МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

Институт естественных наук и математики

УТВЕРЖДАЮ
Проректор по науке
_____ В.В. Кружаев
«___» _____ 2017 г.

ПРОГРАММА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ (ГИА)

Перечень сведений о программе ГИА	**Учетные данные**
Образовательная программа Методы и системы защиты информации, информационная безопасность	**Код ОП**
Направление подготовки Информационная безопасность	**Код направления и уровня подготовки** 10.06.01
Уровень подготовки Подготовка кадров высшей квалификации	
ФГОС ВО	**Реквизиты приказа Минобрнауки РФ об утверждении ФГОС ВО**: от 30.07.2014, № 874 с изменениями от 30.04.2015, приказ № 464

Екатеринбург, 2017 г.

Программа государственной итоговой аттестации составлена авторами:

№	ФИО	Ученая степень, ученое звание	Должность	Структурное подразделение	Подпись
1	Баранский Виталий Анатольевич	Доктор физ.-мат. наук, профессор	профессор	Кафедра алгебры и фундаментальной информатики	
2	Синадский Николай Игоревич	Кандидат тех. наук, доцент	доцент	Кафедра алгебры и фундаментальной информатики	
3	Бакланов Валентин Викторович	Кандидат тех. наук, доцент	доцент	«Учебно-научный центр ”Информационная безопасность”», ИРИТ-РТФ	

Рекомендовано учебно-методическим советом института естественных наук и математики

Председатель учебно-методического совета Е.С. Буянова

Протокол №2 от 18.10.2017 г.

Согласовано:

Заместитель директора ИЕНиМ по научной и инновационной деятельности Е.А. Елфимова

Заместитель директора ИРИТ-РТФ по науке С.И. Кудинов

Начальник ОПНПК Е.А. Бутрина

1. ОБЩАЯ ХАРАКТЕРИСТИКА ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

1.1. Цель государственной итоговой аттестации

Целью государственной итоговой аттестации является установление уровня подготовленности обучающегося, осваивающего образовательную программу высшего образования – программу подготовки научно-педагогических кадров в аспирантуре, выполнению профессиональных задач и соответствия его подготовки требованиям федерального государственного образовательного стандарта высшего образования (требованиям образовательного стандарта, разрабатываемого и утверждаемого университетом самостоятельно) и образовательной программе по направлению подготовки высшего образования, разработанной на основе образовательного стандарта.

В рамках государственной итоговой аттестации проверяется уровень сформированности следующих результатов освоения образовательной программы, заявленных в ОХОП:

РО 1: Системное понимание и критический анализ современного состояния и проблематики обеспечения информационной безопасности.

РО 2: Проектирование и проведение исследований в области обеспечения информационной безопасности с использованием современных методов и средств.

РО 3: Выявление и представление проблематики исследований, научных гипотез и перспективных направлений исследований в области информационной безопасности.

РО 4: Внедрение результатов исследований по обеспечению информационной безопасности

Универсальные компетенции (УК) в соответствии с ФГОС ВО (СУОС):

Код	Универсальные компетенции
УК-1	Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях.
УК-2	Способность проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки.
УК-3	Готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач.
УК-4	Готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках.

УК-5	Способность следовать этическим нормам в профессиональной деятельности.
УК-6	Способность планировать и решать задачи собственного профессионального и личностного развития.

Общепрофессиональные компетенции (ОПК) в соответствии с ФГОС ВО (СУОС):

Код	Общепрофессиональные компетенции
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.
ОПК-2	Способность разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности.
ОПК-3	Способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности.
ОПК-4	Способность организовать работу коллектива по проведению научных исследований в области информационной безопасности.
ОПК-5	Готовность к преподавательской деятельности по основным образовательным программам высшего образования.

Профессиональные компетенции (ПК):

Код	Профессиональные компетенции
ПК-1	Способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности.
ПК-2	Способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах.

ПК-3	Способность использовать нормативные правовые документы в своей профессиональной деятельности.
ПК-4	Способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности.
ПК-5	Способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации.
ПК-6	Способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов.
ПК-7	Способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия.
ПК-8	Способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия.
ПК-9	Способность администрировать подсистемы информационной безопасности объекта.
ПК-10	Способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации.
ПК-11	Способность участвовать в разработке подсистемы управления информационной безопасностью.
ПК-12	Способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности.
ПК-13	Способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности.
ПК-14	Способность применять программные средства системного, прикладного и специального назначения.
ПК-15	Способность использовать инструментальные средства и системы программирования для решения профессиональных задач.

ПК-16	Способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности.
ПК-17	Способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.
ПК-18	Способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности.
ПК-19	Способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов.
ПК-20	Способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов.
ПК-21	Способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности.
ПК-22	Способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности.
ПК-23	Способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью.
ПК-24	Способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью.
ПК-25	Способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации.
ПК-26	Способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации.
ПК-27	Способность участвовать в работах по реализации политики информационной безопасности.
ПК-28	Способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности.
	Педагогическая деятельность:
ПК-29	Способность и готовностью к педагогической деятельности в области профессиональной подготовки в образовательных организациях

	высшего образования, дополнительного профессионального образования, профессиональных образовательных организациях.

Перечень планируемых по образовательной программе результатов обучения и составляющих их компетенций

Результаты обучения (что должен знать, понимать и/или продемонстрировать обучающийся, освоивший программу аспирантуры направленности 10.06.01)	**Компетенции, составляющие результаты обучения**
РО-1. Системное понимание и критический анализ современного состояния и проблематики обеспечения информационной безопасности.	• способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-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 (ОПК-1); • готовность к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-5). • способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1); • способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2); • способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3); • способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4); • способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-7);

	• способность применять программные средства системного, прикладного и специального назначения (ПК-14); • способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-18); • способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-19); • способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-22); • способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-26); • способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-28).
РО 2. Проектирование и проведение исследований в области обеспечения информационной безопасности с использованием современных методов и средств.	• способность проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки (УК-2); • 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 (ОПК-1); • способностью разрабатывать частные методы исследования и применять их в самостоятельной научно-исследовательской деятельности для решения конкретных исследовательских задач в области обеспечения информационной безопасности (ОПК-2); • готовность к преподавательской деятельности по основным образовательным программам высшего образования (ОПК-5). • способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1); • способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2); • способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3); • способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности,

	административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4); • способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6); • способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-7); • способность участвовать в разработке подсистемы управления информационной безопасностью (ПК-11); • способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-12); • способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-17); • способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности (ПК-18); • способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-19); • способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-22); • способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-23); • способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-24); • способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-26); • способность участвовать в работах по реализации политики информационной безопасности (ПК-27); • способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-28).
РО 3. Выявление и представление проблематики исследований, научных гипотез и перспективных направлений исследований в области	• способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях (УК-1); • способность проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с

информационной безопасности.	использованием знаний в области истории и философии науки (УК-2); • готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4); • 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 (ОПК-1); • способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3); • способность использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1); • способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2); • способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3); • способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4); • способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5); • способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6); • способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-7); • способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности (ПК-12); • способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-17);

	• способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов (ПК-19); • способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-21); • способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности (ПК-22); • способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-23); • способностью изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-26); • способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности (ПК-28).
РО 4. Внедрение результатов исследований по обеспечению информационной безопасности	• готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач (УК-3); • готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках (УК-4); • способность следовать этическим нормам в профессиональной деятельности (УК-5); • способность планировать и решать задачи собственного профессионального и личностного развития (УК-6). • способность обоснованно оценивать степень соответствия защищаемых объектов информатизации и информационных систем действующим стандартам в области информационной безопасности (ОПК-3); • способность организовать работу коллектива по проведению научных исследований в области информационной безопасности (ОПК-4); • способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности (ПК-1); • способность понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах (ПК-2); • способность использовать нормативные правовые документы в своей профессиональной деятельности (ПК-3);

	• способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности (ПК-4); • способность организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации (ПК-5); • способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов (ПК-6); • способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия (ПК-7); • способность принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия (ПК-8); • способность администрировать подсистемы информационной безопасности объекта (ПК-9); • способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации (ПК-10); • способность участвовать в разработке подсистемы управления информационной безопасностью (ПК-11); • способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности (ПК-13); • способность применять программные средства системного, прикладного и специального назначения (ПК-14); • способность использовать инструментальные средства и системы программирования для решения профессиональных задач (ПК-15); • способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности (ПК-16); • способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности (ПК-17); • способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов (ПК-20); • способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности (ПК-21);

	• способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью (ПК-23); • способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью (ПК-24); • способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации (ПК-25); • способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации (ПК-26); • способность участвовать в работах по реализации политики информационной безопасности (ПК-27).

1.2. Структура государственной итоговой аттестации:

– подготовка к сдаче и сдача государственного экзамена;

– представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации).

1.3. Форма проведения государственного экзамена

Устный

***1.*4. Трудоемкость государственной итоговой аттестации:**

Общая трудоемкость государственной итоговой аттестации составляет

ГИА (мероприятие)	Семестр	Всего часов	Количество з.е.	Недели
Подготовка к сдаче и сдача государственного экзамена	8	108	3	2
Представление научного доклада об основных результатах подготовленной научно-квалификационной работы (диссертации)	8	216	6	4
	Итого	**324**	**9**	

1.5. Время проведения государственной итоговой аттестации

государственный экзамен – 8 семестр,

научный доклад об основных результатах подготовленной научно-квалификационной работы (диссертации) – 8 семестр,

1.6. Требования к процедуре государственной итоговой аттестации

Требования к порядку планирования, организации и проведения ГИА, к структуре и форме документов по организации ГИА сформулированы в утвержденной в УрФУ документированной процедуре «Положение о порядке проведения государственной итоговой аттестации обучающихся по программам подготовки научно-педагогических кадров в аспирантуре в Уральском федеральном университете имени первого Президента России Б.Н. Ельцина» (СМК-ПВД-7.5-01-100-2016), введенной в действие приказом ректора от 09.01.2017 № 01/03.

1.7. Требования к оцениванию результатов освоения образовательной программы в рамках государственной итоговой аттестации

Объективная оценка уровня соответствия результатов обучения требованиям к освоению образовательной программы обеспечивается системой разработанных критериев (показателей) оценки освоения знаний, сформированности умений и опыта выполнения профессиональных задач.

Критерии оценки утверждены на заседании учебно-методического совета Института естественных наук и математики, реализующего образовательную программу, от «19» мая 2017 г., протокол № 57

2. ТРЕБОВАНИЯ К СОДЕРЖАНИЮ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

2.1. Тематика государственного экзамена

Введение в информационную безопасность. Стратегии и модели информационной защиты

Виды и задачи информационной защиты.

Виды информации, представляющей опасность для человека и общества. Опасность избыточной информации. Виды недобросовестной рекламы. Формы обмана и злоупотребления доверием. Дезинформация и ее виды. Опасная информация в формах угроз, клеветы, оскорбления. Распространение опасных знаний. Способы защиты от опасной информации. Обеспечение исторической правды как форма информационной защиты общества.

Виды деструктивного информационно-психологического воздействия. Убеждение и внушение. Способы манипуляции сознанием и сферой бессознательного. Психологическое воздействие средств массовой информации. Рекламные и политические кампании.

Информационные войны: стратегия, тактика, противник, силы, средства, театры военных действий. Виды, способы и результаты применения информационно-психологического оружия. Формы противодействия информационным войнам.

Опасная компьютерная информация в форме программ и данных. Программирование ЭВМ как опасная для общества профессия.

Защита человека и гражданина от неинформированности. Конституционные права граждан на информированность. Профессиональные права на доступ к информации. Информация, доступная по закону. Потребность человека в информации. Информационный голод, его причины и последствия.

Формирование и защита прав собственности на информацию. Ценность информации.

Уровни представления информации и особенности ее защиты. Характеристика вещественных и энергетических носителей информации. Формы представления компьютерной информации. Семантическая и признаковая информация, особенности их защиты. Формы защиты компьютерной информации на уровне устройств ее записи и считывания. Защитное блокирование и защитное удаление информации. Защита компьютерной информации на логическом уровне. Реализация информационной защиты на уровне файловых систем. Особенности представления дискретной информации на синтаксическом уровне. Виды кодирования и их использование в защите информации. Защита информации на семантическом и прагматическом уровнях.

Виды и общая характеристика информационных угроз. Таксономия угроз. Уязвимости информационных систем. Понятие «информационной мишени» по С.П. Расторгуеву. Источники и носители информационных угроз. Виды ущерба от информационных атак. Управление информационными рисками.

Стратегии и модели информационной защиты. Разработка моделей как способ комплексирования средств и методов информационной защиты. Модель абсолютной защиты С. П. Расторгуева как базис для разработки частных моделей.

Общие понятия о принципах информационной защиты. Содержание и обоснование основных принципов.

Стратегия пассивной защиты. Виды изоляции от внешнего доступа. Вещественные, энергетические, логические и организационные барьеры на пути распространения и рассеяния информации. Требования к эшелонированной защите. Оценка эффективности пассивной защиты.

Стратегия ликвидации опасности. Правовые, организационные, экономические и технологические основания для ликвидации источников и носителей угроз. Виды защитного уничтожения угроз и «нарушителей». Экономические, организационные, правовые и технологические формы ликвидации опасности. Показатели эффективности для данной стратегии защиты.

Стратегия маневра. Эвакуация защищаемых ценностей. Отключение от источника опасности. Уклонение от опасности. Особенности маневра в пространствах памяти, радиодиапазона и др.

Стратегия информационного сокрытия (маскировки, имитации). Методы вещественного сокрытия ценностей машинных носителей информации. Правила оборудования тайников. Энергетические скрытие сигналов в шуме. Эффективность линейного и пространственного зашумления. Скрытие информации на уровне средств взаимодействия с носителем. Виды логического сокрытия программ и данных. Формы синтаксического сокрытия. Семантическое и прагматическое скрытие.

Подходы к составлению модели информационного нарушителя. Классификация и категории информационных нарушителей. Цели нарушителей. Оценка опасности нарушителя на основании его осведомленности, оснащенности и подготовленности. Ресурсы нарушителя. Оценка рисков неправомерного доступа для объекта атаки и

нарушителя. Сложившиеся приоритеты в выборе тактики действий нарушителя. Модель поведения человека-нарушителя в экстремальных ситуациях.

Демаскирующие признаки веществ, материалов, инструмента и принадлежностей, используемых информационными нарушителями. Демаскирующие признаки нарушителя, позволяющие его обнаружить и идентифицировать. Геометрическая, биомеханическая, физико-химическая и социальная модели человека-нарушителя. Признаки присутствия и функционирования автономных средств технической разведки и вредоносных компьютерных программ.

Понятие о комплексной защите информации от несанкционированного доступа. Тактика НСД к автоматизированным системам и машинным носителям информации. Построение «деревьев атак». Характерные признаки и следы НСД в памяти компьютерных систем. Составные части комплексной информационной защиты. Требования к рубежу сопротивления вторжению. Контроль (обнаружение) вторжения: вероятность обнаружения и наработка на ложную тревогу. Средства и методы обнаружения активного и пассивного «нарушителя». Виды систем контроля и распознавания образов: охранная сигнализация, системы контроля доступа, технические средства наблюдения, компьютерные системы идентификации, аутентификации и аудита событий, системы обнаружения компьютерных атак и др. Рубеж реагирования на вторжение, его элементы. Регистрация следов вторжения с целью привлечения злоумышленников к юридической ответственности.

Общие подходы к оценке эффективности информационной защиты. Критерии и параметры оценки: временные, вероятностные и затратные. Методика оценки эффективности защитных мер.

Теоретические основы компьютерной безопасности

Понятие политики и моделей безопасности информации в компьютерных системах. Субъектно-объектная модель Щербакова. Аксиомы защищенности компьютерных систем. Политики безопасности компьютерных систем. Монитор безопасности. Гарантии выполнения политики безопасности. Изолированная программная среда.

Пятимерное пространство Хартсона. Модели на основе матрицы доступа. Модель Харрисона-Руззо-Ульмана (HRU). Расширения модели HRU. Модели на основе типизированной матрицы доступа. Модель TAKE-GRANT. Расширенная модель TAKE-GRANT.

Общая характеристика моделей мандатного доступа. Основные положения моделей мандатного доступа. Решетка уровней безопасности. Модель Белла-ЛаПадулы. Расширения модели Белла-ЛаПадулы. Безопасная функция перехода (Мак-Лин).

Общая характеристика моделей тематического разграничения доступа. Иерархическая тематическая классификация. Политика тематического разграничения доступа. Тематически решетки. Решетка мультирубрик.

Общая характеристика моделей на основе политики функционально-ролевых отношений. Отношения и функции при иерархической организации ролей. Модель MMS (military message system).

Модели информационного невмешательств и информационной невыводимости. Автоматная система Гогена-Мессигера.

Общая характеристика моделей обеспечения целостности данных. Понятие целостности данных. Мандатная модель Биба. Дискреционная модель Кларка-Вильсона. Объединение модели Биба и Кларка-Вильсона.

Понятие распределенной компьютерной системы. Общая схема системы взаимодействующих сегментов. Политика безопасности в распределенных компьютерных системах.

Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Двудольный граф назначений доступа. Граф назначений доступа при иерархической организации системы объектов. Граф индивидуально-групповых назначении доступа. Матричное представление графа. Количественные характеристики систем индивидуально-группового доступа к иерархически организованным информационным ресурсам.

Нормативно-правовые методы обеспечения информационной безопасности

Деятельность по защите информации ограниченного доступа в общей системе обеспечения национальной безопасности РФ. Характеристика и структура системы законодательных актов и основные направления государственного регулирования в сфере информационной безопасности.

Доктрина информационной безопасности РФ. Национальные интересы РФ в информационной сфере и их обеспечение. Виды и источники угроз информационной безопасности РФ. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Общие методы обеспечения информационной безопасности РФ. Особенности обеспечения информационной безопасности РФ в различных сферах общественной жизни. Международное сотрудничество РФ в области обеспечения информационной безопасности. Основные положения государственной политики обеспечения информационной безопасности РФ и первоочередные мероприятия по ее реализации.

Конституционные гарантии интересов личности в информационной сфере. Законодательная база обеспечения информационной безопасности. Принципы правового регулирования отношений и основные понятия в сфере информации, информационных технологий и защиты информации. Разделение информации по категориям доступа. Конфиденциальность информации. Виды информации ограниченного доступа и режимы ее защиты: государственная тайна, персональные данные, коммерческая тайна, банковская тайна, налоговая тайна. Ответственность за нарушение защиты информации ограниченного доступа.

Гражданско-правовой оборот информации; понятие информационных ресурсов; содержание правового режима защиты информационных ресурсов; виды информации по уровню и категориям доступа.

Государственная тайна как особый вид защищаемой информации; принципы и порядок отнесения сведений к государственной тайне; перечни сведений, составляющих государственную тайну; методология засекречивания сведений. Степени секретности сведений и грифы секретности их носителей; порядок рассекречивания сведений и их носителей. Распоряжение сведениями, составляющими государственную тайну; ограничение прав собственности на информацию в связи с ее засекречиванием. Система защиты государственной тайны в РФ. Функции, задачи и полномочия органов защиты государственной тайны.

Правовой режим защиты служебной, коммерческой тайны и персональных данных. Принципы защиты информации ограниченного доступа. Правовой режим защиты профессиональных тайн; основные виды тайн; установленные требования и правила защиты.

Интеллектуальные права и право собственности. Автор и правообладатель результатов интеллектуальной деятельности. Виды лицензионных договоров. Защита

личных неимущественных и исключительных прав. Авторское и смежные права и их объекты. Охрана авторских прав на программы для ЭВМ и смежных прав на базы данных и технические средства их защиты. Ответственность за нарушение авторских и смежных прав.

Общая характеристика административно-правовых институтов в сфере защиты информации. Лицензирование деятельности в сфере защиты информации; организационная структура и общая характеристика систем лицензирования.

Цели и принципы сертификации. Органы добровольной и обязательной сертификации; их аккредитация. Системы сертификации в сфере защиты информации; особенности разработки, производства и эксплуатации средств защиты информации.

Особенности и причины информационных преступлений. Понятие о неправомерном обороте информации. Преступления в форме незаконного распространения, разглашения и передачи информации. Незаконное воспрепятствование доступу к информации. Клевета и оскорбление. Незаконное хранение и использование конфиденциальной информации. Компьютерные формы мошенничества и фальсификации.

Особенности компьютерных преступлений. Преступления в сфере компьютерной информации. Место компьютерных систем в преступной деятельности. Компьютер как орудие, средство преступления и хранилище информации о преступной деятельности. Компьютер как предмет преступления. Особенности подготовки компьютерных преступлений.

Элементы криминологии и виктимологии в проблематике информационных преступлений и информационной защиты. Мотивация преступной деятельности в сфере высоких информационных технологий. «Специальности» информационных преступников. Особенности, присущие информационным и компьютерным правонарушениям. Портрет «жертвы» компьютерных атак. Категории «внутренних» нарушителей. Причины, побуждающие сотрудников к совершению информационных правонарушений против интересов своей организации.

Уголовно-правовая характеристика преступлений в сфере компьютерной информации. Характеристика объективной стороны преступлений, предусмотренных гл. 28 УК РФ. Виды ЭВМ по отношению к преступной деятельности. Способы нарушения работы ЭВМ, системы ЭВМ и их сети. Формы несанкционированного копирования, удаления, модификации и блокирования защищаемой законом компьютерной информации. Ответственность за совершение преступлений, предусмотренных ст. 272 – 274 УК РФ.

Административные правонарушения в сфере защиты информации ограниченного доступа. Органы государственной власти, уполномоченные рассматривать дела об административных правонарушениях; порядок производства дел об административных правонарушениях в области защиты информации; исполнение постановлений по делам об административных правонарушениях.

Порядок взаимодействия специалистов по информационной безопасности с сотрудниками правоохранительных органов при раскрытии информационных и компьютерных преступлений. Понятие о системе оперативно-розыскных мероприятий в сетях документальной электросвязи. Порядок предоставления информации сотрудникам правоохранительных органов. Общие требования к проведению некоторых процессуальных действий, связанных с расследованием компьютерных преступлений. Роль и функции специалиста и эксперта в раскрытии компьютерных преступлений.

1. Формы правового регулирования в сфере информационных технологий и защиты информации. Федеральные законы, регулирующие эту сферу деятельности. Свойства и

особенности информации как объекта правового регулирования. Нормативные определения информации и компьютерной информации. Понятия информационных технологий и информационной системы. Виды и особенности эксплуатации информационных систем. Понятие обладателя информации и оператора информационной системы. Права и обязанности обладателя информации.

2. Понятие информационно-телекоммуникационной сети. Правовые принципы использования информационно-телекоммуникационной сетей на территории РФ. Понятия средства массовой информации и сетевого издания. Требование к информации, распространяемой без использования средств массовой информации. Понятие организатора распространения информации по сети «Интернет» и его обязанности, предусмотренные законом. Ответственность организатора распространения информации по сети «Интернет» за невыполнение предусмотренных законом обязанностей. На каких из указанных организаторов не распространяются эти обязанности?

3. Понятия сайта в сети «Интернет» и интернет-страницы. Предусмотренные законом понятия доменного имени и сетевого адреса. Существующие виды доменных имён и сетевых адресов. Понятия владельца сайта сети «Интернет», провайдера хостинга и их обязанности, предусмотренные законом.

4. Предусмотренные законом понятия защиты информации и конфиденциальности. Категории информации по видам доступа и распространения (предоставления). Ответственность за неправомерное ограничение доступа к информации. Виды общедоступной информации, распространение которой в РФ ограничено или запрещено законом. Ответственность за противоправное распространение такой информации. Предусмотренные законом формы ограничения доступа к информации, распространяемой с помощью информационно-телекоммуникационных сетей.

7. Понятия коммерческой тайны и информации, составляющей коммерческую тайну. Меры, предусмотренные законодательством по защите коммерческой тайны. Порядок отнесения сведений к коммерческой тайне. Ответственность за правонарушения в сфере защиты коммерческой тайны.

8. Понятие оператора связи и абонента. Тайна связи и правовые основы её ограничения. Базы данных об абонентах оператора связи, их содержание и охрана. Ответственность за нарушение охраны тайны связи и баз данных об абонентах оператора связи.

9. Информация, размещаемая в сети «Интернет» государственными органами и органами местного самоуправления в соответствии с законом. Определение официального сайта государственного органа или органа местного самоуправления Понятие и назначение российского государственного сегмента сети «Интернет». Понятие информационных систем общего пользования и их классификация. Мероприятия по обеспечению защиты информации в информационных системах общего пользования.

10. Понятия персональных данных, оператора персональных данных и информационной системы персональных данных. Условия обработки персональных данных. Права субъекта персональных данных. Ограничение права субъекта персональных данных на доступ к своим персональным данным. Биометрические персональные данные и правила их обработки. Специальные категории персональных данных и условия их обработки. Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных ФЗ «О персональных данных». Меры, по обеспечению безопасности персональных данных при их обработке. Определение уровня защищённости персональных данных. Государственные органы, уполномоченные осуществлять контроль и надзор за выполнением мер по обеспечению безопасности персональных данных. Ответственность за правонарушения (преступления) в сфере защиты персональных данных.

11. Уголовно-наказуемые деяния в сфере компьютерной информации: предусмотренные УК РФ составы (названия), признаки деяний, последствий

12. Понятия критической информационной инфраструктуры (КИИ), её объекта, субъекта, компьютерной атаки и компьютерного инцидента. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности и его компетенция. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и его компетенция. Основания и порядок категорирования объектов КИИ. Права и обязанности субъектов КИИ.

Организационные методы защиты информации ограниченного доступа

Организационная система обеспечения информационной безопасности предприятия, учреждения, фирмы. Задачи, функции и типовая структура службы безопасности предприятия. Подразделения по защите государственной тайны предприятия (ПЗГТ): планирование и организация работы ПЗГТ предприятия; нормативные условия функционирования и размещения; функциональные обязанности сотрудников по защите информации.

Подбор и особенности приема сотрудников в контексте защиты информации; человеческий фактор в угрозах информационной безопасности. Допуск должностных лиц и граждан к государственной тайне, к работе со сведениями ограниченного доступа. Порядок оформления и условия прекращения допусков. Ограничение прав лиц, допущенных к ознакомлению со сведениями ограниченного доступа.

Разрешительная система доступа к информации (индивидуально-избирательная, мандатная, тематическая, зонально-функциональная). Положение о разрешительной системе доступа. Учет осведомленности должностных лиц в сведениях ограниченного доступа. Обязанности лиц, допущенных к конфиденциальным работам, документам и изделиям. Порядок командирования в другие организации и за границу лиц, допущенных к сведениям ограниченного доступа. Особенности увольнения сотрудников, осведомленных с конфиденциальной информацией.

Основные принципы организационно-распорядительной защиты: изоляция носителей информации, минимальная информированность исполнителей, производственная дисциплина, регламентация служебного времени, минимизация неслужебных контактов, объединение и разделение полномочий. Формы контроля и надзора за персоналом. Дезинформация и легендирование.

Порядок проведения совещаний, переговоров по конфиденциальным вопросам. Делопроизводство и документооборот конфиденциальных документов; реквизиты конфиденциальных документов; подготовка, учет, регистрация, исполнение хранение и уничтожение конфиденциальных документов.

Объектовые режимы. Физическая охрана объекта; рубежно-зональный принцип и организационно-технические основы обеспечения. Пропускной режим; тактика и методы действий персонала охраны по обеспечению пропуска лиц, транспорта, грузов; выявлению электронных устройств негласного получения информации, цифровых устройств хранения информации; методы и средства проверки подлинности документов; порядок действий дежурной смены по тревожным сигналам охранной сигнализации. Требования к режимным зонам и режимным помещениям; регламент служебного времени; регламентация пребывания на объекте командированных лиц и посетителей.

Требования нормативных правовых актов, регламентирующих деятельность предприятий при осуществлении международного научно-технического и экономического

сотрудничества. Обеспечение сохранности конфиденциальной информации при участии (проведении) в международных и отечественных выставках. Организация Web-сайта предприятия.

Нарушения в сфере защиты информации, влекущие дисциплинарную ответственность сотрудников предприятия; меры дисциплинарно-административного принуждения, материального и морального побуждения (стимулирования) сотрудников в части соблюдения требований по защите информации.

Порядок проведения служебного расследования по фактам разглашения сведений, составляющих государственную тайну, утраты носителей, содержащих такие сведения. Организация розыска утраченных или похищенных документов и изделий.

Подготовка кадров и повышение квалификации сотрудников в сфере защиты информации. Квалификационные требования к специалистам по защите информации.

Общие требования к защите компьютерной информации в автоматизированных системах (АС)

Основные термины в сфере защиты компьютерной информации. Руководящие документы ФСТЭК России (Гостехкомиссии при Президенте РФ) по защите от НСД к информации. Общая характеристика стандартов ГОСТ Р ИСО/МЭК 15408-2002 и ISO/IEC 17799-2000.

Порядок приобретения компьютеров, комплектующих узлов и машинных носителей для обработки информации ограниченного доступа. Объем, содержание и порядок проведения специальной лабораторной проверки компонентов и узлов СВТ. Требования к режимным помещениям, предназначенным для размещения АС. Размещение АС на рабочих местах пользователей. Категорирование АС. Назначение, объем и содержание специальных исследований АС. Изменение режимов работы аппаратуры, подключение и отключение оборудования. Проведение повторных специальных проверок и исследований. Оформление предписания на эксплуатацию и формуляра АС. Ввод АС в эксплуатацию. Порядок приобретения и получения общесистемного и прикладного программного обеспечения АС. Организация работы с физическими и юридическими лицами, разрабатывающими программное обеспечение АС.

Особенности ввода в эксплуатацию компьютеров, предназначенных для использования в сети Интернет. Защита АС от несанкционированного доступа и внедрения вредоносных программ из открытых телекоммуникационных сетей. Защита аппаратуры и оборудования абонентских пунктов Интернет от технической разведки противника.

Порядок распечатки документов, содержащих конфиденциальные сведения. Требования к эксплуатации принтеров.

Проведение ремонта и технического обслуживания ЭВМ, категорированных для обработки информации ограниченного доступа. Ремонт ЭВМ в сторонних организациях.

Общесистемные и специализированные программные средства и методы логического и физического удаления компьютерной информации, оценка их эффективности. Программные способы удаления хранимой компьютерной информации. Аппаратные устройства мгновенного размагничивания магнитных носителей, их характеристики. Автоматическое и ручное восстановление системной информации, удаленных и испорченных данных, дефектных носителей. Существующие способы и средства реставрации удаленной компьютерной информации и восстановления поврежденных машинных носителей.Резервирование компьютерной информации как основная мера обеспечения ее сохранности. Порядок хранения и обновления архивных копий. Сравнительные характеристики программ-архиваторов. Виды архивирования.

Восстановление системной информации, данных и программного обеспечения с резервных копий. Виды и стратегии резервирования. Использование стандартных средств резервирования системной информации и данных, программ-архиваторов. Устройства и носители, используемые для резервного копирования.

Организация отказоустойчивых дисковых конфигураций (RAID). Создание зеркальных и дуплексных наборов. Чередование дисков с записью четности. Восстановление информации из зеркальных наборов и наборов с чередованием и контролем четности.

Защита компьютерной информации в операционных системах

Ключевые элементы программной архитектуры операционных систем (ОС), определяющие защиту компьютерной информации и безопасность ЭВМ. Основные отличия в реализации защитных механизмов операционных систем семейств Windows и UNIX. Архитектура операционной системы.

Защищенные файловые системы. Файл как универсальный объект ОС. Изменение разрешений на доступ к файлам. Размещение элементов файловой системы на дисковом пространстве. Структура и назначение метаданных файлов. Механизмы образования технологического информационного мусора. Восстановление поврежденных файлов. Использование утилит для работы с поврежденными файловыми системами.

Понятие политики разграничения доступа в компьютерных системах. Одноуровневая и многоуровневая модели разграничения доступа, их достоинства и недостатки. Реализация технологии разграничения доступа в операционных системах.

Модель безопасности и ее архитектура. Администрирование учетных записей пользователей. Группы пользователей. Права и привилегии пользователей и групп. Управление системной политикой безопасности. Стратегия предоставления прав на доступ к ресурсам. Хранение парольной информации. Алгоритм сетевой аутентификации. Обеспечение безопасности при удаленном доступе.

Криптографические механизмы защиты информации от НСД, реализованные на уровне ОС.

Безопасность системных данных. Структура, редактирование и критичные настройки системного реестра ОС Windows*. Способы защиты реестра и конфигурационных файлов от незаконной модификации.

Защита на уровне межпроцессного взаимодействия. Создание и уничтожение процессов. Скрытие процессов. Реализация защитных требований на уровне командной оболочки.

Аудит событий безопасности. Настройка адекватной политики аудита. Анализ событий аудита. Разделение функций администратора и аудитора.

Настройка сетевых служб операционных систем. Основные ошибки и просчеты в администрировании операционных систем.

Средства и методы защиты от вредоносных компьютерных программ

Классификация и технические возможности вредоносных программ для ЭВМ. Понятие об опасных компьютерных программах и данных. Оценка опасностей, связанных с разработкой и использованием программ для ЭВМ. Состав вредоносных программ и команд. Классификация вредоносных программ по основным свойствам и признакам. Основные признаки и возможности компьютерных вирусов, программных закладок, «логических бомб», сетевых «червей», программ «удаленного администрирования» и иных

видов опасных программ. Деструктивные воздействия и их последствия. Инструментарий для создания вредоносных программ.

Изучение функциональных возможностей вредоносных программ. Программные воздействия, заведомо приводящие к опасным последствиям. Сущность вредоносных блокирования, удаления, модификации защищаемой компьютерной информации. Программно управляемые формы несанкционированного копирования информации. Механизмы вирусного заражения. Виды и формы программно управляемого нарушения работы ЭВМ. Способы несанкционированного запуска опасных программ и команд.

Способы внедрения и запуска вредоносных программ. Уязвимые места программного обеспечения АС, способствующие внедрению, сокрытию, распространению и запуску вредоносных программ. Способы проникновения вредоносных программ в локальные и сетевые ЭВМ. Потенциально опасные функции операционной системы. Уязвимости ОС и штатного программного обеспечения, способствующие распространению вредоносных программ. Внедрение и запуск программного кода на этапах самотестирования ПЭВМ и загрузки операционной системы. Способы подготовки вредоносных программ к автоматическому запуску. Типичные варианты обмана пользователей, провоцирующих их на запуск неизвестных программ. Внедрение и запуск опасных программ с применением «троянских» оболочек. Возможности программ-«джойнеров».

Понятие о сигнатуре вредоносного программного кода. Принцип антивирусного сканирования. Понятие о механизмах скрытности вредоносных программ. Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. «Stealth»-технологии. Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ-«руткитов». Мониторинг подозрительной активности программ. Виды и возможности антивирусных программ. Статическое и динамическое исследование подозрительных программ. Меры по реализации изолированной программной среды.

Защита информации в телекоммуникационных каналах

Виды информационных угроз для канала связи и передаваемой информации. Незаконное использование канала. Фальсификация передаваемых данных. Несанкционированное подключение к каналу связи абонентских устройств. Виды перехвата информации в канале связи. Использование побочных каналов утечки информации. Способы защиты передаваемой информации от характерных атак.

Основные методы энергетического, временного сокрытия сигналов в каналах связи; сигналы с расширенной базой, каналы с шумоподобными сигналами; сверхбыстродействующие передачи.

Способы незаконного подключения к проводным телефонным коммуникациям. Виды и типовые схемы телефонных закладок, их возможный камуфляж. Демаскирующие признаки средств перехвата информации, работающих на телефонных линиях. Защита проводных телефонных коммуникаций от незаконного подключения. Организационные и технические способы противодействия несанкционированному использованию телефонных линий. Типовые схемы защиты от высокочастотного навязывания. Порядок проверки телефонных аппаратов. Методы контроля телефонных линий. Устройства пассивной и активной технической защиты от несанкционированного подключения к проводным телефонным коммуникациям, их структурные схемы, принцип действия и основные параметры. Рекомендации по применению технических средств защиты.

Фильтрация сигналов в проводных каналах, выходящих за пределы объекта

информатизации. Экранирование проводных каналов связи. Контроль за целостностью проводных каналов связи. Нормы защиты радиорелейных линий связи от радиоперехвата.

Стандарты цифровых сотовых сетей. Система сотовой связи стандарта GSM. Схема построения и состав оборудования сетей. Структура и формирование сигналов. Защита и безопасность информации (аутентификация, секретность передачи данных, секретность абонента, секретность направления вызова).

Принципы функционирования и защиты беспроводных компьютерных сетей. Используемые способы кодирования и модуляции. Протоколы обмена физического и канального уровней. Инфракрасные локальные сети. Радиочастотные сети с расширенным спектром. Сети с узкополосным СВЧ-каналом. Характеристика и особенности стандартов беспроводных локальных сетей. Применяемые средства защиты от НСД.

Проектирование защищенных автоматизированных систем

Понятия "система", "автоматизированная система", "информационные технологии", "управление", "автоматизированный процесс", "автоматический процесс". Виды АС по ГОСТ 34.003-90, (РД 50-680-88). Соотношение понятий "автоматизированная система" и "информационная система". Общая характеристика систем автоматизации управленческой деятельности. Информационная база автоматизированных (информационных) систем, понятия "база данных", "система управления базами данных", "банк данных". Структура автоматизированных систем по видам обеспечения (по РД 50-680-88) – назначение и компоненты информационного, технического, программного, математического, лингвистического, организационного и правового обеспечения. Автоматизированные рабочие места, пользователи и эксплуатационный персонал.

Понятие "безопасность автоматизированной системы". Безопасность информации в АС (конфиденциальность, целостность и правомерная доступность информации). Безопасность (надежность) функционирования АС (безотказность функций АС на основе безотказности/надежности программного обеспечения и безотказности/надежности технических средств и коммуникаций АС, аутентичность функций АС на основе целостности ПО и целостности параметров конфигурации ПО). Программно-техническая структура АС с точки зрения защиты информации и обеспечения безопасности функционирования.

Понятия "идентификация", "аутентификация", "авторизация", "спецификация", "классификация", "категорирование" и "каталогизация".

Классификационные схемы объектов защиты в автоматизированных (компьютерных) системах. Объекты защиты в АС (по ГОСТ Р 51624-2000). Реестр средств и их классификация по ISO/IEC 17799:2000. Объекты воздействия угроз по BSI (германскому стандарту безопасности ИТ). Защищаемые активы продуктов и систем ИТ (в идеологии «Общих критериев» - по ГОСТ Р ИСО/МЭК 15408-2002 и руководящим документам Гостехкомиссии/ФСТЭК). Идентификация и спецификация объектов защиты – выявление экземпляра объекта определенного вида и присвоение ему уникального идентификатора, авторизация (установление владельца), локализация местонахождения, оценка абсолютной/относительной стоимости и/или значимости. Методы и способы оценивания стоимости и/или значимости объектов защиты, интервальные и ранговые шкалы оценки (категорирование).

Понятие угрозы, угрозы безопасности информации в компьютерных системах. Классификационные схемы (каталогизация) угроз. Каталог угроз по BSI. ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию". Примеры угроз защищаемым активам в продуктах и системах ИТ (по РД

Гостехкомиссии "Безопасность ИТ. Руководство по разработке профилей защиты и заданий по безопасности"). Идентификация и спецификация (описание) угроз – выявление угрозы определенного типа и присвоение ей уникального идентификатора, определение и описания источника (природы) угрозы, активов/объектов, подверженных воздействию угрозы, особенностей реализации/осуществления. Общая схема оценивания угроз – оценка [вероятности] реализации и оценка ущерба. Оценка рисков, методы и шкалы оценки. Человеческий фактор в угрозах безопасности и модель нарушителя информационной безопасности.

Понятия функциональной и системной архитектуры (структуры) автоматизированных (компьютерных) систем. Целевая декомпозиция подсистем безопасности компьютерных систем (цели, задачи, функции, процедуры). Иерархический и функционально-модульный принцип структуры (архитектуры) монитора (ядра, системы) безопасности.

Общая характеристика стандартов безопасности компьютерных систем. Номинально-ранговый принцип оценивания безопасности (защищенности) компьютерных систем (классы/уровни безопасности/защищенности) в зависимости от реализации установленных для соответствующих классов/уровней наборов функциональных требований, сгруппированных в функциональные подсистемы или семейства. Концепция и общая характеристика "Критериев оценки безопасных (надежных) компьютерных систем" (США, 1983г., т.н. "Оранжевая книга").

Система защиты от НСД к информации в СВТ по ГОСТ Р 50739-95. Подсистемы и функциональные требования. Схема групп и классов защищенности АС по руководящим документам Гостехкомиссии. Система защиты от НСД к информации в АС по ГОСТ Р 51583-2000, РД Госттехкомиссии "АС. Защита от НСД к информации. Классификация АС и требования по защите информации", подсистемы и функциональные требования по классам защищенности.

Концепция и общая характеристика ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий" (т.н. "Общие критерии"), изделие (продукт или система) ИТ, объект оценки и среда безопасности, парадигма доверия и система оценочных уровней доверия к реализации требований по безопасности. Представление (система) функциональных требований безопасности к продуктам и системам ИТ – классы функциональных требований, их семейства, компоненты семейств, их функциональные элементы. Пакеты функциональных требований по типам и группам изделий ИТ (ОС, СУБД, МЭ и т.д.).

Архитектура систем защиты информации при взаимодействии открытых систем (ВОС). Структура стандартов в области ВОС (Госпрофиль ВОС – Рекомендации по стандартизации Р 50.1.022-2000 "Информационная технология. Государственный профиль взаимосвязи открытых систем России"). ГОСТ Р ИСО 7498-2-99 "Взаимосвязь открытых систем. Базовая эталонная модель. Ч.2. Архитектура защиты информации". Услуги безопасности, общеархитектурные и специальные механизмы их реализации. Взаимоотношение (размещение) между услугами защиты и уровнями эталонной модели ВОС.

Жизненный цикл АС – создание (обоснование необходимости, определение целей создания, требований, задач и функций АС, проектирование, реализация проектных решений, внедрение, ввод в эксплуатацию), эксплуатация и развитие (использование и применение по назначению, администрирование, сопровождение программных средств, техническое обслуживание и ремонт аппаратных средств), вывод из эксплуатации.

Общие положения и стандарты по созданию автоматизированных систем. Создание АС как продукции единичного производства проектным путем на плановой основе по техническому заданию. Принципы создания и требования по созданию АС (по РД 50-680-88).

Регламентация (по ГОСТ 34.601-90) процесса создания АС: предпроектные работы, их стадии и этапы (формирование требований к АС; разработка концепции АС; разработка, согласование и утверждение Технического задания); проектирование (эскизный проект, технический проект, рабочая документация); ввод в эксплуатацию (ввод в действие, сопровождение). Содержание работ на этапах создания. Методы обследования объекта информатизации, перечень и содержание документов, разрабатываемых на предпроектных стадиях (по РД 50-34.698-90). Особенности предпроектных работ при создании защищенных автоматизированных АС (АС в защищенном исполнении), в т.ч. анализ условий функционирования объекта информатизации и определение факторов, воздействующих на информацию (идентификация, спецификация и оценивание угроз безопасности), анализ категорий важности защищаемой информации, формирование требований по защите информации, принятие решения о классе защищенности АС.

Техническое задание на создание защищенных АС. Структура, порядок разработки, оформления, согласования и утверждения (по ГОСТ 34.602-89). Состав и содержание работ на стадии технорабочего проектирования. Понятие эскизного, технического и рабочего проекта (рабочей документации), требования к содержанию документов (по РД 50-34.698-90). Состав и содержание работ стадиях внедрения и сопровождения.

Обеспечение безопасности компьютерных сетей

Факторы, обуславливающие уязвимость компьютерной сети. Классификация атак на компьютерные сети. Основные типы и средства реализации сетевых атак. Формы и методы сетевой компьютерной разведки. Получение информации о программном обеспечении атакуемых сетей и узлов. Перехват трафика и его виды. Общая характеристика удаленного доступа в компьютерные сети. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Оценка риска удаленного доступа для объекта атаки и нарушителя.

Роль межсетевых экранов в корпоративной сети. Требования руководящих документов ФСТЭК России к межсетевым экранам. Типы межсетевых экранов. Схемы межсетевого экранирования. Критерии и правила фильтрации пакетов. Реализация пакетных фильтров. Понятие демилитаризованной зоны. Укрепленный компьютер бастионного типа. Особенности защитной фильтрации сетевого трафика. Персональные межсетевые экраны. Анализ эффективности применения средств межсетевого экранирования. Организация сетевых узлов для отвлечения внимания злоумышленника.

Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Классификация систем обнаружения атак. Варианты размещения систем обнаружения атак. Проблемы, связанные с системами обнаружения атак. Реагирование на инциденты. Анализ эффективности применяемых систем обнаружения компьютерных атак.

Средства и методы семантического сокрытия информации

Аналоговое и цифровое скремблирование речевых сигналов; принципы построения и характеристики аналоговых и цифровых скремблеров.

Современные симметричные криптосистемы и примеры их аппаратной и программной реализации. Понятие криптограммы. Классическая задача криптографии. Криптографические методы защиты хранимой и передаваемой информации.

Зашифрование, расшифрование, дешифрование. Система засекреченной связи. Ключи и ключевое пространство. Криптостойкость алгоритмов. Атаки на криптоалгоритмы. Типы алгоритмов шифрования. Абсолютно стойкие шифры. Условие абсолютной стойкости шифра К. Шеннона. Правило Керкхоффа. Методы, затрудняющие криптоанализ. Симметричные шифры. Сети Фейстеля. Алгоритмы DES, Triple-DES, ГОСТ 28147-89, AES. Поточные алгоритмы. Вероятностные шифры.

Асимметричные криптосистемы. Алгоритмы хэширования и электронной цифровой подписи. Односторонние функции, односторонние функции с секретом. Алгоритм RSA. Требования к хэш-функциям. Алгоритмы SHA, ГОСТ Р 34.11. Схемы построения ЭЦП. Механизмы распределения ключей. Нарушения в процессе информационного обмена, обнаруживаемые при помощи ЭЦП. Сравнительный анализ симметричных и асимметричных алгоритмов. Гибридная схема шифрования.

Сущность технологий VPN (Virtual Private Network), цели и задачи их использования. Свойства VPN-подключений. Компоненты VPN. Туннелирование в VPN. Протоколы шифрования на канальном, сетевом, транспортном и прикладном уровнях.

Принципы криптографической защиты электронной почты. Основные угрозы в системах электронной почты. Средства защиты PEM, S/MIME, PGP.

Принципы и основные понятия компьютерной стеганографии. Возможности сокрытия информации в распространенных типах файлов. «Нестандартные» способы сокрытия. Методы использования для сокрытия информации наименее значимых бит. Стеганографическое сокрытие информации в графических, текстовых и звуковых файлах с помощью свободно распространяемого программного обеспечения.

Защита объектов информатизации от физического доступа

Классификация информационных нарушителей. Общая характеристика удаленного доступа на объект информатизации. Непосредственные атаки на объекты информатизации. Геометрическая модель нарушителя. Биомеханическая модель человека. Физико-химическая модель человеческого тела. Социальная модель. Использование нарушителем инструментов для взлома. Признаки присутствия и функционирования автономных средств технической разведки и вредоносных компьютерных программ. Тактика непосредственного доступа к автоматизированным системам и машинным носителям информации. Характерные признаки непосредственного доступа.

Вероятная тактика нарушителей, определяемая целью проникновения и качеством охраны объекта. Модель поведения человека-нарушителя в экстремальных ситуациях.

Проектирование систем сопротивления физическому вторжению на объекты информатизации. Периметровые ограждения. Строительные нормы и правила оборудования зданий и помещений, предназначенных для хранения и обработки конфиденциальной информации. Размещение режимных помещений в многоэтажных зданиях. Требования к ограждающим конструкциям зданий и помещений. Оборудование оконных проемов, к которым возможен наружный доступ. Требования к защитным решеткам. Виды специальных стекол. Требования к оборудованию дверных проемов. Замковые устройства и ключи повышенной секретности. Оборудование вентиляционных каналов. Проектирование рубежа физической защиты автоматизированных рабочих мест на базе персональных компьютеров. Проектирование рубежей сдерживания нарушителя. Оценка времени сдерживания и трудоемкости строительства и эксплуатации рубежей. Требования к сдерживающим и эстетическим характеристикам механических препятствий. Распыляемые барьеры.

Преобразователи физических величин.. Генераторные и параметрические преобразователи. Типы преобразователей. Классификация средств обнаружения по типу преобразования физических величин. Структура сигнализационных датчиков, приборов, систем и комплексов. Сигнализационные датчики охраны режимных помещений и протяженных участков (периметров объектов).

Сигнализационные датчики первого рубежа охраны: электроконтактные, магнитоконтактные, удароконтактные (датчики разрушения стекла). Основные характеристики и особенности применения активных и пассивных инфракрасных сигнализационных датчиков. Классификация радиотехнических средств обнаружения. Периметровые вибрационные и сейсмические датчики. Влияние дестабилизирующих факторов на работоспособность сигнализационных датчиков. Промышленные образцы сигнализационных изделий отечественного и зарубежного производства. Устройства и системы пожарной сигнализации. Классификация и принципы построения пожарных датчиков. Тактические требования, предъявляемые к системам охранного телевидения. Классификация и обобщенная структура телевизионных средств наблюдения. Устройства обработки видеоизображения: коммутаторы, квадраторы, мультиплексоры, матричные коммутаторы. Устройства дистанционного управления видеосистемами. Особенности выбора технических средств телевизионной системы. Анализ типовых проектных решений.

Основные понятия и определения. Классификация СУД. Специальные режимы пропуска. Идентификация и аутентификация пользователей АИС. Биометрические системы аутентификации. Биометрическая аутентификация по динамическим признакам. Физические носители ключевой информации. Ключевые дискеты и оптические диски. Магнитные карты. Исполнительные устройства управления доступом. Механические, электромеханические замки, автоматические шлагбаумы, турникеты, шлюзы. Методы и средства аутентификации пользователей ЭВМ. Идентификация и аутентификация пользователей ЭВМ.

Приемно-контрольные приборы охранно-пожарной сигнализации. Классификация и основные характеристики ПКП. Обобщенная структурная схема ПКП. Промышленные образцы приемно-контрольных приборов отечественного и зарубежного производства. Системы передачи информации охранно-пожарной сигнализации. Варианты построения систем передачи тревожной информации от периферийных устройств объектовой сигнализации. Создание локальной радиосети для системы сигнализации. Радиоканальные системы передачи информации (РСПИ): приемо-передающая аппаратура, антенны, выбор частотного диапазона, особенности распространения радиоволн в городских условиях, радиопомехи. Использование радиолиний сотовых сетей связи общего пользования, специальных радиосетей передачи данных.

Защита узлов и блоков стационарных компьютеров от НСД. Механические крепежные элементы. Средства, препятствующие хищению составных частей компьютера. Устройства, препятствующие несанкционированному доступу в аппаратные отсеки. Пломбы, печати, голографические наклейки. Защита дисководов и внешних интерфейсов. Использование настроек BIOS для защиты от загрузки внешних программ со сменных машинных носителей. Использование сигнализационных датчиков для контроля вскрытия системного блока. Интеллектуальные возможности контроллеров жестких магнитных дисков с IDE-интерфейсом. Использование сигнализационных датчиков для контроля доступа к рабочему месту пользователя. Контроль за рабочим местом с использованием Web-камер. Возможности операционной системы и прикладных программ по отслеживанию фактов физического доступа к системному блоку и узлам компьютерной системы.

Комплексное применение технических средств при охране объектов. Объединение систем видеонаблюдения, охранной сигнализации и управления доступом в единую интегрированную систему безопасности. Тактика применения технических средств охраны. Общие тактические требования к технической охране. Тактические требования к средствам охраны объектов (помещений), периметровым сигнализационным средствам и заграждениям. Категории охраняемых объектов, рубежи охраны. Критерии, определяющие выбор технических средств охраны. Организация проектирования инженерно-технической защиты. Предпроектные изыскания. Разработка тактико-технических заданий на проектирование. Порядок проведения обследования территории, заданий, помещений, рабочих мест и хранилищ. Требования к техно-рабочему проекту (ТРП). Состав ТРП. Критерии эффективности защиты объектов информатизации от непосредственного доступа. Методика оценки эффективности защитных мер.

Защита компьютерных систем от несанкционированного доступа к хранимой информации

Методы и средства идентификации и аутентификации пользователей ЭВМ. Парольные системы. Требования к выбору паролей, вводу, передаче и хранению парольной информации. Компьютерные устройства аутентификации пользователей по биометрическим признакам и физическим носителям ключевой информации.

Защита узлов и блоков ЭВМ от непосредственного доступа. Средства ограничения НСД в аппаратные отсеки, защита дисководов и внешних интерфейсов. Контроль доступа к ЭВМ с использованием сигнализационных датчиков, Web-камер и специальных программ.

Функции, выполняемые специализированными средствами защиты информации (СЗИ). Механизмы ограничения на вход в компьютерную систему. Взаимодействие СЗИ с BIOS системной платы. Контроль целостности системного программного обеспечения и аппаратных средств. Программно-аппаратная идентификация и аутентификация пользователей. Возможности СЗИ по криптографическому преобразованию информации. Контроль и удаление «технологического мусора».

Механизмы организации контроля доступа до загрузки ОС. Формирование и поддержка изолированной программной среды.

Выявление и нейтрализация электронных средств негласного получения информации (ЭСНПИ)

Классификация ЭСНПИ по способам внедрения на объект, передаче перехваченной информации, электропитанию, камуфляжу и др.

Средства перехвата речевой информации по акустическому каналу. Типы, принцип действия и характеристики конденсаторных, пьезоэлектрических и электретных микрофонов. Использование микрофонного эффекта в оптоволоконной линии. Конструкции направленных микрофонов, особенности их камуфляжа. Инфракрасные (лазерные) приборы для считывание речевой информации за счет вибрации остекленных проемов.

Средства перехвата речевой информации по вибрационному и оптико-электронному каналам. Типы и характеристики электронных стетоскопов. Эффективная дальность перехвата информации по виброакустическому каналу.

Характеристики современных портативных устройств звукозаписи. Методы и средства выявления и подавления работающих диктофонов.

Угрозы, связанные с несанкционированным использованием на объектах информатизации абонентских устройств мобильной связи. Использование сотовых телефонов с целью негласного подслушивания и фотографирования. Устройства для выявления включенных сотовых телефонов и их электромагнитного подавления.

Закладные устройства для негласного подслушивания. Типы и устройства акустических закладок. Каналы передачи информации, электропитание, камуфляж. Возможности скрытой передачи перехваченной голосовой информации. Основные демаскирующие признаки ЭСНПИ. Модель нарушителя, осуществляющего дистанционное прослушивание и звукозапись.

Содержание специальной лабораторной проверки (СЛП) радиоэлектронной аппаратуры. Комплект документации, приборов и инструмента, необходимый для проведения СЛП. Порядок проверки аппаратуры в различных режимах Работы. Разборка и визуальный осмотр аппаратуры. Визуальные демаскирующие признаки аппаратных закладок.

Методика проведения визуального и инструментального досмотра помещений, выделенных для ведения конфиденциальных разговоров. Места и предметы, используемые для скрытого размещения электронных средств негласного подслушивания. Виды и периодичность досмотра. Досмотровая техника и тактика.

Физические принципы обнаружения ЭСНПИ в пассивном состоянии. Принцип нелинейной локации. Металлоискатели. Обнаружители пустот в ограждающих конструкциях помещения.

Современные технические средства радиомониторинга. Индикаторы электромагнитного поля, радиочастотомеры, сканирующие приемники, анализаторы спектра, интерсепторы, программно-аппаратные комплексы. Их основные тактико-технические характеристики и подготовка к работе. Тактика и методика применения технических средств радиомониторинга при проведении поисковых мероприятий.

Принципы защиты информации от технической разведки и утечки по техническим каналам

Характеристики речевой, телевизионной, телематической, видовой информации, циркулирующей на объектах информатизации. Функциональные каналы передачи-приема и отображения информации.

Средства и способы ведения промышленной и коммерческой разведки. Цели и задачи бизнес-разведки. Сведения о клиентах, кредиторах, заемщиках, арендаторах, деловых партнерах, которые допустимо получать легальными способами. Неправомерные методы ведения бизнес-разведки. Использование средств технической разведки со стороны преступных формирований и отдельных лиц.

Принципы и системы визуально-оптической, фотографической, радио-, радиотехнической, радиолокационной, оптико-электронной, тепловизионной, сейсмической, акустической, гидроакустической, радиационной и химической разведок.

Общие принципы противодействия техническим разведкам. Средства и методы предотвращения доступа нарушителей на объекты информатизации. Методы энергетического сокрытия носителей информации. Методы дезинформации, легендирования, сокрытия, камуфляжа. Классификация и характеристика активных способов и средств радиоэлектронного, оптико-электронного, гидроакустического подавления технических средств разведки. Математические модели и методики оценки эффективности применения активных средств радиоэлектронного подавления.

Понятие о технических каналах утечки информации (ТКУИ). Источники «опасных» сигналов. Модель и классификация ТКУИ. Общая характеристика визуально-оптических, электромагнитных, акустических и материально-вещественных каналов утечки информации.

Общие принципы защиты информации от утечки по техническим каналам. Смысловые и энергетические критерии защиты. Отношение энергии «опасного» сигнала и помехи на входе разведывательного приемного устройства. Уменьшение энергетики «опасных» сигналов; схемные и конструктивные решения, направленные на их нейтрализацию; обнаружение и ликвидация «случайных» антенн; экранирование и искусственное зашумление.

Выявление ТКУИ. Объекты исследований и измерений при защите от утечки информации по техническим каналам; измеряемые параметры сигналов. Измерительные приборы: их классификация, характеристика, устройство, подготовка к работе, проведение измерений. Измерительные антенны и их калибровка. Измерение акустических величин. Измерительные преобразователи вибраций. Измерительные микрофоны. Погрешности измерений и измерительных приборов; обработка результатов измерений;

Аппаратные и программные средства для пространственного измерения уровня побочных электромагнитных и акустических излучений. Порядок проведения измерений. Измерения, проводимые на рабочих местах. Измерения побочных излучений, проводимые в условиях специальной лаборатории (безэховой камеры). Интерполяция и экстраполяция результатов измерений. Порядок проведения расчетов и построения границ контролируемой зоны на местности. Оформление итоговых отчетных документов по результатам исследований.

Методики инструментальных специальных исследований технических средств; методика контроля защищенности информации от утечки за счет ПЭМИН; методики измерений и расчета параметров технических средств на соответствие нормам в речевом диапазоне частот; методики измерений и расчета параметров средств передачи дискретной информации на соответствие нормам защиты.

Методы и средства защиты основных технических средств. Фильтрация сигналов в проводных каналах, выходящих за пределы объекта информатизации. Экранирование проводных каналов связи, модулей, блоков и корпусов РЭА, помещений; основные требования; используемые материалы и конструкции; правила, технология экранирования.

Пространственное и линейное зашумление; виды шумов; генераторы шума; расчет требуемой интенсивности «белого» и «окрашенного» шума; адаптивные генераторы шума.

Показатели и нормы эффективности защиты информации от технических разведок и утечки по техническим каналам; их физический смысл.

Технология защиты информации от технической разведки и утечки по визуально-оптическому каналу

Физические основы возникновения первичных демаскирующих признаков объектов в ультрафиолетовом, видимом и инфракрасном диапазонах электромагнитных волн. Визуальный и тепловой контраст объекта наблюдения и фона. Источники оптического излучения. Параметры излучения и отражения. Факторы, обуславливающие оптическую видимость объектов.

Принципы построения и функционирования средств визуальной оптической и оптико-электронной разведок; характеристики и возможности зрительной системы человека, линзовых и зеркальных систем; принципы построения и основные характеристики пассивных и активных приборов ночного видения; средств телевизионной

и тепловизионной разведок; методики оценки возможностей средств визуальной оптической и оптико-электронной разведок.

Принципы построения и функционирования средств фотографической разведки; основные характеристики фотоаппаратов. Показатели качества изображения, получаемых техническими средствами разведки; дешифрование изображений, получаемых средствами видовой разведки; методики оценки возможностей систем фотографической и оптико-электронной разведок по обнаружению и распознаванию объектов.

Современные средства видеосъемки и их возможности. Характеристики передающих телевизионных камер. Средства видеозаписи и видеовоспроизведения.

Возможности и характеристики современных тепловизоров. Методы и средства инфракрасной маскировки.

Противодействие средствам и методам оптического наблюдения. Энергетическое сокрытие объектов в оптическом диапазоне. Сокрытие визуальных признаков объектов от воздушной и наземной разведки. Общие принципы визуальной маскировки. Принципы камуфляжа. Маскировочное окрашивание. Уменьшение оптической прозрачности среды. Визуальная дезинформация противника. Ложные объекты.

Технология защиты информации от технической разведки и утечки по электромагнитному каналу

Физические основы образования электромагнитных каналов утечки информации. Электрическое поле одиночного заряда и электрического диполя. Магнитное поле одиночного провода с током и симметричной линии. Механизмы побочного электромагнитного излучения радиоэлементов и проводников радиоэлектронной аппаратуры. Электромагнитные поля, создаваемые в ближней и дальней зонах элементарными излучателями (диполем, нитью тока, листком тока, плоской бесконечной поверхностью тока). Зоны излучения типовых излучателей. Зависимость излучаемой энергии от координат точки наблюдения и частоты колебаний. Спектр побочных излучений, наблюдаемых при протекании по цепям токов импульсной формы.

Электромагнитные влияния между проводными линиями связи. Влияния, обусловленные электрическими и магнитными связями. Оценка взаимного влияния между симметричными и коаксиальными линиями. Защита линий связи от взаимного влияния. Принципы и схемы скрещивания. Скрутка цепей, шаг скрутки. Симметрирование цепей. Потери на связь для симметричной и витой пары.

Виды заземляющих устройств. Явления при стекании тока в землю. Пространственное распределение потенциала заземленного проводника. Расчет сопротивления растеканию тока для заземлителей простой формы. Варианты подключения аппаратуры к шинам заземления. Типовые ошибки при оборудовании заземляющих устройств. Утечка сигнальных токов по цепям заземления. Защита заземляющих устройств от съема информации по цепям заземления.

Паразитные цепи утечки сигнальных токов в сеть промышленного электропитания. Утечка за счет неравномерности потребления тока. Использование цепей промышленного электропитания в качестве канала передачи перехваченной информации. Фильтры электропитания и оценка их эффективности.

Характеристика технических каналов утечки информации, возникающих при использовании средств вычислительной техники (СВТ). Особенности образования каналов утечки компьютерной информации. Каналы утечки конфиденциальной информации при ее клавиатурном вводе в ЭВМ. Виды и возможности аппаратного перехвата клавиатурного ввода. Способы перехвата компьютерной информации при ее выводе на печать.

Возможности восстановления печатаемой информации по излучаемым и перехватываемым сигналам. Каналы утечки информации из компьютерных мониторов и видеоадаптеров. Меры по снижению электромагнитной утечки из СВТ. Пассивные компоненты, используемые техническими разведками для увеличения уровня побочных излучений. Утечка информации, передаваемой по проводным каналам локальных вычислительных сетей.

Принципы электромагнитного экранирования. Скин-эффект. Виды экранирования. Правила эффективного экранирования. Требования, предъявляемые к электромагнитному экранированию электрических кабелей. Экранирование корпусов и блоков РЭА. Материалы, рекомендуемые для экранирования помещений. Порядок выполнения работ по экранированию помещений. Использование для экранирования подвесных металлизированных потолков, металлизированных обоев, линолеума, армированных стекол. Типовые ошибки, допускаемые при электромагнитном экранировании помещений.

Линейное и пространственное электромагнитное зашумление. Спектральные характеристики типовых сигналов в каналах утечки. Виды шумоподобных сигналов. Генераторы шума. Расчет требуемой интенсивности шумов.

Технология защиты информации от технической разведки и утечки по акустическому и виброакустическому каналам

Физические основы образования акустических и виброакустических каналов утечки информации. Распространение звука в газах, жидкостях и твердых телах. Преломление, отражение и рассеяние звуковых волн. Первичный речевой сигнал и его характеристики. Фонемы и звуки речи. Оценка разборчивости речи. Голосовой импульс, высота голоса, форманты.

Физические основы образования акустоэлектрических каналов утечки информации. Электроакустические преобразователи. Физические принципы акустоэлектрических и электроакустических преобразователей. Элементы и устройства с «микрофонным» эффектом. Электростатические, электромагнитные, пьезоэлектрические и магнитострикционные преобразователи. Типовые побочные преобразователи акустических сигналов. Воздействие акустических сигналов на резонансные цепи гетеродинов радио- и телеприемников.

Защита акустической информации путем зашумления и экранирования. Оценка качества перехваченного сообщения. Разборчивость слогов, слов и фраз. Виброакустическое зашумление помещений; типовые источники акустического шума; средства постановки акустических и виброакустических помех, их характеристики, порядок использования; санитарно-гигиенические нормы на уровень шумов.

Архитектурно-строительные средства и методы защиты помещений от незаконного прослушивания. Общие принципы звукоизоляции и нормы проектирования помещений, выделенных для ведения конфиденциальных разговоров. Звукоизолирующие и звукопоглощающие свойства строительных и отделочных материалов. Специальные звукопоглощающие покрытия. Звукоизолирующие конструкции дверей и окон, вентиляционных и технологических каналов, систем водоснабжения, отопления и канализации. Акустические экраны. Звукоизолирующие кабины.

Общие правила конфиденциального речевого общения.

Технология защиты информации от технической разведки и утечки по материально-вещественному каналу

Понятие о признаковой информации. Особенности материально-вещественного канала утечки информации.

Виды вещественных носителей информации. Стойкость запечатления семантической информации. Классификация способов защитного удаления информации.

Общие правила уничтожения секретных документальных материалов. Хранение документов и черновиков, предназначенных для уничтожения. Методы утилизации бумажных носителей, фото- кинопленок, специальных носителей. Устройства для механического измельчения вещественных носителей информации.

Механизмы копирования, модификации и удаления компьютерной информации на машинных носителях. Методы и средства восстановления компьютерной информации. Автоматическое и ручное восстановление системной информации, удаленных и испорченных данных, дефектных носителей. Восстановление системной информации, данных и программного обеспечения с резервных копий. Специальные способы и средства реставрации удаленной компьютерной информации на машинных носителях. Возможности лабораторий, специализирующихся на восстановлении уничтоженной компьютерной информации.

Программные средства физического и логического удаления компьютерной информации, оценка их эффективности. Аппаратные средства мгновенного размагничивания магнитных носителей. Магнитные сейфы. Аппаратно-программные средства стирания машинных носителей с дистанционным и событийным управлением.

Защита компьютерной информации от ее непреднамеренного распространения. Регламентация порядка обращения с машинными носителями конфиденциальной информации. Утилизация машинных носителей различного типа. Защитные технологии копирования и тиражирования конфиденциальной информации. Требования к сбору, хранению и утилизации отходов печати и ксерокопирования.

Уничтожение вещественных носителей в экстремальных ситуациях. Специальные устройства для транспортировки секретных документов.

Педагогика высшей школы

Приоритетные стратегии и тенденции развития высшего образования в России.

Методологические проблемы реализации ФГ'ОС в высшей школе.

Качество профессионального образования и его технологическое обеспечение.

Нормативно-правовое обеспечение педагогического процесса и деятельности преподавателей в вузе.

Педагогическое проектирование - ведущий аспект деятельности современного преподавателя вуза.

Современные модели организации учебного процесса в высшей школе.

Проблемы педагогической квалиметрии в высшей школе.

Педагогический процесс как форма организации, воспитания в вузе. Профессиональное воспитание в вузе.

Профессионально-педагогические компетенции преподавателя высшей школы.

Профессиональная культура преподавателя. Профессионально-личностное саморазвитие преподавателя.

2.2. Научно-квалификационная работа (доклад)

Научное содержание научно-квалификационной работы аспиранта должно удовлетворять установленным требованиям к содержанию диссертаций на соискание ученой степени кандидата наук по выбранной научной специальности и паспортом специальности.

3. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

3.1. Рекомендуемая литература

3.1.1. Основная литература

1. Андрончик А.Н. и др. Защита информации в компьютерных сетях. Практический курс: учебное пособие / А.Н. Андрончик, В.В. Богданов, Н.А. Домуховский, А.С. Коллеров, Н.И. Синадский, Д.А. Хорьков, М.Ю. Щербаков; Под ред. Н.И. Синадского. – Екатеринбург: ГОУ ВПО УГТУ - УПИ, 2007. – 246 с.
2. Бакланов В.В. Администрирование и безопасность операционных систем Linux : учебное пособие [для вузов] / В. В. Бакланов ; науч. ред. Н. А. Гайдамакин. — Екатеринбург : [УГТУ-УПИ], 2006 . — 92 с. : ил. — (Информационная безопасность) . — Библиогр.: с. 85. 15 экз.
3. Бакланов В.В. Введение в информационную безопасность. Направления информационной защиты : курс лекций : учеб. пособие для вузов / В. В. Бакланов.— Екатеринбург : Изд-во Уральского университета, 2007 .— 232 с. — (Приоритетный национальный проект "Образование") (Математика. Компьютерные науки) .— Библиогр.: с. 229-232 .— ISBN 5-7996-0259-5.
4. Бакланов В.В. Защитные механизмы операционной системы Linux.: учеб. пособие для вузов. В.В. Бакланов. Под ред. Н.А. Гайдамакина. Екатеринбург, УрФУ, 2012 г. 354 с. ISBN 978-5-321-01966-5.
5. Бакланов В.В. Защитные механизмы текстового процессора Microsoft Word: учеб. пособие для вузов. В.В. Бакланов. Под ред. Н.А. Гайдамакина. Екатеринбург, УрФУ, 2012 г. 112 с.
6. Бакланов В.В., Пономарев М.Э. Опасная компьютерная информация: учеб. пособие для вузов. В.В. Бакланов. Екатеринбург, УрФУ, 2013 г. 216 с.
7. Бакланов В.В. Стратегии и модели информационной защиты. Монография. Екатеринбург, УРФУ, 2007 г., 324 с.
8. Бакланов В.В., Духан Е.И., Шамонин Е.Д. Оценка эффективности средств физической защиты: учеб. Пособие для вузов. В.В.Бакланов. Екатеринбург, УрФУ, 2016 г., 284 с.
9. Бузов Г.А., Защита от утечки информации по техническим каналам : учеб. пособие для подгот. экспертов системы Гостехкомиссии России / Г. А. Бузов, С. В. Калинин, А. В. Кондратьев .— М. : Горячая линия - Телеком, 2005. — 416 с.
10. Гайдамакин Н.А. Автоматизированные информационные системы, базы и банки данных. Вводный курс : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем" / Н. А. Гайдамакин. — Москва : Гелиос АРВ, 2002. — 368 с. : ил. ; 20 см .— Библиогр.: с. 354-355 (34 назв.). — допущено в качестве учебного пособия .— ISBN 5854380358 : 90.00.
11. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / Н. А. Гайдамакин. — Екатеринбург : Издательство Уральского университета, 2003 .— 328 с. : ил. ; 21 см .— Алф.-предм. указ.: с. 306-316. — Библиогр.: с. 317-322 (80 назв.). — ISBN 5-86037-024-5 : 40.00.
12. Духан Е.И. Применение программно-аппаратных средств защиты компьютерной

информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106 / Е. И. Духан, Н. И. Синадский, Д. А. Хорьков ; науч. ред. Н. А. Гайдамакин ; Урал. гос. техн. ун-т - УПИ .— Екатеринбург : УГТУ-УПИ, 2008. — 182 с.

13. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телекоммуникац. систем" / С. П. Расторгуев .— Москва : Академия, 2007 .— 188 с. ; 22 см .— (Высшее профессиональное образование, Информационная безопасность) .— Слов. терминов: с. 182-185. — Библиогр.: с. 180-181 (39 назв.). — Допущено в качестве учебного пособия. — ISBN 978-5-7695-3098-2.
14. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс: учебное пособие / А.Н. Андрончик, А.С. Коллеров, Н.И. Синадский, М.Ю. Щербаков; под ред. Н.И. Синадского. – Екатеринбург: УрФУ, 2011. – 160 с.
15. Синадский Н.И. Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие / Н. И. Синадский ; науч. ред. В. В. Бакланов .— Екатеринбург : [ГОУ ВПО УГТУ-УПИ], 2007. — 136 с. 90 экз.
16. Синицын С.В. Операционные системы : учебник для вузов / С. В. Синицын, А. В. Батаев, Н. Ю. Налютин .— 3-е изд., стер. — Москва : Издательский центр "Академия", 2013 .— 296 с. 9 экз.
17. Торокин, А.А. Инженерно-техническая защита информации : учеб. пособие для студентов вузов, обучающихся по специальностям в области информ. безопасности / А. А. Торокин .— Москва : Гелиос АРВ, 2005 .— 960 с.
18. Фергюсон Н. Практическая криптография / Нильс Фергюсон, Брюс Шнайер ; [пер. с англ. Н. Н. Селиной под ред. А. В. Журавлева] .— Москва ; Санкт-Петербург ; Киев : Диалектика, 2005 .— 424 с. ; 24 см .— Предм. указ.: с. 418-421. — Пер. изд.: Practical Cryptography / N. Ferguson, B. Schneier. - 2003. — Библиогр.: с. 410-417.
19. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : учеб. пособие для студентов вузов, обучающихся по направлению 23100 (654600) "Информатика и вычисл. техника" / П. Б. Хорев .— М. : Academia, 2005 .— 256 с. 29 экз.

3.1.2. Дополнительная литература

* Конституция РФ (принята на всенародном голосовании 12 декабря 1993 г.).

* Налоговый кодекс РФ, часть первая от 31 июля 1998 г. № 146-ФЗ

* и часть вторая от 5 августа 2000 г. № 117-ФЗ.

* Кодекс об административных правонарушениях РФ от 30 декабря 2011 г. № 195-ФЗ.

* Уголовный кодекс РФ от 13 июня 1996 г. № 63-ФЗ.

* Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

* Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне».

* Закон РФ от 21 июля1993 г. № 5485-I «О государственной тайне».

* Федеральный закон от 2 декабря 1990 г. № 395-I «О банках и банковской деятельности».

* Федеральный закон от 27 июля 2011 г. № 161-ФЗ «О национальной платежной системе».

* Федеральный закон от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

* Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

* Федеральный закон от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности».

* Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в РФ».

* Закон РФ от 2 июля 1992 г. № 3185-I «О психиатрической помощи и гарантиях прав граждан при ее оказании».

* Федеральный закон от 9 февраля 2009 г. № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления».

* Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

* Федеральный закон от от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

* Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).

* Указ Президента РФ от 19 марта 2008 г. № 351 «О мерах по обеспечению

информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

* Указ Президента РФ от 22 мая 2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

* Постановление Правительства РФ № 1119 от 1.11.2012 г. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

* Требования о защите информации, содержащейся в информационных системах общего пользования (утв. приказом ФСБ России и Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. № 416/489).

* Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / под ред. Т. А. Поляковой, А. А. Стрельцова. — М. : Издательство Юрайт, 2016. — 325 с. — Серия : Бакалавр и магистр. Академический курс.

* Интернет-право: Учеб. пособие для студентов вузов, обучающихся по специальности 021100 «Юриспруденция» / И.М. Рассолов. — М.: ЮНИТИ-ДАНА, Закон и право, 2012. — 143 с. — (Серия «Высшее профессиональное образование: Юриспруденция»).

20. Барсуков, В. С. Современные технологии безопасности: интегральный подход / В.С. Барсуков, В.В. Водолазкий .— М. : Нолидж, 2000 .— 496 с.
21. Бил Дж.и др. Snort 2.1 Обнаружение вторжений. – М.: Бином, 2009. – 656 с.
22. Введение в криптографию: Учебник / В.В. Ященко, Н.П. Варновский, Ю.В. Нестеренко и др. ; Под общ. ред. В.В. Ященко .— СПб.; М.; Харьков; Минск : МЦНМО: Питер, 2001 .— 288 с. : ил.; 24 см .— (Новые математические дисциплины) .— Библиогр. в конце гл. — Прил.: Отрывок из ст. К. Шеннона "Теория связи в секретных системах": с. 251-287. — без грифа .— ISBN 5-318-00443-1 : 80.00.

23. Галатенко, В. А. Стандарты информационной безопасности. Курс лекций : учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. технологий / В. А. Галатенко ; под ред. В. Б. Бетелина .— 2-е изд. — Москва : Интернет-Университет Информационных Технологий, 2009 .— 264 с.
24. Галатенко, В. А. Основы информационной безопасности : Курс лекций: Учеб. пособие для вузов / В. А. Галатенко ; Под ред. В. Б. Бетелина .— 2-е изд., испр. — М. : Интернет-Ун-т Информ. Технологий, 2004 .— 264 с. — (Основы информационных технологий). — Рек. Учеб.-метод. об-нием в обл. прикладной информатики .— Библиогр.: с. 256-260. — ISBN 5-9556-0015-9 : 200-00.
25. Гультяев А.К. Восстановление данных / А. К. Гультяев. — 2-е изд. — СПб. : Питер, 2006 .— 379 с.
26. Копылов, Виктор Александрович. Информационное право : учебник / В. А. Копылов ; М-во образования РФ, Моск. гос. юрид. акад. — Изд. 2-е, перераб. и доп. — М. : Юристъ, 2005 .— 511 с.
27. Мельников, В. П. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обучающихся по специальности 230201 "Информ. системы и технол." / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова .— Москва : Академия, 2006 .— 336 с.
28. Меньшаков Ю. К. Защита объектов и информации от технических средств разведки: учебник. РГГУ, 2002. — 400 с.
29. Основы информационной безопасности : учеб. пособие для вузов / Е. Б. Белов [и др.]. — М.: Горячая линия-Телеком, 2006 .— 544 с. : ил. — Допущено М-вом образования и науки РФ .— ISBN 5-93517-292-5.
30. Олифер В. Г. Сетевые операционные системы : учеб. для вузов / В. Г. Олифер, Н. А. Олифер .— 2-е изд. — Москва [и др.] : Питер, 2008 .— 669 с. 10 экз.
31. Пог.Д. Mac OS X Leopard. Основное руководство / Дэвид Пог ; [пер. с англ. С. Маккавеева] .— Санкт-Петербург ; Москва : Символ-Плюс, 2008 .— 880 с. 1 экз.
32. Петраков, А.В. Основы практической защиты информации : Учеб. пособие для вузов по спец. 20. 18. 00 "Защищенные системы связи" / А.В. Петраков .— 2-е изд. — М. : Радио и связь, 2000 .— 368 с.
33. Платонов В.В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : учеб. пособие для студентов вузов, обучающихся по специальностям 090102, 090105 / В. В. Платонов .— Москва : Академия, 2006 .— 240 с. 10 экз.
34. Платонов В. В. Программно-аппаратные средства защиты информации : учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность" / В. В. Платонов .— Москва : Академия, 2013 .— 336 с.
35. Проскурин В. Г. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах : Учеб. пособие для студентов вузов, обучающихся по спец. "Защищенные телекоммуникационные системы", "Орг. и технология защиты информации", "Комплексное обеспечение информ. безопасности автоматизир. систем" / В. Г. Проскурин, С. В. Крутов, И. В. Мацкевич. — М. : Радио и связь, 2000 .— 168 с.
36. Рассолов, И. М. Интернет-право / И.М. Рассолов .— Москва : Юнити-Дана, 2015 .— 143 с.
37. Робачевский А.М. Операционная система UNIX : Учеб. пособие для студентов вузов / А.М. Робачевский. — Дюссельдорф; Киев; М.; СПб. : БХВ-Петербург, 2002. — 514 с. 9. экз.
38. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.
39. Скляров Д.И. Искусство защиты и взлома информации / Д. В. Скляров .— СПб. :

БХВ-Петербург, 2004 .— 288 с. : ил. ; 24 см .— Библиогр.: с. 273-276 (67 назв.). — ISBN 5-94157-331-6.

3.2. Методические разработки

40. Бакланов, В. В. Основы информационной безопасности / Бакланов В.В. — 2007. — Курс "Основы информационной безопасности" предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11063>.
41. Бакланов В. В. Программно-аппаратная защита информации / Бакланов В.В., Ваулин С.С., Синадский Н.И. — УМК. — 2007. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=7232>.
42. Бакланов, В. В. Основы информационной безопасности / Бакланов В.В., Вострецова Е.В., Гайдамакин Н.А., Лучинин А.С. — УМК. — 2010 .— в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=9407>.
43. Гайдамакин Н.А. Теоретические основы компьютерной безопасности / Гайдамакин Н.А. — <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11073>. — 2008 .— Курс "Теоретические основы компьютерной безопасности" предназначен для студентов специальности "Компьютерная безопасность".
44. Гайдамакин Н.А. Учебно-методический комплекс дисциплины "Основы создания и эксплуатации защищенных компьютерных систем" [Электронный ресурс] / Н. А. Гайдамакин ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (8,17 Мб) .— Екатеринбург : [б. и.], 2007 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки
45. Исследование технических каналов утечки информации и методов борьбы с ними : метод. указания к лаб. работам по дисциплине "Техн. средства и методы защиты информации" для студентов специальности 075600 - Информ. безопасность телекоммуникац. систем / Урал. гос. техн. ун-т - УПИ ; [сост. А. С. Лучинин ; науч. ред. А. П. Мальцев] .— Екатеринбург : УГТУ-УПИ, 2004 .— 39 с.
46. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Т. 1. Законодательные акты РФ, указы и распоряжения Президента РФ, постановления и распоряжения Правительства РФ / Урал. гос. техн. ун-т - УПИ, Регион. учеб.-науч. центр по проблемам информ. безопасности ; [авт.-сост. Н. А. Гайдамакин] .— Екатеринбург : Гриф, 2006 .— 658 с. ; 29 см .— Библиогр. в тексте, библиогр. в примеч. — ISBN 5-98058-021-2.
47. Сборник нормативных правовых актов по компьютерной и информационной безопасности. Т. 2. Ведомственные нормативные правовые акты и руководящие документы / Урал. гос. техн. ун-т - УПИ, Регион. учеб.-науч. центр по проблемам информ. безопасности ; [авт.-сост. Н. А. Гайдамакин] .— Екатеринбург : Гриф, 2006. — 740 с.
48. Синадский Н.И. Безопасность операционных систем. УМК, 2007. Метаданные ресурса №7029.
49. Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.
50. Синадский Н. И. Специализированные программно-аппаратные средства защиты информации / Синадский Н.И. — 2008. — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11071>.

3.3. Программное обеспечение

MS Office, Операционные системы семейства MS Windows , ОС Linux.

3.4. Базы данных, информационно-справочные и поисковые системы

1. http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»
2. http://www.edu.ru/ - Федеральный портал. Российское образование.
3. http://study.urfu.ru –портал информационно-образовательных ресурсов УрФУ
4. http://rtf.urfu.ru - официальный сайт ИРИТ-РтФ

3.5. Электронные образовательные ресурсы

1. Портал информационно-образовательных ресурсов УрФУ http://study.urfu.ru/info/default.aspx
2. Официальный сайт ИРИТ-РтФ http://rtf.urfu.ru
3. Официальный сайт кафедры ТОР УрФУ http://tor.rtf.urfu.ru

4. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ГОСУДАРСТВЕННОЙ ИТОГОВОЙ АТТЕСТАЦИИ

Персональные компьютеры. Мультимедийный проектор с экраном. Сетевое оборудование. Локальная сеть с выходом в сеть Интернет.

КАРТА КОМПЕТЕНЦИЙ

Шифр и название КОМПЕТЕНЦИИ:

УК-1 Способность к критическому анализу и оценке современных научных достижений, генерированию новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ, Тип КОМПЕТЕНЦИИ:

Универсальная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: основные методы научно-исследовательской деятельности.

• УМЕТЬ: выделять и систематизировать основные идеи в научных текстах; критически оценивать любую поступающую информацию, вне зависимости от источника; избегать автоматического применения стандартных формул и приемов при решении задач

• ВЛАДЕТЬ: навыками сбора, обработки, анализа и систематизации информации по теме исследования; навыками выбора методов и средств решения задач исследования

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (УК-1) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций)	1	2	3	4	5
ЗНАТЬ: методы критического анализа и оценки современных научных достижений, а также методы генерирования новых идей при решении исследовательских и практических задач, в том числе в	Отсутствие знаний	Фрагментарные знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач	Общие, но не структурированные знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач	Сформированные, но содержащие отдельные пробелы знания основных методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских и практических задач, в том числе междисциплинарных	Сформированные систематические знания методов критического анализа и оценки современных научных достижений, а также методов генерирования новых идей при решении исследовательских

междисциплинарных областях Шифр: З 1.УК-1					и практических задач, в том числе междисциплинарных
УМЕТЬ: анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов Шифр: У 1. УК-1	Отсутствие умений	Частично освоенное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов	В целом успешно, но не систематически осуществляемые анализ альтернативных вариантов решения исследовательских и практических задач и оценка потенциальных выигрышей/проигрышей реализации этих вариантов	В целом успешные, но содержащие отдельные пробелы анализ альтернативных вариантов решения исследовательских задач и оценка потенциальных выигрышей/проигрышей реализации этих вариантов	Сформированное умение анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов
УМЕТЬ: при решении исследовательских и практических задач генерировать новые идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений Шифр: У 2. УК-1	Отсутствие умений	Частично освоенное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	В целом успешное, но не систематически осуществляемое умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	В целом успешное, но содержащее отдельные пробелы умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений	Сформированное умение при решении исследовательских и практических задач генерировать идеи, поддающиеся операционализации исходя из наличных ресурсов и ограничений
ВЛАДЕТЬ: навыками анализа методологических проблем, возникающих при решении исследовательских и практических задач, в том числе в междисциплинарных областях Шифр: В 1. УК-1	Отсутствие навыков	Фрагментарное применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач	В целом успешное, но не систематическое применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач	В целом успешное, но содержащее отдельные пробелы применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач	Успешное и систематическое применение навыков анализа методологических проблем, возникающих при решении исследовательских и практических задач, в том числе в

					междисциплинарных областях
ВЛАДЕТЬ: навыками критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач, в том числе в междисциплинарных областях Шифр: В 2. УК-1	Отсутствие навыков	Фрагментарное применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	В целом успешное, но не систематическое применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	В целом успешное, но содержащее отдельные пробелы применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.	Успешное и систематическое применение технологий критического анализа и оценки современных научных достижений и результатов деятельности по решению исследовательских и практических задач.

Шифр и название КОМПЕТЕНЦИИ:

УК-2: Способность проектировать и осуществлять комплексные исследования, в том числе междисциплинарные, на основе целостного системного научного мировоззрения с использованием знаний в области истории и философии науки.

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Универсальная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры должен:

• ЗНАТЬ: основные направления, проблемы, теории и методы философии, содержание современных философских дискуссий по проблемам общественного развития.

• УМЕТЬ: формировать и аргументированно отстаивать собственную позицию по различным проблемам философии; использовать положения и категории философии для оценивания и анализа различных социальных тенденций, фактов и явлений.

• ВЛАДЕТЬ: навыками восприятия и анализа текстов, имеющих философское содержание, приемами ведения дискуссии и полемики, навыками публичной речи и письменного аргументированного изложения собственной точки зрения.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
	1	2	3	4	5

(показатели достижения заданного уровня освоения компетенций), шифр					
ЗНАТЬ: методы научно- исследовательской деятельности Шифр З 1. УК-2	Отсутствие знаний	Фрагментарные представления о методах научно- исследовательской деятельности	Неполные представления о методах научно- исследовательской деятельности	Сформированные, но содержащие отдельные пробелы представления о методах научно- исследовательской деятельности	Сформированные систематические представления о методах научноисследовательской деятельности
ЗНАТЬ: Основные концепции современной философии науки, основные стадии эволюции науки, функции и основания научной картины мира Шифр З 2.УК-2	Отсутствие знаний	Фрагментарные представления об основных концепциях современной философии науки, основных стадиях эволюции науки, функциях и основаниях научной картины мира	Неполные представления об основных концепциях современной философии науки, основных стадиях эволюции науки, функциях и основаниях научной картины мира	Сформированные, но содержащие отдельные пробелы представления об основных концепциях современной философии науки, основных стадиях эволюции науки, функциях и основаниях научной картины мира	Сформированные систематические представления об основных концепциях современной философии науки, основных стадиях эволюции науки, функциях и основаниях научной картины мира
УМЕТЬ: использовать положения и категории философии науки для анализа и оценивания различных фактов и явлений Шифр: У 1. УК-2	Отсутствие умений	Фрагментарное использование положений и категорий философии науки для оценивания и анализа различных фактов и явлений	В целом успешное, но не систематическое использование положений и категорий философии науки для оценивания и анализа различных фактов и явлений	В целом успешное, но содержащее отдельные пробелы использование положений и категорий философии науки для оценивания и анализа различных фактов и явлений	Сформированное умение использовать положения и категории философии науки для оценивания и анализа различных фактов и явлений
ВЛАДЕТЬ: навыками анализа основных	Отсутствие навыков	Фрагментарное применение навыков анализа основных мировоззренческих и	В целом успешное, но не систематическое применение навыков анализа основных	В целом успешное, но содержащее отдельные пробелы	Успешное и систематическое применение навыков анализа основных мировоззренческих и

мировоззренческих и методологических проблем, в.т.ч. междисциплинарного характера, возникающих в науке на современном этапе ее развития Шифр: В 1. УК-2		методологических проблем, возникающих в науке на современном этапе ее развития	мировоззренческих и методологических проблем, возникающих в науке на современном этапе ее развития	применение навыков анализа основных мировоззренческих и методологических проблем, возникающих в науке на современном этапе ее развития	методологических проблем, возникающих в науке на современном этапе ее развития
ВЛАДЕТЬ: технологиями планирования в профессиональной деятельности в сфере научных исследований Шифр: В 2. УК-2	Отсутствие навыков	Фрагментарное применение технологий планирования в профессиональной деятельности	В целом успешное, но не систематическое применение технологий планирования в профессиональной деятельности	В целом успешное, но содержащее отдельные пробелы применение технологий планирования в профессиональной деятельности	Успешное и систематическое применение технологий планирования в профессиональной деятельности

Шифр и название КОМПЕТЕНЦИИ:

УК-3: готовность участвовать в работе российских и международных исследовательских коллективов по решению научных и научно-образовательных задач.

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Универсальная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: методы критического анализа и оценки современных научных достижений, методы генерирования новых идей при решении исследовательских и практических задач, в том числе в междисциплинарных областях, методы научно-исследовательской деятельности.

• УМЕТЬ: анализировать альтернативные варианты решения исследовательских и практических задач и оценивать потенциальные выигрыши/проигрыши реализации этих вариантов

• ВЛАДЕТЬ: навыками анализа основных мировоззренческих и методологических проблем, в т.ч. междисциплинарного характера возникающих в науке на современном этапе ее развития, владеть технологиями планирования профессиональной деятельности в сфере научных исследований

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (УК-3) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
ЗНАТЬ: особенности представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах Шифр: З 1. УК-3	Отсутствие знаний	Фрагментарные знания особенностей предоставления результатов научной деятельности в устной и письменной форме	Неполные знания особенностей представления результатов научной деятельности в устной и письменной форме, при работе в российских и международных коллективах	Сформированные, но содержащие отдельные пробелы знания основных особенностей представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах	Сформированные и систематические знания особенностей представления результатов научной деятельности в устной и письменной форме при работе в российских и международных исследовательских коллективах
УМЕТЬ: следовать нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач Шифр: У 1. УК-3	Отсутствие умений	Фрагментарное следование нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач	В целом успешное, но не систематическое следование нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научнообразовательных задач	В целом успешное, но содержащее отдельные пробелы умение следовать основным нормам, принятым в научном общении при работе в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач	Успешное и систематическое следование нормам, принятым в научном общении, для успешной работы в российских и международных исследовательских коллективах с целью решения научных и научно-образовательных задач
УМЕТЬ: осуществлять личностный выбор в процессе работы в российских и	Отсутствие умений	Частично освоенное умение осуществлять личностный выбор в процессе работы в российских и	В целом успешное, но не систематическое умение осуществлять личностный выбор в	В целом успешное, но содержащее отдельные пробелы умение осуществлять личностный выбор в	Успешное и систематическое умение осуществлять личностный выбор в процессе работы в российских и

международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом Шифр: У 2. УК-3		международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	процессе работы в российских и международных исследовательских коллективах, оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом	международных исследовательских коллективах,оценивать последствия принятого решения и нести за него ответственность перед собой, коллегами и обществом
ВЛАДЕТЬ: навыками анализа основных мировоззренческих и методологических проблем, в.т.ч. междисциплинарного характера, возникающих при работе по решению научных и научно- образовательных задач в российских или международных исследовательских коллективах Шифр: В 1. УК-3	Отсутствие навыков	Фрагментарное применение навыков анализа основных мировоззренческих и методологических проблем, в т.ч. междисциплинарно го характера, возникающих при работе по решению научных и научнообразовательных задач в российских или международных исследовательских коллективах	В целом успешное, но не систематическое применение навыков анализа основных мировоззренческих и методологических проблем, в т.ч. междисциплинарного характера, возникающих при работе по решению научных и научнообразовательных задач в российских или международных исследовательских коллективах	В целом успешное, но сопровождающееся отдельными ошибками применение навыков анализа основных мировоззренческих и методологических проблем, в т.ч. междисциплинарного характера, возникающих при работе по решению научных и научно- образовательных задач в российских или международных исследовательских коллективах	Успешное и систематическое применение навыков анализа основных мировоззренческих и методологических проблем, в т.ч. междисциплинарного характера, возникающих при работе по решению научных и научно- образовательных задач в российских или международных исследовательских коллективах
ВЛАДЕТЬ: технологиями оценки результатов коллективной деятельности по решению научных и	Отсутствие навыков	Фрагментарное применение технологий оценки результатов коллективной деятельности по решению научных	В целом успешное, но не систематическое применение технологий оценки результатов коллективной	В целом успешное, но сопровождающееся отдельными ошибками применение технологий оценки результатов коллективной	Успешное и систематическое применение технологий оценки результатов

научно-образовательных задач, в том числе ведущейся на иностранном языке Шифр: В 2. УК-3		и научно-образовательных задач, в том числе ведущейся на иностранном языке	деятельности по решению научных и научнообразовательных задач, в том числе ведущейся на иностранном языке	деятельности по решению научных и научнообразовательных задач, в том числе ведущейся на иностранном языке	коллективной деятельности по решению научных и научно-образовательных задач, в том числе ведущейся на иностранном языке
ВЛАДЕТЬ: технологиями планирования деятельности в рамках работы в российских и международных коллективах по решению научных и научнообразовательных задач Шифр: В 3. УК-3	Отсутствие навыков	Фрагментарное применение технологий планирования деятельности в рамках работы в российских и международных коллективах по решению научных и научно-образовательных задач	В целом успешное, но не систематическое применение технологий планирования деятельности в рамках работы в российских и международных коллективах по решению научных и научнообразовательных задач	В целом успешное, но сопровождающееся отдельными ошибками применение технологий планирования деятельности в рамках работы в российских и международных коллективах по решению научных и научно-образовательных задач	Успешное и систематическое применение технологий планирования деятельности в рамках работы в российских и международных коллективах по решению научных и научно-образовательных задач
ВЛАДЕТЬ: различными типами коммуникаций при осуществлении работы в российских и международных коллективах по решению научных и научнообразовательных задач Шифр: В 4. УК-3	Отсутствие навыков	Фрагментарное применение навыков использования различных типов коммуникаций при осуществлении работы в российских и международных коллективах по решению научных и научно-образовательных задач	В целом успешное, но не систематическое применение навыков использования различных типов коммуникаций при осуществлении работы в российских и международных коллективах по решению научных и научнообразовательных задач	В целом успешное, но содержащее отдельные пробелы применение навыков использования различных типов коммуникаций при осуществлении работы в российских и международных коллективах по решению научных и научно-образовательных задач	Успешное и систематическое владение различными типами коммуникаций при осуществлении работы в российских и международных коллективах по решению научных и научно-образовательных задач

образовательных задач

Шифр и название КОМПЕТЕНЦИИ:

УК-4: готовность использовать современные методы и технологии научной коммуникации на государственном и иностранном языках.

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Универсальная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: виды и особенности письменных текстов и устных выступлений; понимать общее содержание сложных текстов на абстрактные и конкретные темы, в том числе узкоспециальные тексты.

• УМЕТЬ: подбирать литературу по теме, составлять двуязычный словник, переводить и реферировать специальную литературу, подготавливать научные доклады и презентации на базе прочитанной специальной литературы, объяснить свою точку зрения и рассказать о своих планах

• ВЛАДЕТЬ: навыками обсуждения знакомой темы, делая важные замечания и отвечая на вопросы; создания простого связного текста по знакомым или интересующим его темам, адаптируя его для целевой аудитории

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (УК-4) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций)	1	2	3	4	5
ЗНАТЬ:					
методы и технологии научной коммуникации на государственном и иностранном языках	Отсутствие знаний	Фрагментарные знания методов и технологий научной коммуникации на государственном и иностранном языках	Неполные знания методов и технологий научной коммуникации на государственном и иностранном языках	Сформированные, но содержащие отдельные пробелы знания методов и технологий научной коммуникации на государственном и иностранном языках	Сформированные и систематические знания методов и технологий научной коммуникации на государственном и иностранном языках

Шифр: З 1. УК-4

ЗНАТЬ: стилистические особенности представления результатов научной деятельности в устной и письменной форме на государственном и иностранном языках Шифр: З 2. УК-4	Отсутствие знаний	Фрагментарные знания стилистических особенностей представления результатов научной деятельности в устной и письменной форме на государственном и иностранном языках	Неполные знания стилистических особенностей представления результатов научной деятельности в устной и письменной форме на государственном и иностранном языках	Сформированные, но содержащие отдельные пробелы знания основных стилистических особенностей представления результатов научной деятельности в устной и письменной форме на государственном и иностранном языках	Сформированные систематические знания стилистических особенностей представления результатов научной деятельности в устной и письменной форме на государственном и иностранном языках
УМЕТЬ: следовать основным нормам, принятым в научном общении на государственном и иностранном языках Шифр: У 1. УК-4	Отсутствие умений	Частично освоенное умение следовать основным нормам, принятым в научном общении на государственном и иностранном языках	В целом успешное, но не систематическое умение следовать основным нормам, принятым в научном общении на государственном и иностранном языках	В целом успешное, но содержащее отдельные пробелы умение следовать основным нормам, принятым в научном общении на государственном и иностранном языках	Успешное и систематическое умение следовать основным нормам, принятым в научном общении на государственном и иностранном языках
ВЛАДЕТЬ: навыками анализа научных текстов на государственном и иностранном языках Шифр: В 1. УК-4	Отсутствие навыков	Фрагментарное применение навыков анализа научных текстов на государственном и иностранном языках	В целом успешное, но не систематическое применение навыков анализа научных текстов на государственном и иностранном языках	В целом успешное, но сопровождающееся отдельными ошибками применение навыков анализа научных текстов на государственном и иностранном языках	Успешное и систематическое применение навыков анализа научных текстов на государственном и иностранном языках
ВЛАДЕТЬ: навыками критической оценки эффективности различных методов и технологий научной коммуникации на государственном и иностранном языках Шифр: В 2. УК-4	Отсутствие навыков	Фрагментарное применение навыков критической оценки эффективности различных методов и технологий научной коммуникации на государственном и иностранном языках	В целом успешное, но не систематическое применение навыков критической оценки эффективности различных методов и технологий научной коммуникации на государственном и иностранном языках	В целом успешное, но сопровождающееся отдельными ошибками применение навыков критической оценки эффективности различных методов и технологий научной коммуникации на государственном и иностранном языках	Успешное и систематическое применение навыков критической оценки эффективности различных методов и технологий научной коммуникации на государственном и иностранном языках

ВЛАДЕТЬ: различными методами, технологиями и типами коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках	Отсутствие навыков	Фрагментарное применение различных методов, технологий и типов коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках	В целом успешное, но не систематическое применение различных методов, технологий и типов коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках	В целом успешное, но сопровождающееся отдельными ошибками применение различных методов, технологий и типов коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках	Успешное и систематическое применение различных методов, технологий и типов коммуникаций при осуществлении профессиональной деятельности на государственном и иностранном языках

Шифр: В 3. УК-4

Шифр и название КОМПЕТЕНЦИИ:

УК-5: способностью следовать этическим нормам в профессиональной деятельности.

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Универсальная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры должен:

• ЗНАТЬ: основы интеллектуальной собственности; права собственности, патенты, коммерческая тайна; интеллектуальная собственность и международное право, правовые основы работы с информацией и программным обеспечением, этические нормы и стандарты; этические кодексы и их осуществление на практике (IEEE, ACM, SE, AITP и пр.), этические и законодательные основы личной безопасности.

• УМЕТЬ: оценивать аспекты профессиональной деятельности с позиций этики; понимать социальные аспекты разработки программного обеспечения; учитывать возможные последствия, выявлять риски, связанные с применением компьютерных систем; обеспечивать конфиденциальность персональной информации в базах данных; принимать технологические решения для обеспечения конфиденциальности.

• ВЛАДЕТЬ: культурой речи, проявляющейся в умении грамотно, доходчиво и точно передавать мысли, придерживаясь речевых норм: ясности, обеспечивающей доступность и простоту в общении; грамотности, основанной на использовании общепринятых правил русского литературного языка; содержательности, выражающейся в продуманности, осмысленности и информативности обращения; логичности, предполагающей последовательность, непротиворечивость и обоснованность изложения мыслей; доказательности, включающей в себя достоверность и объективность информации; лаконичности, отражающей краткость и понятность речи.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (УК-5) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Критерии оценивания результатов обучения

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	1	2	3	4	5
ЗНАТЬ: основы интеллектуальной собственности; права собственности, патенты, коммерческая тайна; интеллектуальная собственность и международное право, правовые основы работы с информацией и программным Шифр: З 1. УК-5	Не имеет базовых знаний об основах интеллектуальной собственности; права собственности, патенты, коммерческая тайна; интеллектуальная собственность и международное право, правовые основы работы с информацией и программным обеспечением, этические нормы и стандарты.	Допускает существенные ошибки при раскрытии содержания основ интеллектуальной собственности; права собственности, правовых основхы работы с информацией и программным обеспечением, этические нормы и стандарты процесса целеполагания, его особенностей и способов реализации.	Демонстрирует частичные знания основы интеллектуальной собственности; права собственности, патенты, коммерческая тайна; интеллектуальная собственность и международное право, правовые основы работы с информацией и программным обеспечением, этические нормы и возможность их использования в конкретных ситуациях.	Демонстрирует знания основы интеллектуальной собственности; права собственности, патенты, коммерческая тайна; интеллектуальная собственность и международное право, при решении профессиональных задач.	Раскрывает полное содержание основ интеллектуальной собственности; права собственности, патенты, коммерческая тайна; интеллектуальная собственность и международное право, правовые основы работы с информацией и программным обеспечением, этические нормы и стандарты; этические кодексы и их осуществление на практике (IEEE, ACM, SE, AITP и пр.), этические и законодательные основы личной безопасностипри решении профессиональных задач.
УМЕТЬ: оценивать аспекты профессиональной деятельности с позиций этики;	Не умеет и не готов оценивать аспекты профессиональной деятельности с позиций этики;	Имеет базовые представления об аспектах профессиональной деятельности с позиций этики;	При формулировке целей профессионального и личностного развития не учитывает возможные последствия, не	Формулирует социальные аспекты разработки программного обеспечения; учитывает возможные риски обеспечения конфиденциальност	Готов и умеет оценивать аспекты профессиональной деятельности с позиций этики; понимать социальные аспекты разработки программного обеспечения; учитывать

понимать социальные аспекты разработки программного обеспечения; учитывать возможные последствия, выявлять риски, связанные с применением компьютерных систем; обеспечивать конфиденциальность персональной информации в базах данных; принимать технологические решения для обеспечения конфиденциальности	понимать социальные аспекты разработки программного обеспечения	понимать социальные аспекты разработки программного обеспечения; учитывать возможные последствия, выявлять риски, связанные с применением компьютерных систем	умеет выявлять риски, связанные с применением компьютерных систем; обеспечивать конфиденциальность персональной информации в базах данных.	ь персональной информации в базах данных; но не полностью учитывает возможные этапы технологических решениий для обеспечения конфиденциальности и цели личностного и профессионального развития.	возможные последствия, выявлять риски, связанные с применением компьютерных систем; обеспечивать конфиденциальность персональной информации в базах данных; принимать технологические решения для обеспечения конфиденциальности
Шифр: У 1. УК-5					
ВЛАДЕТЬ: культурой речи, проявляющейся в умении грамотно, доходчиво и точно передавать мысли. Шифр: В 1. УК-5	Не владеет приемами доходчиво и точно передавать мысли, придерживаясь речевых норм и оценивать результаты деятельности по решению профессиональных задач.	Владеет отдельными приемами и технологиями целеполагания, и целереализации и оценки результатов деятельности по решению стандартных профессиональных задач, допуская ошибки при выборе приемов и	Владеет отдельными и приемами и технологиями целеполагания, и целереализации оценки результатов деятельности по решению стандартных профессиональных задач, давая не полностью аргументированное обоснование	Владеет приемами и технологиями целеполагания, целереализации и оценки результатов деятельности по решению стандартных профессиональных задач, полностью аргументируя предлагаемые варианты решения.	Демонстрирует владение системой приемов и технологий целеполагания, целереализации и оценки результатов деятельности по решению нестандартных профессиональных задач, полностью аргументируя выбор предлагаемого варианта решения.

		технологий и их реализации.	предлагаемого варианта решения.		

Шифр и название КОМПЕТЕНЦИИ:

УК-6: способность планировать и решать задачи собственного профессионального и личностного развития.

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Универсальная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры должен:

• ЗНАТЬ: возможные сферы и направления профессиональной самореализации; приемы и технологии целеполагания и целереализации; пути достижения более высоких уровней профессионального и личного развития.

• УМЕТЬ: выявлять и формулировать проблемы собственного развития, исходя из этапов профессионального роста и требований рынка труда к специалисту; формулировать цели профессионального и личностного развития, оценивать свои возможности, реалистичность и адекватность намеченных способов и путей достижения планируемых целей

• ВЛАДЕТЬ: приемами целеполагания, планирования, реализации необходимых видов деятельности, оценки и самооценки результатов деятельности по решению профессиональных задач; приемами выявления и осознания своих возможностей, личностных и профессионально-значимых качеств с целью их совершенствования.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (УК-5) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
ЗНАТЬ: содержание процесса целеполагания профессионального и личностного развития, его особенности и способы реализации при решении профессиональных	Не имеет базовых знаний о сущности процесса целеполагания, его особенностях и способах реализации.	Допускает существенные ошибки при раскрытии содержания процесса целеполагания, его особенностей и способов реализации.	Демонстрирует частичные знания содержания процесса целеполагания, некоторых особенностей профессионального развития и	Демонстрирует знания сущности процесса целеполагания, отдельных особенностей процесса и способов его реализации,	Раскрывает полное содержание процесса целеполагания, всех его особенностей, аргументированно обосновывает критерии выбора способов профессиональной и личностной

задач, исходя из этапов карьерного роста и требований рынка труда. Шифр: З 1. УК-5			самореализации личности, указывает способы реализации, но не может обосновать возможность их использования в конкретных ситуациях.	характеристик профессионального развития личности, но не выделяет критерии выбора способов целереализации при решении профессиональных задач.	целереализации при решении профессиональных задач.
УМЕТЬ: формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуальнолич ностных особенностей. Шифр: У 1. УК-5	Не умеет и не готов формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуальнолич ностных особенностей.	Имея базовые представления о тенденциях развития профессиональной деятельности и этапах профессионального роста, не способен сформулировать цели профессионального и личностного развития.	При формулировке целей профессионального и личностного развития не учитывает тенденции развития сферы профессиональной деятельности и индивидуальнолич ностные особенности.	Формулирует цели личностного и профессионального развития, исходя из тенденций развития сферы профессиональной деятельности и индивидуальнолич ностных особенностей, но не полностью учитывает возможные этапы профессиональной социализации.	Готов и умеет формулировать цели личностного и профессионального развития и условия их достижения, исходя из тенденций развития области профессиональной деятельности, этапов профессионального роста, индивидуально-личностных особенностей.
УМЕТЬ: осуществлять личностный выбор в различных профессиональных и моральноценностн ых ситуациях, оценивать последствия принятого решения и нести за него ответственность	Не готов и не умеет осуществлять личностный выбор в различных профессиональных и моральноценностн ых ситуациях, оценивать последствия принятого решения и нести за него ответственность перед собой и обществом.	Готов осуществлять личностный выбор в конкретных профессиональных и моральноценностн ых ситуациях, но не умеет оценивать последствия принятого решения и нести за него ответственность перед собой и обществом.	Осуществляет личностный выбор в конкретных профессиональных и моральноценностн ых ситуациях, оценивает некоторые последствия принятого решения, но не готов нести за него ответственность перед собой и обществом.	Осуществляет личностный выбор в стандартных профессиональных и моральноценностн ых ситуациях, оценивает некоторые последствия принятого решения и готов нести за него ответственность	Умеет осуществлять личностный выбор в различных нестандартных профессиональных и морально-ценностных ситуациях, оценивать последствия принятого решения и нести за

перед собой и обществом. Шифр: У 2. УК-5				перед собой и обществом.	него ответственность перед собой и обществом.
ВЛАДЕТЬ: приемами и технологиями целеполагания, целереализации и оценки результатов деятельности по решению профессиональных задач. Шифр: В 1. УК-5	Не владеет приемами и технологиями целеполагания, целереализации и оценки результатов деятельности по решению профессиональных задач.	Владеет отдельными приемами и технологиями целеполагания, целереализации и оценки результатов деятельности по решению стандартных профессиональных задач, допуская ошибки при выборе приемов и технологий и их реализации.	Владеет отдельными приемами и технологиями целеполагания, целереализации и оценки результатов деятельности по решению стандартных профессиональных задач, давая не полностью аргументированное обоснование предлагаемого варианта решения.	Владеет приемами и технологиями целеполагания, целереализации и оценки результатов деятельности по решению стандартных профессиональных задач, полностью аргументируя предлагаемые варианты решения.	Демонстрирует владение системой приемов и технологий целеполагания, целереализации и оценки результатов деятельности по решению нестандартных профессиональных задач, полностью аргументируя выбор предлагаемого варианта решения.
ВЛАДЕТЬ: способами выявления и оценки индивидуальноличностных, профессиональнозначимых качеств и путями достижения более высокого уровня их развития. Шифр: В 2. УК-5	Не владеет способами выявления и оценки индивидуальноличностных, профессиональнозначимых качеств и путями достижения более высокого уровня их развития.	Владеет информацией о способах выявления и оценки индивидуальноличностных, профессиональнозначимых качеств и путях достижения более высокого уровня их развития, допуская существенные ошибки при применении данных знаний.	Владеет некоторыми способами выявления и оценки индивидуально- личностных и профессиональнозначимых качеств, необходимых для выполнения профессиональной деятельности, при этом не демонстрирует способность оценки этих качеств и выделения конкретных путей их совершенствования.	Владеет отдельными способами выявления и оценки индивидуально- личностных и профессиональнозначимых качеств, необходимых для выполнения профессиональной деятельности, и выделяет конкретные пути самосовершенствования.	Владеет системой способов выявления и оценки индивидуально-личностных и профессиональнозначимых качеств, необходимых для профессиональной самореализации, и определяет адекватные пути самосовершенствования.

Шифр и название КОМПЕТЕНЦИИ:

ОПК-1: способность самостоятельно осуществлять научно-исследовательскую деятельность в соответствующей профессиональной области с использованием современных методов исследования и информационно-коммуникационных технологий

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Общепрофессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры должен:

• ЗНАТЬ: цели и задачи научных исследований по направлению деятельности, базовые принципы и методы их организации; основные источники научной информации и требования к представлению информационных материалов

• УМЕТЬ: составлять общий план работы по заданной теме, предлагать методы исследования и способы обработки результатов, проводить исследования по согласованному с руководителем плану, представлять полученные результаты

• ВЛАДЕТЬ: систематическими знаниями по направлению деятельности; углубленными знаниями по выбранной направленности подготовки, базовыми навыками проведения научно-исследовательских работ по предложенной теме.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ОПК-1) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр	1	2	3	4	5
ЗНАТЬ: современные способы использования информационнокоммуникационных технологий в выбранной сфере деятельности Шифр З 1. ОПК-1	Отсутствие знаний	Фрагментарные представления о базовых принципах и методах их организации; основных источниках научной информации и требованиях к представлению информационных материалов	В целом успешные, но не систематические представления о о базовых принципах и методах их организации; основных источниках научной информации и требованиях к представлению информационных материалов	В целом успешные, но содержащие отдельные пробелы, представления о о базовых принципах и методах их организации; основных источниках научной информации и требованиях к представлению информационных материалов	Сформированные представления о о базовых принципах и методах их организации; основных источниках научной информации и требованиях к представлению информационных материалов
УМЕТЬ: выбирать и применять в профессиональной	Отсутствие умений	Фрагментарное использование умения составлять	В целом успешное, но не систематическое использование	В целом успешное, но содержащее отдельные	Сформированное умение использование умения

деятельности экспериментальные и расчетно-теоретические методы исследования Шифр: У 1. ОПК-1			общий план работы по заданной теме, предлагать методы исследования и способы обработки результатов, проводить исследования по согласованному с руководителем плану, представлять	умения составлять общий план работы по заданной теме, предлагать методы исследования и способы обработки результатов, проводить исследования по	пробелы использование умения составлять общий план работы по заданной теме, предлагать методы исследования и способы обработки результатов, проводить исследования по согласованному с руководителем плану,	составлять общий план работы по заданной теме, предлагать методы исследования и способы обработки результатов, проводить исследования по
		полученные результаты	согласованному с руководителем плану, представлять полученные результаты		представлять полученные результаты	согласованному с руководителем плану, представлять полученные результаты
ВЛАДЕТЬ: навыками поиска (в том числе с использованием информационных систем и баз банных) и критического анализа информации по тематике проводимых исследований Шифр: В 1. ОПК-1	Отсутствие навыков	Фрагментарное применение навыков поиска и критического анализа научной и технической информации	В целом успешное, но не систематическое применение навыков поиска и критического анализа научной и технической информации	В целом успешное, но содержащее отдельные пробелы применение навыков поиска и критического анализа научной и технической информации	Успешное и систематическое применение навыков поиска и критического анализа научной и технической информации
ВЛАДЕТЬ: навыками планирования научного исследования, анализа получаемых результатов и формулировки выводов Шифр: В 2. ОПК-1	Отсутствие навыков	Фрагментарное применение навыков планирования научного исследования, анализа получаемых результатов и формулировки выводов	В целом успешное, но не систематическое применение навыков планирования научного исследования, анализа получаемых результатов и формулировки выводов	В целом успешное, но содержащее отдельные пробелы применение навыков планирования научного исследования, анализа получаемых результатов и формулировки выводов	Успешное и систематическое применение навыков планирования научного исследования, анализа получаемых результатов и формулировки выводов
ВЛАДЕТЬ:	Отсутствие навыков	Фрагментарное	В целом успешное, но не систематическое	В целом успешное, но содержащее отдельные пробелы	Успешное и

навыками представления и продвижения результатов интеллектуальной деятельности	применение навыков представления и продвижения результатов интеллектуальной деятельности	применение навыков представления и продвижения результатов интеллектуальной деятельности	применение навыков представления и продвижения результатов интеллектуальной деятельности	систематическое применение навыков представления и продвижения результатов интеллектуальной деятельности

Шифр: В 3. ОПК-1

Шифр и название КОМПЕТЕНЦИИ:

ОПК-2: владением культурой научного исследования, в том числе с использованием современных ИКТ

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Общепрофессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность; осваивается в течение всего периода обучения в рамках дисциплин (модулей) базовой и вариативной части.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

• ЗНАТЬ: основные тенденции развития в соответствующей области науки.

• УМЕТЬ: использовать современную вычислительную технику и специализированное программное обеспечение в научноисследовательской работе.

• ВЛАДЕТЬ: навыками использования программных средств и работы в компьютерных сетях, использования ресурсов Интернет; владение основными методами, способами и средствами получения, хранения, переработки информации, навыками синхронного восприятия и документирования мультимедийной информации на иностранных языках

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ОПК-3) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций)	1	2	3	4	5
ЗНАТЬ: нормативноправовые основы преподавательской деятельности в системе высшего образования	отсутствие знаний	фрагментарные представления об основных тенденциях развития в соответствующей области науки я	сформированные знания об основных тенденциях развития в соответствующей области науки я	сформированные знания представления об основных тенденциях развития в соответствующей области науки я	сформированные знания представления об основных тенденциях развития в соответствующей области науки я

Шифр: З 1. ОПК-2

УМЕТЬ: использовать современную вычислительную технику и специализированное программное обеспечение в научноисследовательской работе. Шифр: У 1. ОПК-2	отсутствие умений	затруднения с выбором специализированного программное обеспечение в научноисследовательской работе.	сформированные умения выбора специализированного программное обеспечение в научноисследовательской работе	отбор и использование методов с учетом специфики направленности (профиля) подготовки	отбор и использование методов преподавания с учетом специфики направления подготовки
ВЛАДЕТЬ: навыками использования программных средств и работы в компьютерных сетях, использования ресурсов Интернет; Шифр: В 1. ОПК-2	не владеет	Фрагментарное применение навыков использования программных средств и работы в компьютерных сетях, использования ресурсов	В целом успешное, но не систематическое применение навыков использования программных средств и работы в компьютерных сетях, использования ресурсов	В целом успешное, но содержащее отдельные пробелы применение навыков использования программных средств и работы в компьютерных сетях, использования ресурсов	Успешное и систематическое применение навыков использования программных средств и работы в компьютерных сетях, использования ресурсов
ВЛАДЕТЬ: владение основными методами, способами и средствами получения, хранения, переработки информации, навыками синхронного восприятия и документирования мультимедийной информации на иностранных языках Шифр: В 2. ОПК-2	не владеет	Фрагментарное применение навыков владения основными методами, способами и средствами получения, хранения, переработки информации, навыками синхронного восприятия и документирования мультимедийной информации на иностранных языках	В целом успешное, но не систематическое применение навыков владения основными методами, способами и средствами получения, хранения, переработки информации,	В целом успешное, но содержащее отдельные пробелы применение методов, способов и средств получения, хранения, переработки информации, навыками синхронного восприятия и документирования	Успешное и систематическое применение навыков методов, способов и средств получения, хранения, переработки информации, навыками синхронного восприятия и документирования

Шифр и название КОМПЕТЕНЦИИ:

ОПК-3: способностью к разработке новых методов исследования и их применению в самостоятельной научно-исследовательской деятельности в области профессиональной деятельности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Общепрофессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность;

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

• ЗНАТЬ: знания основные тенденции развития информатики и естественнонаучного и математического знания в соответствующей области науки.

• УМЕТЬ: самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности.

• ВЛАДЕТЬ: способностью к самостоятельному обучению и разработке новых методов исследования, к изменению научного и научно-производственного профиля деятельности;

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ОПК-3) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
ЗНАТЬ: знания основные тенденции развития информатики и естественнонаучного и математического знания в соответствующей области науки Шифр: З 1. ОПК-3	отсутствие знаний	фрагментарные представления об основных тенденциях развития информатики и естественнонаучного и математического знания в соответствующей области науки	сформированные знания об основных тенденциях развития информатики и естественнонаучного и математического знания в соответствующей области науки	сформированные знания представления об основных тенденциях развития информатики и естественнонаучного и математического знания в соответствующей области науки	сформированные знания представления об основных тенденциях развития информатики и естественнонаучного и математического знания в соответствующей области науки
УМЕТЬ: самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой	отсутствие умений	затруднения с самостоятельным получением новых знаний ром	сформированные умения самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения	сформированные умения самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения в том числе в новых областях знаний, непосредственно не	сформированные умения самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения в том числе в новых областях знаний, непосредственно не

деятельности работе. Шифр: У 1. ОПК-3				связанных со сферой деятельности.	связанных со сферой деятельности
ВЛАДЕТЬ: способностью к самостоятельному обучению и разработке новых методов исследования, к изменению научного и научнопроизводственного профиля деятельности Шифр: В 1. ОПК-3	не владеет	Фрагментарное применение навыков самостоятельного обучения и разработке новых методов исследования, к изменению научного и научнопроизводственного профиля деятельности	В целом успешное, но не систематическое применение навыков самостоятельногообучения и разработке новых методов исследования, к изменению научного и научно-производственного профиля деятельности	В целом успешное, но содержащее отдельные пробелы применение навыков самостоятельного обучения и разработке новых методов исследования, к изменению научного и научнопроизводственного профиля деятельности	Успешное и систематическое применение навыков обучения и разработке новых методов исследования, к изменению научного и научнопроизводственного профиля деятельности

Шифр и название КОМПЕТЕНЦИИ:

ОПК-4: готовностью организовать работу исследовательского коллектива в области профессиональной деятельности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Общепрофессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

• ЗНАТЬ: знания основные этапы организации работы коллектива в области профессиональной деятельности

• УМЕТЬ: самостоятельно определять порядок выполнения работ.

• ВЛАДЕТЬ: способностью самостоятельной организации работы коллектива исполнителей;

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ОПК-4) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения				
	1	2	3	4	5
ЗНАТЬ: основные этапы организации работы коллектива	отсутствие знаний	фрагментарные представления об основных основные этапы организации работы коллектива	сформированные знания об основных тенденциях развития	сформированные	сформированные знания представления об основных тенденциях

в области профессиональной деятельности Шифр: З 1. ОПК-4		в области профессиональной деятельности	информатики и естественнонаучного и математического знания в соответствующей области науки	знания представления об основных тенденциях развития информатики и естественнонаучного и математического знания в соответствующей области науки	развития информатики и естественнонаучного и математического знания в соответствующей области науки
УМЕТЬ: самостоятельно определять порядок выполнения работ Шифр: У 1. ОПК-4	отсутствие умений	затруднения с определением основных этапов и порядка работ	сформированные умения самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения	сформированные умения самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности.	сформированные умения самостоятельно приобретать с помощью ИКТ и использовать в практической деятельности новые знания и умения в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности
ВЛАДЕТЬ: способностью самостоятельной организации работы коллектива исполнителей Шифр: В 1. ОПК-4	не владеет	Фрагментарное применение навыков самостоятельной организации работы коллектива исполнителей	В целом успешное, но не систематическое применение навыков самостоятельной организации работы коллектива исполнителей	В целом успешное применение навыков самостоятельной организации работы коллектива исполнителей	Успешное и систематическое применение навыков самостоятельной организации работы коллектива исполнителей
ВЛАДЕТЬ: методами планирования, подготовки, проведения НИР, анализа полученных	Отсутствие навыков	Фрагментарное применение методов планирования, подготовки и проведения НИР, анализа и обсуждения полученных данных	В целом успешное, но не систематическое применение методов планирования, подготовки,	В целом успешное, но содержащее отдельные пробелы применение методов планирования,	Успешное и систематическое применение методов планирования, подготовки и проведения НИР и анализа и обсуждения

данных, формулировки выводов и рекомендаций Шифр В 2. ОПК-4			проведения НИР, анализа полученных данных	подготовки, проведения НИР, анализа полученных данных, формулировка выводов по результатам НИР	экспериментальных данных; формулировка выводов и рекомендаций по результатам НИР
ВЛАДЕТЬ: навыками составления и подачи конкурсных заявок на выполнение научно-исследовательских и проектных работ Шифр: В 3. ОПК-4	Отсутствие навыков	Фрагментарное применение навыков составления и подачи конкурсных заявок на выполнение научно-исследовательских и проектных работ по направленности подготовки	В целом успешное, но не систематическое применение навыков составления и подачи конкурсных заявок на выполнение научно-исследовательских и проектных работ по направленности подготовки	В целом успешное, но содержащее отдельные пробелы применение навыков составления и подачи конкурсных заявок на выполнение научно-исследовательских и проектных работ по направленности подготовки	Успешное и систематическое применение навыков составления и подачи конкурсных заявок на выполнение научноисследовательских и проектных работ по направленности подготовки

Шифр и название КОМПЕТЕНЦИИ:

ОПК-5: способностью объективно оценивать результаты исследований и разработок, выполненных другими специалистами и в других научных учреждениях

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Общепрофессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность;

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

• ЗНАТЬ: основные направления, проблемы и методы в области исследования

• УМЕТЬ: формировать и аргументировано отстаивать научную новизну собственных исследований

• ВЛАДЕТЬ: технологиями планирования в профессиональной деятельности в сфере научных исследований

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций), шифр	Критерии оценивания результатов обучения				
	1	2	3	4	5
ЗНАТЬ: основные направления, проблемы и методы в области исследования Шифр З 1. ОПК-5	Отсутствие знаний	Фрагментарные представления об основных направлениях, проблемах и методах в области исследования	Неполные представления основных направлениях, проблемах и методах в области исследования	Сформированные, но содержащие отдельные пробелы представления о направлениях, проблемах и методах в области исследования	Сформированные систематические представления о направлениях, проблемах и методах в области исследования
УМЕТЬ: формировать и аргументировано отстаивать научную новизну собственных исследований Шифр: У 1. ОПК-5	Отсутствие умений	Фрагментарное использование умений для оценивания и анализа различных фактов и явлений	В целом успешное, но не систематическое использование умений для оценивания и анализа различных фактов и явлений	В целом успешное, но содержащее отдельные пробелы умений для оценивания и анализа различных фактов и явлений	Сформированное умение использовать формировать и аргументировано отстаивать научную новизну собственных исследований
ВЛАДЕТЬ: технологиями планирования в профессиональной деятельности в сфере научных исследований Шифр: В 1. ОПК-5	Отсутствие навыков	Фрагментарное применение технологий планирования в профессиональной деятельности	В целом успешное, но не систематическое применение технологий планирования в профессиональной деятельности	В целом успешное, но содержащее отдельные пробелы применение технологий планирования в профессиональной деятельности	Успешное и систематическое применение технологий планирования в профессиональной деятельности

Шифр и название КОМПЕТЕНЦИИ:

ПК-1: способностью использовать основные естественнонаучные законы, применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры должен:

• ЗНАТЬ: основные естественнонаучные законы и математический аппарат, используемый в профессиональной деятельности

• УМЕТЬ: применять математический аппарат в профессиональной деятельности, выявлять сущность проблем, возникающих в ходе профессиональной деятельности

• ВЛАДЕТЬ способностью использовать основные естественнонаучные законы, умением применять математический аппарат в профессиональной деятельности.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-1) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр	1	2	3	4	5
ЗНАТЬ:					
Основные естетвеннонаучные законы, математический аппарат, применяемый в профессиональной деятельности	Отсутствие знаний	Фрагментарные представления о естественнонаучных законах и математическом аппарате	В целом успешные, но не систематические представления о естественнонаучных законах и математическом аппарате	В целом успешные, но содержащие отдельные пробелы, представления о естественнонаучных законах и математическом аппарате	Сформированные представления о естественнонаучных законах и математическом аппарате
Шифр. ПК-1					
УМЕТЬ: выбирать и применять в профессиональной деятельности естественнонаучные законы и математический аппарат Шифр: ПК-1	Отсутствие умений	Фрагментарное использование умения применять в профессиональной деятельности естественнонаучные законы и математический аппарат	В целом успешное, но не систематическое использование умения применять в профессиональной деятельности естественнонаучные законы и математический аппарат	В целом успешное, но содержащее отдельные пробелы использование умения применять в профессиональной деятельности естественнонаучные законы и математический аппарат	Сформированное умение применять в профессиональной деятельности естественнонаучные законы и математический аппарат

ВЛАДЕТЬ: навыками применения в профессиональной деятельности естественнонаучных законов и математического аппарата	Отсутствие навыков	Фрагментарное владение применением в профессиональной деятельности естественнонаучных законов и математического аппарата	В целом успешное но не систематическое владение применением в профессиональной деятельности естественнонаучных законов и математического аппарата	В целом успешное, но содержащее отдельные пробелы владение применением в профессиональной деятельности естественнонаучных законов и математического аппарата	Успешное и систематическое владение применением в профессиональной деятельности естественнонаучных законов и математического аппарата

Шифр и название КОМПЕТЕНЦИИ:

ПК-2: способностью понимать сущность и значение информации в развитии современного общества, применять достижения информатики и вычислительной техники, перерабатывать большие объемы информации проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры должен:

• ЗНАТЬ: основные достижения информатики и вычислительной техники

• УМЕТЬ: применять достижения информатики и вычислительной техники в профессиональной деятельности

• ВЛАДЕТЬ способностью перерабатывать большие объемы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-2) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр	1	2	3	4	5
ЗНАТЬ:	Отсутствие знаний	Фрагментарные представления о	В целом успешные, но не	В целом успешные, но содержащие	Сформированные представления о

Основные достижения информатики и вычислительной техники в профессиональной деятельности		достижениях информатики и вычислительной техники в профессиональной деятельности	систематические представления о достижениях информатики и вычислительной техники в профессиональной деятельности	отдельные пробелы, представления о достижениях информатики и вычислительной техники в профессиональной деятельности	достижениях информатики и вычислительной техники в профессиональной деятельности
Шифр. ПК-2					
УМЕТЬ: применять достижения информатики и вычислительной техники в профессиональной деятельности Шифр: ПК-2	Отсутствие умений	Фрагментарное использование умения применять в профессиональной деятельности достижения информатики и вычислительной техники	В целом успешное, но не систематическое использование умения применять в профессиональной деятельности достижения информатики и вычислительной техники	В целом успешное, но содержащее отдельные пробелы использование умения применять в профессиональной деятельности достижения информатики и вычислительной техники	Сформированное умение применять в профессиональной деятельности достижения информатики и вычислительной техники
ВЛАДЕТЬ: навыками перерабатывать большие объемы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах	Отсутствие навыков	Фрагментарное владение навыками перерабатывать большие объемы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах	В целом успешное но не систематическое владение навыкамиперерабатывать большие объемы информации, проводить целенаправленный поиск в различных источниках информации по профилю деятельности, в том числе в глобальных компьютерных системах	В целом усп но содержа отдельные владение перерабаты большие об информаци проводить целенаправ поиск в раз источниках информаци профилю деятельност числе в глоб компьютерн системах	

Шифр и название КОМПЕТЕНЦИИ:

ПК-3: способностью использовать нормативные правовые документы в своей профессиональной деятельности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: основные нормативные правовые документы в своей профессиональной деятельности

• УМЕТЬ: применять основные нормативные правовые документы в профессиональной деятельности

• ВЛАДЕТЬ способностью использовать основные нормативные правовые документы в профессиональной деятельности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-3) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-3	1	2	3	4	5
ЗНАТЬ: основные нормативные правовые документы в своей профессиональной деятельности Шифр. ПК-3	Отсутствие знаний	Фрагментарные представления об основных нормативных правовых документах в своей профессиональной деятельности	В целом успешные, но не систематические представления об основных нормативных правовых документах в своей профессиональной	В целом успешные, но содержащие отдельные пробелы, представления об основных нормативных правовых документах в своей профессиональной деятельности	Сформированные представления об основных нормативных правовых документах в своей профессиональной деятельности
УМЕТЬ: применять в профессиональной деятельности основные нормативные правовые документы Шифр: ПК-3	Отсутствие умений	Фрагментарное использование умения применять в профессиональной деятельности основные нормативные правовые документы	В целом успешное, но не систематическое использование умения применять в профессиональной деятельности основные нормативные правовые документы	В целом успешное, но содержащее отдельные пробелы использование умения применять в профессиональной деятельности основные нормативные правовые документы	Сформированное умение применять в профессиональной деятельности основные нормативные правовые документы
ВЛАДЕТЬ: навыками применения в профессиональной	Отсутствие навыков	Фрагментарное владение применением в профессиональной деятельности	В целом успешное но не систематическое владение применением в профессиональной	В целом успешное, но содержащее отдельные пробелы владение применением в	Успешное и систематическое владение применением в профессиональной

деятельности основные нормативные правовые документы		основных нормативных правовых документов	деятельности основных нормативных правовых документов а	профессиональной деятельности основных нормативных правовых документов	деятельности основных нормативных правовых документов

Шифр и название КОМПЕТЕНЦИИ:

ПК-4: способность формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: правовую обоснованность, административно-управленческую и техническую реализуемость, экономическую целесообразность мер информационной безопасности

• УМЕТЬ: проектировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

• ВЛАДЕТЬ способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-4) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-4	1	2	3	4	5
ЗНАТЬ: правовую обоснованность, административно-управленческую и техническую реализуемость, экономическую целесообразность мер	Отсутствие знаний	Фрагментарные представления о правовой обоснованности, административно-управленческой и технической реализуемости, экономической	В целом успешные, но не систематические представления об основных о правовой обоснованности, административно-управленческой и	В целом успешные, но содержащие отдельные пробелы, представления о правовой обоснованности, административно-управленческой и	Сформированные представления о правовой обоснованности, административно-управленческой и технической реализуемости, экономической

информационной безопасности Шифр. ПК-4		целесообразности мер информационной безопасности	технической реализуемости, экономической целесообразности мер информационной безопасности	технической реализуемости, экономической целесообразности мер информационной безопасности	целесообразности мер информационной безопасности
УМЕТЬ: проектировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности Шифр: ПК-4	Отсутствие умений	Фрагментарное использование умения проектировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	В целом успешное, но не систематическое использование умения проектировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	В целом успешное, но содержащее отдельные пробелы использование умения проектировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	Сформированное умение проектировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности
ВЛАДЕТЬ: навыками формирования комплекса мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	Отсутствие навыков	Фрагментарное владение навыками формирования комплекса мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	В целом успешное но не систематическое владение навыками формирования комплекса мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	В целом успешное, но содержащее отдельные пробелы владение навыками формирования комплекса мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности	Успешное и систематическое владение навыками формирования комплекса мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

Шифр и название КОМПЕТЕНЦИИ:

ПК-5: способностью организовывать и поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты, внешних воздействий, вероятных угроз и уровня развития технологий защиты информации

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: мер по информационной безопасности, вероятные угрозы и уровень развития технологий защиты информации

• УМЕТЬ: организовывать комплекс мер по информационной безопасности с учетом решаемых задач и организационной структуры объекта защиты

• ВЛАДЕТЬ способностью поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-5) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-5	1	2	3	4	5
ЗНАТЬ: меры по информационной безопасности, вероятные угрозы и уровень развития технологий защиты информации Шифр. ПК-5	Отсутствие знаний	Фрагментарные представления о мерах по информационной безопасности, вероятных угрозах и уровне развития технологий защиты информации	В целом успешные, но не систематические представления о мерах по информационной безопасности, вероятных угрозах и уровне развития технологий защиты информации	В целом успешные, но содержащие отдельные пробелы, представления о мерах по информационной безопасности, вероятных угрозах и уровне развития технологий защиты информации	Сформированные представления о мерах по информационной безопасности, вероятных угрозах и уровне развития технологий защиты информации
УМЕТЬ: организовывать комплекс мер по информационной безопасности с учетом решаемых задач и организационной структуры объекта защиты Шифр: ПК-5	Отсутствие умений	Фрагментарное использование умения организовывать комплекс мер по информационной безопасности с учетом решаемых задач и организационной структуры объекта	В целом успешное, но не систематическое использование умения организовывать комплекс мер по информационной безопасности с учетом решаемых задач и	В целом успешное, но содержащее отдельные пробелы использование умения организовывать комплекс мер по информационной безопасности с учетом решаемых задач и	Сформированное умение организовывать комплекс мер по информационной безопасности с учетом решаемых задач и организационной структуры объекта

			организационной структуры объекта	организационной структуры объекта	
ВЛАДЕТЬ: способностью поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты	Отсутствие навыков	Фрагментарное владение способностью поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты	В целом успешное но не систематическое владение способностью поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты	В целом успешное, но содержащее отдельные пробелы владение способностью поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты	Успешное и систематическое владение способностью поддерживать выполнение комплекса мер по информационной безопасности, управлять процессом их реализации с учетом решаемых задач и организационной структуры объекта защиты

Шифр и название КОМПЕТЕНЦИИ:

ПК-6: способность организовать проведение и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: требования государственных нормативных документов по аттестации объектов в области информационной безопасности

• УМЕТЬ: организовывать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов

• ВЛАДЕТЬ: способностью проводить и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-6) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
	1	2	3	4	5

(показатели достижения заданного уровня освоения компетенций), шифр ПК-6					
ЗНАТЬ: требования государственных нормативных документов по аттестации объектов в области информационной безопасности Шифр. ПК-6	Отсутствие знаний	Фрагментарные представления о требованиях государственных нормативных документов по аттестации объектов в области информационной безопасности	В целом успешные, но не систематические представления о требованиях государственных нормативных документов по аттестации объектов в области информационной безопасности	В целом успешные, но содержащие отдельные пробелы, представления о требованиях государственных нормативных документов по аттестации объектов в области информационной безопасности	Сформированные представления о требованиях государственных нормативных документов по аттестации объектов в области информационной безопасности
УМЕТЬ: организовывать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов Шифр: ПК-6	Отсутствие умений	Фрагментарное использование умения организовывать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	В целом успешное, но не систематическое использование умения организовывать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	В целом успешное, но содержащее отдельные пробелы использование умения организовывать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	Сформированное умение организовывать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов
ВЛАДЕТЬ: способностью проводить и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	Отсутствие навыков	Фрагментарное владение способностью проводить и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	В целом успешное но не систематическое владение способностью проводить и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	В целом успешное, но содержащее отдельные пробелы владение способностью проводить и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов	Успешное и систематическое владение способностью проводить и сопровождать аттестацию объекта на соответствие требованиям государственных или корпоративных нормативных документов

Шифр и название КОМПЕТЕНЦИИ:

ПК-7: способность определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

• УМЕТЬ: определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

• ВЛАДЕТЬ: способностью выявлять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-7) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-7					
ЗНАТЬ: виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач	Отсутствие знаний	Фрагментарные представления о видах и формах информации, подверженной угрозам, видах и возможных методах и пути реализации угроз для структуры и содержания информационных процессов предприятия	В целом успешные, но не систематические представления о видах и формах информации, подверженной угрозам, видах и возможных методах и пути реализации угроз для структуры и содержания информационных процессов предприятия	В целом успешные, но содержащие отдельные пробелы, представления о видах и формах информации, подверженной угрозам, видах и возможных методах и пути реализации угроз для структуры и содержания информационных процессов	Сформированные представления о видах и формах информации, подверженной угрозам, видах и возможных методах и пути реализации угроз для структуры и содержания информационных процессов

деятельности предприятия					
Шифр. ПК-7					
УМЕТЬ: определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия Шифр: ПК-7	Отсутствие умений	Фрагментарное использование умения определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	В целом успешное, но не систематическое использование умения определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	В целом успешное, но содержащее отдельные пробелы использование умения определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	Сформированное умение определять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз на основе анализа структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия
ВЛАДЕТЬ: способностью выявлять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	Отсутствие навыков	Фрагментарное владение способностью выявлять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	В целом успешное но не систематическое владение способностью выявлять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	В целом успешное, но содержащее отдельные пробелы владение способностью выявлять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия	Успешное и систематическое владение способностью выявлять виды и формы информации, подверженной угрозам, виды и возможные методы и пути реализации угроз для структуры и содержания информационных процессов предприятия, целей и задач деятельности предприятия

Шифр и название КОМПЕТЕНЦИИ:

ПК-8: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: подсистемы управления информационной безопасностью предприятия

• УМЕТЬ: управлять подсистемами управления информационной безопасностью предприятия

• ВЛАДЕТЬ: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-8) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-8	1	2	3	4	5
ЗНАТЬ: подсистемы управления информационной безопасностью предприятия Шифр. ПК-8	Отсутствие знаний	Фрагментарные представления о подсистемах управления информационной безопасностью предприятия	В целом успешные, но не систематические представления о подсистемах управления информационной безопасностью предприятия	В целом успешные, но содержащие отдельные пробелы, представления о подсистемах управления информационной безопасностью предприятия	Сформированные представления о подсистемах управления информационной безопасностью предприятия
УМЕТЬ: управлять подсистемами управления информационной безопасностью предприятия Шифр: ПК-8	Отсутствие умений	Фрагментарное использование умения управлять подсистемами управления информационной безопасностью предприятия	В целом успешное, но не систематическое использование умения управлять подсистемами управления информационной безопасностью предприятия	В целом успешное, но содержащее отдельные пробелы использование умения управлять подсистемами управления информационной безопасностью предприятия	Сформированное умение управлять подсистемами управления информационной безопасностью предприятия
ВЛАДЕТЬ: способностью принимать участие	Отсутствие навыков	Фрагментарное владение способностью	В целом успешное но не систематическое владение	В целом успешное, но содержащее отдельные пробелы	Успешное и систематическое владение

в эксплуатации подсистем управления информационной безопасностью предприятия	принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	владение способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия

Шифр и название КОМПЕТЕНЦИИ:

ПК-9 способность администрировать подсистемы информационной безопасности объекта

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: подсистемы управления информационной безопасностью объектов

• УМЕТЬ: администрировать подсистемы информационной безопасности объекта

• ВЛАДЕТЬ: способностью администрировать подсистемы информационной безопасности объекта

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-9) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-9	1	2	3	4	5
ЗНАТЬ: подсистемы управления информационной безопасностью объектов Шифр. ПК-9	Отсутствие знаний	Фрагментарные представления о подсистемах управления информационной безопасностью объектов	В целом успешные, но не систематические представления о подсистемах управления информационной безопасностью объектов	В целом успешные, но содержащие отдельные пробелы, представления о подсистемах управления информационной безопасностью объектов	Сформированные представления о подсистемах управления информационной безопасностью объектов

УМЕТЬ: администрировать подсистемы информационной безопасности объекта Шифр: ПК-9	Отсутствие умений	Фрагментарное использование умения администрировать подсистемы информационной безопасности объекта	В целом успешное, но не систематическое использование умения администрировать подсистемы информационной безопасности объекта	В целом успешное, но содержащее отдельные пробелы использование умения администрировать подсистемы информационной безопасности объекта	Сформированное умение администрировать подсистемы информационной безопасности объекта
ВЛАДЕТЬ: способностью администрировать подсистемы информационной безопасности объекта	Отсутствие навыков	Фрагментарное владение способностью администрировать подсистемы информационной безопасности объекта	В целом успешное но не систематическое владение способностью администрировать подсистемы информационной безопасности объекта	В целом успешное, но содержащее отдельные пробелы владение способностью администрировать подсистемы информационной безопасности объекта	Успешное и систематическое владение способностью администрировать подсистемы информационной безопасности объекта

Шифр и название КОМПЕТЕНЦИИ:

ПК-10: способность выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: технические и программно-аппаратные средства защиты информации

• УМЕТЬ: выполнять установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации

• ВЛАДЕТЬ: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-10) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
	1	2	3	4	5

(показатели достижения заданного уровня освоения компетенций), шифр ПК-10					
ЗНАТЬ: технические и программно-аппаратные средства защиты информации Шифр. ПК-10	Отсутствие знаний	Фрагментарные представления о технических и программно-аппаратных средствах защиты информации	В целом успешные, но не систематические представления о технических и программно-аппаратных средствах защиты информации	В целом успешные, но содержащие отдельные пробелы, представления о технических и программно-аппаратных средствах защиты информации	Сформированные представления о технических и программно-аппаратных средствах защиты информации
УМЕТЬ: выполнять установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации Шифр: ПК-10	Отсутствие умений	Фрагментарное использование умения выполнять установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации	В целом успешное, но не систематическое использование умения выполнять установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации	В целом успешное, но содержащее отдельные пробелы использование умения выполнять установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации	Сформированное умение выполнять установку, настройку и обслуживание технических и программно-аппаратных средств защиты информации
ВЛАДЕТЬ: способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	Отсутствие навыков	Фрагментарное владение способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	В целом успешное но не систематическое владение способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	В целом успешное, но содержащее отдельные пробелы владение способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации	Успешное и систематическое владение способностью выполнять работы по установке, настройке и обслуживанию технических и программно-аппаратных средств защиты информации

Шифр и название КОМПЕТЕНЦИИ:

ПК-11: способность участвовать в разработке подсистемы управления информационной безопасностью

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: методы разработки подсистем управления информационной безопасностью

• УМЕТЬ: применять методы разработки подсистем управления информационной безопасностью

• ВЛАДЕТЬ: способностью разрабатывать подсистемы управления информационной безопасностью

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-11) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций), шифр ПК-11	Критерии оценивания результатов обучения				
	1	2	3	4	5
ЗНАТЬ: методы разработки подсистем управления информационной безопасностью Шифр. ПК-11	Отсутствие знаний	Фрагментарные представления о методах разработки подсистем управления информационной безопасностью	В целом успешные, но не систематические представления о методах разработки подсистем управления информационной безопасностью	В целом успешные, но содержащие отдельные пробелы, представления о методах разработки подсистем управления информационной безопасностью	Сформированные представления о методах разработки подсистем управления информационной безопасностью
УМЕТЬ: применять методы разработки подсистем управления информационной безопасностью Шифр: ПК-11	Отсутствие умений	Фрагментарное использование умения применять методы разработки подсистем управления информационной безопасностью	В целом успешное, но не систематическое использование умения применять методы разработки подсистем управления информационной безопасностью	В целом успешное, но содержащее отдельные пробелы использование умения применять методы разработки подсистем управления информационной безопасностью	Сформированное умение применять методы разработки подсистем управления информационной безопасностью
ВЛАДЕТЬ: способностью разрабатывать	Отсутствие навыков	Фрагментарное владение способностью	В целом успешное но не систематическое владение	В целом успешное, но содержащее отдельные пробелы	Успешное и систематическое владение

подсистемы управления информационной безопасностью		разрабатывать подсистемы управления информационной безопасностью	способностью разрабатывать подсистемы управления информационной безопасностью	владение способностью разрабатывать подсистемы управления информационной безопасностью	способностью разрабатывать подсистемы управления информационной безопасностью

Шифр и название КОМПЕТЕНЦИИ:

ПК-12: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности

• УМЕТЬ: применять основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности

• ВЛАДЕТЬ: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-12) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-12	1	2	3	4	5
ЗНАТЬ: основы технико-экономического анализа и обоснования проектных решений по обеспечению	Отсутствие знаний	Фрагментарные представления об основах технико-экономического анализа и обоснования проектных решений по обеспечению	В целом успешные, но не систематические представления об основах технико-экономического анализа и обоснования проектных решений	В целом успешные, но содержащие отдельные пробелы, представления об основах технико-экономического анализа и обоснования	Сформированные представления об основах технико-экономического анализа и обоснования проектных решений по обеспечению информационной

информационной безопасности Шифр. ПК-12		информационной безопасности	по обеспечению информационной безопасности	проектных решений по обеспечению информационной	
УМЕТЬ: применять основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности Шифр: ПК-12	Отсутствие умений	Фрагментарное использование умения применять основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	В целом успешное, но не систематическое использование умения применять основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	В целом успешное, но содержащее отдельные пробелы использование умения применять основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	Сформированное умение применять основы технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности
ВЛАДЕТЬ: способность к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	Отсутствие навыков	Фрагментарное владение способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	В целом успешное но не систематическое владение способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	В целом успешное, но содержащее отдельные пробелы владение способностью безопасностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности	Успешное и систематическое владение способностью к проведению предварительного технико-экономического анализа и обоснования проектных решений по обеспечению информационной безопасности

Шифр и название КОМПЕТЕНЦИИ:

ПК-13: способность оформить рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: действующие нормативные и методические документы в области информационной безопасности по оформлению рабочей технической документации

• УМЕТЬ: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности

• ВЛАДЕТЬ:

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-13) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-13					
ЗНАТЬ: действующие нормативные и методические документы в области информационной безопасности по оформлению рабочей технической документации Шифр. ПК-13	Отсутствие знаний	Фрагментарные представления о действующих нормативных и методических документах в области информационной безопасности по оформлению рабочей технической документации	В целом успешные, но не систематические представления о действующих нормативных и методических документах в области информационной безопасности по оформлению рабочей технической документации	В целом успешные, но содержащие отдельные пробелы, представления о действующих нормативных и методических документах в области информационной безопасности по оформлению рабочей технической документации	Сформированные представления о действующих нормативных и методических документах в области информационной безопасности по оформлению рабочей технической документации
УМЕТЬ: оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности Шифр: ПК-13	Отсутствие умений	Фрагментарное использование умения оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	В целом успешное, но не систематическое использование умения оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	В целом успешное, но содержащее отдельные пробелы использование умения оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности	Сформированное умение оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов в области информационной безопасности
ВЛАДЕТЬ: способность к оформлению	Отсутствие навыков	Фрагментарное владение способностью к	В целом успешное но не систематическое владение	В целом успешное, но содержащее отдельные пробелы	Успешное и систематическое владение

рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности		оформлению рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности	способностью к оформлению рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности	владение способностью к оформлению рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности	способностью к оформлению рабочей технической документации с учетом действующих нормативных и методических документов в области информационной безопасности

Шифр и название КОМПЕТЕНЦИИ:

ПК-14: способность применять программные средства системного, прикладного и специального назначения

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: программные средства системного, прикладного и специального назначения в области информационной безопасности

• УМЕТЬ: применять программные средства системного, прикладного и специального назначения

• ВЛАДЕТЬ: способность применять программные средства системного, прикладного и специального назначения

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-14) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-14					
ЗНАТЬ: программные средства системного, прикладного и	Отсутствие знаний	Фрагментарные представления о программных средствах системного,	В целом успешные, но не систематические представления о программных	В целом успешные, но содержащие отдельные пробелы, представления о	Сформированные представления о программных средствах системного, прикладного и

специального назначения в области информационной безопасности		прикладного и специального назначения в области информационной безопасности	средствах системного, прикладного и специального назначения в области информационной безопасности	программных средствах системного, прикладного и специального назначения в области информационной безопасности	специального назначения в области информационной безопасности
Шифр. ПК-14					
УМЕТЬ: применять программные средства системного, прикладного и специального назначения безопасности	Отсутствие умений	Фрагментарное использование умения применять программные средства системного, прикладного и специального назначения безопасности	В целом успешное, но не систематическое использование умения применять программные средства системного, прикладного и специального назначения безопасности	В целом успешное, но содержащее отдельные пробелы использование умения применять программные средства системного, прикладного и специального назначения безопасности	Сформированное умение применять программные средства системного, прикладного и специального назначения безопасности
Шифр: ПК-14					
ВЛАДЕТЬ: способность применять программные средства системного, прикладного и специального назначения	Отсутствие навыков	Фрагментарное владение способностью применять программные средства системного, прикладного и специального назначения	В целом успешное но не систематическое владение способностью применять программные средства системного, прикладного и специального назначения	В целом успешное, но содержащее отдельные пробелы владение способностью применять программные средства системного, прикладного и специального назначения	Успешное и систематическое владение способностью применять программные средства системного, прикладного и специального назначения

Шифр и название КОМПЕТЕНЦИИ:

ПК-15: способность использовать инструментальные средства и системы программирования для решения профессиональных задач

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: инструментальные средства и системы программирования для решения профессиональных задач

• УМЕТЬ: применять инструментальные средства и системы программирования для решения профессиональных задач

• ВЛАДЕТЬ: способностью использовать инструментальные средства и системы программирования для решения профессиональных задач

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-15) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-15					
ЗНАТЬ: инструментальные средства и системы программирования для решения профессиональных задач Шифр. ПК-15	Отсутствие знаний	Фрагментарные представления о инструментальных средствах и системах программирования для решения профессиональных задач	В целом успешные, но не систематические представления о инструментальных средствах и системах программирования для решения профессиональных задач	В целом успешные, но содержащие отдельные пробелы, представления о инструментальных средствах и системах программирования для решения профессиональных задач	Сформированные представления о инструментальных средствах и системах программирования для решения профессиональных задач
УМЕТЬ: применять инструментальные средства и системы программирования для решения профессиональных задач Шифр: ПК-15	Отсутствие умений	Фрагментарное использование умения применять инструментальные средства и системы программирования для решения профессиональных задач	В целом успешное, но не систематическое использование умения применять инструментальные средства и системы программирования для решения профессиональных задач	В целом успешное, но содержащее отдельные пробелы использование умения применять инструментальные средства и системы программирования для решения профессиональных задач	Сформированное умение применять инструментальные средства и системы программирования для решения профессиональных задач
ВЛАДЕТЬ: способность использовать инструментальные средства и системы программирования для решения	Отсутствие навыков	Фрагментарное владение способностью применять инструментальные средства и системы программирования для решения	В целом успешное но не систематическое владение способностью применять инструментальные средства и системы программирования для	В целом успешное, но содержащее отдельные пробелы владение способностью применять инструментальные средства и системы	Успешное и систематическое владение способностью применять инструментальные средства и системы программирования

профессиональных задач	профессиональных задач	решения профессиональных задач	программирования для решения профессиональных задач	для решения профессиональных задач

Шифр и название КОМПЕТЕНЦИИ:

ПК-16: способность к программной реализации алгоритмов решения типовых задач обеспечения информационной безопасности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: алгоритмы решения типовых задач обеспечения информационной безопасности

• УМЕТЬ: применять методы программной реализации алгоритмов

• ВЛАДЕТЬ: способностью создавать программные реализации алгоритмов решения типовых задач обеспечения информационной безопасности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-16) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-16					
ЗНАТЬ: алгоритмы решения типовых задач обеспечения информационной безопасности	Отсутствие знаний	Фрагментарные представления об алгоритмах решения типовых задач обеспечения информационной безопасности	В целом успешные, но не систематические представления об алгоритмах решения типовых задач обеспечения информационной безопасности	В целом успешные, но содержащие отдельные пробелы, представления об алгоритмах решения типовых задач обеспечения информационной безопасности	Сформированные представления об алгоритмах решения типовых задач обеспечения информационной безопасности
Шифр. ПК-16					

УМЕТЬ: применять методы программной реализации алгоритмов Шифр: ПК-16	Отсутствие умений	Фрагментарное использование умения применять методы программной реализации алгоритмов	В целом успешное, но не систематическое использование умения применять методы программной реализации алгоритмов	В целом успешное, но содержащее отдельные пробелы использование умения применять методы программной реализации алгоритмов	Сформированное умение применять методы программной реализации алгоритмов
ВЛАДЕТЬ: способность создавать программные реализации алгоритмов решения типовых задач обеспечения информационной безопасности	Отсутствие навыков	Фрагментарное владение способностью создавать программные реализации алгоритмов решения типовых задач обеспечения информационной безопасности	В целом успешное но не систематическое владение способностью создавать программные реализации алгоритмов решения типовых задач обеспечения информационной безопасности способностью	В целом успешное, но содержащее отдельные пробелы владение способностью создавать программные реализации алгоритмов решения типовых задач обеспечения информационной безопасности	Успешное и систематическое владение способностью создавать программные реализации алгоритмов решения типовых задач обеспечения информационной безопасности

Шифр и название КОМПЕТЕНЦИИ:

ПК-17: способность собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: виды исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

• УМЕТЬ: применять методы для сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

• ВЛАДЕТЬ: способностью сбора и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-17) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Критерии оценивания результатов обучения

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-17 ЗНАТЬ: виды исходных данных для проектирования подсистем и средств обеспечения информационной безопасности Шифр. ПК-17	Отсутствие знаний	Фрагментарные представления о видах исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешные, но не систематические представления о видах исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешные, но содержащие отдельные пробелы, представления о видах исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Сформированные представления о видах исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
УМЕТЬ: применять методы для сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности Шифр: ПК-17	Отсутствие умений	Фрагментарное использование умения применять методы для сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешное, но не систематическое использование умения применять методы для сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешное, но содержащее отдельные пробелы использование умения применять методы для сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Сформированное умение применять методы для сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
ВЛАДЕТЬ: способностью сбора и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Отсутствие навыков	Фрагментарное владение способностью сбора и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешное но не систематическое владение способностью сбора и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	В целом успешное, но содержащее отдельные пробелы владение способностью сбора и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности	Успешное и систематическое владение способностью сбора и анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

Шифр и название КОМПЕТЕНЦИИ:

ПК-18: способность составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: виды обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности

• УМЕТЬ: проектировать обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности

• ВЛАДЕТЬ: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-18) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-18					
ЗНАТЬ: виды обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности Шифр. ПК-18	Отсутствие знаний	Фрагментарные представления о видах обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности	В целом успешные, но не систематические представления о видах обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности	В целом успешные, но содержащие отдельные пробелы, представления о видах обзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности	Сформированные представления о видахобзоров по вопросам обеспечения информационной безопасности по профилю своей деятельности
УМЕТЬ: проектировать обзор по вопросам обеспечения информационной безопасности по	Отсутствие умений	Фрагментарное использование умения проектировать обзор по вопросам обеспечения	В целом успешное, но не систематическое использование умения проектировать обзор	В целом успешное, но содержащее отдельные пробелы использование умения проектировать обзор	Сформированное умение проектировать обзор по вопросам обеспечения информационной

профилю своей деятельности		информационной безопасности по профилю своей деятельности	по вопросам обеспечения информационной безопасности по профилю своей деятельности	по вопросам обеспечения информационной безопасности по профилю своей деятельности	безопасности по профилю своей деятельности
Шифр: ПК-18					
ВЛАДЕТЬ: способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	Отсутствие навыков	Фрагментарное владение способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	В целом успешное но не систематическое владение способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	В целом успешное, но содержащее отдельные пробелы владение способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности	Успешное и систематическое владение способностью составить обзор по вопросам обеспечения информационной безопасности по профилю своей деятельности

Шифр и название КОМПЕТЕНЦИИ:

ПК-19: способность проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: отечественные и зарубежные стандарты по вопросам обеспечения информационной безопасности

• УМЕТЬ: применять отечественные и зарубежные стандарты для анализа информационной безопасности объектов

• ВЛАДЕТЬ: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-19) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня	1	2	3	4	5

освоения компетенций),					
шифр ПК-19					
ЗНАТЬ: отечественные и зарубежные стандарты по вопросам обеспечения информационной безопасности	Отсутствие знаний	Фрагментарные представления об отечественных и зарубежных стандартах по вопросам обеспечения информационной безопасности	В целом успешные, но не систематические представления об отечественных и зарубежных стандартах по вопросам обеспечения информационной безопасности	В целом успешные, но содержащие отдельные пробелы, представления об отечественных и зарубежных стандартах по вопросам обеспечения информационной безопасности	Сформированные представления об отечественных и зарубежных стандартах по вопросам обеспечения информационной безопасности
Шифр. ПК-19					
УМЕТЬ: применять отечественные и зарубежные стандарты для анализа информационной безопасности объектов	Отсутствие умений	Фрагментарное использование умения применять отечественные и зарубежные стандарты для анализа информационной безопасности объектов	В целом успешное, но не систематическое использование умения применять отечественные и зарубежные стандарты для анализа информационной безопасности объектов	В целом успешное, но содержащее отдельные пробелы использование умения применять отечественные и зарубежные стандарты для анализа информационной безопасности объектов	Сформированное умение применять отечественные и зарубежные стандарты для анализа информационной безопасности объектов
Шифр: ПК-19					
ВЛАДЕТЬ: способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов	Отсутствие навыков	Фрагментарное владение способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов	В целом успешное но не систематическое владение способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов	В целом успешное, но содержащее отдельные пробелы владение способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов	Успешное и систематическое владение способностью проводить анализ информационной безопасности объектов и систем с использованием отечественных и зарубежных стандартов

Шифр и название КОМПЕТЕНЦИИ:

ПК-20: способность проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: методы проведения экспериментов по заданной методике

• УМЕТЬ: проводить обработку результатов, оценку погрешности и достоверности результатов экспериментов

• ВЛАДЕТЬ: способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-20) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-20	1	2	3	4	5
ЗНАТЬ: методы проведения экспериментов по заданной методике Шифр. ПК-20	Отсутствие знаний	Фрагментарные представления о методах проведения экспериментов по заданной методике	В целом успешные, но не систематические представления о методах проведения экспериментов по заданной методике	В целом успешные, но содержащие отдельные пробелы, представления о методах проведения экспериментов по заданной методике	Сформированные представления о методах проведения экспериментов по заданной методике
УМЕТЬ: проводить обработку результатов, оценку погрешности и достоверности результатов экспериментов Шифр: ПК-20	Отсутствие умений	Фрагментарное использование умения проводить обработку результатов, оценку погрешности и достоверности результатов экспериментов	В целом успешное, но не систематическое использование умения проводить обработку результатов, оценку погрешности и достоверности результатов экспериментов	В целом успешное, но содержащее отдельные пробелы использование умения проводить обработку результатов, оценку погрешности и достоверности результатов экспериментов	Сформированное умение проводить обработку результатов, оценку погрешности и достоверности результатов экспериментов
ВЛАДЕТЬ: способностью	Отсутствие навыков	Фрагментарное владение	В целом успешное но не систематическое	В целом успешное, но содержащее	Успешное и систематическое

проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов	способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов	владение способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов	отдельные пробелы владение способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов	владение способностью проводить эксперименты по заданной методике, обработку результатов, оценку погрешности и достоверности их результатов

Шифр и название КОМПЕТЕНЦИИ:

ПК-21: способность принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности

• УМЕТЬ: применять методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности

• ВЛАДЕТЬ: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-21) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-21	Отсутствие знаний	Фрагментарные представления о	В целом успешные, но не	В целом успешные, но содержащие	Сформированные представления о

ЗНАТЬ: методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности		методах проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	систематические представления о методах проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	отдельные пробелы, представления о методах проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	методах проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности
Шифр. ПК-21					
УМЕТЬ: применять методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности экспериментов	Отсутствие умений	Фрагментарное использование умения применять методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	В целом успешное, но не систематическое использование умения применять методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	В целом успешное, но содержащее отдельные пробелы использование умения применять методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	Сформированное умение применять методы проведения экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности
Шифр: ПК-21					
ВЛАДЕТЬ: способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	Отсутствие навыков	Фрагментарное владение способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	В целом успешное но не систематическое владение способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	В целом успешное, но содержащее отдельные пробелы владение способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности	Успешное и систематическое владение способностью принимать участие в проведении экспериментально-исследовательских работ системы защиты информации с учетом требований по обеспечению информационной безопасности

Шифр и название КОМПЕТЕНЦИИ:

ПК-22: способность осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

• УМЕТЬ: применять методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

• ВЛАДЕТЬ: осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-22) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-22	1	2	3	4	5
ЗНАТЬ: методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	Отсутствие знаний	Фрагментарные представления о методах проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	В целом успешные, но не систематические представления о методах проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	В целом успешные, но содержащие отдельные пробелы, представления о методах проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	Сформированные представления о методах проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

Шифр. ПК-22

УМЕТЬ: применять методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	Отсутствие умений	Фрагментарное использование умения применять методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	В целом успешное, но не систематическое использование умения применять методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	В целом успешное, но содержащее отдельные пробелы использование умения применять методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	Сформированное умение применять методы проведения подбора, изучения и обобщения научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

Шифр: ПК-22

ВЛАДЕТЬ: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	Отсутствие навыков	Фрагментарное владение способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	В целом успешное но не систематическое владение способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	В целом успешное, но содержащее отдельные пробелы владение способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности	Успешное и систематическое владение способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения информационной безопасности

Шифр и название КОМПЕТЕНЦИИ:

ПК-23: способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: современные системы управления информационной безопасностью

• УМЕТЬ: применять методы по совершенствованию системы управления информационной безопасностью

• ВЛАДЕТЬ: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-23) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-23					
ЗНАТЬ: современные системы управления информационной безопасностью ной безопасности	Отсутствие знаний	Фрагментарные представления о современных системах управления информационной безопасностью	В целом успешные, но не систематические представления о современных системах управления информационной безопасностью	В целом успешные, но содержащие отдельные пробелы, представления о современных системах управления информационной безопасностью	Сформированные представления о современных системах управления информационной безопасностью
Шифр. ПК-23					
УМЕТЬ: применять методы по совершенствованию системы управления информационной безопасностью	Отсутствие умений	Фрагментарное использование умения применять методы по совершенствованию системы управления информационной безопасностью	В целом успешное, но не систематическое использование умения применять методы по совершенствованию системы управления информационной безопасностью	В целом успешное, но содержащее отдельные пробелы использование умения применять методы по совершенствованию системы управления информационной безопасностью	Сформированное умение применять методы по совершенствованию системы управления информационной безопасностью
Шифр: ПК-23					

ВЛАДЕТЬ: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Отсутствие навыков	Фрагментарное владение способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	В целом успешное но не систематическое владение способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	В целом успешное, но содержащее отдельные пробелы владение способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	Успешное и систематическое владение способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Шифр и название КОМПЕТЕНЦИИ:

ПК-24: способность формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: правила, процедуры, практические приемы и пр. для управления информационной безопасностью

• УМЕТЬ: проектировать комплекс мер для управления информационной безопасностью

• ВЛАДЕТЬ: способностью формировать комплекс мер для управления информационной безопасностью

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-24) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня	1	2	3	4	5

освоения компетенций), шифр ПК-24					
ЗНАТЬ: правила, процедуры, практические приемы и пр. для управления информационной безопасностью Шифр. ПК-24	Отсутствие знаний	Фрагментарные представления о правилах, процедурах, практических приемах и пр. для управления информационной безопасностью	В целом успешные, но не систематические представления о правилах, процедурах, практических приемах и пр. для управления информационной безопасностью	В целом успешные, но содержащие отдельные пробелы, представления о правилах, процедурах, практических приемах и пр. для управления информационной безопасностью	Сформированные представления о правилах, процедурах, практических приемах и пр. для управления информационной безопасностью
УМЕТЬ: проектировать комплекс мер для управления информационной безопасностью Шифр: ПК-24	Отсутствие умений	Фрагментарное использование умения проектировать комплекс мер для управления информационной безопасностью	В целом успешное, но не систематическое использование умения проектировать комплекс мер для управления информационной безопасностью	В целом успешное, но содержащее отдельные пробелы использование умения проектировать комплекс мер для управления информационной безопасностью	Сформированное умение проектировать комплекс мер для управления информационной безопасностью
ВЛАДЕТЬ: способностью формировать комплекс мер для управления информационной безопасностью безопасностью	Отсутствие навыков	Фрагментарное владение способностью формировать комплекс мер для управления информационной безопасностью	В целом успешное но не систематическое владение способностью формировать комплекс мер для управления информационной безопасностью	В целом успешное, но содержащее отдельные пробелы владение способностью формировать комплекс мер для управления информационной безопасностью	Успешное и систематическое владение способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью

Шифр и название КОМПЕТЕНЦИИ:

ПК-25: способность принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: виды проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

• УМЕТЬ: проектировать контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

• ВЛАДЕТЬ: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-25) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций),	1	2	3	4	5
шифр ПК-25					
ЗНАТЬ: виды проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Отсутствие знаний	Фрагментарные представления о видах проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	В целом успешные, но не систематические представления о видах проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	В целом успешные, но содержащие отдельные пробелы, представления о видах проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Сформированные представления о видах проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации
Шифр. ПК-25					
УМЕТЬ: проектировать контрольные проверки работоспособности и эффективности	Отсутствие умений	Фрагментарное использование умения проектировать контрольные проверки	В целом успешное, но не систематическое использование умения проектировать	В целом успешное, но содержащее отдельные пробелы использование умения проектировать	Сформированное умение проектировать контрольные проверки работоспособности и

применяемых программно-аппаратных, криптографических и технических средств защиты информации Шифр: ПК-25		работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации
ВЛАДЕТЬ: способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Отсутствие навыков	Фрагментарное владение способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	В целом успешное но не систематическое владение способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	В целом успешное, но содержащее отдельные пробелы владение способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	Успешное и систематическое владение способностью принимать участие в организации контрольных проверок работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

Шифр и название КОМПЕТЕНЦИИ:

ПК-26: способность изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: опыт работы учреждений, организаций и предприятий в области повышения эффективности защиты информации

• УМЕТЬ: изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации

• ВЛАДЕТЬ: способностью принимать участие в работах по повышению эффективности защиты информации

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-267) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций), шифр ПК-26	Критерии оценивания результатов обучения				
	1	2	3	4	5
ЗНАТЬ: опыт работы учреждений, организаций и предприятий в области повышения эффективности защиты информации Шифр. ПК-26	Отсутствие знаний	Фрагментарные представления об опыте работы учреждений, организаций и предприятий в области повышения эффективности защиты информации	В целом успешные, но не систематические представления об опыте работы учреждений, организаций и предприятий в области повышения эффективности защиты информации	В целом успешные, но содержащие отдельные пробелы, представления об опыте работы учреждений, организаций и предприятий в области повышения эффективности защиты информации	Сформированные представления об опыте работы учреждений, организаций и предприятий в области повышения эффективности защиты информации
УМЕТЬ: изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации Шифр: ПК-26	Отсутствие умений	Фрагментарное использование умения изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации	В целом успешное, но не систематическое использование умения изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации	В целом успешное, но содержащее отдельные пробелы использование умения изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации	Сформированное умение изучать и обобщать опыт работы других учреждений, организаций и предприятий в области повышения эффективности защиты информации

ВЛАДЕТЬ: способностью принимать участие в работах по повышению эффективности защиты информации	Отсутствие навыков	Фрагментарное владение способностью принимать участие в работах по повышению эффективности защиты информации	В целом успешное но не систематическое владение способностью принимать участие в работах по повышению эффективности защиты информации	В целом успешное, но содержащее отдельные пробелы владение способностью принимать участие в работах по повышению эффективности защиты информации	Успешное и систематическое владение способностью принимать участие в работах по повышению эффективности защиты информации

Шифр и название КОМПЕТЕНЦИИ:

ПК-27: способность участвовать в работах по реализации политики информационной безопасности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: виды политик информационной безопасности

• УМЕТЬ: проектировать политики информационной безопасности

• ВЛАДЕТЬ: способностью принимать участие в работах по реализации политики информационной безопасности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-27) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня	1	2	3	4	5

освоения компетенций), шифр ПК-27					
ЗНАТЬ: виды политик информационной безопасности	Отсутствие знаний	Фрагментарные представления о видах политик информационной безопасности	В целом успешные, но не систематические представления о видах политик информационной безопасности	В целом успешные, но содержащие отдельные пробелы, представления о видах политик информационной безопасности	Сформированные представления о видах политик информационной безопасности
Шифр. ПК-27					
УМЕТЬ: проектировать политики информационной безопасности	Отсутствие умений	Фрагментарное использование умения проектировать политики информационной безопасности	В целом успешное, но не систематическое использование умения проектировать политики информационной безопасности	В целом успешное, но содержащее отдельные пробелы использование умения проектировать политики информационной безопасности	Сформированное умение проектировать политики информационной безопасности
Шифр: ПК-27					
ВЛАДЕТЬ: способностью принимать участие в работах по реализации политики информационной безопасности	Отсутствие навыков	Фрагментарное владение способностью принимать участие в работах по реализации политики информационной безопасности	В целом успешное но не систематическое владение способностью принимать участие в работах по реализации политики информационной безопасности	В целом успешное, но содержащее отдельные пробелы владение способностью принимать участие в работах по реализации политики информационной безопасности	Успешное и систематическое владение способностью принимать участие в работах по реализации политики информационной безопасности

Шифр и название КОМПЕТЕНЦИИ:

ПК-28: способность применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: виды комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности

• УМЕТЬ: проектировать комплексный подход к обеспечению информационной безопасности в различных сферах деятельности

• ВЛАДЕТЬ: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-28) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Планируемые результаты обучения	Критерии оценивания результатов обучения				
(показатели достижения заданного уровня освоения компетенций), шифр ПК-28	1	2	3	4	5
ЗНАТЬ: виды комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности Шифр. ПК-28	Отсутствие знаний	Фрагментарные представления о видах комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности	В целом успешные, но не систематические представления о видах комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности	В целом успешные, но содержащие отдельные пробелы, представления о видах комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности	Сформированные представления о видах комплексного подхода к обеспечению информационной безопасности в различных сферах деятельности
УМЕТЬ: проектировать комплексный подход к обеспечению информационной безопасности в различных сферах деятельности Шифр: ПК-28	Отсутствие умений	Фрагментарное использование умения проектировать комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	В целом успешное, но не систематическое использование умения проектировать комплексный подход к обеспечению информационной безопасности в	В целом успешное, но содержащее отдельные пробелы использование умения проектировать комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	Сформированное умение проектировать комплексный подход к обеспечению информационной безопасности в различных сферах деятельности

		различных сферах деятельности			
ВЛАДЕТЬ: способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности безопасности	Отсутствие навыков	Фрагментарное владение способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	В целом успешное но не систематическое владение способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	В целом успешное, но содержащее отдельные пробелы владение способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности	Успешное и систематическое владение способностью применять комплексный подход к обеспечению информационной безопасности в различных сферах деятельности

Шифр и название КОМПЕТЕНЦИИ:

ПК-29: способность и готовностью к педагогической деятельности в области профессиональной подготовки в образовательных организациях высшего образования, дополнительного профессионального образования, профессиональных образовательных организациях

ОБЩАЯ ХАРАКТЕРИСТИКА КОМПЕТЕНЦИИ Тип КОМПЕТЕНЦИИ:

Профессиональная компетенция выпускника программы аспирантуры по направлению подготовки 10.06.01 Информационная безопасность.

ПОРОГОВЫЙ (ВХОДНОЙ) УРОВНЬ ЗНАНИЙ, УМЕНИЙ, ОПЫТА ДЕЯТЕЛЬНОСТИ, ТРЕБУЕМЫЙ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ

Для того чтобы формирование данной компетенции было возможно, обучающийся, приступивший к освоению программы аспирантуры, должен:

• ЗНАТЬ: основы педагогической деятельности

• УМЕТЬ: организовать учебный процесс

• ВЛАДЕТЬ: способностью вести педагогическую деятельность в области профессиональной подготовки

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ДЛЯ ФОРМИРОВАНИЯ КОМПЕТЕНЦИИ (ПК-29) И КРИТЕРИИ ИХ ОЦЕНИВАНИЯ

Критерии оценивания результатов обучения

Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций), шифр ПК-29	1	2	3	4	5
ЗНАТЬ: основы педагогической деятельности	Отсутствие знаний	Фрагментарные представления об основах педагогической деятельности	В целом успешные, но не систематические представления об основах педагогической деятельности	В целом успешные, но содержащие отдельные пробелы, представления об основах педагогической деятельности	Сформированные представления об основах педагогической деятельности
Шифр. ПК-29					
УМЕТЬ: организовать учебный процесс	Отсутствие умений	Фрагментарное использование умения организовать учебный процесс	В целом успешное, но не систематическое использование умения организовать учебный процесс	В целом успешное, но содержащее отдельные пробелы использование умения организовать учебный процесс	Сформированное умение организовать учебный процесс
Шифр: ПК-29					
ВЛАДЕТЬ: способностью вести педагогическую деятельность в области профессиональной подготовки	Отсутствие навыков	Фрагментарное владение способностью вести педагогическую деятельность в области профессиональной подготовки	В целом успешное но не систематическое владение способностью вести педагогическую деятельность в области профессиональной подготовки	В целом успешное, но содержащее отдельные пробелы владение способностью вести педагогическую деятельность в области профессиональной подготовки	Успешное и систематическое владение способностью вести педагогическую деятельность в области профессиональной подготовки