

Приложение ПССЗ по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем 2023-2024 уч.г.: Методические рекомендации по организации самостоятельной работы студентов по междисциплинарному курсу МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»**

**Методические рекомендации
по организации самостоятельной работы студентов
по МДК.03.02 Инженерно-технические средства физической
защиты объектов информатизации**

**для специальности
10.02.05 Обеспечение информационной безопасности
автоматизированных систем**

Методические рекомендации по организации самостоятельной работы студентов разработаны на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Составитель:

Зюбан Е.В., преподаватель ОГАПОУ «Алексеевский колледж»

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

- 1. ТЕМАТИЧЕСКИЙ ПЛАН ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**
- 2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ ЗАДАНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**
- 3. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ**

ВВЕДЕНИЕ

Методические рекомендации по организации самостоятельной работы студентов по МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем определяют содержание самостоятельной работы обучающихся, ее назначение, формы организации и виды контроля.

Контролируемая самостоятельная работа направлена на углубление и закрепление знаний студента, развитие аналитических навыков по проблематике МДК.

Самостоятельная работа обучающихся, рассматривается в как управляемая преподавателями (без их прямого участия) система организационно-педагогических условий, направленная на освоение практического опыта, умений и знаний в рамках предметов, дисциплин, междисциплинарных курсов по специальностям и профессиям в соответствии с ФГОС СПО.

Для обучающегося самостоятельная работа - способ активного, целенаправленного освоения, без непосредственного участия преподавателя, новых знаний, умений и опыта, личностных результатов, закладывающих основания в становлении профессиональных и общих компетенций, требуемых ФГОС СПО по специальности.

В рамках выполнения самостоятельной работы обучающийся должен владеть способами предметной деятельности: уметь понимать предложенные преподавателем цели, формулировать их самому; моделировать собственную деятельность и программировать ее; уметь оценивать конечные и промежуточные результаты своих действий; корректировать деятельность, иметь личностную готовность (высокий уровень самосознания, адекватность самооценки, рефлексивность мышления, самостоятельность, организованность, целенаправленность личности, сформированность волевых качеств) саморегуляции.

Целью самостоятельной работы обучающихся является:

- 1) формирование личностных результатов, общих и профессиональных компетенций;
- 2) формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- 3) формирование самостоятельности мышления, способностей к саморазвитию, совершенствованию и самоорганизации;
- 4) углубление и расширение теоретических знаний;
- 5) систематизация и закрепление полученных теоретических знаний и

практических умений обучающихся;

б) развитие познавательных способностей и активности обучающихся: творческой инициативы, самостоятельности, ответственности, организованности.

Основными формами самостоятельной работы обучающихся являются поиск информации и подготовка сообщений.

В соответствии с рабочей программой на самостоятельную учебную работу обучающегося отводится 2 часа.

1. ТЕМАТИЧЕСКИЙ ПЛАН ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

№ п/п	Наименование разделов и тем	Кол- во часов	Виды заданий		Форма отчётности
1	2	3	4		5
	МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации	2			
	Раздел 1. Построение и основные характеристики инженерно-технических средств физической защиты	2			
3.	Тема 1.1. Цели и задачи физической защиты объектов информатизации	2	Подготовка презентации	Меры по защите информации внутри зоны	Наглядным образом продемонстрировать результаты работы
	ВСЕГО:	2			

2. МЕТОДИЧЕСКИЕ УКАЗАНИЯ К ВЫПОЛНЕНИЮ ЗАДАНИЙ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по подготовке презентации

Презентация – электронный образовательный ресурс (ЦОР).

Электронная презентация - логически связанная последовательность слайдов, объединенная одной тематикой и общими принципами оформления. Презентация обладает наглядностью и выразительностью, является прекрасным дидактическим и мотивационным средством, способствующим лучшему запоминанию учебного материала. Презентация требует комментариев и дополнений. Все презентации строятся по одной и той же логической схеме:

1. Первый слайд- это всегда заголовок презентации.
2. Второй слайд – определение термина или общее пояснение к теме.
3. Два-три, четыре – пять слайдов, посвящаются иллюстрациям, примерам, применению объекта изучения, то есть выделению его наиболее ярких особенностей.
4. Несколько слайдов могут содержать материал в виде таблиц, диаграмм, графиков.
5. Последний слайд – итог, то есть выделяется то главное, что должно быть понято и должно остаться в памяти у слушателей.

Требования к презентации:

1. Презентация создается с помощью программы MicrosoftOfficePowerPoint 2007 с использованием анимации и вставок в виде рисунков, таблиц, диаграмм, клипов, звука и видеофильмов.
2. Содержание изучаемого материала должно быть представлено коротко и наглядно (норма - 17 слов на слайде).
3. 1-3 рисунка или фотографии на слайде. Минимальный текст к иллюстрации. Основной текст (также небольшого объема) можно выполнять с применением гиперссылок, используя программу MicrosoftWord.
4. На слайде используется не более 3 цветов.
5. Стилль фона слайда выбирается в соответствии с темой и должен быть сквозным (на всех слайдах одинаковым). Предпочтителен темный фон, а текст выделяют контрастным светлым цветом.

Советы:

1. Перед созданием презентации изучите содержание материала темы по рекомендуемой литературе и другим источникам.
2. Разбейте содержание материала по смысловым группам. Наметьте план презентации.
3. На бумаге смоделируйте макет презентации. Определите количество слайдов и содержание каждого слайда согласно требованиям, предъявляемым к презентации. Продумайте содержание текстов, рисунков, схем, таблиц, диаграмм и видеоклипов. Продумайте музыкальные вставки и анимацию.
4. Затем приступайте к созданию презентации.

Критерии оценки:

«5» («Отлично») – Работа выполнена полностью, презентация отображает абсолютно верные данные, при её разработке использованы эффективные средства и методы, работа имеет методически верное оформление.

«4» («Хорошо») – Работа выполнена полностью, презентация отображает абсолютно верные или практически верные данные, при разработке не использовались эффективные средства и методы, работа имеет не совсем аккуратное, методически верное оформление.

«3» («Удовлетворительно») – Работа выполнена полностью, презентация отображает не совсем верные данные, при разработке не использовались эффективные средства и методы, работа в значительной степени имеет неаккуратное, методически неверное оформление.

«2» («Неудовлетворительно») – Работа выполнена не полностью или презентация отображает совершенно не правильные данные, или работа имеет значительные недостатки в аккуратности, не соблюдены методические рекомендации по оформлению.

Формы контроля – мультимедийная презентация.

3. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

перечень учебных изданий, электронных изданий, электронных и Интернет-ресурсов, образовательных платформ, электронно-библиотечных систем, веб-систем для организации дистанционного обучения и управления им, используемые в образовательном процессе как основные и дополнительные источники.

Основные источники:

1. Техническая защита информации в объектах информационной инфраструктуры (1-е изд.) учебник Бубнов А.А., М.: ИЦ Академия, 2019 – 272 с.

Дополнительные источники:

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 2014.

2. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие -Москва: МИФИ, 2012.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

3. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2012 – 416 с.

4. Мельников В.П., Клейменов С.А., Петраков А.М.: Информационная безопасность и защита информации Академия, - 336 с. – 2012

5. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2 Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2013 – 172 с.
6. Организационно-правовое обеспечение Информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2017 – 336с.
7. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2015
8. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд во: ДМК Пресс, - 2012
9. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
10. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
11. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».
12. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».
13. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».
14. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
15. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
16. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
17. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
18. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
19. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в

информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

20. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

21. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

22. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

23. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России

24. от 30 августа 2002 г. № 282.

25. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

26. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России

27. от 31 августа 2010 г. № 416/489.

28. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

29. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

30. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недеklarированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

31. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

32. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели

менеджмента безопасности информационных и телекоммуникационных технологий

33. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

34. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

35. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

36. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

37. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

38. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

39. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

40. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

41. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

42. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

43. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

44. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

45. ГОСТ Р 51624-2000 Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.
47. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
48. Номенклатура показателей качества. Ростехрегулирование, 2005.
49. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.
50. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.
51. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.
52. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.
53. ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.
54. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.
55. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
56. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.
57. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

58. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.
59. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.
60. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
61. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные издания (электронные ресурсы):

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с.
2. <https://urait.ru/bcode/456793>
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с.
4. <https://urait.ru/bcode/449548>
5. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2020. — 325 с.
6. <https://urait.ru/bcode/451933>
Интерфейсы периферийных устройств –
<https://intuit.ru/studies/courses/92/92/lecture/28396>
7. О компонентах системного блока — подробно –
<https://intuit.ru/studies/courses/3685/927/lecture/19564?page=2>
8. Портативные компьютеры –
<https://intuit.ru/studies/courses/13910/1276/lecture/24146>
9. Сравнительные характеристики процессоров –
<https://intuit.ru/studies/courses/15812/478/lecture/21074>
10. Технические средства информационных технологий –
<https://intuit.ru/studies/courses/3481/723/lecture/14240>
11. Устройства ввода информации –

<https://intuit.ru/studies/courses/3460/702/lecture/14158>

12. Устройства вывода информации –

<https://intuit.ru/studies/courses/3460/702/lecture/14157>

13. Цифровая образовательная среда СПО PROФобразование:

- Старостин, А. А. Технические средства автоматизации и управления : учебное пособие для СПО / А. А. Старостин, А. В. Лаптева ; под редакцией Ю. Н. Чеснокова. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 168 с. — ISBN 978-5-4488-0503-5, 978-5-7996-2842-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROФобразование : [сайт]. — URL: <https://profspo.ru/books/87882> (дата обращения: 31.08.2020). — Режим доступа: для авторизир. пользователей

Электронно-библиотечная система:

IPRBOOKS - <http://www.iprbookshop.ru/78574.html>

Веб-система для организации дистанционного обучения и управления им:

Система дистанционного обучения ОГАПОУ «Алексеевский колледж»
<http://moodle.alcollege.ru/>