
17. Типовые функциональные возможности. Анализ информации при контроле каналов передачи. Лингвистический анализ
18. Типовые функциональные возможности. Анализ информации при контроле каналов передачи. Статистические методы
19. Системы контроля и предотвращения утечек информации. Типовая структура. Основные компоненты
20. Системы контроля и предотвращения утечек информации. Концепция применения. Основные стадии применения
21. Испытания защищенных систем в соответствии с ГОСТ 34.603.
22. Виды испытаний программных СЗИ. Документы, оформляемые при проведении испытаний: программа и методика испытаний, протоколы испытаний

23. Общий подход к оценке эффективности программных СЗИ. Классификация СЗИ АС по способам реализации. Основные защитные механизмы, которые подвергаются оценке

24. Общий подход к оценке эффективности программных СЗИ. Задачи контроля эффективности

25. Определение технологии виртуализации. Классификация виртуализации. Аппаратная виртуализация

26. Классификация виртуализации. Программная виртуализация.

27. Структура виртуальной инфраструктуры. Гипервизор. Виртуальная машина. Основная и гостевая ОС. Система хранения данных.

28. Объекты виртуальной инфраструктуры, на которые может осуществляться воздействие.

29. Проблемы обеспечения безопасности. Угрозы безопасности виртуальной инфраструктуры.

Раздел 3

1. Информационные характеристики бизнеса (деятельности)
2. Уязвимости процессов накопления знаний
3. Общая структура информационной сферы
4. Правовая среда бизнеса и ее свойства
5. Риски, рисковые события, ущербы и уязвимости
6. Обобщенная модель распределения ресурсов организации в условиях рисков
7. Риск-ориентированный подход к обеспечению информационной безопасности
8. Идентификация событий информационной безопасности
9. Предварительный анализ событий информационной безопасности
10. Накопление знаний о событиях информационной безопасности
11. Интерпретация характеристик риска для управления информационной безопасностью
12. Общая модель обеспечения информационной безопасности бизнеса
13. Модель организации как совокупности процессов. Управление информационной сферой
14. Обеспечение адекватности целей информационной безопасности целям информационной сферы организации
15. Управление информационной безопасностью сложных изменяющихся систем
16. Деструктивное информационное воздействие (дезинформирование, манипулирование информацией, повышение меры хаоса в принятии решений)
17. Способы обеспечения достоверности информации (выбор доверенного источника, сравнение информации, полученной из разных источников, проверка целостности информации)
18. Управление информационной безопасностью сложных систем принятия решений
19. Угрозы информационной безопасности, связанные с персоналом. Модели угроз (деятельность в рамках полномочий, превышение полномочий, сговор, использование внешних связей)
20. Снижение риска информационной безопасности, связанного с персоналом (обеспечение осведомлённости об информационной безопасности, скрытность

противодействия, управление системой ролей, применение аппаратно-программных средств защиты от утечки информации)

21. Управление информационной безопасностью, связанной с персоналом

Раздел 4

1. Методические, научно-технические и организационные проблемы защиты информации.
2. Уязвимости используемых методов защиты информации в телекоммуникационных системах в условиях конфликтного функционирования.
3. Тенденции развития имеющихся методов и средств защиты информации.
4. Проблемы натурных испытаний перспективных защищенных телекоммуникационных систем в условиях непрерывного ведения технической разведки иностранными государствами.
5. Нормативные документы. Классы защищенности, грифы секретности.
6. Проблемы организации взаимодействия общедоступных телекоммуникационных систем и систем специального назначения.
7. Обеспечение полноты, точности и достоверности результатов статистических исследований моделей.
8. Цели и задачи противоборствующих сторон в информационном конфликте.
9. Угрозы телекоммуникационной системе специального назначения на разных стадиях информационного конфликта.
10. Алгоритмы адаптации телекоммуникационной системы специального назначения к различным условиям и стадиям развития информационного конфликта.
11. Обеспечение взаимоувязанности задач управления с функциями передачи информации и функциями обеспечения информационной безопасности.
12. Уязвимости исполнительной, управляющей подсистем и подсистемы информационной безопасности.
13. Системы радиоэлектронной борьбы иностранных государств.
14. Типовые средства, используемые для обеспечения функций защиты информации.
15. Способы повышения защищенности средств, реализующих функции передачи информации и управления.

2.3. Проверка сформированности компетенций с использованием оценочных средств

В результате освоения данной ОПОП ВО аспирантуры выпускник должен обладать следующими компетенциями, овладение которыми подлежит контролю на государственном экзамене:

Планируемые результаты обучения		**Оценочные средства**	**Материалы, в содержании которых проводится оценка**
Код компетенции	Наименование компетенции		
ОПК-1	способностью формулировать научные задачи в области обеспечения информационной безопасности, применять для их решения методологии теоретических и	ответ на вопросы билета	Материалы разделов 3, 4

	экспериментальных научных исследований, внедрять полученные результаты в практическую деятельность		
ОПК-5	готовностью к преподавательской деятельности по основным образовательным программам высшего образования	ответ на вопросы билета	Материалы разделов 3,4
ПК-1	способностью отбирать, обобщать и адаптировать результаты современных исследований в области информационной безопасности для целей преподавания учебных дисциплин в образовательных организациях высшего образования	ответ на вопросы билета	Материалы раздела 1
ПК-3	способностью использовать современные программные средства и электронные ресурсы в соответствии со спецификой научно-исследовательской деятельности в предметной области информационной безопасности	ответ на вопросы билета	Материалы раздела 2
ПК-4	способностью разрабатывать методы и модели информационной безопасности, проводить анализ защищенности и оценивать информационную безопасность объектов	ответ на вопросы билета	Материалы раздела 3
ПК-5	способностью анализировать риски информационной безопасности, разрабатывать и применять современные методы и модели информационной безопасности, оценки информационной безопасности автоматизированных систем	ответ на вопросы билета	Материалы раздела 3
ПК-6	способностью анализировать риски информационной безопасности, разрабатывать и применять современные методы обеспечения информационной безопасности в телекоммуникационных системах специального назначения	ответ на вопросы билета	Материалы раздела 4
ПК-7	способностью создавать и исследовать модели систем защиты информации различного назначения, проводить анализ и обосновывать выбор решений по их применению	ответ на вопросы билета	Материалы раздела 3
ПК-8	способностью анализировать проблемы обеспечения безопасности информации ограниченного доступа и применять методы защиты информации при ее обработке в информационных системах	ответ на вопросы билета	Материалы разделов 2, 4

УК-5	способностью следовать этическим нормам в профессиональной деятельности	ответ на вопросы билета	Материалы раздела 1
УК-6	способностью планировать и решать задачи собственного профессионального и личностного развития	ответ на вопросы билета	Материалы раздела 1

Результаты государственного экзамена определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Оценки «отлично», «хорошо», «удовлетворительно» означают успешное прохождение государственного экзамена.

Критерии оценки устного ответа аспиранта на ГЭ

Оценка «отлично» выставляется в том случае, если аспирант излагает материал билета последовательно, логично, с соблюдение норм литературной речи, демонстрируя глубокое знание программного материала, творчески подходя к представлению своего интеллектуального багажа, грамотно применяя специальную научную терминологию, уверенно защищая оригинальную и аргументированную авторскую позицию по тем или иным проблемам профессиональной области знаний.

Оценка «хорошо» ставится аспирантам, которые при ответе демонстрируют твердое знание программного материала, соблюдают нормы литературной речи, грамотно применяют при ответе специальную научную терминологию, допускают отдельные погрешности и неточности при формулировках ответа.

Оценка «удовлетворительно» предполагает серьезные пробелы в знании программного материала, существенные погрешности в представлении формулировок устного ответа и выполнения задания третьего раздела, но при понимании основных категорий и терминологии профессиональной области знаний.

Оценка «неудовлетворительно» выставляется в случае демонстрации полного незнания существа предмета, теории и практики исследований, заметных нарушений литературной речи, некорректной и нелогичной подачи материала при устном ответе и выполнении задания третьего раздела.

3. Рекомендуемая литература:

1. Психолого-педагогические основы сотрудничества в высшей школе: Монография/Н.Е.Соколкова - М.: Вузовский учебник, НИЦ ИНФРА-М, 2015. - 216 с. http://znanium.com/catalog.php?bookinfo=504553

2. Основы профессиональной дидактики: Учебное пособие / Образцов П.И. - М.:Вузовский учебник, НИЦ ИНФРА-М, 2015. - 288 с . - http://znanium.com/catalog.php?bookinfo=491458

3. Система интенсивного обучения в высших учебных заведениях. Теория и практика: Монография / А.О. Горбенко, А.В. Мамасуев. - М.: КУРС: НИЦ ИНФРА-М, 2015. - 240 с.: http://znanium.com/catalog.php?bookinfo=467723

4. Аспирант вуза: технологии научного творчества и педагогической деятельности: Учебник / Резник С.Д. - 5-е изд., перераб. - М.: НИЦ ИНФРА-М, 2015. – 444с.-

5. Шаньгин, В.Ф. Информационная безопасность [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2014. — 702 с. — Режим доступа: https://e.lanbook.com/book/50578. — Загл. с экрана.

6. Расторгуев С.П. Математические модели в информационном противоборстве. Экзистенциальная математика. – Электрон. дан. — М.: АНО ЦСОиП, 2014. – 260 с. – Режим доступа: csef.ru/media/articles/5310/5310.pdf. – Загл. с экрана

7. Обеспечение информационной безопасности бизнеса/В.В.Андрианов,

С.Л.Зефиров, В.Б.Голованов, Н.А.Голдуев. – М.: Альпина Паблишерс, 2011. – 373с http://znanium.com/bookread2.php?book=556539.

8. Информационная безопасность систем организационного управления. Теоретические основы [Текст]: в 2т/ Н.А.Кузнецов, В.В.Кульба, Е.А.Микрин и др. Институт проблем передачи информации РАН. – М.: Наука, 2006 1 экз.

9. ГОСТ Р ИСО/МЭК 27001 Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасности – Требования [Электронный ресурс] http://www.internet-law.ru/gosts/gost/5736/

10. ГОСТ Р ИСО/МЭК 27002 Информационная технология – Методы и средства обеспечения безопасности – Свод норм и правил менеджмента информационной безопасности [Электронный ресурс] http://www.internet-law.ru/gosts/gost/54705

11. ГОСТ Р ИСО/МЭК 27004 Информационная технология – Методы и средства обеспечения безопасности – Менеджмент информационной безопасности – Измерения [Электронный ресурс] http://www.internet-law.ru/gosts/gost/51406

12. Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем [Электронный ресурс]: Учебное пособие/ Щеглов А.Ю.— Электрон. текстовые данные.— СПб.: Университет ИТМО, 2014.— 95 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=68667

13. Прокушев Я.Е. Программно-аппаратные средства защиты информации [Электронный ресурс]: Учебное пособие/ Прокушев Я.Е.— Электрон. текстовые данные.— СПб.: Интермедия, 2017.— 160 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=66799

14. Бирюков, А.А. Информационная безопасность: защита и нападение [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2017. — 434 с. — Режим доступа: https://e.lanbook.com/book/93278. — Загл. с экрана.

15. Леандро, К. Windows Server 2012 Hyper-V. Книга рецептов [Электронный ресурс] — Электрон. дан. — Москва : ДМК Пресс, 2013. — 302 с. — Режим доступа: https://e.lanbook.com/book/58692. — Загл. с экрана.

16. Яковлев В.В. Технологии виртуализации и консолидации информационных ресурсов [Электронный ресурс]: Учебное пособие/ Яковлев В.В.— Электрон. текстовые данные.— М.: Учебно-методический центр по образованию на железнодорожном транспорте, 2015.— 156 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=45322.

17. Лапонина О.Р. Межсетевое экранирование [Электронный ресурс]: Учебное пособие/ Лапонина О.Р.— Электрон. текстовые данные.— Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017.— 344 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=67391

18. Шаньгин, В.Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учеб. пособие — Электрон. дан. — Москва : ДМК Пресс, 2012. — 592 с. — Режим доступа: https://e.lanbook.com/book/3032. — Загл. с экрана.

19. Савельев А.О. Решения Microsoft для виртуализации ИТ-инфраструктуры предприятий [Электронный ресурс]/ Савельев А.О.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 284 с.— Режим доступа: http://www.bibliocomplectator.ru/book/?id=52175

Сведения о переутверждении программы на очередной учебный год и регистрации изменений

Учебный год	Решение кафедры (№ протокола, дата, подпись зав. кафедрой)	Внесенные изменения	Номера листов (страниц)		
			заменен-ных	новых	аннулиро-ванных
2016-2017	Переутверждена п/л №1 от 8.09.16	Без изменений			
2017-2018	Переутверждена п/л №1 от 31.08.17	Без изменений			
2018-2019	Переутверждена п/л №1 от 7.09.17	Без изменений			