Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий

Корсунский А.С.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ ПО ДИСЦИПЛИНЕ «СЕРТИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ»

Для студентов специалитета по специальности 10.05.03 очной формы обучения

Ульяновск, 2020

Методические указания для самостоятельной работы студентов по дисциплине «Сертификация средств защиты информации» / составитель: А.С. Корсунский. - Ульяновск: УлГУ, 2021. Настоящие методические указания предназначены для студентов специалитета по специальности 10.05.03 очной формы обучения. В работе приведены литература по дисциплине, основные темы курса и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля и тесты для самостоятельной работы. Студентам очной формы обучения они будут полезны при подготовке к лекциям, семинарам, лабораторным и курсовым работам и к экзамену по данной дисциплине.

Рекомендованы к введению в образовательный процесс Ученым советом факультета математики, информационных и авиационных технологий УлГУ (протокол № 6/20 от 22.09.2020 г.).

Содержание

№ п/п	Наименование раздела	Стр.
1.	Литература для изучения дисциплины	4
2.	Методические указания	6
2.1	Раздел 1. Основы сертификации средств защиты информации по требованиям безопасности информации. Тема 1. Виды и системы сертификации	6
2.2	Раздел 1. Тема 2. Участники и порядок сертификации по требованиям защиты информации	7
2.3	Раздел 1. Тема 3. Руководящие документы ФСТЭК России	8
2.4	Раздел 2. Порядок проведения сертификации средств защиты информации. Тема 4. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации	9
2.5	Раздел 2. Тема 5. Сертификация программного обеспечения по требованиям безопасности информации	11
2.6	Раздел 2. Тема 6. Сертификация по требованиям безопасности информации по «Общим критериям»	12
2.7	Раздел 3. Методы и средства проведения сертификационных испытаний. Тема 7. Применение автоматизированных средств	13
2.8	Раздел 3. Тема 8. Порядок проведения сертификационных испытаний	14
2.9	Раздел 3. Тема 9. Проверка производства сертифицированных средств защиты информации	15

1. ЛИТЕРАТУРА ДЛЯ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ

основная

1. Положение о системе сертификации средств защиты информации (Приказ ФСТЭК от 03.04.2018 № 55).

2. Положение о сертификации СЗИ по требованиям безопасности информации (Приказ Председателя Гостехкомиссии № 199).

3. Свинарев Н.А., Инструментальный контроль и защита информации [Электронный ресурс]: учеб. пособие / Свинарев Н.А., Ланкин О.В., Данилкин А.П, Потехецкий С.В., Перетокин О.И. - Воронеж: ВГУИТ, 2013. - 192 с. - ISBN 978-5-00032-018-1 - Режим доступа: http://www.studentlibrary.ru/book/ISBN9785000320181.html

4. Руководство по эксплуатации программного средства «АК-ВС» (www.npo-echelon.ru).

дополнительная

1. ГОСТ Р 50739-95. СВТ. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России

2. ГОСТ Р 50922-96. ЗИ. Основные термины и определения. Госстандарт России

3. ГОСТ Р 51188-98. ЗИ. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство. Госстандарт России

4. ГОСТ Р 51275-99. ЗИ. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Госстандарт России

5. ГОСТ Р ИСО 7498-1-99. ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель. Госстандарт России

6. ГОСТ Р ИСО 7498-2-99. ИТ. Взаимосвязь открытых систем. Базовая эталонная модель.

Часть 2. Архитектура защиты информации. Госстандарт России ГОСТ Р ИСО/МЭК 15408-1-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Ведение и общая модель. Госстандарт России

7. ГОСТ Р ИСО/МЭК 15408-2-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности. Госстандарт России

8. ГОСТ Р ИСО/МЭК 15408-3-2002. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. Госстандарт России

9. ГОСТ Р 40.003-2008 Система сертификации ГОСТ Р. Регистр систем качества. Порядок сертификации СМК на соответствие ГОСТ Р ИСО 9001-2008 (ИСО 9001:2008)

10. ГОСТ Р 14.11-2005 Экологический менеджмент. Общие требования к органам, проводящим оценку и сертификацию/регистрацию СЭМ (ИСО/МЭК 66)

11. ГОСТ Р 51000.6-2008 Общие требования к аккредитации органов по сертификации продукции и услуг

12.ГОСТ Р ИСО/МЭК 65-2000 Общие требования к органам по сертификации продукции

13. ГОСТ Р ИСО/МЭК 17021-2008 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента

14. ГОСТ Р 40.002-2000 Система сертификации ГОСТ Р. Регистр систем качества. Основные положения

15. ГОСТ Р 50460-92 Знак соответствия при обязательной сертификации. Форма, размеры и технические требования

16. ГОСТ Р 51171-98 Качество служебной информации. Правила предъявления ИТ на сертификацию

17. ГОСТ Р 51169-98 Качество служебной информации. Система сертификации ИТ в области качества служебной информации. Термины и определения

18. ГОСТ Р 40.101-95 Государственная регистрация систем добровольной сертификации и их знаков соответствия

19. ГОСТ Р 14.11-2005 Экологический менеджмент. Общие требования к органам, проводящим оценку и сертификацию/регистрацию СЭМ (ИСО/МЭК 66)

20. ГОСТ Р 51000.6-2008 Общие требования к аккредитации органов по сертификации продукции и услуг

21. ГОСТ Р ИСО/МЭК 65-2000 Общие требования к органам по сертификации продукции

22. ГОСТ Р ИСО/МЭК 17021-2008 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента

23. Р 50.4.003-2000. Рекомендации по аккредитации. Инспекционный контроль за деятельностью в системе сертификации ГОСТ Р аккредитованных испытательных лабораторий.

учебно-методическая

1. Методические указания по написанию курсовых и дипломных работ для студентов специальности «Компьютерная безопасность» /А.С. Андреев, А.М. Иванцов, С.М. Рацеев. - Ульяновск: УлГУ, 2017. - 40 с. URL:ftp://10.2.5.225/FullText/Text/Andreev_2017.pdf.

2. Методические указания для проведения лабораторных работ по защите информации для студентов специальностей "Компьютерная безопасность", «Математическое обеспечение и администрирование информационных систем", "Инфокоммуникационные технологии и системы связи", «Системный анализ и управление» / А.С. Андреев, С.М. Бородин, А.М. Иванцов. - Ульяновск: УлГУ, 2015. 54 с.

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ

2.1. РАЗДЕЛ 1. ОСНОВЫ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ТЕМА 1. ВИДЫ И СИСТЕМЫ СЕРТИФИКАЦИИ

Основные вопросы:

1. Назначение сертификации по требованиям защиты информации.
2. Законодательно-правовые основы сертификации.
3. Обязательность сертификации.
4. Ответственность разработчиков средств защиты информации за сертификацию программных, аппаратно-программных и аппаратных средств.

Рекомендации по изучению темы:

Вопрос 1 изложен в [1].

Для самостоятельного изучения вопроса 2 следует обратиться к [1, 2].

Вопрос 2 изложен в [1].

Вопрос 3 изложен в [1].

Вопрос 4 изложен в [1, 2].

Контрольные вопросы по теме 1:

1. Основные виды сертификации.
2. Основные системы сертификации по требованиям безопасности информации.
3. Основные нормативные документы по сертификации.
4. Для кого сертификация является обязательной?
5. Ответственность разработчиков средств защиты информации ограниченного распространения.

Тесты для самостоятельной работы:

1. Какой документ, из перечисленных, не относится к сфере сертификации по требованиям безопасности информации?

а) Федеральный закон от 27 декабря 2002 г. № 184 - ФЗ «О техническом регулировании»

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

в) Положение о сертификации СЗИ по требованиям безопасности информации (Приказ Председателя Гостехкомиссии № 199).

г) ГОСТ 29339-92. Защита информации от утечки за счет побочных

электромагнитных излучений и наводок при ее обработке средствами вычислительной техники. Общие технические требования. Постановление Госстандарта России от 30.03.1992 № 343.

2. Какая из перечисленных систем сертификации не существует?
а) Система ФСТЭК России
б) Система МЧС России
в) Система ФСБ России
г) Система Минобороны России

3. Для кого сертификация по требованиям безопасности информации не является обязательной?
а) Разработчик средств защиты информации для систем, обрабатывающих персональные данные
б) Разработчик средств защиты информации для систем электронной торговли в сети Интернет
в) Разработчик средств защиты информации продукции оборонно-промышленного комплекса

2.2. РАЗДЕЛ 1. ОСНОВЫ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ТЕМА 2. УЧАСТНИКИ И ПОРЯДОК СЕРТИФИКАЦИИ ПО ТРЕБОВАНИЯМ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

1. Особенности систем сертификации ФСТЭК России, Минобороны России, ФСБ России, СВР России
2. Виды сертификационных испытаний средств защиты информации и автоматизированных систем в защищенном исполнении.
3. Инструментальная база сертификационных испытаний

Рекомендации по изучению темы:

Вопрос 1 изложен в [1].
Вопрос 2 изложен в [1].
Вопрос 3 изложен в [2].

Контрольные вопросы по теме 2:

1. Какие средства защиты информации подлежат сертификации в различных системах сертификации?
2. Какие виды сертификационных испытаний вы знаете?
3. Привести 3-4 примера сертификации средств защиты информации.
4. Что такое статический анализ кода?

5. Что такое динамический анализ кода?

Тесты для самостоятельной работы:

1. В какой системе сертификации сертифицируются средства криптографической защиты информации:

а) Система ФСТЭК России
б) Система ФСБ России
в) Система Минобороны России

2. Какой вид сертификации не существует:

а) По уровню контроля отсутствия недекларируемых возможностей.
б) На реально декларируемые возможности
в) На реальное отсутствие программных уязвимостей

3. Какой анализ кода проводится во время сертификационных испытаний:

а) Статический и динамический анализ
б) Экспертно-статистический анализ
в) Эмпирический анализ

2.3. РАЗДЕЛ 1. ОСНОВЫ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

ТЕМА 3. РУКОВОДЯЩИЕ ДОКУМЕНТЫ ФСТЭК РОССИИ

Основные вопросы:

1. Классификация АС
2. Показатели защищенности от НСД
3. Классификация по уровню отсутствия НДВ
4. Сертификация по стандарту ГОСТ ИСО /МЭК 15408.

Рекомендации по изучению темы:

Вопрос 1 изложен в РД АС. Защита от НСД к информации. Классификация АС и требования по защите информации.

Вопрос 2 изложен в РД СВТ. Защита от НСД к информации. Показатели защищенности от НСД.

Вопрос 3 изложен в РД АС. Защита от НСД к информации. Классификация АС и требования по защите информации.

Вопрос 4 изложен в [6,7,8].

Контрольные вопросы по теме 3

1. Перечислить основные классы защищенности АС.

2. Перечислить основные показатели защищенности от НСД к информации.

3. Назвать основные подсистемы защиты от НСД и их функции.

4. Уровни контроля отсутствия недекларированных возможностей.

5. Основные отличия сертификации по ГОСТ ИСО /МЭК 15408.

Тесты для самостоятельной работы:

1. Какой из нижеперечисленных классов защищенности не существует?

а) 2А

б) 1В

в) 3Д

2. Что не является исходными для классификации АС?

а) Перечень защищаемых ресурсов

б) Матрица доступа или полномочий субъектов доступа

в) Перечень внешних связей, выходящих за границу АС

г) Режим обработки данных

3. Какая подсистема защиты от НСД не существует?

а) Управления доступом

б) Регистрации и учета

в) Авторизации, идентификации, аутентификации и верификации

г) Криптографическая

д) Обеспечения целостности

4. Разработку каких документов предусматривает ГОСТ ИСО /МЭК 15408?

а) Задание по безопасности

б) Протокол учета уязвимостей кода

в) Профиль защиты

2.4. РАЗДЕЛ 2. ПОРЯДОК ПРОВЕДЕНИЯ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 4. СЕРТИФИКАЦИЯ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ (СВТ) ПО ТРЕБОВАНИЯМ ЗАЩИЩЕННОСТИ ОТ НСД К ИНФОРМАЦИИ

Основные вопросы:

1. Сертификация средств вычислительной техники (СВТ) по требованиям защищенности от НСД к информации

2. Порядок проведения сертификационных испытаний на соответствие классам защищенности СВТ.

3. Отчетность по результатам испытаний.

Рекомендации по изучению темы:

Вопрос 1 изложен в РД СВТ. Защита от НСД к информации. Показатели защищенности от НСД.

Вопрос 2 изложен в РД СВТ. Защита от НСД к информации. Показатели защищенности от НСД.

Вопрос 3 изложен в [1].

Контрольные вопросы по теме 4:

1. Основные показатели защищенности СВТ от НСД.
2. Требования к показателям защищенности.
3. Порядок проведения тестирования программного обеспечения
4. Дискреционный принцип контроля доступа
5. Мандатный принцип контроля доступа
6. Содержание руководства пользователя
7. Порядок формирования отчета

Тесты для самостоятельной работы:

1. Какие показатели защищенности отсутствуют в перечне показателей?

а) Очистка памяти
б) Изоляция модулей потребления
в) Очистка свободного места
г) Маркировка документов

2. Какие документы разрабатываются при проведении сертификационных испытаний?

а) Заявка на проведение сертификации
б) Решение о проведении сертификации
в) Акт отбора образца
г) Интегральная оценка уязвимостей кода
д) Методика испытаний

3. Что является объектом сертификационных испытаний?

а) Программно-аппаратные компоненты
б) Эксплуатационная документация
в) Техническая документация
г) Технологическая документация

4. Что не подлежит отбору испытательной лабораторией?

а) Дистрибутив программного обеспечения
б) Аппаратные компоненты СВТ
в) Тестовое программное обеспечение
г) Документация на СВТ

2.5. РАЗДЕЛ 2. ПОРЯДОК ПРОВЕДЕНИЯ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 5. СЕРТИФИКАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

Основные вопросы:

1. Выбор требуемого класса защищенности и уровня контроля отсутствия НДВ.
2. Сертификация ПО в информационных системах, обрабатывающих персональные данные.

Рекомендации по изучению темы:

Вопрос 1 изложен в РД Защита от НСД к информации. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия НДВ.

Вопрос 2 изложен в [1].

Контрольные вопросы по теме 5:

1. Требования к показателям защищенности первого класса.
2. Требования к показателям защищенности второго класса.
3. Требования к показателям защищенности третьего класса.
4. Требования к показателям защищенности четвертого, пятого, шестого и седьмого классов.
5. Нормативная база защиты персональных данных (документы ФСТЭК России)
6. Порядок проведения сертификационных испытаний в системах, обрабатывающих персональные данные.

Тесты для самостоятельной работы:

1. В каких классах защищенности применяется мандатная защита?

а) 7
б) 6 и 5
в) 4, 3 и 2
г) 1

2. Кто не является регулятором по защите персональных данных?

а) ФСТЭК России
б) ФСБ России
в) МЧС России
г) Роскомнадзор

3. Какая категория персональных данных позволяет идентифицировать Субъекта и получить о нем дополнительную информацию?
а) 4
б) 3
в) 2
г) 1

2.6. РАЗДЕЛ 2. ПОРЯДОК ПРОВЕДЕНИЯ СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ТЕМА 6. СЕРТИФИКАЦИЯ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ПО «ОБЩИМ КРИТЕРИЯМ»

Основные вопросы:
1. Определение системы оценки
2. Оценочные уровни доверия
3. Функции безопасности объекта оценки

Рекомендации по изучению темы:
Вопросы 1-3 изложены в [6,7,8].

Контрольные вопросы по теме 6:
1. Перечислить недостатки, присущие стандартам первого поколения.
2. Дать характеристику основным идеям «Общих критериев».
3. Дать характеристику угрозам безопасности.
4. Дать характеристику режима записи информации на накопители с точки зрения утечки информации.
5. Дать характеристику аспектам среды объекта оценки.
6. Дать характеристику потенциально информативных и неинформативных излучений.
7. Какие документы разрабатываются для задания требований к объекту оценки
8. Какие ограничения присущи «Общим критериям»?
9. Структура и содержание профиля защиты
10. Структура и содержание Задания по безопасности.

Тесты для самостоятельной работы:
1. Каким параметром не характеризуется угроза безопасности?
а) Источники угрозы
б) Предполагаемый способ реализации угрозы
в) Нарушаемые свойства безопасности активов
г) Реакция объекта оценки

2. Что включает в себя обоснование профиля защиты?
а) Логическое обоснование стоимости системы безопасности
б) Логическое обоснование целей и требований безопасности
в) Логическое обоснование качества оцениваемых параметров

3. Что содержит краткая спецификация объекта оценки?
а) Изложение функций безопасности объекта оценки и мер доверия
б) Изложение меры интеграционной оценки
в) Изложение логического обоснования спецификации объекта оценки

2.7. РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

ТЕМА 7. ПРИМЕНЕНИЕ АВТОМАТИЗИРОВАННЫХ СРЕДСТВ

Основные вопросы:
1. Статический анализ программного кода.
2. Динамический анализ программного кода.

Рекомендации по изучению темы:
Вопрос 1 изложен в [3] стр. 11.
Вопрос 2 изложен в [3] стр. 22.

Контрольные вопросы по теме 7:
1. Порядок действий при проведении статического анализа.
2. Дать характеристику основным параметрам отчета о статическом анализе.
3. Порядок действий при проведении динамического анализа.
4. Внедрение датчиков.
5. Дать характеристику основным параметрам отчета о динамическом анализе.

Тесты для самостоятельной работы:
1. На чем не основан статический анализ исходных текстов программ?
а) На структурном анализе
б) На декомпозиции исходных текстов
в) На семантической интеграции и исключении избыточности

2. На чем основан не динамический анализ исходных текстов программ?
а) На контроле соответствия РДВ
б) На идентификации фактических маршрутов выполнения функциональных объектов с последующим сопоставлением маршрутам, построенным в процессе проведения статического анализа
в) На перманентном контроле избыточности кода

2.8. РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

ТЕМА 8. ПОРЯДОК ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

Основные вопросы:

1. Порядок оформления заявки на сертификацию
2. Порядок оформления акта отбора образца
3. Перечень документации, представляемой в испытательную лабораторию

Рекомендации по изучению темы:

Вопросы 1-3 изложены в [1].

Контрольные вопросы по теме 8:

1. Что отражается в заявке на сертификацию?
2. Содержание акта отбора образца.
3. Порядок оформления решения о проведении сертификации.
4. Перечень документации, представляемой в испытательную лабораторию
5. Порядок получения сертификата соответствия
6. Применение знака соответствия

Тесты для самостоятельной работы:

1. Какие данные не содержит заявка на сертификацию?

а) Реквизиты заявителя
б) Схема испытаний
в) Указание на соответствие чему сертифицируется продукт
г) Стоимость работ

2. Каким документом определяется испытательная лаборатория?

а) Актом отбора образца
б) Приложением к заявке на сертификацию
в) Решением регулятора на сертификацию

3. Кто выдает сертификат соответствия?

а) Испытательная лаборатория
б) Орган муниципальной власти в регионе
в) Ведомственный регулятор

2.9. РАЗДЕЛ 3. МЕТОДЫ И СРЕДСТВА ПРОВЕДЕНИЯ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

ТЕМА 9. ПРОВЕРКА ПРОИЗВОДСТВА СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Основные вопросы:

1. Исходные данные для проведения предварительной проверки производства (ППП)
2. Порядок работы комиссии по ППП
3. Инспекционный контроль

Рекомендации по изучению темы:

Вопросы 1-3 изложены в [1].

Контрольные вопросы по теме 9:

1. Состав исходных данных для проведения ППП
2. Порядок работы комиссии
3. Порядок оформления акта
4. Особенности проведения ППП программного и аппаратно-программного средств защиты информации
5. Порядок проведения инспекционного контроля

Тесты для самостоятельной работы:

1. Что не содержат исходные данные для предварительной проверки производства?

а) Перечень испытательного оборудования
б) Перечень лицензий и сертификатов
в) Перечень стандартов менеджмента качества
г) Стоимость работ

2. Кто утверждает акт предварительной проверки производства?

а) Генеральный директор предприятия
б) Ведомственный регулятор
в) Испытательная лаборатория

3. При каком изменении ПО проводится инспекционный контроль?

а) менее 5%
б) более 5%
в) более 30%
г) более 50 %