МИНОБРНАУКИ РОССИИ
Федеральное государственные бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
«4» 04 2022 г.

СИСТЕМА СЕРТИФИКАЦИИ И АТТЕСТАЦИИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Система сертификации и аттестации телекоммуникационных систем» очной формы обучения

Курск 2022

УДК 654.01

Составитель М.А. Ефремов

Рецензент
Кандидат технических наук, доцент *А.Л. Марухленко*

Система сертификации и аттестации телекоммуникационных систем: методические рекомендации для самостоятельной подготовки к занятиям студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Система сертификации и аттестации телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: М.А. Ефремов. Курск, 2022. - 12 с.

Содержат информацию, необходимую студентам в процессе самостоятельной подготовки к занятиям по дисциплине.

Методические рекомендации соответствуют требованиям программы, утвержденной учебно-методическими объединениями по специальностям.

Предназначены для студентов направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Система сертификации и аттестации телекоммуникационных систем», очной формы обучения.

Текст печатается в авторской редакции

Подписано в печать Формат 60х84 1/16
Усл.печ.л. 1,10 Уч.-изд.л. 1,00 Заказ 902 Тираж 100 экз. Бесплатно
Юго-Западный государственный университет
305040, г. Курск, ул. 50 лет Октября, 94

ПРЕДИСЛОВИЕ

Методические рекомендации разработаны с целью оказания помощи студентам направлений подготовки, учебные планы которых предусматривают изучение дисциплины «Система сертификации и аттестации телекоммуникационных систем», очной формы обучения, при самостоятельной подготовке к занятиям по дисциплине.

Методические рекомендации разработаны в соответствии с Федеральными государственными образовательными стандартами высшего образования соответствующих направлений подготовки.

Предлагаемые методические рекомендации содержат краткое содержание рассматриваемых тем дисциплины и задания для самоконтроля в форме вопросов.

Студентам предлагается список учебной литературы по дисциплине и перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям.

Методические указания для обучающихся по освоению дисциплины

Основными видами аудиторной работы обучающихся являются лекции и практические занятия.

В ходе лекций преподаватель излагает и разъясняет основные, наиболее сложные понятия темы, а также связанные с ней теоретические и практические проблемы, дает рекомендации на практическое занятие и указания на самостоятельную работу.

Практические занятия завершают изучение наиболее важных тем учебной дисциплины. Они служат для закрепления изученного материала, развития умений и навыков подготовки докладов, сообщений, приобретения опыта устных публичных выступлений, ведения дискуссии, аргументации и защиты выдвигаемых положений, а также для контроля преподавателем степени подготовленности студентов по изучаемой дисциплине.

Практические занятия предполагают свободный обмен мнениями по избранной тематике. Занятие начинается со вступительного слова преподавателя, формулирующего цель занятия и характеризующего его основную проблематику. Затем, как правило, заслушиваются сообщения студентов. Обсуждение сообщения совмещается с рассмотрением намеченных вопросов. Сообщения, предполагающие анализ публикаций по отдельным вопросам семинара, заслушиваются обычно в середине занятия. Поощряется выдвижение и обсуждение альтернативных мнений. В заключительном слове преподаватель подводит итоги обсуждения и объявляет баллы выступавшим студентам. В целях контроля подготовленности студентов и привития им навыков краткого письменного изложения своих мыслей преподаватель в ходе практических занятий может осуществлять текущий контроль знаний в виде тестовых заданий.

При подготовке к занятию студенты имеют возможность воспользоваться консультациями преподавателя. Кроме указанных тем, студенты вправе, по согласованию с преподавателем, избирать и другие интересующие их темы.

Качество учебной работы студентов преподаватель оценивает в конце занятия.

При освоении данного курса студент может пользоваться библиотекой вуза, которая в полной мере обеспечена соответствующей литературой.

В процессе *подготовки к зачету* студенту следует руководствоваться следующими рекомендациями:

- необходимо стремиться к пониманию всего материала, чтобы еще до экзамена не оставалось непонятных вопросов;
- необходимо строго следить за точностью своих выражений и правильностью употребляемых терминов;
- не следует опасаться дополнительных вопросов – чаще всего преподаватель использует их как один из способов помочь студенту или сэкономить время;
- прежде чем отвечать на вопрос, необходимо сначала правильно его понять.

Содержание дисциплины, структурированное по темам (разделам)

Таблица 1 – Содержание дисциплины, структурированное по темам (разделам)

№ п/п	Раздел (тема) дисциплины	Содержание
1.	Оценочные стандарты в информационной безопасности	Роль стандартов ИБ, «Оранжевая книга» как оценочный стандарт, Международный стандарт ISO/IEC 15408, критерии оценки безопасности информационных систем.
2.	Стандарты управления информационной безопасностью	Стандарты управления информационной безопасностью BS 7799 и ISO/IEC 17799. Их основные положения, международный стандарт ISO/IEC 27001:2005, сертификация СУИБ на соответствие ISO 27001.
3.	Международные стандарты	Стандарты комитета технической безопасности ETSI. Стандарт «надлежащей практики».

	информационной безопасности	Североамериканская корпорация по надежности электроснабжения (NERC). Рамки информационной безопасности NIST (NIST CSF). RFC 2196 ISA / IEC-62443. Программа оценки соответствия. Немецкий стандарт BSI
4.	Стандартизация в области облачных технологий	Стандарты, регулирующие безопасность облачных услуг. совместимость систем управления облаком между провайдером и заказчиком. Проекты международных стандартов по облачным вычислениям. Российская стандартизация облачных вычислений
5.	Управление рисками. Основные понятия.	Выбор анализируемых объектов и уровня детализации их рассмотрения. Выбор методики оценки рисков.. Инвентаризация активов. Анализ угроз и их последствий, выявление уязвимых мест в защите. Оценка рисков.. Обработка рисков. Выбор защитных мер. Реализация и проверка выбранных мер.. Оценка остаточного риска
6.	Методика оценки рисков информационной безопасности компании Digital Security	Описание архитектуры ИС. Расчет рисков по угрозе конфиденциальность Учет наличия доступа при помощи VPN. Расчет рисков по угрозе целостность
7.	Методики и технологии управления рисками	Качественные методики управления рисками, количественные методики управления рисками, метод CRAMM.
8.	Разработка корпоративной методики анализа рисков	Методы оценивания информационных рисков, табличные методы оценки рисков, методика анализа рисков Microsoft

Задания для самоконтроля по темам курса

Тема 1. Оценочные стандарты в информационной безопасности.

1. Назначение стандартов в области информационной безопасности
2. Опишите понятие «оценочный» применительно к стандартам информационной безопасности
3. Опишите структуру оценочного стандарта
4. Характеристики основных классов защищённости
5. Для каких категорий пользователей формируются стандарты ИБ?

Тема 2. Стандарты управления информационной безопасностью.

1. Дайте определение понятию «управление ИБ»
2. Охарактеризуйте структуру стандартов управления ИБ
3. Какие элементы управления являются фундаментальными в области информационной безопасности и почему?
4. Охарактеризуйте область применения стандартов ИБ
5. Охарактеризуйте этапы формирования системы управления информационной безопасностью
6. Охарактеризуйте процедуру сертификации системы управления информационной безопасностью

Тема 3. Международные стандарты информационной безопасности.

1. Охарактеризуйте стандарты, разработанные CISQ
2. Охарактеризуйте стандарты, разработанные североамериканской корпорацией по надежности электроснабжения
3. Охарактеризуйте стандарты, разработанные NIST CSF
4. Охарактеризуйте стандарт ISA / IEC-62443
5. Охарактеризуйте стандарт ISO 17065
6. Охарактеризуйте стандарт BSI

Тема 4. Стандартизация в области облачных технологий.

1. Особенности облачных технологий, влияющие на формирование политик безопасности для них
2. Органы, отвечающие за выработку стандартов в области безопасности облачных вычислений
3. Какие стандарты обеспечивают совместимость в облачных сервисах?
4. Есть ли специальные стандарты ISO для облачных услуг?
5. Охарактеризуйте современное состояние в области стандартизации и сертификации технологий безопасности облачных вычислений
6. Российская стандартизация облачных вычислений

Тема 5. Управление рисками. Основные понятия.

1. На каком направлении информационной безопасности требуется сосредоточить наибольшее внимание?

2. В чём состоит суть мероприятий по управлению рисками?

3. Этапы процесса управления рисками

4. Методологические основы для формирования модели угроз и уязвимостей

5. Основные понятия модели управления рисками

6. Приведите пример расчета рисков на основе расчета угроз безопасности

7. Приведите пример расчета рисков на основе модели угроз и уязвимостей

Тема 6. Методика оценки рисков информационной безопасности компании Digital Security.

1. Опишите метод оценки рисков на основе модели информационных потоков.

2. Как влияет архитектура инфокоммуникационной системы на модель управления рисками

3. Что такое коэффициент локальной защищённости информации

4. Как влияет наличие в системе доступа в глобальную сеть на защищённость отдельных видов информации?

5. Как получается интегральная характеристика риска из отдельных рисков для каждого вида информации?

Тема 7. Методики и технологии управления рисками.

1. Что предполагает методики управление информационными рисками любой компании?

2. Что такое методика COBRA?

3. Основные цели методики CRAMM

4. Как формируются границы исследуемой системы при управлении рисками?

5. Как происходит идентификация ресурсов и построение модели системы с точки зрения ИБ?

6. Когда необходимо определение ценности информации?

7. На основе каких параметров формируется шкала ущерба?

Тема 8. Разработка корпоративной методики анализа рисков.

1. Цели и задачи работ по анализу рисков в системе

2. Этапы проведения работ по анализу рисков

3. Как формируется стратегия управления рисками и на основании каких критериев

4. Опишите основные методы анализа рисков

5. Приведите пример оценки риска.

6. Назначение и задачи планирования управления рисками

Учебная литература, необходимая для самостоятельной подготовки к занятиям

1 Крылова, Г. Д. Основы стандартизации, сертификации, метрологии [Электронный ресурс]: учебник / Г. Д. Крылова. - 3-е изд., перераб. и доп. - М.: Юнити-Дана, 2015. - 671 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=114433

2 Камардин, Н. Б. Метрология, стандартизация, подтверждение соответствия [Электронный ресурс] : учебное пособие / Н. Б. Камардин, И. Ю. Суркова ; Министерство

образования и науки России, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Казанский национальный исследовательский технологический университет». - Казань : Издательство КНИТУ, 2013. - 240 с. - Режим доступа: http://biblioclub.ru/index.php?page=book&id=258829

3. Кошевая И. П. Метрология, стандартизация и сертификация [Текст]/ И. П. Кошевая – М.: Форум; ИНФРА-М, 2007.

4. Никифоров А. Д. Метрология, стандартизация и сертификация [Текст]/ А.Д. Никифоров– М.: Высшая школа; 2010.

5. Стандартизация и разработка программных систем [Электронный ресурс] / учеб. пособие / В. Н. Гусятников, А. И. Безруков. - М.: Финансы и статистика, 2010. - Режим доступа:http://www.studentlibrary.ru/book/ISBN9785279034505.html

6. Постановление Правительства Российской Федерации от 26.06.95 № 608 "Положение о сертификации средств защиты информации" / Там же. № 27. Ст. 2579. Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны. Утверждено постановлением Правительства РФ от 15.04.95 № 333 / Там же. № 17. Ст. 1540.

7. Аттестационные испытания автоматизированных систем от несанкционированного доступа по требованиям безопасности

информации [Текст]: учебное пособие / В.С. Горбатов [и др.]. – М.: НИЯУ МИФИ, 2014. – 560 с.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для самостоятельной подготовки к занятиям по дисциплине

1) Федеральная служба безопасности [официальный сайт]. Режим доступа: http://www.fsb.ru/

2) Федеральная служба по техническому и экспортному контролю [официальный сайт]. Режим доступа: http://fstec.ru/

3) Электронно-библиотечная система «Университетская библиотека онлайн» Режим доступа: http://biblioclub.ru

4) Компания «Консультант Плюс» [официальный сайт]. Режим доступа: http://www.consultant.ru

5) Справочно-поисковая система «Гарант» [официальный сайт]. Режим доступа: http://www.garant.ru

6) Научно-информационный портал ВИНИТИ РАН [официальный сайт]. Режим доступа: http://www.consultant.ru/