Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. А. Бабаева

АТТЕСТАЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЬЕКТОВ ГИС

Учебно-методическое пособие по изучению дисциплины для студентов специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.056.57 (076)

Рецензент
кандидат физико-математических наук, доцент кафедры информационной безопасности ФГБОУ ВО «Калининградский государственный технический университет Н. Я. Великите

Бабаева, А. А.
Аттестация по информационной безопасности объектов ГИС: учебно-методическое пособие по изучению дисциплины для студентов специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем» / А. А. Бабаева. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 27 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Аттестация по информационной безопасности объектов ГИС» студентами специалитета 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем». В документе представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, указания к изучению каждой темы, вопросы для изучения методических материалов к занятиям, методические указаний по выполнению самостоятельной работы, содержатся требования к текущей и промежуточной аттестации.

Учебно-методическое пособие предназначено для изучения и эффективного освоения знаний и практических навыков в области оценки и обеспечения безопасности информации в ГИС, аттестации по информационной безопасности объектов ГИС.

Табл. 2, список лит. – 23 наименования

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 26.05.2025 г., протокол № 4

УДК 004.056.57 (076)

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специалитета 10.05.03 Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем», изучающих дисциплину «Аттестация по информационной безопасности объектов ГИС**».**

ПК-1: способен разрабатывать проектные решения по защите информации в автоматизированных системах, обеспечивать их внедрение и сопровождение.

Цель освоения дисциплины: формирование знаний об организации системы государственного лицензировании в области защиты информации, сертификации и аттестации объектов защиты информации, а также организации мероприятий по информационной безопасности на объекте информатизации и об их правовом обеспечении.

В курсе студенты изучают нормативно-правовую базу, регулирующую вопросы защиты информации в государственных системах. Приобретают навыки анализа угроз информационной безопасности и оценки рисков для информационных ресурсов, изучают методы и инструменты аттестации объектов, включая организацию проверок, тестирование защищенности и оформление документации. Учатся разрабатывать и реализовывать комплекс мер, обеспечивающих соответствие систем требованиям защиты информации. Готовятся к профессиональному взаимодействию с надзорными органами и проведения аттестационных процедур в соответствии с современными стандартами.

В результате освоения дисциплины обучающийся должен:

знать:

– методики сертификационных испытаний технических средств защиты информации от несанкционированного доступа и утечки по техническим каналам на соответствие требованиям по безопасности информации;

– методы защиты информации от несанкционированного доступа и утечки по техническим каналам;

уметь:

– определять класс защищенности автоматизированных систем и ее составных частей;

– проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы;

владеть:

– навыками обоснования перечня сертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы.

Задачи дисциплины:

– изучение основных принципов и нормативных требований, связанных с аттестацией объектов государственных информационных систем;

– изучение методик проведения мероприятий по защите информации от несанкционированного доступа, утечек и угроз;

– формирование умений проводить анализ рисков и разрабатывать меры по повышению уровня безопасности систем;

– подготовка к практической реализации процедур аттестации, включая оформление документации и взаимодействие с надзорными органами.

Дисциплина «Аттестация по информационной безопасности объектов ГИС» относится к Модулю 1 «Информационная безопасность государственных информационных систем (ГИС)» части, формируемой участниками образовательных отношений студентов специалитета 10.05.03 «Информационная безопасность автоматизированных систем».

Основными видами аудиторных учебных занятий по дисциплине являются лекции и лабораторные занятия.

Формирование знаний, обучающихся обеспечивается проведением лекционных занятий.

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины; возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе «Содержание дисциплины» приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки, каждая тема имеет ссылки на литературу (или иные информационные ресурсы) и контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделе ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Программное обеспечение:

1.MicrosoftDesktopEducation. Операционные системы: MicrosoftWindowsDesktopoperatingsystems, офисные приложения: MicrosoftOffice, по соглашению V9002148 OpenValueSubscription (срок действия: три года).

2. ТЕМАТИЧЕСКИЙ ПЛАН

2.1 Очная форма обучения

Таблица 1

	Раздел (модуль) дисцип-лины	Тема	Объем контактной работы, ч	Объем самостоятельной работы, ч
Теоретическое обучение (лекции)				
Осенний семестр (9)				
1		Структура системы аттестации объектов информатизации	10	10
2		Организация проведения предаттестационных мероприятий, проводимых заявителем	10	10
3		Порядок проведения аттестации объектов информатизации	12	10
		Итого по курсу	**32**	**30**
	Практические занятия			
1		Организация аттестации объектов информатизации на соответствие требованиям безопасности информации	8	12
2		Организация и выполнение мероприятий по аттестации объектов информатизации по требованиям безопасности информации	8	12
		Итого за семестр	**16**	**24**
	Рубежный (текущий) и итоговый контроль			
		Тестирование	**КА - 0,15**	
		Итоговое тестирование (зачет)	**РЭ – 5**	**0,85**
		Всего	**48**	**54,85**
				ИТОГО 108

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1 Раздел 1. Структура системы аттестации объектов информатизации

Перечень изучаемых вопросов

1. Нормативно-правовая база:

– основные законодательные акты и нормативные документы, регулирующие аттестацию объектов информатизации;

– требования к защите информации в государственных информационных системах.

2. Элементы системы аттестации:

– основные компоненты системы аттестации: объекты аттестации, субъекты, документация;

– структура взаимодействия участников процесса аттестации.

3. Процедура аттестации:

– порядок проведения работ по аттестации объектов информатизации;

– этапы процесса аттестации и их последовательность.

4. Риски и уязвимости:

– анализ потенциальных угроз безопасности информации;

– инструменты и методы выявления уязвимостей в государственных информационных системах.

Методические указания к изучению

Структура системы аттестации объектов информатизации включает изучение нормативно-правовой базы, которая охватывает основные законодательные акты и нормативные документы, регулирующие процесс аттестации, а также требования к защите информации в государственных информационных системах. Также рассматриваются элементы системы аттестации, включая объекты аттестации, субъекты и документацию, а также структура взаимодействия участников процесса. Процедура аттестации охватывает порядок выполнения работ, последовательность этапов и их специфику. Важным аспектом являются анализ потенциальных угроз безопасности информации и использование инструментов и методов для выявления уязвимостей в государственных информационных системах, что способствует повышению уровня их защищенности.

Литература: [1, с. 56–62], [3, с. 91–102], [4, с. 123–156].

Контрольные вопросы

1. Законодательные акты и нормативные документы, регулирующие процесс аттестации объектов ГИС по требованиям безопасности.
2. Основные элементы, входящие в структуру системы аттестации объектов ГИС
3. Основные этапы проведения аттестации объектов ГИС по требованиям безопасности и их последовательность.

4. Требования к защите информации в государственных информационных системах.

5. Инструменты и методы для выявления уязвимостей в государственных информационных системах

6. Потенциальные угрозы безопасности информации, актуальные при проведении аттестации объектов ГИС.

3.2 Раздел 2. Организация проведения предаттестационных мероприятий, проводимых заявителем

Перечень изучаемых вопросов

1. Планирование предаттестационных мероприятий:

– разработка плана мероприятий для подготовки объекта к аттестации;

– определение этапов предаттестационной подготовки.

2. Назначение ответственных лиц:

– формирование группы специалистов для выполнения мероприятий;

– распределение обязанностей и ролей среди сотрудников.

3. Первичный аудит и анализ соответствия:

– проведение первичной оценки объекта на предмет соответствия требованиям информационной безопасности;

– идентификация слабых мест и потенциальных рисков.

4. Сбор и подготовка документации:

– формирование исходных данных для аттестации;

– подготовка обязательной документации, включая технические паспорта и отчеты по защищенности.

Методические указания к изучению

Организация проведения предаттестационных мероприятий включает разработку плана подготовки объекта к аттестации, определение этапов предаттестационной подготовки, а также назначение ответственных лиц, включая формирование группы специалистов и распределение обязанностей между ними. Важной частью процесса является проведение первичного аудита и анализ соответствия объекта требованиям информационной безопасности с целью выявления слабых мест и потенциальных рисков. Кроме того, осуществляется сбор исходных данных для аттестации и подготовка обязательной документации, такой как технические паспорта и отчеты по защищенности, обеспечивающие основу для успешного завершения аттестационных мероприятий.

Литература: [1, с. 12–34], [3, с. 91–102], [4, с. 100–145].

Контрольные вопросы

1. Этапы, которые включены в планирование предаттестационных мероприятий по подготовке объекта к аттестации.

2. Роль ответственных лиц в проведении предаттестационных мероприятий, и как обязанности распределяются между специалистами.

3. Процедура первичного аудита и анализа соответствия объекта ГИС требованиям информационной безопасности.

4. Методы выявления слабых мест и потенциальных рисков в рамках предаттестационной подготовки объектов ГИС.

5. Данные, необходимые для успешного проведения аттестации, и их роль в подготовительном процессе проведения предаттестационных мероприятий объектов ГИС.

6. Виды документации, подготавливаемой в процессе предаттестационных мероприятий и требования к их оформлению.

3.3 Раздел 3. Порядок проведения аттестации объектов информатизации

Перечень изучаемых вопросов

1. Цели и задачи аттестации: основные цели проведения аттестации и задачи, решаемые в рамках обеспечения информационной безопасности.

2. Этапы аттестации: последовательность этапов аттестации, включая подготовительный, основной и заключительный этапы.

3. Проведение предварительного анализа: подготовка объекта и оценка его исходного состояния с точки зрения соответствия требованиям безопасности.

4. Проверка на соответствие требованиям: методы и инструменты, используемые для проверки защищенности государственных информационных систем.

5. Оформление результатов аттестации: требования к составлению отчетов, актов и другой документации по итогам аттестации.

6. Контроль соответствия нормативным требованиям: проверка объекта на соответствие нормативной и правовой базе, регулирующей информационную безопасность.

7. Рекомендации по устранению несоответствий: разработка корректирующих мер для повышения уровня защищенности объектов.

8. Взаимодействие с надзорными органами: порядок взаимодействия с уполномоченными органами при проведении аттестации.

Методические указания к изучению

Порядок проведения аттестации объектов государственных информационных систем включает определение целей и задач аттестации, направленных на обеспечение информационной безопасности, а также последовательное выполнение этапов: подготовительного, основного и заключительного. Предварительный анализ предполагает подготовку объекта и оценку его исходного состояния на соответствие требованиям безопасности,

после чего проводится проверка защищенности с использованием различных методов и инструментов. Оформление результатов аттестации включает составление отчетов, актов и другой документации, которые отражают итоги выполненных мероприятий. Контроль соответствия нормативной и правовой базе играет ключевую роль в подтверждении уровня защищенности объекта, а рекомендации по устранению несоответствий способствуют его улучшению. Взаимодействие с надзорными органами обеспечивает соблюдение всех процедур и требований, предусмотренных законодательством.

Литература: [1, с. 12–34], [2, с. 23- 66] [3, с. 91–102], [4, с. 100–150].

Контрольные вопросы

1. Основные цели и задачи проведения аттестации объектов государственных информационных систем.
2. Этапы, которые включает порядок проведения аттестации, и как они последовательно выполняются.
3. Предварительный анализ объекта перед аттестацией и аспекты оцениваются для оценивания.
4. Методы и инструменты, используемые для проверки защищенности государственных информационных систем.
5. Виды документации, которые необходимо оформить по итогам аттестации, и каковы требования к их содержанию.
6. Правила и этапы осуществления взаимодействие с надзорными органами в процессе проведения аттестации.

4. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПОДГОТОВКЕ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Практические занятия направлены на углубление знаний и закрепление основных понятий и методов, изучаемых в рамках дисциплины. Основная цель занятий – научиться применять теоретические знания для решения прикладных задач.

Рекомендации к подготовке

1. *Изучение лекционного материала и конспектов*:

– перед лабораторными занятиями необходимо проработать соответствующие разделы лекционного материала;

– рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом лабораторного занятия.

2. *Проработка учебной литературы:*

– используйте основные учебники и методические пособия, рекомендованные преподавателем;

– для глубокого понимания теории рекомендуется обращаться к дополнительной литературе.

3. Решение типовых задач:

– проработать примеры и типовые задачи из учебных материалов, методических указаний;

– выполните задачи, предложенные преподавателем для самостоятельной работы, что обеспечит лучшее понимание методов и подходов к решению задач.

4. Подготовка вопросов:

– составьте список вопросов по материалу, вызвавшему затруднения;

– обсуждение этих вопросов на лабораторном занятии поможет устранить пробелы в знаниях.

5. Вопросы для самоконтроля:

– перед каждым занятием рекомендуется проверять себя с помощью вопросов для самоконтроля из методических указаний к лекционным занятиям. Это позволит оценить уровень своей подготовки.

Тематический план практических занятий приводится в разделе «Тематический план».

Подробная информация по выполнению практических работ и рекомендуемая литература приведены в УМП по выполнению практических работ по дисциплине «Аттестация по информационной безопасности объектов ГИС».

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО САМОСТОЯТЕЛЬНОЙ РАБОТЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);
- воспитывающая (формируются и развиваются профессиональные качества специалиста);
- исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

– изучить рекомендуемые литературные источники:

– изучить основные понятия, представленные в глоссарии;

– ответить на контрольные вопросы:

– решить предложенные задачи, кейсы, ситуации;

– выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам:
2. Выполнение письменных контрольных и курсовых работ;
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов:
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) – важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых проектов и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (мини кейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с рабочей программой учебной дисциплины. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента не регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

Для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet.

Для закрепления и систематизации знании:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника,

дополнительной литературы, аудиовидеозаписей):

- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена.

Для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений:
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;
- проектирование и моделирование разных видов и компонентов профессиональной деятельности;
- создание проспектов, проектов, моделей;
- экспериментальная работа, участие в НИР;
- рефлексивный анализ профессиональных умений с использованием аудиовидеотехники и компьютерных расчетных программ, и электронных практикумов;
- подготовка курсовых проектов и дипломных работ.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

Вопросы и задачи для самопроверки:

1. Законодательные акты и нормативные документы, регулирующие процесс аттестации объектов ГИС по требованиям безопасности.
2. Основные элементы, входящие в структуру системы аттестации объектов ГИС.
3. Основные этапы проведения аттестации объектов ГИС по требованиям безопасности и их последовательность.
4. Требования к защите информации в государственных информационных системах.
5. Инструменты и методы для выявления уязвимостей в государственных информационных системах.
6. Потенциальные угрозы безопасности информации, актуальные при проведении аттестации объектов ГИС.

7. Этапы, которые включены в планирование предаттестационных мероприятий по подготовке объекта к аттестации.

8. Роль ответственных лиц в проведении предаттестационных мероприятий, и как обязанности распределяются между специалистами.

9. Процедура первичного аудита и анализа соответствия объекта ГИС требованиям информационной безопасности.

10. Методы выявления слабых мест и потенциальных рисков в рамках предаттестационной подготовки объектов ГИС.

11. Данные, необходимые для успешного проведения аттестации, и их роль в подготовительном процессе проведения предаттестационных мероприятий объектов ГИС.

12. Виды документации, подготавливаемой в процессе предаттестационных мероприятий и требования к их оформлению.

13. Основные цели и задачи проведения аттестации объектов государственных информационных систем.

14. Этапы, которые включает порядок проведения аттестации, и как они последовательно выполняются.

15. Предварительный анализ объекта перед аттестацией и аспекты оцениваются для оценивания.

16. Методы и инструменты, используемые для проверки защищенности государственных информационных систем.

17. Виды документации, которые необходимо оформить по итогам аттестации, и каковы требования к их содержанию.

18. Правила и этапы осуществления взаимодействие с надзорными органами в процессе проведения аттестации.

6. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

6.1. Текущая аттестация

В ходе изучения дисциплины студентам предстоит пройти следующие этапы текущей аттестации: контроль самостоятельной работы по темам дисциплины, контроль выполнения лабораторных работ, К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

– зачетные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов.

6.1.1 Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-

балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетво-рительно»	«удовлетво-рительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
1 . Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2. Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпрети-ровать и систематизир овать необходимую информацию в рамках поставленно й задачи	Может найти, систематизи-ровать необходимую информацию, а также выявить новые, дополнитель-ные источники информации в рамках поставленной задачи
3. Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений,	В состоянии осуществлять научно-корректный анализ предоставленн	В состоянии осуществ-лять системати-ческий и научно-	В состоянии осуществлять системати-ческий и научно-корректный

Система оценок / Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлетво-рительно»	«удовлетво-рительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
	в состоянии проанализировать только некоторые из имеющихся у него сведений	ой информации	корректный анализ предостав-ленной информации, вовлекает в исследование новые релевантные задаче данные	анализ предостав-ленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4. Освоение стандартных алгоритмов решения профес-сиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставлен-ные задачи в соответствии с заданным алгоритмом, понимает основы предложен-ного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

6.1.2 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

6.1.3 Условия получения положительной оценки:

Завершающим этапом изучения дисциплины является промежуточная аттестация, представляющая собой зачет.

Тестовые задания для проведения зачетного тестирования приведены в фонде оценочных средств по дисциплине.

Допуск к итоговой аттестации возможен при:

– всех выполненных, сданных (проверенных, защищенных) практических работах, наличии отчётов по ним;

– наличии показателей приемлемого уровня освоения материалов курса: более 50 % посещений от общего числа требуемых по учебному плану.

Зачет может проводиться как в традиционной форме, так и в виде экзаменационного тестирования. Тестовые задания для проведения экзаменационного тестирования приведены в фонде оценочных средств по дисциплине.

6.2. Примерные вопросы к зачету по дисциплине

1. Законодательные акты, регулирующие аттестацию объектов ГИС
2. Основные элементы системы аттестации объектов ГИС
3. Этапы проведения аттестации объектов государственных информационных систем по требованиям безопасности
4. Задачи предаттестационных мероприятий объектов ГИС, проводимых заявителем
5. Методы проверки соответствия объектов ГИС требованиям безопасности информации
6. Проведение первичного аудита объекта ГИС по требованиям безопасности
7. Анализ угроз и оценка рисков безопасности информации ГИС
8. Формирование отчетной документации по итогам аттестации
9. Взаимодействие с надзорными органами при проведении аттестации объектов ГИС
10. Разработка корректирующих мер при обнаружении несоответствий
11. Требования к защите информации в государственных информационных системах
12. Контроль соответствия объекта ГИС нормативной базе
13. Организация проведения предаттестационных мероприятий объектов государственных информационных систем по требованиям безопасности
14. Процедура тестирования защищенности системы
15. Аттестация объектов ГИС, обрабатывающих персональные данные
16. Структура взаимодействия участников процесса аттестации ГИС
17. Роль ответственных лиц при подготовке к аттестации

18. Порядок оформления технической документации
19. Методы выявления уязвимостей в информационных системах
20. Требования к документам по результатам аттестации
21. Цели аттестации объектов государственных информационных систем
22. Нормативные требования к защите информации ГИС
23. Проверка эффективности защитных мер
24. Этапы проведения предварительного анализа объекта
25. Условия успешного выполнения предаттестационной подготовки
26. Оценка исходного состояния объекта
27. Организация группы специалистов для аттестации
28. Рекомендации по устранению угроз безопасности
29. Формирование плана мероприятий по аттестации
30. Разработка мер повышения защищенности объекта
31. Документы, предоставляемые в надзорные органы
32. Анализ рисков утечки информации
33. Составление акта соответствия требованиям безопасности
34. Требования к итоговым отчетам по аттестации ГИС

7. ЗАКЛЮЧЕНИЕ

В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешением их как непосредственно в ходе занятий, так и в ходе самостоятельной работы. Реализация программы предполагает использование интерактивных форм проведения лабораторных занятий. Проведение практических занятий подразумевает обучение, построенное на групповой совместной деятельности студентов, в том числе с использованием персонального компьютера.

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно, ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

– развивающая (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);

– информационно-обучающая (учебная деятельность студентов на аудиторных занятиях, не подкрепленная самостоятельной работой, становится малорезультативной);

– ориентирующая и стимулирующая (процессу обучения придается профессиональное ускорение);

– воспитывающая (формируются и развиваются профессиональные качества специалиста);

– исследовательская (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводится с целью:

– систематизации и закрепления полученных теоретических знаний и практических умений студентов;

– углубления и расширения теоретических знаний;

– формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;

– развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;

– формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;

– развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

– изучить рекомендуемые литературные источники:

– изучить основные понятия, представленные в глоссарии;

– ответить на контрольные вопросы.

Работа студентов в основном складывается из следующих элементов:

– изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам;

– подготовка и сдача итогового зачета.

8. СПИСОК ЛИТЕРАТУРЫ

1. Сертификация средств защиты информации: учеб. пособие / А. А. Миняев, Д. В. Юркин, М. М. Ковцур, К. А. Ахрамееева. – Санкт-Петербург: СПбГУТ им. М. А. Бонч-Бруевича, 2020. – 88 с. – ISBN 978-5-89160-213-7. – Текст: электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/180100 (дата обращения: 07.06.2024). – Режим доступа: для авториз. пользователей.

2. Тумбинская, М. В. Защита информации на предприятии: учеб. пособие / М. В. Тумбинская, М. В. Петровский. – Санкт-Петербург: Лань, 2020. – 184 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/130184 (дата обращения: 08.10.2024). – ISBN 978-5-8114-4291-1. – Текст : электронный

3. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии: учебник / М. В. Тумбинская, М. В. Петровский. – Санкт-Петербург: Лань, 2022. – 344 с. – Режим доступа: для авториз. Пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/207095 (дата обращения: 08.10.2024). – ISBN 978-5-8114-3940-9. — Текст : электронный.

Дополнительная литература

4. Иванов, А. В. Оценка защищенности информации от утечки по каналам побочных электромагнитных излучений и наводок: учеб. пособие / А. В. Иванов. – Новосибирск: Новосибирский государственный технический университет, 2018. – 64 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=575420 (дата обращения: 07.06. 2024). – Библиогр. в кн. – ISBN 978-5-7782-3713-1. – Текст: электронный

5. Цветкова, Е. М. Технический контроль и информационная защита: учеб. пособие / Е. М. Цветкова, И. О. Танрывердиев; Поволжский государственный технологический университет. – Йошкар-Ола: Поволжский государственный технологический университет, 2019. – 64 с.: ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=612595 (дата обращения:07.06. 2024). – Библиогр. в кн. – ISBN 978-5-8158-2145-3. – Текст: электронный.

6. Свешников, И. В. Основы информационной безопасности телекоммуникационных систем: учеб. пособие / И. В. Свешников, В. В. Савватеев. – Чита: ЗабГУ, 2022. – 230 с. – ISBN 978-5-9293-3034-6. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/363503 (дата обращения: 08.06.2024). – Режим доступа: для авториз. пользователей.

7. Раханов, К. Я. Обеспечение конфиденциальности информации в сети Интернет: учеб. пособие / К. Я. Раханов, Н. А. Раханова. – Новополоцк: ПГУ, 2021. – 192 с. – ISBN 978-985-531-723-5. – Текст: электронный // Лань:

электронно-библиотечная система. – URL: https://e.lanbook.com/book/366821 (дата обращения: 08.06.2024). – Режим доступа: для авториз. пользователей.

8. Кухарский, А. Н. Информационная безопасность политического процесса в системе государственного и муниципального управления: монография / А. Н. Кухарский. – Чита: ЗабГУ, 2021. – 260 с. – ISBN 978-5-9293-2742-1. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/271505 (дата обращения: 08.06.2024). – Режим доступа: для авториз. пользователей.

Периодические издания

9. «Безопасность информационных технологий», «Информационно-управляющие системы», «Гражданская защита», «Морские интеллектуальные технологии».

Учебно-методические пособия, нормативная литература

10. Жестовский, А. Г. Программно-аппаратные средства обеспечения информационной безопасности: учеб. пособие для студентов высш. учеб. заведений, обучающихся по направлению «Информ. безопасность», по прогр. подгот. бакалавров, магистров, специалистов / А. Г. Жестовский, В. В. Подтопельный; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2018. – Текст : непосредственный. Ч. 2 : Настройка систем защиты информации от несанкционированного доступа. – 2018. – 100 с. – ISBN 978-5-7481- 0389-3.

11. Булычёв, Г. Г. Программно-аппаратные средства защиты информации: учеб.-метод. пособие / Г. Г. Булычёв. – Москва: РТУ МИРЭА, 2022. – Ч. 1. – 2022. – 203 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/310781 (дата обращения: 09.12.2024). – ISBN 978-5-7339-1652-1. – Текст : электронный.

12. Булычёв, Г. Г. Программно-аппаратные средства защиты информации: учеб.-метод. пособие / Г. Г. Булычёв. – Москва: РТУ МИРЭА, 2022. – Ч. 2. – 2022. – 177 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/310784 (дата обращения: 09.12.2024). – ISBN 978-5-7339-1653-8. – Текст : электронный.

13. «ГОСТ Р ИСО/МЭК 27000-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» (утв. и введен в действие Приказом Росстандарта от 19.05.2021 N 392-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

14. «ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» (утв. и введен в действие Приказом Росстандарта от 30.11.2021 N

1653-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

15. «ГОСТ Р ИСО/МЭК 27002-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности» (утв. и введен в действие Приказом Росстандарта от 20.05.2021 N 416-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

16. «ГОСТ Р ИСО/МЭК 27003-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации» (утв. и введен в действие Приказом Росстандарта от 19.05.2021 N 387-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

17. «ГОСТ Р ИСО/МЭК 27005-2010. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (утв. и введен в действие Приказом Росстандарта от 30.11.2010 N 632-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

18. «ГОСТ Р ИСО/МЭК 27007-2014. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности» (утв. и введен в действие Приказом Росстандарта от 11.06.2014 N 563-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

19. «ГОСТ Р ИСО/МЭК 18045-2013. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий» (утв. и введен в действие Приказом Росстандарта от 28.08.2013 N 624-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

20. «ГОСТ Р ИСО 22301-2021. Национальный стандарт Российской Федерации. Надежность в технике. Системы менеджмента непрерывности деятельности. Требования» (утв. и введен в действие Приказом Росстандарта от 05.10.2021 N 1059-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

21. «ГОСТ Р ИСО/МЭК 13335-1-2006. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (утв. и введен в действие Приказом Ростехрегулирования от 19.12.2006 N317-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

22. «ГОСТ Р 55.0.02-2014/ИСО 55001:2014. Национальный стандарт Российской Федерации. Управление активами. Национальная система стандартов. Системы менеджмента. Требования» (утв. и введен в действие Приказом Росстандарта от 25.12.2014 N 2139-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный. 1.

23. Приказ ФСТЭК России от 11.02.2013 N 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (Зарегистрировано в Минюсте России 31.05.2013 N 28608) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

Локальный электронный методический материал

Алина Андреевна Бабаева

АТТЕСТАЦИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЬЕКТОВ ГИС

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 2,1. Печ. л. 1,7.

Издательство федерального государственного бюджетного
образовательного учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1