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

А. А. Бабаева

ЗАЩИТА ИНФОРМАЦИИ В 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,
доцент кафедры информационной безопасности
ФГБОУ ВО «Калининградский государственный технический университет»
Н. Я. Великите

Бабаева, А. А.
Защита информации в 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. – 35 с.

Учебно-методическое пособие является руководством по изучению дисциплины «Защита информации в ГИС» студентами специалитета по специальности 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, оценки угроз в 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 по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем», изучающих дисциплину «Защита информации в ГИС».

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

Цель освоения дисциплины: изучение особенностей функционирования ГИС и системы защиты в них. Получение знаний и навыков в области анализа угроз информационной безопасности в ГИС.

В курсе студенты изучают основные информационные технологии, используемые в ГИС, способы и средства защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации, основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации, особенности создания и эксплуатации систем защиты информации в ГИС, нормативно- правовую базу в области защиты информации для ГИС, руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации.

Получают практические навыки в умении определять комплекс мер для обеспечения безопасности информационной в ГИС, выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и ГИС, разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем и ГИС, проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в составе ГИС с целью обеспечения требуемого уровня защищенности автоматизированной системы, определять эффективность применения средств информатизации.

Получают практические навыки в умении владеть навыками проведения оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах и ГИС, проведения технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы.

В результате освоения дисциплины обучающийся должен:

знать:

– основные информационные технологии, используемые в автоматизированных системах;

– способы и средства защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации.

– основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации

– особенности создания и эксплуатации систем защиты информации в ГИС

– нормативно- правовую базу в области защиты информации для ГИС

– руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;

уметь:

– определять комплекс мер для обеспечения безопасности информационной в автоматизированных системах;

– выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и ГИС;

– разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем и ГИС;

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

– определять эффективность применения средств информатизации;

владеть:

– навыками проведения оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах и ГИС;

– навыками проведения технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы;

– навыками разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах.

Задачи дисциплины:

– изучение основных информационные технологии, используемые в ГИС;

– изучение способов и средств защиты информации от несанкционированного доступа и утечки по техническим каналам и контроля эффективности защиты информации;

– изучение основных средств и способов обеспечения безопасности информации, принципов построения систем защиты информации, особенностей создания и эксплуатации систем защиты информации в ГИС;

– изучение руководящих и методических документов уполномоченных федеральных органов исполнительной власти по защите информации;

– формирование умений определять комплекс мер для обеспечения безопасности информационной в ГИС, выявлять уязвимости информационно-технологических ресурсов автоматизированных систем и ГИС, разрабатывать предложения по совершенствованию системы управления защиты информации автоматизированных систем и ГИС, проводить выбор программно-аппаратных средств обеспечения безопасности информации для использования их в

составе ГИС с целью обеспечения требуемого уровня защищенности автоматизированной системы;

– формирование умений определять эффективность применения средств информатизации, проведение оценки показателей качества и эффективности работы вычислительных систем, программных и программно-аппаратных средств, используемых для построения систем защиты информации в автоматизированных системах и ГИС, проведения технико-экономической оценки целесообразности создания системы защиты информации автоматизированной системы;

– формирование умений разработки предложений по совершенствованию системы управления безопасностью информации в автоматизированных системах и ГИС.

Дисциплина «Защита информации в ГИС» относится к Модулю 1 «Информационная безопасность государственных информационных систем (ГИС)» части, формируемой участниками образовательных отношений специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем».

Основными видами аудиторных учебных занятий по дисциплине являются лекции и практические 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 – экзамену.

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.Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription (срок действия: три года).

2. ТЕМАТИЧЕСКИЙ ПЛАН

2.1. Очная форма обучения

	Раздел (модуль) дисциплины	Тема	Объем контакт-ной работы, ч	Объем самос-тоятельной работы, ч
		Теоретическое обучение (лекции) Весенний семестр (А)		
1	Раздел 1 Защита информации в ГИС	Тема 1. Виды информационных систем. Особенности функционирования ГИС	4	10
2		Тема 2. Особенности обеспечения защиты информации в ГИС. Введение в проблему информационной безопасности	4	10
3		Тема 3 Основные понятия защиты информации	10	10
4		Тема 4. Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности	10	10
5		Тема 5. Угрозы информационной безопасности. Подходы к построению систем защиты информации	4	10
			32	**50**
		Практические (лабораторные занятия)		
1	Раздел 1 Защита информации в ГИС	Анализ структуры и архитектуры выбранного объекта ГИС	8	10
2		Оценка исходной защищенности объекта	8	10
3		Анализ актуальных уязвимостей и каналов НСД	8	5
4		Анализ актуальных угроз и нарушителей	8	5
5		Подбор мер и средств для повышения уровня защищенности	6	10
6		Оценка эффективности предложенных решений	10	2
			48	**42**

	Раздел (модуль) дисциплины	Тема	Объем контакт-ной работы, ч	Объем самос-тоятельной работы, ч
		Рубежный (текущий) и итоговый контроль		
2.1	РЭ, КА		8	1,25
	Итоговый контроль (экзамен)			34,75
			0	**34,75**

Всего	88	128
	ИТОГО	216

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1. Раздел 1 Защита информации в ГИС

3.1.1 Тема 1 Виды информационных систем. Особенности функционирования ГИС

Перечень изучаемых вопросов:

– Определение и классификация видов информационных систем:

Информационные системы можно определить, как совокупность технических, программных, информационных и организационных средств, направленных на сбор, обработку, хранение, передачу и использование информации. Классификация таких систем осуществляется по различным критериям, включая назначение, область применения, способ обработки данных, архитектуру и уровень автоматизации. Например, выделяются операционные, аналитические, управленческие и другие информационные системы. В рамках курса уделяется внимание пониманию различных видов систем для определения их особенностей и специфических требований к защите данных.

– Особенности функционирования автоматизированных информационных систем:

Автоматизированные информационные системы представляют собой системы, в которых часть функций по обработке и управлению информацией выполняется с использованием программного обеспечения и вычислительных ресурсов. Они позволяют минимизировать человеческий фактор, повысить точность обработки данных и ускорить выполнение процессов. Особенности таких систем включают использование алгоритмов для автоматизации рутинных задач, интеграцию с другими системами, поддержку сложных вычислений и способность работать с большими объемами информации. Однако их функционирование также связано с определенными рисками, такими как возможность несанкционированного доступа и зависимость от технологических ресурсов.

– Роль и задачи государственных информационных систем в обеспечении государственных функций:

Государственные информационные системы играют ключевую роль в выполнении задач государственных органов, обеспечивая эффективное управление процессами и взаимодействие с гражданами. Они предназначены для обработки и хранения информации, связанной с деятельностью государственных учреждений, включая персональные данные, финансовые отчеты, документы и другую критически важную информацию. Их задачи включают повышение прозрачности работы государственных органов, упрощение предоставления услуг населению и обеспечение оперативного принятия решений на основе актуальных данных.

– Основные отличия государственных информационных систем от других видов систем:

– Государственные информационные системы отличаются рядом уникальных характеристик. Во-первых, они подчиняются строгим требованиям

по безопасности и нормативному регулированию, так как обрабатывают конфиденциальную и государственную информацию. Во-вторых, их использование затрагивает широкий круг пользователей, включая граждан, органы власти и бизнес-структуры. Эти системы ориентированы на масштабные и социально значимые процессы, что накладывает дополнительные требования к их надежности, доступности и защите от киберугроз.

– Примеры и типология государственных информационных систем:

1. Государственные информационные системы (ГИС) представляют собой комплекс программно-технических средств, предназначенных для автоматизации и повышения эффективности работы органов государственной власти. Эти системы классифицируются по различным критериям, включая назначение, функциональные возможности, масштабы применения, архитектуру и уровень интеграции.

Типология государственных информационных систем:

1. **По назначению и функциональности**:

- **Системы управления государственными ресурсами**: предназначены для учета, распределения и контроля государственных активов и ресурсов. Примером могут служить системы учета бюджетных средств, управления государственным имуществом.
- **Системы электронного документооборота**: используются для автоматизации документооборота, согласования и хранения документации. Пример – система «МЭДО» (Межведомственный Электронный Документооборот).
- **Системы оказания государственных услуг**: направлены на упрощение взаимодействия граждан и государства через предоставление услуг в электронном виде. Пример – порталы «Госуслуги».
- **Системы обеспечения национальной безопасности**: разработаны для контроля и защиты данных, связанных с национальной безопасностью, включая разведывательные и оборонные системы.

2. **По масштабу применения**:

- **Федеральные информационные системы**: охватывают деятельность на уровне всей страны. Пример – система управления государственными финансами (Федеральное казначейство).
- **Региональные информационные системы**: предназначены для решения задач в определенном регионе. Например, информационные системы здравоохранения, работающие в границах субъекта РФ.
- **Муниципальные информационные системы**: ориентированы на решение задач местного самоуправления, таких как управление коммунальными услугами и жилищным фондом.

3. **По архитектурным особенностям**:

- **Централизованные системы**: вся информация хранится и обрабатывается на одном сервере или в единой инфраструктуре. Пример – Единая государственная система миграционного учета.

- **Распределенные системы**: данные хранятся и обрабатываются на нескольких серверах, связанных между собой, обеспечивая большую гибкость и устойчивость.

4. **По уровню интеграции**:

- **Автономные системы**: функционируют независимо и не требуют взаимодействия с другими информационными системами.
- **Интегрированные системы**: могут взаимодействовать с другими государственными или частными системами для обмена данными. Например, взаимодействие налоговых систем с банковскими.

Государственные информационные системы играют важнейшую роль в обеспечении эффективного функционирования органов власти, позволяя упорядочивать процессы управления и взаимодействие с населением. Они предназначены для сбора, обработки и хранения данных, связанных с деятельностью государственных структур, включая сведения о гражданах, финансовую отчетность, служебную документацию и другие критически важные информационные ресурсы. Их основная цель – сделать деятельность государственных органов более прозрачной, облегчить предоставление услуг населению и повысить оперативность принятия решений на основе актуальной информации.

Ключевые особенности государственных информационных систем: Государственные информационные системы обладают рядом уникальных свойств, отличающих их от других информационных платформ. Во-первых, они строго соответствуют требованиям информационной безопасности и регулируются законодательными нормами, поскольку работают с конфиденциальными и государственными данными. Во-вторых, их аудитория охватывает широкий спектр пользователей – от граждан и представителей власти до бизнес-сообщества. Такие системы предназначены для управления сложными социально значимыми процессами, что требует высокой надежности, стабильности работы и защиты от возможных киберугроз.

Методические указания к изучению

Структура для изучения раздела «Виды информационных систем. Особенности функционирования Государственных информационных систем» включает рассмотрение ключевых аспектов, таких как определение и классификация видов информационных систем, где анализируются их характеристики и принципы работы. Особое внимание уделяется изучению автоматизированных информационных систем, их особенностей и влияния на эффективность обработки данных. Исследуется роль государственных информационных систем в реализации задач государственных органов, их уникальные функции и значимость для обеспечения государственных нужд. Кроме того, рассматриваются отличия государственных информационных систем от других видов, включая требования к безопасности, масштаб применения и социальную значимость. Такая структура позволяет глубже

понять специфику функционирования и защиты данных в контексте государственных информационных систем.

Литература: [1, с. 48–72], [2, с. 120–167].

Контрольные вопросы

1. Какие критерии используются для классификации информационных систем, и какие основные виды информационных систем можно выделить?
2. Какие особенности функционирования автоматизированных информационных систем влияют на их эффективность и безопасность?
3. Какую роль выполняют государственные информационные системы в обеспечении выполнения функций государственных органов?
4. Какие уникальные характеристики отличают государственные информационные системы от других видов информационных систем?
5. Какие требования предъявляются к защите информации в государственных информационных системах?
6. Как структурная архитектура государственных информационных систем обеспечивает их функционирование и взаимодействие компонентов?
7. Какие топологии ГИС бывают?

3.1.2 Тема 2 Особенности обеспечения защиты информации в ГИС. Введение в проблему информационной безопасности

Перечень изучаемых вопросов

1. Требования к защите информации в государственных информационных системах:

Защита информации в государственных информационных системах регулируется законодательными и нормативными актами, включая требования к конфиденциальности, целостности, доступности и защищенности данных. Главные цели – предотвращение несанкционированного доступа, утечек, модификации или уничтожения данных, а также обеспечение защиты персональной и государственной информации. Требования к защите включают применение сертифицированных средств защиты информации, разработку и внедрение политики информационной безопасности, создание резервных копий данных, использование систем контроля доступа и шифрование информации. Особое внимание уделяется защите информации от киберугроз и соблюдению стандартов, таких как ГОСТы и международные рекомендации.

2. Структура и архитектура государственных информационных систем:

Структура государственных информационных систем представляет собой совокупность взаимосвязанных компонентов, включая аппаратное обеспечение, программные средства, базы данных и каналы связи. Архитектура таких систем зависит от их функциональных задач и может быть централизованной, распределенной или гибридной. Централизованная архитектура предполагает хранение всех данных в едином хранилище, что упрощает управление, но

требует высокой защищенности. Распределенная архитектура базируется на сети узлов, что повышает устойчивость системы, но усложняет управление. Государственные системы часто используют модульный подход, где каждая компонента выполняет свою задачу, что упрощает масштабирование и модернизацию системы.

3. Основные принципы взаимодействия между компонентами информационных систем:

Взаимодействие между компонентами информационных систем обеспечивается интеграцией программных и аппаратных средств через стандартизированные протоколы связи. Основные принципы включают согласованность данных, поддержку взаимодействия в режиме реального времени, надежность и отказоустойчивость. Также важна безопасность взаимодействия – обмен данными происходит с использованием защищенных каналов, а компоненты системы проверяются на подлинность. Важной задачей является обеспечение совместимости между различными компонентами, особенно в системах, интегрирующих несколько информационных платформ и технологий.

4. Уязвимости и риски, связанные с использованием государственных информационных систем.

Государственные информационные системы подвержены ряду уязвимостей и рисков, связанных как с внутренними, так и с внешними угрозами. К внутренним рискам относятся ошибки конфигурации, недостаточная квалификация персонала, несоответствие технических средств требованиям безопасности. Внешние угрозы включают кибератаки, вирусы, попытки несанкционированного доступа. Также риски могут быть связаны с использованием устаревших технологий и недостаточной защитой каналов связи. Устранение уязвимостей требует регулярных проверок, обновления программного обеспечения, обучения персонала и внедрения современных средств защиты информации.

5. Организация контроля и мониторинга функционирования государственных информационных систем:

Контроль и мониторинг работы государственных информационных систем обеспечивают их стабильное функционирование и своевременное реагирование на возникающие угрозы. Контроль включает проверку соответствия системы нормативным требованиям, оценку эффективности защитных мер, анализ логов и данных о работе системы. Мониторинг осуществляется с использованием автоматизированных систем, способных отслеживать состояние сети, выявлять подозрительную активность и предупреждать о возможных атаках. Организация мониторинга включает разработку политики мониторинга, использование специализированного программного обеспечения и обучение специалистов, ответственных за процесс контроля.

Структура государственных информационных систем представляет собой совокупность взаимосвязанных элементов, включая оборудование, программное обеспечение, базы данных и каналы передачи данных. Архитектура таких систем

определяется их функциональными возможностями и может быть централизованной, распределенной или комбинированной.

Централизованный вариант предполагает хранение всей информации в едином хранилище, что облегчает администрирование, но требует усиленной защиты. Распределенная архитектура строится на сети взаимосвязанных узлов, обеспечивая устойчивость, но усложняя процессы управления.

Государственные системы нередко применяют модульный принцип, при котором каждая часть выполняет конкретную задачу, что способствует удобному масштабированию и модернизации инфраструктуры.

Методические указания к изучению

Структура для изучения включает рассмотрение требований к защите информации в государственных информационных системах, включая нормативные стандарты и методы обеспечения конфиденциальности, целостности и доступности данных. Анализируется структура и архитектура таких систем, их основные компоненты и особенности построения (централизованная, распределенная или модульная архитектура). Важное место занимает изучение принципов взаимодействия между компонентами информационных систем, где внимание уделяется интеграции, совместимости и безопасности обмена данными. Также рассматриваются уязвимости и риски, связанные с использованием государственных информационных систем, включая как внутренние, так и внешние угрозы. Завершается изучение темой организации контроля и мониторинга функционирования государственных информационных систем, включая методы оценки эффективности защитных мер, анализ логов и использование систем автоматизированного мониторинга для обеспечения устойчивости и предотвращения угроз. Эта структура помогает сформировать целостное понимание защиты и функционирования данных систем.

Литература: [1, с. 20–45], [2, с. 38–49], [3, с. 40–49].

Контрольные вопросы

1. Какие нормативные требования и методы используются для обеспечения конфиденциальности, целостности и доступности данных в государственных информационных системах?
2. Какова структура и архитектура государственных информационных систем, и какие типы архитектуры наиболее часто применяются?
3. Какие принципы обеспечивают эффективное и безопасное взаимодействие между компонентами информационных систем?
4. Какие внутренние и внешние уязвимости могут возникать при использовании государственных информационных систем, и как можно минимизировать связанные с ними риски?
5. Какие методы контроля и мониторинга функционирования государственных информационных систем применяются для своевременного обнаружения угроз и обеспечения их устойчивости?

6. Как использование систем автоматизированного мониторинга помогает предотвращать угрозы и оптимизировать работу государственных информационных систем?

3.1.3 Тема 3 Основные понятия защиты информации

Перечень изучаемых вопросов

1. Понятие и цели защиты информации в государственных информационных системах.

2. Основные свойства информации: конфиденциальность, целостность, доступность.

3. Виды информации, подлежащей защите в государственных системах.

4. Угрозы и риски для информации в государственных информационных системах.

5. Методы и средства защиты информации: организационные, технические, программные.

Методические указания к изучению

Структура для изучения темы «Основные понятия защиты информации» в рамках дисциплины «Защита информации в государственных информационных системах» включает рассмотрение понятия и целей защиты информации, с акцентом на ее ключевые свойства: конфиденциальность, целостность и доступность. Также изучается классификация видов информации, подлежащей защите, и их особенности в государственных системах. Особое внимание уделяется анализу угроз и рисков, связанных с информацией, обрабатываемой в государственных системах, а также методам и средствам защиты, включая организационные, технические и программные меры. Изучение нормативных и правовых документов, регулирующих защиту информации, дополняется анализом этапов реализации мер безопасности. Завершается структура изучением современных технологий и подходов к защите информации, что позволяет сформировать полное представление о данной теме.

Литература: [1, с. 70–81], [2, с. 45–51], [3, с. 10–41].

Контрольные вопросы

1. Каковы основные цели защиты информации в государственных информационных системах, и какие ключевые свойства информации необходимо обеспечивать?

2. Какие виды информации подлежат обязательной защите в государственных информационных системах, и как они классифицируются?

3. Какие основные угрозы и риски характерны для информации, обрабатываемой в государственных информационных системах?

4. Какие организационные, технические и программные методы используются для защиты информации в государственных информационных системах?

5. Каковы основные этапы реализации мер по защите информации в государственных информационных системах?

3.1.4 Тема 4 Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности

Перечень изучаемых вопросов

1. Основные законодательные акты Российской Федерации в области информационной безопасности.

2. Федеральные законы о защите информации и персональных данных.

3. Положение о защите государственной тайны и регулирование доступа к секретной информации.

4. Основные требования нормативных документов к безопасности информации в государственных информационных системах.

5. Государственные стандарты (ГОСТы), регулирующие вопросы информационной безопасности.

6. Порядок сертификации и лицензирования средств защиты информации.

7. Обязанности субъектов при выполнении требований законодательства о защите информации.

8. Правовые последствия нарушения требований информационной безопасности.

9. Организация взаимодействия с надзорными органами и выполнение их предписаний.

Методические указания к изучению

Структура для изучения темы «Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности» включает рассмотрение основных законодательных актов Российской Федерации, регулирующих защиту информации, включая законы о защите персональных данных и государственной тайны. Изучаются требования нормативных документов к информационной безопасности в государственных системах, а также государственные стандарты (ГОСТы) и международные стандарты, такие как ISO/IEC 27001 и ISO/IEC 27002. Важное внимание уделяется порядку сертификации и лицензирования средств защиты информации, обязанностям субъектов при выполнении требований законодательства, а также правовым последствиям за их нарушение. Завершается изучение анализом взаимодействия с надзорными органами, выполнения их предписаний и роли стандартов в организации эффективной системы защиты информации. Такой подход обеспечивает комплексное понимание законодательной и нормативной базы информационной безопасности.

Литература: [1, с. 30–62], [3, с. 90–102], [4, с. 100–156].

Контрольные вопросы

1. Какие основные законодательные акты Российской Федерации регулируют защиту информации, и каковы их ключевые положения?
2. Какие требования к защите персональных данных устанавливаются Федеральным законом «О персональных данных»?
3. Какие государственные стандарты (ГОСТы) и международные стандарты применяются в области информационной безопасности, и в чем их основные отличия?
4. Как организован порядок сертификации и лицензирования средств защиты информации, и какие требования предъявляются к этим процессам?
5. Какие обязанности возлагаются на субъекты при соблюдении законодательства о защите информации в государственных информационных системах?
6. Какие правовые последствия возникают в случае нарушения требований информационной безопасности, и как осуществляется взаимодействие с надзорными органами?

3.1.5 Тема 5 *Угрозы информационной безопасности. Подходы к построению систем защиты информации*

Перечень изучаемых вопросов

1. Классификация угроз информационной безопасности: внутренние и внешние угрозы.
2. Уязвимости информационных систем и их влияние на безопасность.
3. Технологические угрозы: вредоносное ПО, атаки на сети, утечки данных.
4. Человеческий фактор как источник угроз информационной безопасности.
5. Риски информационной безопасности и методы их анализа.
6. Основные принципы построения систем защиты информации в государственных информационных системах.
7. Модели угроз и подходы к их идентификации и предотвращению.

Информационная безопасность играет ключевую роль в защите данных от несанкционированного доступа, потери или повреждения. В условиях цифровизации и активного использования государственных и корпоративных информационных систем угрозы становятся все более сложными.

Основные угрозы информационной безопасности

Современные угрозы можно разделить на несколько категорий:

- Кибератаки – вредоносные действия хакеров, направленные на взлом систем, похищение данных и нарушение работы сервисов. Среди наиболее распространенных атак – DDoS, фишинг, эксплойты уязвимостей.

- Вирусные заражения – вредоносное ПО (вирусы, трояны, шпионские программы), способное нарушить работу системы, уничтожить или похитить данные.
- Социальная инженерия – методы манипуляции, с помощью которых злоумышленники получают доступ к конфиденциальной информации, например, путем обмана пользователей.
- Инсайдерские угрозы – утечка данных изнутри компании или организации, происходящая по вине сотрудников либо в результате халатности.
- Аппаратные и программные сбои – ошибки оборудования или ПО, ведущие к потере данных и нарушению работоспособности системы.

Подходы к построению систем защиты информации

Чтобы эффективно противостоять угрозам, используются различные стратегии и механизмы защиты:

1. Технические меры
   - Шифрование данных – обеспечение конфиденциальности информации путем преобразования ее в зашифрованный вид.
   - Аутентификация и авторизация – использование паролей, биометрических данных, двухфакторной аутентификации для ограничения доступа.
   - Антивирусное ПО и защитные системы – предотвращение проникновения вредоносных программ.
   - Мониторинг и анализ — постоянное отслеживание активности системы для выявления подозрительных действий.
2. Организационные меры
   - Разграничение прав доступа – установление четкой системы ролей и полномочий для сотрудников.
   - Проведение аудитов и проверок – регулярное тестирование систем на наличие уязвимостей.
   - Обучение персонала – повышение осведомленности сотрудников о правилах безопасности.
   - Разработка внутренних регламентов – стандартизация процедур защиты данных.
3. Правовые меры
   - Соблюдение законодательных норм – соответствие требованиям национальных и международных стандартов (например, GDPR, ФЗ-152 «О персональных данных»).
   - Заключение соглашений о конфиденциальности – правовая защита данных сотрудников и клиентов.
   - Ответственность за нарушения – внедрение мер по предотвращению утечек и наказанию виновных.

Эффективная система защиты информации базируется на комплексном подходе, объединяющем технические, организационные и правовые методы. Только скоординированные меры помогут создать надежную защиту данных в условиях современных киберугроз.

Методические указания к изучению

Структура для изучения темы –«Угрозы информационной безопасности. Подходы к построению систем защиты информации» начинается с анализа классификации угроз, включая внутренние и внешние, а также их влияние на безопасность систем. Рассматриваются уязвимости информационных систем и способы их минимизации, а также технологические угрозы, такие как вредоносное ПО, сетевые атаки и утечки данных. Изучение роли человеческого фактора в возникновении угроз дополняется анализом рисков информационной безопасности и методами их оценки. Особое внимание уделяется принципам построения систем защиты информации в государственных информационных системах, а также моделям угроз и подходам к их идентификации и предотвращению. Такой комплексный подход обеспечивает базу для изучения организационных и технических мер защиты в рамках дисциплины.

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

Контрольные вопросы:

1. Какие основные виды угроз информационной безопасности выделяют, и как различаются внутренние и внешние угрозы?
2. В чем заключается роль уязвимостей информационных систем в обеспечении их безопасности, и как они влияют на риск возникновения угроз?
3. Какие технологические угрозы наиболее опасны для государственных информационных систем, и какие примеры можно привести?
4. Как человеческий фактор может стать источником угроз информационной безопасности, и какие меры снижают его влияние?
5. Какие методы используются для анализа и оценки рисков информационной безопасности в государственных информационных системах?
6. Какие принципы лежат в основе построения систем защиты информации, и как они применяются в государственных информационных системах?

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 практическими занятиями необходимо проработать соответствующие разделы лекционного материала;

– рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом практического 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 «Защита информации в 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. Какие критерии используются для классификации информационных систем, и какие основные виды информационных систем можно выделить?
2. Какие особенности функционирования автоматизированных информационных систем влияют на их эффективность и безопасность?
3. Какую роль выполняют государственные информационные системы в обеспечении выполнения функций государственных органов?
4. Какие уникальные характеристики отличают государственные информационные системы от других видов информационных систем?
5. Какие требования предъявляются к защите информации в государственных информационных системах?
6. Как структурная архитектура государственных информационных систем обеспечивает их функционирование и взаимодействие компонентов?
7. Какие топологии ГИС бывают?

1. Какие нормативные требования и методы используются для обеспечения конфиденциальности, целостности и доступности данных в государственных информационных системах?

2. Какова структура и архитектура государственных информационных систем, и какие типы архитектуры наиболее часто применяются?

3. Какие принципы обеспечивают эффективное и безопасное взаимодействие между компонентами информационных систем?

4. Какие внутренние и внешние уязвимости могут возникать при использовании государственных информационных систем, и как можно минимизировать связанные с ними риски?

5. Какие методы контроля и мониторинга функционирования государственных информационных систем применяются для своевременного обнаружения угроз и обеспечения их устойчивости?

6. Как использование систем автоматизированного мониторинга помогает предотвращать угрозы и оптимизировать работу государственных информационных систем?

7. Какие основные виды угроз информационной безопасности выделяют, и как различаются внутренние и внешние угрозы?

8. В чем заключается роль уязвимостей информационных систем в обеспечении их безопасности, и как они влияют на риск возникновения угроз?

9. Какие технологические угрозы наиболее опасны для государственных информационных систем, и какие примеры можно привести?

10. Как человеческий фактор может стать источником угроз информационной безопасности, и какие меры снижают его влияние?

11. Какие методы используются для анализа и оценки рисков информационной безопасности в государственных информационных системах?

12. Какие принципы лежат в основе построения систем защиты информации, и как они применяются в государственных информационных системах?

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 практических работ.

К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

– экзаменационные 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 %**
	«неудовлет-ворительно»	**«удовлет-ворительно»**	**«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 систематизировать необходимую информацию в рамках поставлен-ной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополни-тельные источники информации в рамках поставленной задачи
3 Научное осмысление	Не может делать научно-	В состоянии осуществлять	В состоянии осущест-	В состоянии осуществлять

Система оценок / Критерий	2	3	4	5
	0–40 %	41–60 %	61–80 %	81–100 %
	«неудовлет-ворительно»	«удовлет-ворительно»	«хорошо»	«отлично»
	«не зачтено»	«зачтено»		
изучаемого явления, процесса, объекта	корректных выводов из имеющихся у него сведений, в состоянии проанализи-ровать только некоторые из имеющихся у него сведений	научно-корректный анализ предостав-ленной информации	влять системати-ческий и научно-корректный анализ предостав-ленной информации, вовлекает в исследование новые релевантные задаче данные	систематичес-кий и научно-корректный анализ предостав-ленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессионал ьных 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 предложенно го 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 итоговая аттестация, представляющая собой экзамен.

Тестовые задания для проведения 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.

Экзамен 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.

ПРИМЕРНЫЕ ВОПРОСЫ К ЭКЗАМЕНУ ПО ДИСЦИПЛИНЕ

1. Что такое защита информации и какие ее основные цели?
2. Какие существуют основные угрозы информационной безопасности в ГИС?
3. Какие законы и нормативные акты регулируют защиту информации в государственных системах?
4. Что такое конфиденциальность, целостность и доступность информации?
5. В чем разница между криптографической и административной защитой данных?

Технические аспекты защиты информации

6. Какие методы шифрования используются для защиты данных в государственных информационных системах?
7. В чем разница между симметричным и асимметричным шифрованием?
8. Как функционируют электронные цифровые подписи и их роль в ГИС?
9. Что такое двухфакторная аутентификация и почему она важна?
10. Какие меры используются для защиты сетевого трафика в ГИС?

Организационные меры безопасности

11. Какие категории пользователей существуют в ГИС и как их права доступа регулируются?

12. Какие методы управления доступом применяются в ГИС?
13. Как осуществляется мониторинг безопасности в государственных системах?
14. Какие процедуры восстановления данных применяются в случае их потери?
15. В чем заключается роль аудита информационной безопасности в ГИС?

Кибератаки и методы защиты

16. Какие виды кибератак наиболее опасны для государственных информационных систем?
17. В чем суть атаки типа «человек посередине» и как ей противостоять?
18. Какие методы социальной инженерии применяются для получения несанкционированного доступа?
19. Как работают антивирусные системы в контексте защиты информации?
20. Что такое DDoS-атака и какие способы ее предотвращения существуют?

Криптография и защита данных

21. Как используются цифровые сертификаты в защите информации?
22. Что такое хеширование и как оно применяется для обеспечения безопасности?
23. Какие алгоритмы шифрования используются в современных ГИС?
24. Что такое биометрическая аутентификация и как она применяется?
25. Как работают VPN и их роль в обеспечении безопасности данных?

Правовые аспекты защиты информации

26. Какие требования к защите персональных данных существуют в рамках законодательства?
27. Как регулируется хранение и обработка данных в государственных системах?
28. Какие санкции могут быть применены за нарушение требований информационной безопасности?
29. Какие международные стандарты информационной безопасности используются в ГИС?
30. Как осуществляется взаимодействие государственных органов в обеспечении информационной безопасности?

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 экзамена.

8. ЛИТЕРАТУРА

Основная литература

1. Маршаков, Д. В. Программно-аппаратные средства защиты информации: учеб. пособие / Д. В. Маршаков, Д. В. Фатхи. – Ростов-на-Дону: Донской ГТУ, 2021. – 228 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/237770 (дата обращения: 11.11.2024). – ISBN 978-5-7890-1878-1. – Текст : электронный.

2. Прохорова, О. В. Информационная безопасность и защита информации: учебник / О. В. Прохорова. – 5-е изд., стер. – Санкт-Петербург: Лань, 2023. – 124 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/293009 (дата обращения: 10.10.2024). – ISBN 978-5-507-46010-6. – Текст : электронный.

3. Мирошников, А. И. Основы информационной безопасности и защита информации: учеб. пособие / А. И. Мирошников, А. С. Сысоев. – Липецк: Липецкий ГТУ, 2022. – 107 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/388007 (дата обращения: 10.10.2024). – ISBN 978-5-00175-160-1. – Текст : электронный.

4. Зырянова, Т. Ю. Управление информационной безопасностью: учеб. пособие / Т. Ю. Зырянова. – Екатеринбург, 2023. – 96 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/369482 (дата обращения: 10.12.2024). – Текст : электронный.

Дополнительная литература

5. Груздева, Л. М. Основы информационной безопасности: учеб. пособие: в 2 ч. / Л. М. Груздева. – Москва: РУТ (МИИТ), 2017. – Ч. 1. – 2017. – 101 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/188704 (дата обращения: 10.11. 2024). – Текст : электронный.

6. Мандрица, И. В. Управление проектами по информационной безопасности и экономика защиты информации. Ч. 1 / И. В. Мандрица, В. И. Петренко, О. В. Мандрица. – Санкт-Петербург: Лань, 2023. – 124 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/311825 (дата обращения: 10.11. 2024). – ISBN 978-5-507-45723-6. – Текст: электронный.

7. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд., стер. – Санкт-Петербург: Лань, 2024. – 324 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/370967 (дата обращения: 09.10.2024). – ISBN 978-5-507-49077-6. – Текст : электронный.

8. Вейцман, В. М. Проектирование информационных систем: учеб. пособие для вузов / В. М. Вейцман. – 2-е изд., стер. – Санкт-Петербург: Лань,

2022. – 316 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/208946 (дата обращения: 10.10.2024). – ISBN 978-5-8114-9982-3. – Текст : электронный.

Периодические издания:

9. «Интерэкспо Гео-Сибирь», «НБИ технологии», «Известия Тульского государственного университета. Технические науки».

Учебно-методические пособия, нормативная литература:

10. Крыжановский, А. В. Организационное и правовое обеспечение информационной безопасности: метод. указания / А. В. Крыжановский. – Самара: ПГУТИ, 2018. – 86 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/182281 (дата обращения: 10.11.2024). – Текст : электронный.

11. Никулин, В. В. Безопасность и защита информации. Лабораторный практикум: учеб.-метод. пособие / В. В. Никулин. – Брянск: Брянский ГАУ, 2021. – 128 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/304352 (дата обращения: 09.12.2024). – Текст : электронный.

12. Защита информации в центрах обработки данных: учеб.-метод. пособие / И. А. Ушаков, В. А. Десницкий, А. А. Чечулин, Т. Е. Захарова. – Санкт-Петербург: СПбГУТ им. М. А. Бонч-Бруевича, 2019. – 44 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/180094 (дата обращения: 09.12.2024). – Текст : электронный.

13. «Доктрина информационной безопасности Российской Федерации» (утв. Указом Президентом РФ 05.12.2016 № 646 (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

14. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

15. Федеральный закон от 28.12.2010 N 390-ФЗ «О безопасности» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

16. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

17. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных» (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

18. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (в действующей редакции). - Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

19. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера» (в действующей редакции). - Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

20. «ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (принят и введен в действие Постановлением Госстандарта РФ от 09.02.1995 N 49) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

21. «ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения» (утв. и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 373-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

22. «Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. Решением Гостехкомиссии России от 30.03.1992) (в действующей редакции). - Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

23. «Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. Решением Гостехкомиссии России 30.03.1992) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

Локальный электронный методический материал

Алина Андреевна Бабаева

ЗАЩИТА ИНФОРМАЦИИ В ГИС

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 2,7. Печ. л. 2,2.

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