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

Н. Я. Великите

РАЗРАБОТКА ПРОЕКТНОЙ ДОКУМЕНТАЦИИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

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

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.7(076)

Рецензент
кандидат технических наук, доцент кафедры теории машин и механизмов и деталей машин ФГБОУ ВО «Калининградский государственный технический университет» О. С. Витренко

Великите, Н. Я.
Разработка проектной документации для информационных систем: учебно-методическое пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем» / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 55 с.

Учебно-методическое пособие является руководством к изучению дисциплины «Разработка проектной документации для информационных систем» для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем». В нем представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, темы практических занятий, указания к изучению каждой темы, рекомендации по выполнению практических заданий. Содержатся требования к текущей и промежуточной аттестации, определены условия получения положительной оценки.
Табл. 3, рис. 2, список лит. – 11 наименований

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий 29 апреля 2025 г., протокол № 3

УДК 004.7(076)

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем, изучающих дисциплину «Разработка проектной документации для информационных систем».

Целью освоения дисциплины «Разработка проектной документации для информационных систем» является: формирование знаний, умений и навыков, которые позволяют углубленно рассмотреть отдельные аспекты, отражённые в трудовых функциях профессионального стандарта.

Задачи дисциплины:

– изучить требования к оформлению текстовой документации, порядок и правила оформления организационно-распорядительных документов, программ проведения испытаний, аттестаций, опытной эксплуатации и форм заполнения соответствующей проектной документации при создании или модернизации АСЗИ;

– применять стандартизированную форму заполнения конструкторской документации на АСЗИ с учетом требований ГОСТ, а также требований НПА и МД уполномоченных ФОИВ и НС по ЗИ.

В результате изучения дисциплины студент должен:

знать:

– основные виды конструкторской документации;

уметь:

– разрабатывать проектную и эксплуатационную документацию в соответствии с требованиями ЕСКД, ЕСПД;

владеть:

– навыками разработки проектов нормативных документов, регламентирующих работу по защите информации в автоматизированных системах.

Дисциплина «Разработка проектной документации для информационных систем» является дисциплиной РПМ «Профессиональный модуль» относящейся к части дисциплин учебного плана, которая формируется участниками образовательных отношений. В учебно-методическом документе представлен тематический план, содержащий перечень изучаемых тем, практических занятий, мероприятий текущей аттестации.

Реализация компетентностного подхода при изучении дисциплины «Разработка проектной документации для информационных систем» предполагает использование в учебном процессе разбор конкретных ситуаций, что в сочетании с внеаудиторной работой формирует и развивает профессиональные навыки студентов.

В разделе «Содержание дисциплины» приведены 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).

Раздел «Требования к аттестации по дисциплине» содержит описание обязательных требований к промежуточной аттестации – зачету с оценкой. Помимо данного УМП, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые оперативно вносятся изменения для адаптации дисциплины под конкретную учебную группу.

Лекционные и практические занятия проводятся в специализированных аудиториях с применением мультимедийных технологий и предусматривают развитие полученных теоретических знаний с использованием рекомендованной учебной литературы и других источников информации, в том числе информационных ресурсов сети Интернет. В ходе самостоятельной работы, при подготовке к плановым занятиям и зачёту с оценкой студенты анализируют поставленные преподавателем практические задания с использованием учебно-методической литературы, материалов, найденных в глобальной сети Интернет.

2. ТЕМАТИЧЕСКИЙ ПЛАН

Тематический план изучения дисциплины «Разработка проектной документации для информационных систем» представлен в таблице 1.

Таблица 1 – Тематический план изучения дисциплины «Разработка проектной документации для информационных систем»

	Раздел (модуль) дисциплины	Тема	Объем контактной работы, ч	Объем самостоятельной работы, ч
		Теоретическое обучение (лекции)		
1.1	Раздел 1. Нормативная база по проектированию	Тема 1. Законодательство по ИБ в области критической информационной инфраструктуры. Выбор нормативных документов по информационной безопасности АСУ ТП	4	6
1.2		Тема 2. О применении Единой системы программной документации (ЕСПД), о применении Единой системы конструкторской документации (ЕСКД)	5	6
1.3		Тема 3. Оформление документов. Общие требования	5	6
2.1	Раздел 2. Проектирование автоматизированных систем в защищённом исполнении	Тема 4. Техническое задание. Эскизный проект	6	6
2.2		Тема 5. Технический проект. Рабочая документация	6	6
2.3		Тема 6. Внедрение. Сопровождение. Аттестация	6	6
			32	36
		Практические занятия		
1	Раздел 1. Нормативная база по проектированию	Занятие 1. Законодательство по ИБ в области критической информационной инфраструктуры	4	6
2		Занятие 2. Выбор нормативных документов по информационной безопасности АСУ ТП	5	6

	Раздел (модуль) дисциплины	Тема	Объем контактной работы, ч	Объем самостоятельной работы, ч
3		Занятие 3. Нормативная база по проектированию. О применении Единой системы программной документации (ЕСПД). О применении Единой системы конструкторской документации (ЕСКД)	5	6
4	Раздел 2. Проектирование автоматизированных систем в защищённом исполнении	Занятие 4. Техническое оформление документов. Общие требования	6	6
5		Занятие 5. Техническое задание	6	6
6		Занятие 6. Аттестация	6	6
			32	36
		Рубежный (текущий) и итоговый контроль		
1				
2		Итоговое контроль (Зачёт дифференцированный)	6,15	1,85
			70,15	**73,85**

Всего		144

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1 Раздел 1. Нормативная база по проектированию

3.1.1 Тема 1. Законодательство по информационной безопасности в области критической информационной инфраструктуры. Выбор нормативных документов по информационной безопасности АСУ ТП

Перечень изучаемых вопросов

1. Федеральные законы. Указы Президента РФ.
2. Документы Правительства РФ. Документы ФСБ России.
3. Документы ФСТЭК России. ГОСТы.

Методические указания к изучению

В данной теме мы рассмотрим предмет и задачи дисциплины. Рассмотрим специфику, задачи обеспечения безопасности компьютерной информации в автоматизированных системах с точки зрения законодательства и нормативной базы в области критической информационной инфраструктуры (КИИ). В деле обеспечения информационной безопасности успех может принести только комплексный подход. Законодательный уровень является важнейшим для обеспечения информационной безопасности. Законы не должны опережать жизнь, но важно, чтобы отставание не было слишком большим, так как это ведет к снижению информационной безопасности.

В данной теме мы рассмотрим законодательство по ИБ в области критической информационной инфраструктуры. В качестве сферы деятельности будем рассматривать законодательство по информационной безопасности в области критической информационной инфраструктуры. Рассмотрим, какими НПА надо руководствоваться при проектировании и модернизации АСУ ТП.

При проектировании ИС важно определить, является ли ИС субъектом КИИ или не является субъектом КИИ.

Субъект КИИ определяется в соответствии с документами:

– Федеральный закон от 26.07.2017 № 187-ФЗ;

– Постановление Правительства РФ от 08.02.2018 № 127;

– Приказ ФСТЭК России от 21.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий»;

– Документы ФСБ (ГосСОПКА).

Документация на АСЗИ должна разрабатываться с учетом требований [6–8], а также требований НПА и МД уполномоченных ФОИВ и НС по ЗИ.

Рекомендуемая литература: [1, гл. 1; 5].

Контрольные вопросы для самопроверки

1. Какие ключевые законы регулируют защиту КИИ?

2. Какова роль Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»?

3. В каких случаях организация обязана защищать объекты КИИ?

4. Какие обязанности возлагаются на организации, владеющие объектами КИИ?

5. Кто несет ответственность за обеспечение информационной безопасности объектов КИИ?

6. Что такое категорирование объектов КИИ и как оно проводится?

7. Перечислите основные стандарты и руководящие документы, касающиеся информационной безопасности АСУ ТП.

8. Чем отличаются требования к информационной безопасности для АСУ ТП от требований для ИТ-систем общего назначения?

9. Назовите международные стандарты, применяемые для обеспечения информационной безопасности АСУ ТП.

10. Почему важно соблюдать требования ФСТЭК и ФСБ России в отношении защиты КИИ?

11. Какие последствия могут наступить для организаций в случае нарушения требований по защите КИИ?

12. Какие меры защиты предусмотрены законодательством для объектов КИИ?

3.1.2 Тема 2. О применении Единой системы программной документации (ЕСПД), о применении Единой системы конструкторской документации (ЕСКД)

Перечень изучаемых вопросов

1. Коды по КГС и ОКС.
2. Регламентирующие документы.

Методические указания к изучению

Рассмотрим, какие бывают стандарты (фокусируясь на ИТ-области).

1. Международные. Отличительный признак – принят международной организацией. Пример такой организации – ISO (международная организация стандартизации). Пример её стандарта: ISO 2382-12:1988 (Периферийное оборудование). Распространены совместные стандарты ISO и международной электротехнической комиссии (IEC, по-русски – МЭК): например, ISO/IEC 12207:2008 (жизненный цикл ПО).

2. Региональные. Отличительный признак – принят региональной комиссией по стандартизации. К примеру, многие советские ГОСТы сейчас являются

региональным стандартом, так как приняты межгосударственным советом, куда входят некоторые бывшие советские республики. Этим советом принимаются и новые стандарты – и они тоже получают обозначение ГОСТ. Пример: ГОСТ 12.4.240-2013.

3. Стандарты общественных объединений. К примеру, той же МЭК: IEC 60255.

4. Национальные стандарты. Для России в начале таких стандартов – «ГОСТ Р».

Могут быть трех типов:

1) точные копии международных или региональных. Обозначаются неотличимо от «самописных» (национальных, написанных самостоятельно);

2) копии международных или региональных с дополнениями. Обозначаются добавлением к шифру отечественного стандарта шифра международного, который был взят за основу. Например: ГОСТ Р ИСО/МЭК 12207;

3) собственно национальные стандарты. Например, ГОСТ Р 34.11-94.

Системы обозначений на каждом уровне и в каждой организации свои.

Стандарты бывают международные, межгосударственные (региональные) и национальные. ГОСТ, как мы выяснили, это региональный стандарт. Они имеют достаточно запутанную систему обозначений. Полностью она изложена в ГОСТ Р 1.5-2004, приведём минимум, чтобы в ней ориентироваться. Во-первых, надо различать обозначение ГОСТа и его классификацию. Обозначение – это, грубо говоря, уникальный идентификатор стандарта. Код по классификатору – это вспомогательный код, помогающий найти стандарт или определить, к какой области знаний он относится. Классификаторов может быть много, в основном используются два: КГС (классификатор государственных стандартов) и его наследник ОКС (общероссийский классификатор стандартов). Например: «ГОСТ Р 50628–2000» – это обозначение стандарта. По обозначению понятно только то, что он принят в 2000 г. Он имеет код по ОКС «33.100;35.160», т. е. «33» – раздел «Телекоммуникации, аудио, видео», «100» – подраздел «электромагнитная совместимость». Однако он также входит в ветвь классификатора 35.160. «35» – «Информационные технологии. Машины конторские», «160» – «Микропроцессорные системы...». А по КГС он имеет код «Э02», что означает «Э» – «Электронная техника, радиоэлектроника и связь», «0» – «Общие правила и нормы по электронной технике, радиоэлектронике и связи» и т. д.

Если известно обозначение стандарта, то получить его коды по КГС и ОКС можно, к примеру, на сайте.

Итак, вернемся к обозначениям ГОСТов. Их может быть два варианта:

1) стандарт относится к серии стандартов. В этом случае после индекса категории стандарта (например, ГОСТ, ГОСТ Р или ГОСТ РВ) идет код серии,

точка и обозначение стандарта внутри серии. Правила обозначения стандартов внутри серии устанавливаются правилами серии. Например: ГОСТ РВ 15.201-2000, ГОСТ Р 22.8.0-99, ГОСТ 19.101-77;

2. Стандарт не относится к серии стандартов. Тогда после индекса категории идет просто порядковый номер стандарта, тире и год принятия. Например, ГОСТ Р 50628–2000.

Итак, если совсем просто – то обозначение ГОСТа – это либо просто порядковый номер, тире, год, либо номер серии, точка и дальше в зависимости от серии. В реальности все сложнее (к примеру, можно встретить что-то типа ГОСТ 11326.19-79, и это будет вовсе не серия 11326 – но программистам такое нужно очень редко. За подробностями – в ГОСТ Р 1.5 2004).

ЕСПД – одна из таких серий ГОСТов, номер 19. То есть, все стандарты, относящиеся к ЕСПД, начинаются с префикса «19.», например, ГОСТ 19.106-78. Расшифровывается как «Единая система программной документации». Существуют и другие серии:

• ГОСТ ЕСКД (единая система конструкторской документации, префикс «2.»);

• ГОСТ ЕСТД (единая система технологической документации, префикс «3.»);

• ГОСТ Р Система разработки и постановки продукции на производство, префикс «15.»;

• ГОСТ РВ, Вооружение и военная техника. Система разработки и постановки продукции на производство, префикс «15.»;

• ГОСТ, Система технической документации на АСУ, префикс «24.»;

• ГОСТ, Комплекс стандартов на автоматизированные системы, префикс «34.».

Рекомендуемая литература: [3, 4, 6–8].

Контрольные вопросы для самопроверки

1. Что такое Единая система программной документации (ЕСПД)?

2. Какие основные цели и задачи преследует ЕСПД?

3. Какие стандарты входят в состав ЕСПД? Назовите хотя бы три стандарта.

4. Какова структура и содержание документов, разработанных согласно требованиям ЕСПД?

5. В каких случаях применяются требования ЕСПД?

6. Какие обязательные этапы разработки программного обеспечения описаны в стандартах ЕСПД?

7. Какие виды программной документации создаются на различных этапах жизненного цикла ПО?

8. Чем отличается документация технического задания от эксплуатационной документации?

9. Какие требования предъявляются к оформлению программной документации согласно стандартам ЕСПД?

10. Каковы основные принципы унификации и стандартизации в рамках ЕСПД?

11. Что такое Единая система конструкторской документации (ЕСКД)?

12. Какие основные цели и задачи преследует ЕСКД?

13. Какие стандарты входят в состав ЕСКД? Назовите хотя бы три стандарта.

14. Какова структура и содержание конструкторских документов, созданных по правилам ЕСКД?

15. В каких случаях применяются требования ЕСКД?

16. Какие обязательные этапы проектирования и разработки изделий описаны в стандартах ЕСКД?

17. Какие виды конструкторской документации разрабатываются на разных стадиях проекта?

18. Чем отличаются чертежи общего вида от сборочных чертежей?

19. Какие требования предъявляются к оформлению конструкторской документации согласно стандартам ЕСКД?

20. Каковы основные принципы унификации и стандартизации в рамках ЕСКД?

3.1.3 Тема 3. Техническое оформление документов. Общие требования

Перечень изучаемых вопросов

Способы оформления документации.

Методические указания к изучению

С 1 июля 2020 г. действуют новые требования к оформлению текстовой документации. Цель нового свода правил – стандартизировать форму заполнения конструкторской документации. Структура и состав текстов в сфере строительства, машино- и приборостроения должны подчиняться единым нормам. Два нововведения предусмотрены приказом Федерального агентства по техническому регулированию и метрологии № 175-ст от 29.04.2019:

• ГОСТ 2.105-95 утрачивает силу в качестве национального стандарта, но сохраняет действие в качестве межгосударственного;

• ГОСТ Р 2.105-2019 признают национальным.

Обратите внимание и на ряд других ГОСТов, принятых в данной сфере:

• ГОСТ Р 2.106-2019 «Единая система конструкторской документации. Текстовые документы», утверждён приказом Росстандарта от 29.04.2019 № 176-ст;

• ГОСТ Р 2.601-2019 «Единая система конструкторской документации. Эксплуатационные документы», утверждён приказом Росстандарта от 29.04.2019 № 177-ст;

• ГОСТ Р 2.711-2019 «Единая система конструкторской документации. Схема деления изделия на составные части», утверждён приказом Росстандарта от 29.04.2019 № 179-ст;

• ГОСТ Р 2.610-2019 «Единая система конструкторской документации. Правила выполнения эксплуатационных документов», утверждён приказом Росстандарта от 29.04.2019 № 178-ст.

Напомним, требования единой системы конструкторской документации (ЕСКД) в РФ считаются добровольными. И если вы выполняете заказ, можно руководствоваться стандартами, выставленными заказчиком. Если документация оформляется для российского рынка, стоит пользоваться правилами оформления из национального свода.

Продолжить работу по ГОСТ 2.105-95 следует, если вы готовите бумаги для партнеров из ЕАЭС. Когда документами пользуются компании и из России, и из других стран, укажите наименование стандарта, который был использован при их подготовке.

Четыре способа оформления документов Документы можно подготовить как в электронном, так и в рукописном виде. Для каждого варианта есть свои ГОСТы.

1. Машинописным способом в соответствии с ГОСТ 13.1.002-2003. Межгосударственный стандарт. Репрография. Микрография. Документы для микрофильмирования. Общие требования и нормы (введен в действие Постановлением Госстандарта России от 26.02.2004 № 63-ст).

2. Рукописным методом, используя положения ГОСТ 2.304-81. Межгосударственный стандарт. Единая система конструкторской документации. Шрифты чертежные (утверждён Постановлением Госстандарта СССР от 28.03.1981 № 1562).

3. Применяя ЭВМ, согласно ГОСТ 2.004-88. Межгосударственный стандарт. Единая система конструкторской документации. Общие требования к выполнению конструкторских и технологических документов на печатающих и графических устройствах вывода ЭВМ (утверждён Постановлением Госстандарта СССР от 28.11.1988 № 3843).

4. На электронных носителях информации. Обратите внимание, что текстовые документы электронных (ТДЭ), согласно правилам, допускается готовить с использованием стандартизованных информационных моделей про

грамм. Данные будут либо сгенерированы автоматически с помощью специализированных программных средств из заранее подготовленных фрагментов, либо набираются вручную.

Техническое оформление документов. Общие требования Правила ГОСТ к оформлению тестовых документов отличаются. Всё зависит от того, кто утверждал стандарт.

Чего нельзя делать. Запреты.

В требованиях к текстовым документам содержится ряд запретов. Например, требования единой системы конструкторской документации (ЕСКД 2020 г.) запрещают:

1. Указывать индексы стандартов без обозначения присвоенного им регистрационного номера.

2.Писать математические знаки без числового сопровождения.

3.Ставить знак минус для обозначения отрицательных чисел.

4. Перечеркивать круг в качестве обозначения диаметра.

В самом тексте недопустимо применять:

5. Сокращения слов, кроме установленных правилами русской орфографии, соответствующими государственными стандартами, а также в данном документе.

6.Обороты разговорной речи, техницизмы, профессионализмы.

7. Для одного и того же понятия различные научно-технические термины, близкие по смыслу (синонимы), иностранные слова и термины при наличии равнозначных слов и терминов в русском языке.

8. Произвольные словообразования. К физическим величинам тоже есть требования:

9. Нельзя сокращать обозначения единиц физических величин (если они употребляются без цифр, за исключением единиц физических величин в заголовках и боковиках таблиц и в расшифровках буквенных обозначений, входящих в формулы и рисунки).

Отклонение от обязательных требований не допускается, в соответствии с действующими правилами следует оформлять любой элемент текста.

Рекомендуемая литература: [3,4, 6–8].

Контрольные вопросы для самопроверки

1. Какие основные элементы включает в себя титульный лист документа?

2. Каковы стандартные размеры полей документа?

3. Какой шрифт рекомендуется использовать для оформления текста документа? Укажите допустимые размеры шрифта.

4. Что такое межстрочный интервал и какой он должен быть согласно стандартам?

5. Какие правила существуют для нумерации страниц в документе?

6. В каком формате рекомендуется сохранять документ перед печатью?

7. Какие требования предъявляются к оформлению заголовков и подзаголовков?

8. Как правильно оформить списки в документе (нумерованные и маркированные)?

9. Как оформлять таблицы в документе? Укажите основные требования.

10. Какие дополнительные элементы могут присутствовать в документе (например, колонтитулы)? Опишите их назначение.

11. Какие символы используются для обозначения переносов строки и абзацев?

12. Какие существуют требования к длине строк в тексте документа?

13. Какие особенности оформления имеют документы с иллюстрациями и схемами?

14. Как оформляется подпись автора документа?

15. Какие ошибки чаще всего допускаются при оформлении документов и как их избежать?

3.2. Раздел 2. Проектирование автоматизированных систем в защищённом исполнении

3.2.1 Тема 4. Техническое задание. Эскизный проект

Перечень изучаемых вопросов

1. Разработка, оформление, согласование и утверждение ТЗ.

2. Разработка, оформление, согласование и утверждение ЭП.

Методические указания к изучению

В данном разделе мы будем уделять внимание разработке и оформлению, согласованию и утверждению документации при проектировании АСЗИ. Межгосударственный стандарт ГОСТ 34.602-2020 «Информационные технологии. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 19 ноября 2021 г. N 1522-ст). Разработан Акционерным обществом «Всероссийский научно-исследовательский институт сертификации» (АО «ВНИИС») и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ). Внесен Федеральным агентством по техническому регулированию и метрологии.

Принят Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 22 декабря 2020 г. N 58). Настоящий стандарт распространяется на автоматизированные системы (АС), предназначенные для ав-

томатизации различных видов деятельности (управление, проектирование, исследования и т.п.), включая их сочетания, и устанавливает требования к составу, содержанию, правилам оформления документа «Техническое задание на создание (развитие или модернизацию) автоматизированной системы» (далее – ТЗ на АС). ТЗ на АС является основным документом, определяющим требования и порядок создания (развития или модернизации – далее создания) АС, в соответствии с которым проводится разработка АС и ее приемка.

Правила оформления ТЗ на АС ТЗ на АС оформляют в виде текстового документа: номера листов (страниц) ставят, начиная с первого листа, следующего за титульным листом, в верхней части листа (над текстом, посередине). При необходимости в ТЗ на АС могут включаться схемы, рисунки, таблицы и др. иллюстративный материал. Разделы и подразделы ТЗ на АС должны быть размещены в порядке, установленном в разделе 4 настоящего стандарта; оформление документов в соответствии с ЕСКД и ЕСПД.

На титульном листе помещают подписи заказчика и согласующих организаций. Так как титульный лист является первым листом документа, подписи должностных лиц, участвующих в согласовании и рассмотрении проекта ТЗ на АС, помещают на последнем листе.

На титульном листе ТЗ на АС допускается помещать установленные в отрасли отметки, например, гриф секретности, код работы, регистрационный номер ТЗ и другие отметки.

Титульный лист дополнения к ТЗ на АС оформляют аналогично титульному листу технического задания. Вместо наименования «Техническое задание» пишут «Дополнение № ... к ТЗ на АС ...».

На последующих листах дополнения к ТЗ на АС помещают основание для изменения, содержание изменения и ссылки на документы, в соответствии с которыми вносятся эти изменения (при необходимости).

При изложении текста дополнения к ТЗ следует указывать номера соответствующих пунктов, подпунктов, таблиц основного ТЗ на АС и прочие структурные элементы и применять слова: «заменить», «дополнить», «исключить», «изложить в новой редакции».

Эскизный проект.

Разработка предварительных проектных решений по системе в целом и ее частям. Разработка предварительных проектных решений АСЗИ. Технико-экономическое обоснование эффективности вариантов СрЗИ. Разработка ТЗ на СрЗИ и средства контроля эффективности ЗИ. Разработка требований на СрЗИ и средства контроля эффективности ЗИ и АС.

Эскизный проект.

Разработка документации на АС и ее части: разработка, оформление, согласование, утверждение в соответствии с ГОСТ 34.201-89 в объеме, необходи-

мом для описания полной совокупности принятых предварительных проектных решений и достаточном для дальнейшего проведения работ по созданию системы ЗИ.

Рекомендуемая литература: [3, гл. 1].

Контрольные вопросы для самопроверки

1. Какие основные этапы включает процесс разработки технического задания?
2. Каковы ключевые требования к содержанию технического задания?
3. Кто участвует в процессе согласования технического задания? Какие подразделения или лица могут вносить изменения?
4. В каких случаях требуется пересмотр или корректировка технического задания после его утверждения?
5. Какие нормативно-правовые акты регулируют порядок разработки и утверждения технических заданий?
6. Какова роль заказчика в процессе разработки технического задания?
7. Что такое техническое задание и почему оно важно на этапе проектирования?
8. Какие риски могут возникнуть при недостаточно полном или неправильном оформлении технического задания?
9. Какие критерии используются для оценки качества разработанного технического задания?
10. Какая информация должна обязательно присутствовать в разделе «Требования к проекту»?
11. Каково основное назначение эскизного проекта?
12. Какие элементы входят в состав эскизного проекта?
13. Как проходит процесс согласования эскизного проекта?
14. Какие технические решения должны быть отражены в эскизном проекте?
15. В каком случае требуется разработка нескольких вариантов эскизного проекта?
16. Какие документы прилагаются к эскизному проекту?
17. Какие цели преследует этап разработки эскизного проекта?
18. Чем отличается эскизный проект от рабочего проекта?
19. Как происходит утверждение эскизного проекта?
20. Какие ошибки чаще всего допускают при разработке эскизного проекта?

3.2.2 Тема 5. Технический проект. Рабочая документация

Перечень изучаемых вопросов

1. Технический проект. Разработка документации на АС и ее части. Разработка и оформление документации на поставку изделий для комплектования АС и (или) технических требований (технических заданий) на их разработку.

2. Рабочая документация. Разработка рабочей документации на систему и ее части. Разработка и адаптация программ.

Методические указания к изучению Технический проект

Разработка документации на АС и ее части: разработка, оформление, согласование, утверждение согласно ГОСТ 34.201-89. Технический проект. Разработка и оформление документации на поставку изделий для комплектования АС и (или) технических требований (технических заданий) на их разработку, подготовку и оформление документов на поставку ТС и ПС для комплектования системы ЗИ создаваемой (модернизируемой) АСЗИ, определение технических требований и составление ТЗ на разработку специальных СЗИ, специального технологического оборудования, средств контроля и измерений, не изготавливаемых серийно.

Рабочая документация. Разработка рабочей документации на систему и ее части. Разработка и адаптация программ. Рабочая документации. Разработка рабочей документации на систему и ее части, необходимые и достаточные сведения для обеспечения выполнения работ по вводу системы ЗИ АСЗИ в действие и ее эксплуатации, поддержания уровня эксплуатационных характеристик (качества) системы ЗИ, разработка программы и методик испытаний.

Рекомендуемая литература: [2, гл. 1, 2].

Контрольные вопросы для самопроверки

1. Что такое технический проект?
   – Каковы цели и задачи технического проекта?
   – Какие основные этапы разработки технического проекта вы можете назвать?
2. Какие документы входят в состав технического проекта?
   – Перечислите основные компоненты технического проекта.
   – Что включает в себя пояснительная записка к техническому проекту?
3. Рабочая документация – что это?
   – В чем отличие рабочей документации от технического проекта?
   – Какие виды чертежей входят в рабочую документацию?
4. Этапы разработки рабочей документации:
   – Опишите процесс создания рабочей документации.
   – Какие специалисты участвуют в разработке рабочей документации?

5. Требования к оформлению технической документации:

– Какие стандарты и нормы применяются при оформлении технической документации?

– Приведите пример обязательных реквизитов документов.

6. Исполнительная документация:

– Чем отличается исполнительная документация от рабочей?

– Для каких целей используется исполнительная документация?

7. Особенности проектирования инженерных сетей:

– Какие инженерные сети чаще всего включаются в рабочий проект?

– Какие требования предъявляются к проектной документации инженерных сетей?

8. Проверка и утверждение проектной документации:

– Кто проводит проверку проектной документации перед утверждением?

– Какие организации или инстанции могут утверждать проектную документацию?

9. Реализация проекта:

– Какие документы необходимы для начала строительства после утверждения проекта?

– Какие изменения могут вноситься в проектную документацию на этапе реализации?

10. Контроль качества проектной документации:

– Какие методы контроля используются для проверки качества проектной документации?

– Как обеспечивается соответствие проектной документации строительным нормам и правилам?

3.2.3 Тема 6. Внедрение. Сопровождение. Аттестация

Перечень изучаемых вопросов

1. Внедрение. Внедрение системы ЗИ АСЗИ. Ввод в действие.
2. Сопровождение. Сопровождение системы ЗИ в ходе эксплуатации АСЗИ.
3. Содержание организационно-распорядительных документов.
4. Аттестация.

Методические указания к изучению

Внедрение системы ЗИ АСЗИ. Ввод в действие. ГОСТ 34.603-92. ГОСТ 34.601-90.

Установка и настройка СЗИ;

– разработка организационно-распорядительных документов, определяющих мероприятия по ЗИ в ходе эксплуатации;

– предварительные испытания системы ЗИ АСЗИ;

– опытная эксплуатация и доработка системы ЗИ АСЗИ;

– приемочные испытания системы ЗИ АСЗИ;

– аттестацию АСЗИ на соответствие требованиям по ИБ.

Ввод в действие. Испытания системы ЗИ АСЗИ на соответствие ТЗ на систему ЗИ в соответствии с программой и методикой приемочных испытаний анализ результатов испытаний системы ЗИ АСЗИ и устранение недостатков, выявленных при испытаниях.

Проведение приемочных испытаний. Оформление разделов акта о приемке АСЗИ в постоянную эксплуатацию (в части системы ЗИ АСЗИ). Выполнение работ относительно системы ЗИ АСЗИ в соответствии с гарантийными обязательствами и по послегарантийному обслуживанию. Рабочая документация на систему ЗИ. Организационно-распорядительные документы. Выполнение работ в соответствии с гарантийными обязательствами. Послегарантийное обслуживание.

Содержание организационно-распорядительных документов.

1. Акт завершения работ

Документ содержит:

1) наименование завершенной работы (работ);

2) список представителей организации-разработчика и организации-заказчика, составивших акт;

3) дату завершения работ;

4) наименование документа (ов), на основании которого (ых) проводилась работа;

5) основные результаты завершенной работы;

6) заключение о результатах завершенной работы.

2. Акт приемки в опытную эксплуатацию

Документ содержит:

1) наименование АС (или ее части), принимаемой в опытную эксплуатацию и соответствующего объекта автоматизации;

2) наименование документа, на основании которого разработана АС;

3) состав приемочной комиссии и основание для ее работы (наименование, но мер и дату утверждения документа, на основании которого создана комиссия);

4) период времени работы комиссии;

5) наименование организации-разработчика, организации-соисполнителя и организации заказчика;

6) состав функций АС (или ее части), принимаемых в опытную эксплуатацию;

7) перечень составляющих технического, программного, информационного и организационного обеспечений, проверяемых в процессе опытной эксплуатации;

8) перечень документов, предъявляемых комиссии;

9) оценку соответствия принимаемой АС техническому заданию на ее создание;

10) основные результаты приемки в опытную эксплуатацию;

11) решение комиссии о принятии АС в опытную эксплуатацию.

3. Акт приемки в промышленную эксплуатацию

3.1. Документ содержит:

1) наименование объекта автоматизации и АС (или ее части), принимаемой в промышленную эксплуатацию;

2) сведения о статусе приемочной комиссии (государственная, межведомственная, ведомственная), ее составе и основание для работы;

3) период времени работы комиссии;

4) наименование организации-разработчика, организации-соисполнителя и организации заказчика;

5) наименование документа, на основании которого разработана АС;

6) состав функций АС (или ее части), принимаемой в промышленную эксплуатацию;

7) перечень составляющих технического, программного, информационного и организационного обеспечения, принимаемых в промышленную эксплуатацию;

8) список ответственных представителей организаций, выполняющих наладочные работы;

9) указания о порядке устранения ошибок монтажа и лицах, ответственных за выполнения этих работ.

4. Документ «Приказ о начале опытной эксплуатации АС (ее частей)» содержит:

1) наименование АС в целом или ее частей, проходящей опытную эксплуатацию;

2) наименование организации разработчика, организаций-соисполнителей;

3) сроки проведения опытной эксплуатации;

4) список должностных лиц организации-заказчика и организации-разработчика, ответственных за проведение опытной эксплуатации;

5) перечень подразделений организации-заказчика, участвующих в проведении опытной эксплуатации.

5. Документ «Приказ о вводе в промышленную эксплуатацию АС (ее частей)» должен содержать:

1) состав функций АС или ее частей, технических и программных средств, принимаемых в промышленную эксплуатацию;

2) список должностных лиц и перечень подразделений организации-заказчика, ответственных за работу АС;

3) порядок и сроки введения новых форм документов (при необходимости); 4) порядок и сроки перевода персонала на работу в условиях функционирования АС.

6. Приказ о составе приемочной комиссии

6.1. Документ содержит:

1) наименование принимаемой АС в целом или ее частей;

2) сведения о составе комиссии;

3) основание для организации комиссии;

4) наименование организации-заказчика;

5) наименование организации-разработчика, организаций-соисполнителей;

6) назначение и цели работы комиссии;

7) сроки начала завершения работы комиссии;

8) указание о форме завершения работы комиссии.

7. Протокол испытаний

7.1. Документ содержит:

1) наименование объекта испытаний;

2) список должностных лиц, проводивших испытания;

3) цель испытаний;

4) сведения о продолжительности испытаний;

5) перечень пунктов технического задания на создание АС, на соответствие которым проведены испытания;

6) перечень пунктов «Программы испытаний», по которым проведены испытания;

7) сведения о результатах наблюдений за правильностью функционирования АС;

8) сведения об отказах, сбоях и аварийных ситуациях, возникающих при испытаниях;

9) сведения о корректировках параметров объекта испытания и технической документации.

8. Протокол согласования

8.1. Документ содержит:

1) перечень рассмотренных отклонений с указанием документа, отклонения от требований которого являются предметом согласования;

2) перечень должностных лиц, составивших протокол;

3) обоснование принятых отклонений от проектных решений;

4) перечень согласованных отклонений и сроки внесения необходимых изменений в техническую документацию.

Аттестация. Оформление документов по требованиям Федеральной службу по техническому и экспортному контролю. Приказ ФСТЭК России от 29 апреля 2021 г. № 77 зарегистрирован Минюстом России 10 августа 2021 г. № 64589.

Технический паспорт АС; Технический паспорт защищаемого помещения; Акт классификации ИС (АС); Аттестат соответствия.

Программы и методики аттестационных испытаний ОИ.

Заключение по результатам аттестационных испытаний. Протоколы аттестационных испытаний.

Методические указания к изучению

Аттестация объектов информатизации (ОИ) – комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие ОИ требованиям по ЗИ в условиях его эксплуатации.

В качестве заявителей могут выступать заказчики, владельцы или разработчики аттестуемых объектов информатизации. В качестве органов по аттестации могут выступать отраслевые и региональные учреждения, предприятия и организации по защите информации, которые прошли соответствующую аккредитацию во ФСТЭК России.

Органы по аттестации:

• аттестуют объекты информатизации и выдают «Аттестаты соответствия»;

• осуществляют контроль за безопасностью информации, циркулирующей на аттестованных объектах информатизации, и за их эксплуатацией;

• отменяют и приостанавливают действие выданных этим органом «Аттестатов соответствия»;

• формируют фонд нормативной и методической документации, необходимой для аттестации конкретных типов объектов информатизации, участвуют в их разработке;

• ведут информационную базу аттестованных этим органом объектов информатизации;

• осуществляют взаимодействие с ФСТЭК России и ежеквартально информируют его о своей деятельности в области аттестации.

ФСТЭК осуществляет следующие функции в рамках системы аттестации:

• организует обязательную аттестацию объектов информатизации;

• создает системы аттестации объектов информатизации и устанавливает правила для проведения аттестации в этих системах;

• устанавливает правила аккредитации и выдачи лицензий на проведение работ по обязательной аттестации;

• организует, финансирует разработку и утверждает нормативные и методические документы по аттестации объектов информатизации;

• аккредитует органы по аттестации объектов информатизации и выдает им лицензии на проведение определенных видов работ;

• осуществляет государственный контроль и надзор за соблюдением правил аттестации и эксплуатацией аттестованных объектов информатизации;

• рассматривает апелляции, возникающие в процессе аттестации объектов информатизации и контроля за эксплуатацией аттестованных объектов информатизации;

• организует периодическую публикацию информации по функционированию системы аттестации объектов информатизации по требованиям безопасности информации.

Испытательные лаборатории проводят испытания несертифицированной продукции, используемой на аттестуемом объекте информатизации. Со списком органов по аттестации и испытательных лабораторий, прошедших аккредитацию, можно ознакомиться на официальном сайте ФСТЭК России в разделе «Сведения о Системе сертификации средств защиты информации по требованиям безопасности информации».

Заявители:

• проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;

• привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;

• предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;

• привлекают, в необходимых случаях, для проведения испытаний несертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;

• осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в «Аттестате соответствия»;

• извещают орган по аттестации, выдавший «Аттестат соответствия», о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в «Аттестате соответствия»);

• предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию. Для проведения испытаний заявитель предоставляет органу по аттестации следующие документы и данные:

• приемо-сдаточную документацию на объект информатизации;

• акты категорирования выделенных помещений и объектов информатизации;

• инструкции по эксплуатации средств защиты информации;

• технический паспорт на аттестуемый объект;

• документы на эксплуатацию (сертификаты соответствия требованиям безопасности информации) ТСОИ;

• сертификаты соответствия требованиям безопасности информации на ВТСС;

• сертификаты соответствия требованиям безопасности информации на технические средства защиты информации;

• акты на проведенные скрытые работы;

• протоколы измерения звукоизоляции выделенных помещений и эффективности экранирования сооружений и кабин (если они проводились);

• протоколы измерения величины сопротивления заземления;

• протоколы измерения реального затухания информационных сигналов до мест возможного размещения средств разведки;

• данные по уровню подготовки кадров, обеспечивающих защиту информации;

• данные о техническом обеспечении средствами контроля эффективности за щиты информации и их метрологической поверке;

• нормативную и методическую документацию по защите информации и контролю эффективности защиты;

• пояснительную записку, содержащую информационную характеристику и организационную структуру объекта защиты, сведения об организационных и технических мероприятиях по защите информации от утечки по техническим каналам;

• перечень объектов информатизации, подлежащих защите, с указанием мест их расположения и установленной категории защиты;

• перечень выделенных помещений, подлежащих защите, с указанием мест их расположения и установленной категории защиты;

• перечень устанавливаемых ТСОИ с указанием наличия сертификата (предписания на эксплуатацию) и мест их установки;

• перечень устанавливаемых ВТСС с указанием наличия сертификата и мест их установки;

• перечень устанавливаемых технических средств защиты информации с указанием наличия сертификата и мест их установки;

• схему (в масштабе) с указанием плана здания, в котором расположены защищаемые объекты, границы контролируемой зоны, трансформаторной подстанции, заземляющего устройства, трасс прокладки инженерных коммуникаций, линий электропитания, связи, пожарной и охранной сигнализации, мест установки разделительных устройств и т. п.;

• технологические поэтажные планы здания с указанием мест расположения объектов информатизации и выделенных помещений и характеристиками их стен, перекрытий, материалов отделки, типов дверей и окон;

• планы объектов информатизации с указанием мест установки ТСОИ, ВТСС и прокладки их соединительных линий, а также трасс прокладки инженерных коммуникаций и посторонних проводников;

• план-схему инженерных коммуникаций всего здания, включая систему вентиляции;

• план-схему системы заземления объекта с указанием места расположения заземлителя;

• план-схему системы электропитания здания с указанием места расположения разделительного трансформатора (подстанции), всех щитов и разводных коробок;

• план-схему прокладки телефонных линий связи с указанием мест расположения распределительных коробок и установки телефонных аппаратов;

• план-схему систем охранной и пожарной сигнализации с указанием мест установки и типов датчиков, а также распределительных коробок;

• схемы систем активной защиты (если они предусмотрены).

Приведенный общий объем исходных данных и документации может уточняться заявителем в зависимости от особенностей аттестуемого объекта информатизации по согласованию с аттестационной комиссией.

К заключению прилагаются протоколы испытаний, подтверждающие полученные при испытаниях результаты и обосновывающие приведенный в заключении вывод.

Протокол аттестационных испытаний должен включать:

• вид испытаний;

• объект испытаний;

• дату и время проведения испытаний;

• место проведения испытаний;

• перечень использованной в ходе испытаний аппаратуры (наименование, тип, заводской номер, номер свидетельства о поверке и срок его действия);

• перечень нормативно-методических документов, в соответствии с которыми проводились испытания;

• методику проведения испытания (краткое описание);

• результаты измерений;

• результаты расчетов;

• выводы по результатам испытаний.

Протоколы испытаний подписываются экспертами – членами аттестационной комиссии, проводившими испытания, с указанием должности, фамилии и инициалов. Заключение по результатам аттестации подписывается членами аттестационной комиссии, утверждается руководителем органа аттестации и представляется заявителю. Заключение и протоколы испытаний подлежат утверждению органом по аттестации.

Аттестат соответствия должен содержать:

• регистрационный номер;

• дату выдачи;

• срок действия;

• наименование, адрес и местоположение объекта информатизации;

• категорию объекта информатизации;

• класс защищенности автоматизированной системы;

• гриф секретности (конфиденциальности) информации, обрабатываемой на объекте информатизации;

• организационную структуру объекта информатизации и вывод об уровне подготовки специалистов по защите информации;

• номера и даты утверждения программы и методики, в соответствии с которыми проводились аттестационные испытания;

• перечень руководящих документов, в соответствии с которыми проводилась аттестация;

• номер и дата утверждения заключения по результатам аттестационных испытаний;

• состав комплекса технических средств обработки информации ограниченного доступа, перечень вспомогательных технических средств и систем, перечень технических средств защиты информации, а также схемы их размещения в помещениях и относительно границ контролируемой зоны, перечень используемых программных средств;

• организационные мероприятия, при проведении которых разрешается обработка информации ограниченного доступа;

• перечень действий, которые запрещаются при эксплуатации объекта информатизации;

• список лиц, на которых возлагается обеспечение требований по защите информации и контроль за эффективностью реализованных мер и средств защиты информации.

Аттестат соответствия подписывается руководителем аттестационной комиссии и утверждается руководителем органа по аттестации.

Контрольные вопросы для самопроверки

1. Что такое внедрение программного продукта? Какие этапы включает этот процесс?

2. Каковы ключевые роли участников проекта внедрения (заказчик, исполнитель)?

3. Какие риски могут возникать на этапе внедрения системы? Как их минимизировать?

4. Чем отличаются пилотный проект от полноценного внедрения?

5. Какие метрики используются для оценки успешности внедрения ПО?

6. Почему важно документирование процессов внедрения? Приведите пример.

7. Какие подходы существуют для тестирования внедренной системы перед вводом в эксплуатацию?

8. Что такое обучение пользователей при внедрении новых решений и почему оно важно?

9. Какие инструменты управления проектами вы знаете и как они помогают на этапе внедрения?

10. Опишите роль руководства компании в процессе внедрения нового решения.

11. Что подразумевает собой сопровождение программного обеспечения после его внедрения?

12. Какие виды поддержки программного обеспечения бывают (например, техническая поддержка, обновление ПО)?

13. Какой основной инструмент используется для фиксации и отслеживания ошибок/заявок пользователей?

14. Что входит в обязанности службы технической поддержки клиентов?

15. Чем отличается техническая поддержка первого уровня от второго и третьего уровней?

16. Какие показатели эффективности работы службы сопровождения вы можете назвать?

17. Какие методы улучшения качества обслуживания клиентов можно использовать в рамках сопровождения?

18. Какие меры предосторожности принимаются для предотвращения сбоев и отказов системы?

19. Что такое мониторинг производительности системы и зачем он нужен?

20. Какие шаги предпринимаются для обновления и модернизации программного обеспечения?

21. Что такое аттестация информационных систем? Для каких целей она проводится?

22. Какие нормативные акты регулируют аттестационные мероприятия в РФ?

23. Какие требования предъявляются к информационным системам при аттестации?

24. Кто несет ответственность за проведение аттестации?

25. Какие стадии проходит процесс аттестации информационной системы?

26. Какие тесты проводятся в ходе аттестации? Приведите примеры.

27. Какие критерии используются для оценки соответствия системы требованиям безопасности?

28. Какие санкции возможны в случае несоответствия системы установленным стандартам?

29. Можно ли автоматизировать процессы аттестации? Если да, то каким образом?

30. Какие документы оформляются по итогам успешной аттестации?

4. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

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.

Цель практических работ по дисциплине: освоение и закрепление на практических занятиях основных положений ЕСКД и ЕСПД.

Практикум содержит 6 практических работ, при выполнении которых требуется обращение к сети Интернет, то есть предполагается проведение этих занятий в компьютерном классе.

Практические работы проводятся в компьютерных классах института цифровых технологий.

В результате выполнения практических работ ожидается, что студенты приобретут навыки по разработке проектов нормативных документов, регламентирующих работу по защите информации в автоматизированных системах.

Тематический план практических занятий приведён в таблице 1.

Методические указания к изучению

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. Подготовка вопросов:

– Составьте список вопросов по материалу, вызвавшему затруднения.

– Обсуждение этих вопросов на практическом занятии поможет устранить пробелы в знаниях.

4. 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.

Рекомендуется в ходе выполнения задания на практическую работу использовать доступные в компьютерном классе средства компьютеризации и электронного доступа к информационным ресурсам кафедры, сети Интернет.
Подготовка отчета по выполненной практической работе осуществляется в соответствии с рекомендованной преподавателем формой отчета.

Рекомендуется прикрепить отчёт по каждой практической работе в контейнер в ЭИОС. В этой же системе можно посмотреть требования преподавателя по форме отчёта и по срокам выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1
Раздел 1. Нормативная база по проектированию

Тема 1. Законодательство по информационной безопасности в области критической информационной инфраструктуры (КИИ).

Задание: используя возможности глобальной сети Интернет, выбрать ФЗ, Указы Президента РФ, Постановления правительства, Приказы ФСТЭК, документы ФСБ, ГОСТы, другие НПА, которыми надо руководствоваться при про-

ектировании информационных объектов КИИ, при этом можно руководствоваться информацией, представленной на рисунках 1, 2.

Рисунок 1 – Нормативные документы по ИБ АСУ ТП

Согласно рисунку 1 остаётся вопрос, каким образом определиться, как решить вопрос и какие нормативные документы использовать, чтобы определить, что субъект не является субъектом КИИ. В этом случае можно воспользоваться следующей схемой принятия решения (рисунок 2).

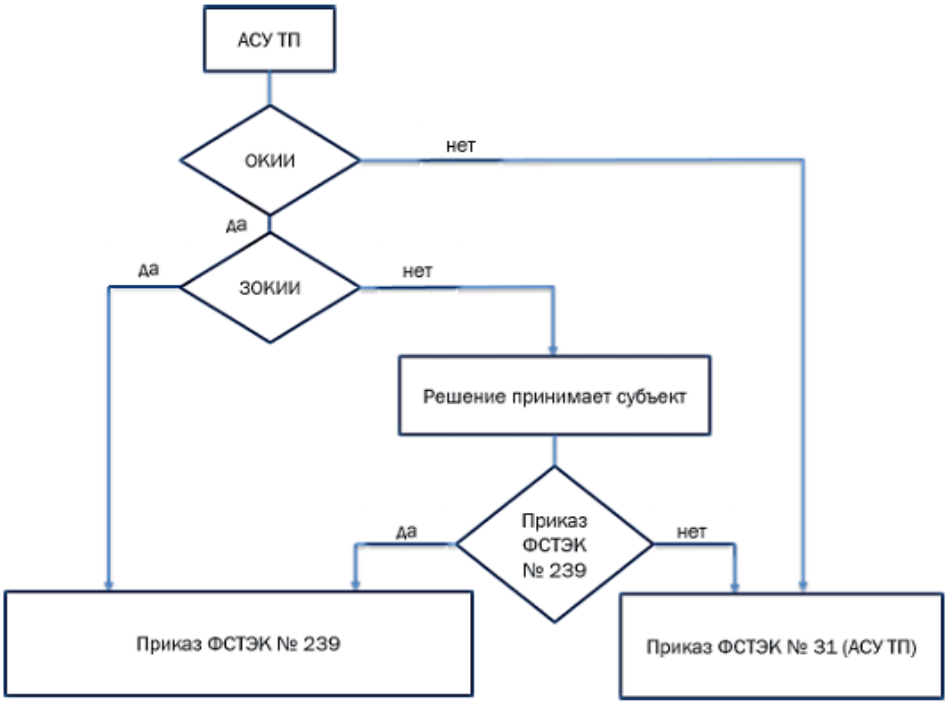

Рисунок 2 – Схема принятия решения при выборе субъекта КИИ и не субъекта КИИ

Методические указания и порядок выполнения работы:

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в данном УМПД.

2. Выполнить индивидуальное задание по практическому занятию, которое выдает преподаватель согласно варианта и порядка выполнения работы.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– выполненное задание.

– ответить на контрольные вопросы.

Контрольные вопросы

1. Какие ключевые нормативные правовые акты регулируют информационную безопасность критической информационной инфраструктуры в России?

2. Какова роль Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в контексте защиты КИИ?

3. Что такое критическая информационная инфраструктура согласно законодательству? Приведите определение.

4. Какие организации относятся к субъектам критической информационной инфраструктуры? Какие отрасли экономики считаются наиболее важными в этой сфере?

5. Кто является ответственным за обеспечение информационной безопасности объектов КИИ? Опишите обязанности владельцев значимых объектов.

6. Какие меры предпринимаются государством для выявления уязвимостей в системах КИИ? Какие методы применяются для оценки рисков?

7. В каких случаях и каким образом происходит аттестация объектов КИИ? Какие требования предъявляются к аттестационным процедурам?

8. Каковы возможные последствия нарушения требований законодательства в области обеспечения информационной безопасности КИИ?

9. Назовите основные этапы проектирования системы защиты информации для объектов КИИ. Какие стандарты и нормы учитываются на каждом этапе?

10. Какое значение имеет взаимодействие между владельцами объектов КИИ и государственными органами, отвечающими за защиту национальной безопасности?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2
Раздел 1. Нормативная база по проектированию

Тема 2. Выбор нормативных документов по информационной безопасности в области АСУ ТП.

Задание: привести нормативные документы, которыми руководствуются при проектировании ИС в топливно-энергетическом комплексе (ТЭК). Отчёт предоставить в электронном виде.

Цель работы: на основании выданного задания (актуальный кейс) по теме практического занятия необходимо проработать и зафиксировать с обоснованием в отчёте информацию по НПА, отражающую проблематику индивидуального кейса.

Методические указания и порядок выполнения работы:

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения, представленные в данном методическом указании.

2. Выполнить задание.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– описание выполнения задания;

– вывод;

– ответить на контрольные вопросы

Контрольные вопросы (и краткие ответы)

1. Какие основные нормативные документы регулируют информационную безопасность в сфере АСУ ТП?

– Ответ: Например, ГОСТ Р 51583-2014, СТО БР ИББС-1.0-2014, РД ФСТЭК России.

2. Что такое ГОСТ Р 51583-2014 и какие требования он устанавливает?

– Ответ: Это российский стандарт, который определяет требования к обеспечению информационной безопасности АСУ ТП. Он включает меры защиты от несанкционированного доступа, обеспечение целостности данных и другие аспекты кибербезопасности.

3. Какие уровни защищенности АСУ ТП выделяются в российских стандартах?

– Ответ: Обычно выделяют несколько уровней, в зависимости от критичности системы. Например, в ГОСТ Р 51583-2014 описаны три уровня защищённости: первый – базовый уровень защиты, второй – повышенный, третий – высокий.

4. Какие особенности имеет нормативно-правовая база в области информационной безопасности АСУ ТП в России?

– Ответ: Она сочетает российские стандарты (например, ГОСТ), отраслевые регламенты (СТО) и рекомендации государственных органов (ФСТЭК).

5. Какие риски учитываются при выборе нормативных документов для обеспечения информационной безопасности АСУ ТП?

– Ответ: Необходимо учитывать угрозы утечки данных, нарушения конфиденциальности, отказы оборудования, возможность вмешательства злоумышленников в процессы управления технологическим оборудованием.

6. Каковы основные этапы процесса выбора нормативных документов для конкретной АСУ ТП?

– Ответ: Процесс включает оценку рисков, определение требований законодательства, выбор стандартов и рекомендаций, разработку плана мероприятий по внедрению мер защиты.

7. Какие требования предъявляются к документации по информационной безопасности АСУ ТП согласно российским стандартам?

– Ответ: Должны быть разработаны политики безопасности, планы реагирования на инциденты, инструкции для персонала, а также процедуры мониторинга и аудита.

8. Какие меры защиты обязательны для реализации в рамках обеспечения информационной безопасности АСУ ТП?

– Ответ: Среди обязательных мер можно назвать внедрение межсетевых экранов, использование шифрования данных, проведение регулярного резервного копирования, управление доступом пользователей.

9. Какие международные стандарты используются для обеспечения информационной безопасности АСУ ТП?

– Ответ: Международные стандарты включают ISO/IEC 27001 (система менеджмента информационной безопасности), IEC 62443 (безопасность промышленных сетей и устройств).

10. Почему важно учитывать специфику отрасли при выборе нормативных документов для АСУ ТП?

– Ответ: В разных отраслях требования к защите данных и управлению рисками различаются. Например, нефтегазовые компании сталкиваются с одними угрозами, тогда как предприятия химической промышленности – с другими.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3
Раздел 1. Нормативная база по проектированию

Тема 3. Нормативная база по проектированию. О применении Единой системы программной документации (ЕСПД). О применении Единой системы конструкторской документации (ЕСКД).

Задание: изучив лекционный материал, распределить представленные в задании стандарты по соответствующим сериям:

ГОСТ Р ИСО/МЭК 15910-2002

ГОСТ 34.003-90

ГОСТ Р 2 .105-2019

ГОСТ-19-102-77

Отчёт предоставить в электронном виде.

Цель работы: изучить лекционный материал и применить на практике знания по применению ЕСКД и ЕСПД.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения.

2. Выполнить задание.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– выполнение задания;

– ответить на контрольные вопросы.

Контрольные вопросы (краткие примерные ответы)

1. Какие стандарты относятся к серии ГОСТ Р ИСО/МЭК?

– Пример ответа: ГОСТ Р ИСО/МЭК 15910-2002

2. Какой стандарт относится к серии ГОСТ 34?

– Пример ответа: ГОСТ 34.003-90

3. Какой стандарт является частью серии ГОСТ Р 2?

– Пример ответа: ГОСТ Р 2.105-2019

4. Какая серия стандартов включает в себя ГОСТ-19-102-77?

– Пример ответа: Серия ГОСТ-19

5. Опишите основную цель стандарта ГОСТ Р ИСО/МЭК 15910-2002.

– Пример ответа: Этот стандарт устанавливает требования к процессу управления конфигурацией программного обеспечения.

6. В каком стандарте описаны правила выполнения конструкторских документов?

– Пример ответа: ГОСТ Р 2.105-2019

7. Для каких целей предназначен стандарт ГОСТ 34.003-90?

– Пример ответа: Стандарт описывает автоматизированные системы и их классификацию.

8. К какой области деятельности относится стандарт ГОСТ-19-102-77?

– Пример ответа: Это стандарт, относящийся к документации на программное обеспечение.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4
Раздел 2. Проектирование автоматизированных систем в защищённом исполнении

Тема 4. Техническое оформление документов. Общие требования

Задание: правила ГОСТ к оформлению тестовых документов отличаются. Всё зависит от того, кто утверждал стандарт. Изучив материал лекции, разобраться и описать разницу и сходство редакций ГОСТ:

– Межгосударственный стандарт ГОСТ 2.105-95»

– Национальный стандарт ГОСТ Р 2.105-2019»

– Отчёт предоставить в электронном виде.

Цель работы: изучить общие принципы оформления технических документов

Методические указания и порядок выполнения работы:

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения.

2. Выполнить задание.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– выполнение задания;

– ответить на контрольные вопросы.

Контрольные вопросы

1. В чём заключается основное назначение стандарта ГОСТ 2.105?

2. Какие изменения были внесены в структуру документа между версиями ГОСТ 2.105-95 и ГОСТ Р 2.105-2019?

3. Опишите различия в области применения двух стандартов.

4. Какая информация содержится в разделе «Обозначения» в каждой версии стандарта? Есть ли отличия?

5. Перечислите основные термины и определения, добавленные в ГОСТ Р 2.105-2019 по сравнению с ГОСТ 2.105-95.

6. В каких аспектах требования к оформлению документов стали строже в новой редакции стандарта?

7. Какие дополнительные требования к графическим документам появились в ГОСТ Р 2.105-2019?

8. Опишите основные элементы структуры документа согласно обеим версиям стандарта.

9. В чём заключаются ключевые улучшения, внесённые в правила оформления титульных листов в ГОСТ Р 2.105-2019?

10. Назовите три примера отличающихся требований к нумерации страниц и разделов в обеих версиях стандарта.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5

Раздел 2. Проектирование автоматизированных систем в защищённом исполнении

Тема 5. Техническое задание

Цель работы: закрепление теоретического материала по теме лекционного материала.

Задание: изучив материал лекции, ознакомиться с примерами оформления ТЗ, которые выложены в ЭИОС. Оформить техническое задание (шаблон взять в ЭИОС) по теме: ТЕХНИЧЕСКОЕ ЗАДАНИЕ на создание системы защиты персональных данных информационной системы персональных данных. Дополнительные входные данные по этому заданию взять у преподавателя. Отчёт предоставить в электронном виде.

Методические указания и порядок выполнения работы:

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и ознакомиться с литературой.

2. Выполнить задание.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– выполнение задания

– ответить на контрольные вопросы

Контрольные вопросы

1. Каковы цели создания системы защиты персональных данных?

2. Какие нормативные акты регулируют требования к защите персональных данных в данном случае?

3. Какие категории персональных данных подлежат защите согласно техническому заданию?

4. Какие угрозы безопасности данных рассматриваются в техническом задании?

5. Какие методы и средства защиты данных предусмотрены техническим заданием?

6. Какие организационные меры по обеспечению безопасности данных включены в техническое задание?

7. Какие технические меры по обеспечению безопасности данных указаны в техническом задании?

8. Какие роли и ответственности сотрудников организации описаны в техническом задании?

9. Какие требования предъявляются к мониторингу и аудиту безопасности данных?

10. Какие критерии оценки эффективности системы защиты данных определены в техническом задании?

11. Какие этапы реализации проекта предусмотрены техническим заданием?

12. Какие сроки выполнения этапов работ установлены в техническом задании?

13. Какие условия приемки выполненных работ предусмотрены техническим заданием?

14. Какие документы и материалы должны быть предоставлены заказчику после завершения каждого этапа работ?

15. Какие гарантии качества выполненных работ предоставляются исполнителем?

16. Какие обязательства сторон закреплены в техническом задании?

17. Какие санкции предусмотрены за нарушение условий технического задания?

18. Какие дополнительные услуги могут быть оказаны исполнителем в рамках данного проекта?

19. Какие риски связаны с реализацией проекта и как они учитываются в техническом задании?

20. Какие изменения могут быть внесены в техническое задание и каким образом они оформляются?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6

Раздел 2. Проектирование автоматизированных систем в защищённом исполнении

Тема 6. Аттестация

Цель работы: закрепление теоретического материала по теме занятия.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и дополнительно литературу.

Задание: изучив материал лекции, ознакомиться с примерами оформления аттестата соответствия требованиям по защите информации, который представлен в ЭИОС. Оформить аттестационный документ защищаемого помещения 363 ауд. Необходимые исходные данные и документы получить у преподавателя. Документ предоставить в электронном виде.

СПИСОК ЛИТЕРАТУРЫ ДЛЯ ПОДГОТОВКИ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

Современные профессиональные базы данных (СПБД) и информационные справочные системы (ИСС).

1. https://www.swrit.ru/gost-espd.html.
2. https://www.swrit.ru/gost-eskd.html.
3. https://www.swrit.ru/gost-iso-mek.html.

При подготовке к практическому занятию изучить материалы справочных систем по теме занятия (см. выше).

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОЙ ПОДГОТОВКЕ

Внеаудиторная самостоятельная работа в рамках данной дисциплины включает в себя:

• подготовку к аудиторным занятиям (лекциям, практическим занятиям) и выполнение соответствующих заданий;

• самостоятельную работу над отдельными темами учебной дисциплины в соответствии с тематическим планом;

• подготовку к экзамену.

Подготовка к лекционным занятиям

При подготовке к лекции рекомендуется повторить ранее изученный материал, что дает возможность получить необходимые разъяснения преподавателя непосредственно в ходе занятия. Рекомендуется вести конспект, главное требование к которому быть систематическим, логически связанным, ясным и кратким. По окончанию занятия обязательно в часы самостоятельной подготовки, по возможности в этот же день, повторить изучаемый материал и доработать конспект.

Подготовка к практическим занятиям

Подготовка к практическим занятиям предусматривает:

• изучение теоретических положений по изучаемой теме;

• детальную проработку учебного материала, рекомендованной литературы и методической разработки на предстоящее занятие.

Самостоятельная работа над отдельными темами учебной дисциплины

При организации самостоятельного изучения ряда тем лекционного курса обучаемый работает в соответствии с указаниями, выданными преподавателем. Указания по изучению теоретического материала курса составляются дифференцированно по каждой теме и включают в себя следующие элементы: название темы; цели и задачи изучения темы; основные вопросы темы; характеристику основных понятий и определений, необходимых обучаемому для усвоения данной темы; список рекомендуемой литературы; наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т. п.; краткие выводы, ориентирующие обучаемого на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить; контрольные вопросы, предназначенные для самопроверки знаний.

Подготовка к диф. зачёту

При подготовке к диф. зачёту большую роль играют правильно подготовленные заранее записи и конспекты. В этом случае остается лишь повторить пройденный материал, учесть, что было пропущено, восполнить пробелы, закрепить ранее изученный материал.

В ходе самостоятельной подготовки к диф. зачёту при анализе имеющегося теоретического и лабораторного материала студенту также рекомендуется проводить постановку различного рода задач по изучаемой теме, что поможет в дальнейшем выявлять критерии принятия тех или иных решений, причины совершения определенного рода ошибок. При ответе на вопросы, поставленные в ходе самостоятельной подготовки, обучающийся вырабатывает в себе способность логически мыслить, искать в анализе событий причинно-следственные связи.

Вопросы и задачи для самоподготовки по вариантам

Номер варианта	**Задание**
01	Какие сведения должен содержать протокол аттестационных испытаний объекта информатизации (АС ЗИ)? Представьте проект документа. Задача. Как Вы считаете, какая будет категория у ИС, если в результате нарушения ее правильного функционирования может быть причинен вред здоровью для 10 человек, а также на территории всей новосибирской области окружающая среда может под-

Номер варианта	Задание
	вергнуться вредным воздействиям
02	Какие сведения должны содержаться в заключении по результатам аттестационных испытаний? Приведите список. Задача. Какой класс защищенности будет у АС, если один пользователь, допущен ко всей информации АС, в которой обрабатывается лишь секретная информация?
03	Какие мероприятия предусматривает этап «Сопровождение эксплуатации» АС ЗИ? Приведите перечень. Задача. Определить класс защищенности ГИС, составить акт классификации ГИС
04	Описание документов, что должно включаться в «Технический проект» на АС ЗИ? Приведите перечень. Задача. Определить тип угрозы для ИСПДн, если в используемой информационной системе имеются недокументированные (не декларированные) возможности в прикладном программном обеспечении
05	Какие этапы включает «Ввод в действие» АС ЗИ? Представьте перечень этапов. Задача. В АС обрабатывается и хранится информация различного уровня конфиденциальности, к которой пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС. Определите группу? От чего зависит класс?
06	В каких случаях проводится повторная аттестация? Перечислите возможные варианты. Задача. Какой тип угроз для ИСПДн будет, если в используемой информационной системе имеются недокументированные (не декларированные) возможности не связаны ни с системным программном обеспечении, ни с прикладным
07	Перечень и описание того, что должно включаться в «Эскизный проект» на АС ЗИ? Приведите перечень. Задача. Как Вы считаете, какая будет категория у ИС, если в результате нарушения ее правильного функционирования может быть снижен объем выпускающей продукции на 20 %? По остальным критериям значимости показатели отсутствуют
08	Какой порядок разработки и утверждения документа «Программа и методики аттестационных испытаний»? Предоставить титульный лист документа с указанием произвольным указанием наименований Заказчика и Исполнителя. Задача. Как Вы считаете, какая будет категория у ИС, если в ре-

Номер варианта	Задание
	зультате нарушения ее правильного функционирования может быть причинен вред здоровью для 10 человек, а также на территории всей новосибирской области окружающая среда может подвергнуться вредным воздействиям
09	Перечислите документы, разрабатываемые лицензиатом в процессе проведения аттестации, форма которых утверждена нормативными документами ФСТЭК России? Оформить перечень. Задача. Как Вы считаете, какая будет категория у ИС, если в результате нарушения ее правильного функционирования может быть срыв подписания межправительственного договора? По остальным критериям значимости показатели отсутствуют
10	В каких случаях аттестат соответствия требования по защите информации на объект информатизации приостанавливается? Задача. Как Вы считаете, какая будет категория у ИС, если в результате нарушения ее правильного функционирования может быть причинен вред здоровью одному человеку? По остальным критериям значимости показатели отсутствуют
11	Какие процедуры (мероприятия) необходимо провести при формировании требований к АС ЗИ? Представить перечень итоговых документов. Задача. В АС обрабатывается и хранится информация различного уровня конфиденциальности, к которой пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС. Определите группу? От чего зависит класс?
12	Перечень документов разрабатываемые владельцем объекта информатизации (АС ЗИ) для представления их в орган по аттестации? Представить перечень Задача. К какой группе относятся многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС?
13	Какие сведения указывают в ТЗ на АС в разделе «Порядок разработки АС». Описать разделы. Задача. Какой класс защищенности будет у АС, если один пользователь, допущен ко всей информации АС, в которой обрабатывается лишь секретная информация?
14	Какую форму оценки соответствия необходимо выбрать для объекта информатизации – АС ЗИ планируемого к эксплуатации в государственном органе для обработки информации содержащей

Номер варианта	Задание
	персональные данные сотрудников организации? Описать этапы оценки соответствия мер защиты информации в АСЗИ. Задача. Определить класс ГИС, если масштаб информационной системы является федеральным, а уровень защищённости УЗ1
15	Какими документами необходимо пользоваться при разработке технического задания на программные средства информационной системы? Представить перечень ГОСТов. Задача. Определить класс ГИС, если масштаб информационной системы является объектовым, а уровень защищённости УЗ1
16	Каков порядок проведения аттестационных испытаний АС ЗИ? Оформить порядок с описанием этапов. Задача. Определить класс ГИС, если масштаб информационной системы является региональным а уровень защищённости УЗ2
17	Каков перечень разрабатываемых документов при разработке рабочей документации на проектируемую АС ЗИ? Представить перечень документов. Задача. Определить уровень значимости информации в ГИС, если степень ущерба от нарушения конфиденциальности высокая, а степень от нарушения доступности и целостности – низкая.
18	Какие основные разделы включены в «Общие сведения» ТЗ на создание АС? Представить разделы с примерами наполнения данного раздела. Задача. Определите уровень защищенности ИСПДН, если в информационной системе обрабатываются персональные данные сотрудников организации. Количество обрабатываемых персональных данных составляет 100 человек. Категория ПДн – иные. Актуальные угрозы безопасности ПДН не связаны с наличием недокументированных возможностей в системном и прикладном программном обеспечении
19	На этапе формирования требований к АС какие цели и задачи решаются их описанием в ТЗ? Привести пример. Задача. Определите уровень защищенности ИСПДН, если в информационной системе обрабатываются персональные данные сотрудников организации. Количество обрабатываемых персональных данных составляет 1000 человек. Категория ПДн – биометрические. Актуальные угрозы безопасности ПДН связаны с наличием недокументированных возможностей в системном программном обеспечении
25	При эксплуатации систем защиты информации информационных

Номер варианта	Задание
	систем должны быть учтены и другие нормативные документы. Представить перечень документов. Задача. Какой тип угроз для ИСПДн будет, если в используемой информационной системе имеются недокументированные (не декларированные) возможности не связаны ни с системным программном обеспечении, ни с прикладным
26	Как происходит аттестация информационной системы по требованиям защиты информации и ввод ее в действие? Описать порядок аттестации и этапы ввода в эксплуатацию Задача. Какой тип угроз для ИСПДн будет, если в используемой информационной системе имеются недокументированные (не декларированные) возможности в системном программном обеспечении
27	Основные этапы внедрения в эксплуатацию автоматизированной системы в защищенном исполнении? Описать этапы и их наполнение Задача. Определить класс защищенности ГИС, составить акт классификации ГИС
28	Кем разрабатывается техническое задание на автоматизированную систему в защищенном исполнении (АС ЗИ) с кем согласовывается и утверждается ТЗ? Разработать и представить титульный лист ТЗ на произвольную систему с произвольным указанием наименований Заказчика и Исполнителя. Задача. Определить тип угрозы для ИСПДн, если в используемой информационной системе имеются недокументированные (не декларированные) возможности в прикладном программном обеспечении
29	Какими документами необходимо пользоваться при разработке технического задания (ТЗ) на технические (аппаратные) средства информационной системы? Представить перечень ГОСТов. Задача. Определите уровень защищенности ИСПДН, если в информационной системе обрабатываются персональные данные сотрудников организации. Количество обрабатываемых персональных данных составляет 500 человек. Категория ПДн – иные. Актуальные угрозы безопасности ПДН связаны с наличием недокументированных возможностей в прикладном программном обеспечении

Пример решения задачи по варианту 8

Какой порядок разработки и утверждения документа «Программа и методики аттестационных испытаний»? Предоставить титульный лист документа с указанием произвольным указанием наименований Заказчика и Исполнителя.

Задача. Как Вы считаете, какая будет категория у ИС, если в результате нарушения ее правильного функционирования может быть причинен вред здоровью для 10 человек, а также на территории всей новосибирской области окружающая среда может подвергнуться вредным воздействиям.

В порядке проведения аттестации объектов информатизации по требованиям безопасности информации одним из действий является:

Разработка программы и методики аттестационных испытаний. Этот шаг является результатом рассмотрения исходных данных и предварительного ознакомления с аттестуемым объектом. Орган по аттестации определяет перечень работ и их продолжительность, методику испытаний, состав аттестационной комиссии, необходимость использования контрольной аппаратуры и тестовых средств или участия испытательных лабораторий. Программа аттестационных испытаний согласовывается с заявителем.

На основании документа: УТВЕРЖДЕН приказом ФСТЭК России от 29 апреля 2021 г. № 77 Зарегистрирован Минюстом России 10 августа 2021 г. № 64589

ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ РАБОТ ПО АТТЕСТАЦИИ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ О ЗАЩИТЕ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА, НЕ СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ

Программа и методики аттестационных испытаний объекта информатизации состоят из следующих разделов:

а) общие положения;

б) программа аттестационных испытаний объекта информатизации;

в) методики аттестационных испытаний объекта информатизации.

Раздел, касающийся общих положений, должен включать следующие сведения:

а) наименование и краткое описание архитектуры объекта информатизации, класс защищенности информационной (автоматизированной) системы, категорию значимого объекта;

б) фамилии, имена, отчества (при наличии), должности экспертов органа по аттестации, назначенных для проведения аттестации объекта информатизации;

в) наименование и реквизиты документов ФСТЭК России, устанавливающих требования по защите информации, на соответствие которым проводится аттестация объекта информатизации;

г) угрозы безопасности информации, актуальные для объекта информатизации, или сведения о модели угроз безопасности информации в случае ее разработки в соответствии с требованиями по защите информации.

Раздел, касающийся программы аттестационных испытаний объекта информатизации, должен включать перечень работ по аттестации объекта информатизации, в том числе работы по обследованию объекта информатизации в условиях его эксплуатации, проведению аттестационных испытаний в соответствии с разрабатываемыми методиками испытаний, оформлению результатов аттестационных испытаний, а также общий срок проведения аттестации объекта информатизации и сроки выполнения каждой работы по аттестации объекта информатизации, фамилию и инициалы эксперта органа по аттестации, ответственного за проведение каждой работы.

Раздел, касающийся методик аттестационных испытаний объекта информатизации, должен включать для каждого аттестационного испытания порядок, условия, исходные данные и методы испытаний, применяемые при проведении испытаний средства контроля эффективности защиты информации от несанкционированного доступа, а также контрольно-измерительное и испытательное оборудование.

Программа и методики аттестационных испытаний объекта информатизации согласовываются органом по аттестации с владельцем объекта информатизации и утверждаются руководителем органа по аттестации до начала аттестационных испытаний.

В ходе аттестационных испытаний объекта информатизации орган по аттестации может вносить изменения в программу и методики аттестационных испытаний объекта информатизации по согласованию с владельцем объекта информатизации.

ДОПОЛНИТЕЛЬНО ВЫДЕРЖКИ ИЗ СТАНДАРТОВ

Стадии жизненного цикла автоматизированных систем по ГОСТ Р 51583 2014

Согласно ГОСТ 34.603-92 Виды испытаний

Для планирования проведения всех видов испытаний разрабатывают документ «Программа и методика испытаний». Разработчик документа устанавливается в договоре или ТЗ.

Программа и методика испытаний должны устанавливать необходимый и достаточный объем испытаний, обеспечивающий заданную достоверность получаемых результатов.

Согласно ГОСТ Р ИСО/МЭК ТО 15271-2002 процесс аттестация относится к вспомогательным процессам жизненного цикла

ГОСТ Р 59795-2021 Информационные технологии. КОМПЛЕКС СТАНДАРТОВ НА АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ Автоматизированные системы. Требования к содержанию документов

Программа и методика испытаний (компонентов, комплексов средств автоматизации, подсистем, систем)

Документ «Программа и методика испытаний» для компонентов АС и комплексов средств автоматизации предназначен для установления техниче-

ских данных, подлежащих проверке при испытании компонентов АС и комплексов средств автоматизации, а также порядка и методов испытаний.

Документ «Программа и методика испытаний» для АС (подсистемы) предназначен для:

– установления данных, обеспечивающих получение и проверку проектных решений;

– выявления причин сбоев;

– определения качества работ;

– оценки качества функционирования АС (подсистемы);

– проверки соответствия АС требованиям техники безопасности;

– установления продолжительности и режима испытаний.

Документ «Программа и методика испытаний» должен содержать перечни конкретных проверок (решаемых задач), которые следует осуществлять при испытаниях для подтверждения выполнения требований ТЗ на АС, со ссылками на соответствующую методику (разделы методики) испытаний.

Документ может содержать одну или несколько методик испытаний.

Перечень проверок, подлежащих включению в программу и методику испытаний, включает проверки:

– соответствия АС требованиям ТЗ на АС;

– комплектности АС;

– качества документации;

– выполнения функций АС или частей АС во всех режимах функционирования, установленных в ТЗ на АС;

– количества и квалификации обслуживающего персонала;

– выполнения требований техники безопасности, противопожарной безопасности, экологичности, эргономики.

Описание методов испытаний АС по отдельным показателям рекомендуется располагать в той же последовательности, в которой эти показатели расположены в требованиях ТЗ на АС.

Программа испытаний должна содержать разделы:

– объект испытаний;

– цель испытаний;

– общие положения;

– объем испытаний;

– условия и порядок проведения испытаний;

– материально-техническое обеспечение испытаний;

– метрологическое обеспечение испытаний;

– отчетность.

В документ включают приложения.

В зависимости от особенностей АС допускается объединять или исключать отдельные разделы при условии изложения их содержания в других разделах программы испытаний, а также включать в нее дополнительные разделы (при необходимости).

Оформление документа

Документ выполняют на формах, установленных соответствующими стандартами Единой системы конструкторской документации (ЕСКД).

Для размещения утверждающих и согласующих подписей к документу рекомендуется составлять титульный лист и (или) лист утверждения.

Текст документа при необходимости разделяют на разделы и подразделы. Разделы, подразделы должны иметь заголовки. Пункты, как правило, заголовков не имеют. Заголовки должны четко и кратко отражать содержание разделов, подразделов.

Текст документа должен быть кратким, четким и не допускать различных толкований.

Согласно Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями)

Информационные системы включают в себя:

1) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

Определение «государственной информационной системы» формируется исходя из ее признаков. Государственная информационная система – это информационная система, которая:

– создана на основании федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов (п. 1 ч. 1 ст. 13 Федерального закона № 149-ФЗ);

– создана в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях (ч. 1 ст. 14 Федерального закона № 149-ФЗ).

ОБ УТВЕРЖДЕНИИ ПРАВИЛ КАТЕГОРИРОВАНИЯ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ, А ТАКЖЕ ПЕРЕЧНЯ ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ИХ ЗНАЧЕНИЙ

(с изменениями от 24 декабря 2021 г., 19 августа 2022 г.)

УТВЕРЖДЕН
постановлением Правительства
Российской Федерации
от 8 февраля 2018 г. N 127
(в ред. постановления Правительства Российской Федерации
от 13 апреля 2019 г. N 452)

ПЕРЕЧЕНЬ ПОКАЗАТЕЛЕЙ КРИТЕРИЕВ ЗНАЧИМОСТИ ОБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ И ИХ ЗНАЧЕНИЯ

Социальная значимость

По показателю

Причинение ущерба жизни и здоровью людей (до 50 человек).

В случае нашей задачи – 10 человек. По показателю социальная значимость ИС относится к III категории.

Экологическая значимость.

По показателю

Вредные воздействия на окружающую среду (например, ухудшение качества воды в поверхностных водоемах, обусловленное сбросами загрязняющих веществ, повышение уровня вредных загрязняющих веществ, в том числе радиоактивных веществ, в атмосферу, ухудшение состояния земель в результате выбросов или сбросов загрязняющих веществ или иные вредные воздействия.), оцениваемые:

а) на территории, на которой окружающая среда может подвергнуться вредным воздействиям;

выход за пределы территории одного муниципального образования (численностью от 2 тыс. чел.) или одной внутригородской территории города федерального значения, **но не за пределы территории одного субъекта Российской Федерации** или территории города федерального значения, с выходом вредных воздействий за пределы территории субъекта критической информационной инфраструктуры.

ОТВЕТ: в случае условия нашей задачи ИС относится по показателю Экологическая зависимость ко II категории

Вопросы для самоподготовки

1. Что понимается под КИИ?

2. Чем определяется принадлежность объектов к КИИ? Что относится к субъектам КИИ?

3. Какие силы и средства относятся к системе ГосСОПКА?

4. Перечислите основные задачи системы безопасности значимого объекта КИИ?

5. Как осуществляется государственный контроль в области обеспечения безопасности значимых объектов КИИ?

6. Обязаны ли субъекты КИИ оказывать содействие должностным лицам ФСБ России в обнаружении компьютерных атак?

7. Какие виды ответственности предусмотрены за нарушение требований Федерального закона № 187-ФЗ?

6. КОНТРОЛЬ И АТТЕСТАЦИЯ

К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

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

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 3).

Таблица 3 – Система оценок и критерии выставления оценки

Система оценок				
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
Критерий	**«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, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное	Не может делать	В состоянии	В состоянии	В состоянии

Система оценок / Критерий				
	0–40 %	**41–60 %**	**61–80 %**	**81–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
осмысление изучаемого явления, процесса, объекта	научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	осуществлять научно-корректный анализ предоставленной информации	осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных 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 поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

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.

Задание открытого и закрытого типа приведены в ФОС (приложении к рабочему модулю).

Типовые контрольные задания и иные материалы, необходимые для оценки результатов освоения дисциплин модуля (в том числе в процессе освоения), а также методические материалы, определяющие процедуры этой оценки приводятся в приложении к рабочей программе модуля. Оценивание результатов обучения проводится с применением электронного обучения, дистанционных образовательных технологий.

7. СПИСОК ЛИТЕРАТУРЫ

Основная литература

1. Правовые нормы защиты информации в автоматизированных системах: учеб. пособие / Н. В. Киреева, А. В. Крыжановский, И. С. Поздняк [и др.]. – Самара: ПГУТИ, 2020. – 60 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/255446 (дата обращения: 09.10.2024). – Текст : электронный.

2. Епишкина, А. В. Нормативное регулирование в области защиты информации. Конспект лекций: учеб. пособие / А. В. Епишкина, С. В. Запечников. – Москва: НИЯУ МИФИ, 2021. – 116 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/284345 (дата обращения: 09.10.2024). – ISBN 978-5-7262-2807-5. – Текст : электронный.

3. Шароватов, Е. В. Разработка защищенных телекоммуникационных систем специального назначения: учеб. пособие / Е. В. Шароватов. – Москва: РТУ МИРЭА, 2024. – 171 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/421046 (дата обращения: 10.12.2024). — ISBN 978-5-7339-2166-2. – Текст : электронный.

Дополнительная литература:

4. Киренберг, А. Г. Защита информации от утечки по техническим каналам: учеб. пособие / А. Г. Киренберг, В. О. Коротин. – Кемерово: КузГТУ имени Т.Ф. Горбачева, 2023. – 222 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/399665 (дата обращения: 09.10.2024). – ISBN 978-5-00137-407-7. – Текст : электронный.

5. Корнилова, А. А. Защита персональных данных: учеб. пособие / А. А. Корнилова, Д. С. Юнусова, А. С. Исмагилова. – Уфа: БашГУ, 2020. – 120 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/179914 (дата обращения: 09.10.2024). – ISBN 978-5-7477-5228-3. – Текст : электронный.

6. 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: 09.10.2024). – Текст : электронный.

Учебно-методические пособия по дисциплине, нормативно-правовые акты

7. Великите, Н. Я. Разработка проектной документации для информационных систем: учеб.-метод. пособие по изучению дисциплины для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 26 с. – URL: https://klgtu.ru/vikon/sveden/files/ril/UMP_Razrabotka_proektnoi_dokumentacii_dlya_informacionnyx_sistem.pdf (дата обращения: 09.10.2024). – Текст : электронный.

8. Проектирование информационных систем: методические указания / сост. В. В. Коваленко. – Сочи: СГУ, 2020. – 40 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/172149 (дата обращения: 09.12.2024). – Текст : электронный.

9. «ГОСТ Р ИСО/МЭК 15408-1-2012. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» (утв. и введен в действие Приказом Росстандарта от 15.11.2012 N 814-ст) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

10. Приказ ФСТЭК России от 14.03.2014 N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» (Зарегистрировано в Минюсте России 30.06.2014 N 32919) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

11. Приказ ФСБ России от 24.07.2018 N 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации послед-

ствий компьютерных атак на информационные ресурсы Российской Федерации» (Зарегистрировано в Минюсте России 06.09.2018 N 52108) (в действующей редакции). – Режим доступа: для авториз. пользователей из справ.-правовой системы КонсультантПлюс. – Текст: электронный.

Состав современных профессиональных баз данных (СПБД) и информационных справочных систем (ИСС)

12. https://www.swrit.ru/gost-espd.html
13. https://www.swrit.ru/gost-eskd.html
14. https://www.swrit.ru/gost-iso-mek.html

Локальный электронный методический материал

Наталья Яронимо Великите

РАЗРАБОТКА ПРОЕКТНОЙ ДОКУМЕНТАЦИИ ДЛЯ ИНФОРМАЦИОННЫХ СИСТЕМ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 4,5. Печ. л. 3,4.

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