Документ подписан квалифицированной электронной подписью
Сертификат: 03489EA30058B4708C45B74E4D79B70F27
Владелец: "АНО ВО "РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ"
Действителен: с 28.05.2026 по 28.08.2027

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ»
(АНО ВО «РосНОУ»)

Методические рекомендации по выполнению и защите курсовой работы по профессиональному модулю ПМ.03 Защита информации техническими средствами

Специальность: *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

Москва 2026

Оглавление

1. Цель, задачи и тематика курсовой работы 4
2 Структура и содержание курсовой работы 6
3 Оформление курсовой работы 6
4 Защита и оценивание курсовой работы 7
4.1 Порядок защиты курсовой работы 7
4.2 Оценивание курсовых работ 7
5. Учебно-методическое и информационное обеспечение 9
5.1. Основная литература: 9
5.2. Дополнительная литература: 9
ПРИЛОЖЕНИЕ А 14
Примерный список тем курсовых работ 14
ПРИЛОЖЕНИЕ Б 16
Образец титульного листа курсовой работы 16
ПРИЛОЖЕНИЕ В 17
Примерная структура и содержание курсовой работы 17
Структура и содержание курсовой работы 17
Бланк отзыва на курсовую работу 18
ПРИЛОЖЕНИЕ Г 19
Бланк задания на курсовую работу 19
ПРИЛОЖЕНИЕ Д 20

1. Цель, задачи и тематика курсовой работы

1.1 Цель и задачи курсовой работы:

Важнейшим компонентом образовательного процесса является подготовка и защита курсовой работы (далее КР), **целью** которой является систематизация и закрепление теоретических знаний и практических навыков студентов по защите информации техническими средствами, укрепление связи учебного процесса с научно-исследовательской деятельностью. Курсовая работа выступает действенным средством усиления целенаправленности профессиональной подготовки студента.

Задачи курсовой работы:

- систематизация и закрепление полученных теоретических знаний и практических умений по защите информации техническими средствами;
- углубление теоретических знаний в соответствии с заданной темой;
- формирования общих и профессиональных компетенций в соответствиис требованиями ФГОС;
- формирование умений использовать справочную, правовую и нормативную документацию;
- развитие творческой инициативы, самостоятельности, ответственностии организованности;
- ориентирование в процессе курсового исследования на подготовку государственной итоговой аттестации.

В результате подготовки, написания и защиты курсовой работы студентыдолжны:

знать:

− порядок технического обслуживания технических средств защиты информации;

− номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;

− физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации;

− порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;

− методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации;

− номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации;

− основные принципы действия и характеристики технических средств физической защиты;

− основные способы физической защиты объектов информатизации;

− номенклатуру применяемых средств физической защиты объектов информатизации.

уметь:

− применять технические средства для криптографической защиты информации конфиденциального характера;

− применять технические средства для уничтожения информации и носителей информации;

− применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;

− применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;

− применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;

− применять инженерно-технические средства физической защиты объектов информатизации.

При подготовке, написании и защиты курсовой работы по профессиональному модулю ПМ.03 Защита информации техническими средствами МДК 03.02 Инженерно-технические средства физической защиты объектов информации у студентов формируются следующие компетенции:

Общие:

Код	Наименование видов деятельности и профессиональных компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

Профессиональные:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	**Защита информации техническими средствами**
ПК 3.1.	Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.2.	Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.
ПК 3.3.	Осуществлять измерение параметров побочных электромагнитных излучений и

	наводок (ПЭМИН), создаваемых техническими средствами обработки информации ограниченного доступа.
ПК 3.4.	Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.
ПК 3.5.	Организовывать отдельные работы по физической защите объектов информатизации.

1.2 Тематика курсовых работ

Тему курсовой работы обучающийся выбирает самостоятельно из числа рекомендованных (Приложение А).

Выдача задания по КР (Приложение Г) сопровождается консультацией, в ходе которой разъясняются назначение и задачи, структура и объем работы, принципы разработки и оформления работы.

Основными функциями руководителя КР являются:

- консультирование по вопросам содержания и последовательности выполнения КР;
- оказание обучающемуся помощи в подборе необходимой литературы;
- контроль хода выполнения КР;
- проверка КР;
- подготовка отзыва на КР (Приложение В).

2 Структура и содержание курсовой работы

Структура и содержание курсовой работы должны соответствовать Положению об организации выполнения и защиты курсовой работы (проекта) по образовательным программам среднего профессионального образования в Частном профессиональном образовательном учреждении «Колледж управления и производства», утвержденному Приказом № 2-ОД/36-19 от 09.09.2020 г.

Образец оформления титульного листа курсовой работы содержится в Приложении Б. Примерная структура и содержание курсовой работы приведенав Приложении В. Требования к оформлению курсовой работы приведены в Приложение Д.

3 Оформление курсовой работы

Курсовая работа выполняется в соответствии с Положением об организации выполнения и защиты курсовой работы (проекта) по образовательным программам среднего профессионального образования в Частном профессиональном образовательном учреждении «Колледж управления и производства», утвержденному Приказом № 2-ОД/36-19 от 09.09.2020 г.

По структуре курсовая работа, по профессиональному модулю ПМ.03 Защита информации техническими[6] средствами МДК 03.02 Инженерно-технические средства физической защиты объектов информации,

реферативного характера включает в себя:

- титульный лист;
- задание;
- содержание;
- аннотацию, с кратким содержанием работ, выполненных в курсовой работе;
- введение, в котором раскрывается актуальность и значение темы, формулируется цель работы;
- теоретическую часть, в которой дается описание истории вопроса, оценивается уровень разработанности проблемы в теории и практике посредством сравнительного анализа литературы;
- заключение, в котором содержатся выводы и рекомендации относительно

возможностей использования материалов работы;

- список литературы; приложения.

4 Защита и оценивание курсовой работы

Защита и оценивание курсовой работа осуществляются в соответствии с Положением об организации выполнения и защиты курсовой работы (проекта) по образовательным программам среднего профессионального образования в Частном профессиональном образовательном учреждении «Колледж управления и производства», утвержденному Приказом № 2-ОД/36-19 от 09.09.2020 г.

4.1 Порядок защиты курсовой работы

4.1.1. По завершении студентом курсовой работы руководитель проверяет, подписывает ее и вместе с письменным отзывом передает заместителю директора по УВР. Письменный отзыв и включает в себя:

- заключение о соответствии курсовой работы заявленной теме;
- оценку сформированных общих и профессиональных компетенций по виду профессиональной деятельности;
- оценку полноты разработки поставленных вопросов, теоретической и практической значимости курсовой работы;
- оценку курсовой работы.

4.1.2. Необходимость и форма защиты курсовой работы определяется руководителем курсовой работы самостоятельно.

4.1.3. Процедура защиты курсовой работы может включает в себя:

- выступление студента по теме и результатам работы (5-8 мин),
- ответы на вопросы руководителя работы.

4.1.4. Во время защиты обучающийся использует подготовленный наглядный материал, иллюстрирующий основные положения курсовой работы (проекта).

4.2 Оценивание курсовых работ

Оценка за КР выставляется на титульном листе КР, заверяется подписью руководителя КР с указанием даты.

Руководитель КР выставляет оценку в зачетную ведомость защиты курсовых работ.

Полные названия курсовых работ вносятся в зачетные книжки обучающихся на отведенных для этого страницах с выставлением оценки по курсовой работе.

Аттестация по всем КР должна быть проведена до начала промежуточной аттестации по учебной дисциплине или МДК. Положительная оценка по дисциплине или МДК, по которым учебным планом по специальности предусматривается курсовая работа, выставляется только при условии успешной сдачи курсовой работы на оценку не ниже «удовлетворительно».

Обучающимся, получившим неудовлетворительную оценку по курсовой работе, предоставляется право выбора новой темы курсовой работы или, по решению преподавателя, доработки прежней темы, при этом определяется новый срок для ее выполнения, но не позднее промежуточной аттестации в текущем семестре.

Не аттестация по КР считается академической задолженностью. Результаты защиты курсовой работы определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно», что соответствует бальной шкале «5, 4, 3, 2».

Итоговая оценка за курсовую работу складывается:

1. Оценивание руководителем КР объема изученной литературы;
2. Оценивание представленного студентом письменного текста с точки зрения его содержания (актуальность и раскрытие темы, самостоятельность исследования, творческие выводы, анализ практики)
3. Оформление курсовой работы (проекта);
4. Оценивание защитной речи и ответов на вопросы по теме работы.

Оценка	***Критерии оценки***
Отлично	работа выполнена в соответствии с утвержденным планом, полностью раскрыто содержание каждого вопроса, студентом сформулированы собственные аргументированные выводы по теме работы. Оформление работы соответствует предъявляемым требованиям. При защите работы студент свободно владеет материалом и отвечает на вопросы.
Хорошо	работа выполнена в соответствии с утвержденным планом, полностью раскрыто содержание каждого вопроса. Незначительные замечания к оформлению работы. При защите работы студент владеет материалом, но отвечает не на все вопросы.
Удовлетворительно	работа выполнена в соответствии с утвержденным планом, но не полностью раскрыто содержание каждого вопроса. Студентом не сделаны собственные выводы по теме работы. Грубые недостатки в оформлении работы. При защите работы студент слабо владеет материалом, отвечает не на все вопросы.

Неудовлетворительно	работа выполнена не в соответствии с утвержденным планом, не раскрыто содержание каждого вопроса. Студентом не сделаны выводы по теме работы. Грубые недостатки в оформлении работы. При защите работы студент не владеет материалом, не отвечает на вопросы.

5. Учебно-методическое и информационное обеспечение

5.1. Основная литература:

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. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/456793

2. *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. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/449548

3. *Стасышин, В. М.* Базы данных: технологии доступа: учебное пособие для среднего профессионального образования / В. М. Стасышин, Т. Л. Стасышина. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2020. — 164 с. — (Профессиональное образование). — ISBN 978-5-534-09888-4. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/455863

5.2. Дополнительная литература:

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

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

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

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. 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».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. 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.

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

13. 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.

14. 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.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

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

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

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

19. Руководящий документ. Геоинформационные системы. Защита

информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. 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 не декларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

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

22. 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

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

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

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

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

27. 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

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

29. 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

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

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

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

33. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов.

Основные положения. Росстандарт, 2013.

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

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

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации.
Номенклатура показателей качества. Ростехрегулирование, 2005.

38. 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.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. 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.

41. 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.

42.ГОСТ Р 50739-95 Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования. Госстандарт России, 1995.

43. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

44. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

46. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

47. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

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

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

50. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru; www.gost.ru/wps/portal/tk362.

5.3 Электронные ресурсы:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) https://fstec.ru/
2. Образовательные порталы по различным направлениям образования и тематике https://depobr.gov35.ru/
3. Справочно-правовая система «Консультант Плюс» http://www.consultant.ru/
4. Справочно-правовая система «Гарант» www.garant.ru
5. Федеральный портал «Российское образование http://www.consultant.ru/
6. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
7. Сайт Научной электронной библиотеки https://www.elibrary.ru/defaultx.asp?

ПРИЛОЖЕНИЕ А

Примерный список тем курсовых работ

1. Методы защиты видовых демаскирующих признаков от технических средств разведок.
2. Методы защиты сигнальных демаскирующих признаков от технических средств разведок.
3. Методы защиты радиосигналов от перехвата техническими средствами разведок.
4. Методы защиты электрических сигналов от перехвата техническими средствами разведок.
5. Методы защиты материальных и вещественных демаскирующих признаков от технических средств разведок.
6. Технические средства наблюдения в видимом и ИК диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.
7. Технические средства наблюдения в радио диапазонах за объектом защиты, методы и средства противодействия средствам наблюдения.
8. Технические средства перехвата конфиденциальной информации передаваемой по линии связи, методы и средства противодействия перехвата конфиденциальной информации.
9. Методы и технические средства съема конфиденциальной речевой информации с использованием вторичных переизлучателей.
10. Методы и технические средства съема конфиденциальной речевой информации с использованием опто-волоконных линий связи.
11. Методы и технические средства съема конфиденциальной речевой информации с использованием средств высокочастотного навязывания.
12. Технические средства подслушивания, методы и средства противодействия средствам подслушивания.
13. Технические средства анализа демаскирующих признаков веществ, методы и средства нейтрализации (утилизации) отходов производства.
14. Технические средства контроля, обнаружения, уничтожение закладных устройств, порядок проведения ЗПМ.
15. Технические средства контроля, обнаружения, уничтожение закладных устройств, в слаботочных линиях связи, порядок проведения ЗПМ.
16. Технические средства контроля, обнаружения, уничтожение закладных устройств в телефонных линиях связи, порядок проведения ЗПМ.
17. Технические средства контроля, обнаружения, уничтожение закладных устройств, в электросетях, цепях заземления, порядок проведения ЗПМ.
18. Способы и средства контроля и порядок проведения ЗПМ в защищаемых помещений на отсутствие закладных устройств.
19. Моделирование вербального объекта защиты, возможных угроз безопасности информации для оптических каналов утечки информации в видимом и ИК диапазонах, разработка способов, методов и технических средств защиты информации.
20. Математические методы моделирования для вербального объекта защиты от возможных угроз безопасности информации для акустических каналов утечки информации.
21. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустических каналов утечки информации, разработка методов и технические средств защиты информации.
22. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустико-радиоэлектронных каналов утечки информации, разработка методов и технических

средств защиты информации.

23. Моделирование вербального объекта защиты, где ведутся конфиденциальные переговоры, возможных угроз безопасности информации для акустико-оптических каналов утечки информации, разработка методов и технических средств защиты информации.
24. Моделирование вербального объекта защиты, где производится обработка информации с использованием СВТ (АС), возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.
25. Моделирование вербального объекта защиты, где производится обработка информации с использованием технических средств обработки информации, возможных угроз безопасности информации и технических каналов утечки информации, разработка методов и технических средств защиты информации.
26. Моделирование вербального объекта защиты, возможных угроз безопасности информации для материально-вещественных каналов утечки информации, разработка методов и технических средств защиты информации.
27. Порядок проведения аттестационных испытаний по требованиям безопасности информации на примере вербального объекта информатизации.
28. Порядок проведения работ по созданию системы защиты информации для вербального объекта информатизации.
29. Организационные методы контроля эффективности защиты информации на примере вербального объекта информатизации.
30. Технические средства контроля эффективности защиты информации на примере вербального объекта информатизации.
31. Расчет основных показателей качества системы охранной сигнализации объекта информатизации.
32. Выбор варианта структуры построения системы сбора и обработки информации объекта информатизации.
33. Построение системы обеспечения безопасности объекта информатизации с заданными показателями качества.

ПРИЛОЖЕНИЕ Б

Образец титульного листа курсовой работы

КУРСОВАЯ РАБОТА

по профессиональному модулю

ПМ.03 Защита информации техническими средствами

на тему «_____
_____»

Выполнил: _____,
обучающийся ____ курса _____ формы обучения
специальность: 10.02.05 Обеспечение информационной безопасности автоматизированных систем
группа _____
Руководитель: _____
(инициалы, фамилия)

_____
(уч. степень, уч. звание)

Оценка _____

Подпись _____

« » _____ 202__ г.

Москва, 202__г

ПРИЛОЖЕНИЕ В

Примерная структура и содержание курсовой работы

Структура и содержание курсовой работы

Разработке проекта плана курсовой работы со стороны студента должно быть уделено особое внимание. Для этого студенту целесообразно придерживаться следующей структуры содержания курсовой работы.

Содержание - указываются наименование разделов и страницы.

Аннотация - содержит краткое содержание работ, выполненных в курсовой работе.

Во введении дается обоснование выбора темы, характеризуется ее актуальность и значение, определяется цель и задачи курсовой работы. В этой частиработы указывается исходный материал, используемый при выполнении работы.

Теоретическую часть, в которой дается описание истории вопроса, оценивается уровень разработанности проблемы в теории и практике посредством сравнительного анализа литературы. Рассматривается нормативная база исследуемого вопроса, раскрываются основные термины и понятия. Дискуссионные вопросы этой части курсовой работы должны сопровождаться обязательной формулировкой собственной позиции ее автора. Дается краткая производственно-экономическая характеристика объекта исследования.

Текст в данном разделе должен быть разбит на параграфы, выделяемые заголовками.

Заключение: Излагаются выводы, которые явились следствием изучения предмета курсовой работы. Заключение представляется в виде тезисов, в предельно сжатом изложении и содержит выводы и рекомендации относительно возможностей использования материалов работы.

Список литературы: указываются использованные при выполнении курсовой работы законодательные акты и постановления правительства, инструкции и нормативные акты соответствующих ведомств, статистические сборники, статьи из журналов и другой периодической печати. Список использованных источников оформляется в соответствии с требованиями ГОСТов.

Приложения: Приложения оформляются как продолжение курсовой работы в виде ее последующих страниц. Каждое приложение начинают с новой страницы с указанием по центру слова «Приложение». Оно должно иметь заголовок и быть пронумеровано большими буквами русского алфавита.

В приложении могут быть даны: выдержки из нормативных документов, таблицы, схемы, примеры практического материала и т.д., необходимые для раскрытия полноты курсовой работы. Размещают приложения в порядке упоминания в тексте ссылок на них.

Материал курсовой работы следует излагать своими словами, ясно, обстоятельно и кратко.

По спорным вопросам, трактуемым разными авторами по-разному, или идущими в разрез с инструктивными материалами и нормативными актами студент должен сформировать свое мнение, обосновав его соответствующими

аргументами.

ПРИЛОЖЕНИЕ Д
Требования к оформлению курсовой работы

Текст курсовой работы (проекта) должен быть набран на персональном компьютере и распечатан на принтере, шрифт 14 пт (Times New Roman), с межстрочным интервалом – 1,5. Требования к полям: левое – 30 мм, правое – 10 мм, верхнее – 20 мм, нижнее – 20 мм. Абзацный отступ составляет (12,5 мм) 5 знаков. Текст выравнивается по ширине.

Содержание работы структурируется по главам и параграфам. Главы и параграфы должны иметь заголовки. Заголовки глав выравнивают по левому краю, печатаются жирным (16 пт) шрифтом (Times New Roman). Заголовки параграфов выравнивают по левому краю и печатаются жирным (14 пт) шрифтом(Times New Roman).

Между пунктом и текстом одна свободная строка с межстрочным 1,5 интервалом. Текст заголовков, состоящих из нескольких строк, набирается с межстрочным интервалом – 1,5.

В тексте ничего не подчеркивается, курсивом не выделяется, в конце заголовков точки не ставятся.

В содержании и по тексту заголовки глав и параграфов нумеруются арабскими цифрами. Номер параграфа состоит из номера главы и параграфа, разделенных точкой. Трехуровневое дробление заголовков (на подпараграфы) в курсовой работе (проекте) не рекомендуется и допускается только в виде обоснованного исключения.

Заголовки разделов «Введение», «Заключение», «Список использованных источников», «Приложения» не нумеруются. Каждый заголовок должен состоять только из одного предложения.

Страницы текста курсовой работы (проекта) нумеруются, номер страницы ставится в центре нижней части листа без точки. «Титульный лист» считается первым, но номер на нем *не проставляется*. «Задание» − второй лист; «Содержание» − третий; «Введение» − четвертый. Нумерация проставляется со второй страницы введения (примерно, пятый лист). Затем далее располагаются: «Главы», «Заключение», «Список использованных источников», «Приложения». Каждая глава

начинается с новой страницы. Параграфы начинать с новой страницы нецелесообразно. Глава не может содержать менее двух параграфов.

В тексте курсовой работы могут быть перечисления. Перед каждой позицией перечисления ставится прочерк, в конце каждой позиции – точка с запятой.

Надписи на иллюстрациях, наименования и подрисуночный текст выравниваются по центру. В подрисуночном тексте применяют полуторный интервал между строк. После наименования рисунка точка не ставится. Выше и ниже каждой иллюстрации следует оставить не менее одной свободной строки (межстрочный интервал – 1,5). Перенос части иллюстрации на другую страницу не допускается.

На все иллюстрации в тексте должны быть ссылки и разъяснения.

Таблицы имеют сквозную нумерацию. По левому краю выравнивают номер таблицы и размещают название. Номер таблицы, название и все заполнения выполняются шрифтом 14 пт, при этом, в случае необходимости, внутри таблицы можно применять и более мелкий шрифт (до 10 пт), интервал между строк – минимальный.

После таблицы необходимо оставить одну свободную строку (межстрочный интервал – 1,0).

Если таблица имеет размеры, не превышающие размер страницы, перенос части таблицы на другую страницу не допускается. Если таблица имеет размеры более, чем одна страница, перенос таблицы допускается. При этом на каждой новой странице в левом верхнем углу делается надпись «Продолжение таблицы …» с указанием ее номера (название таблицы при переносе не повторяется). Далее через один межстрочный интервал повторяются заголовки граф. Ссылки по тексту на таблицы следует давать в полном виде. Допускается помещать таблицу вдоль длинной стороны листа (альбомный вариант).

Ссылки по тексту на источники, которыми пользовался студент при выполнении курсовой работы, обозначаются числом в квадратных скобках. Рекомендуется указывать не только источник, но и страницу этого источника. Образец ссылки: [21, с. 621]. Первое число в скобках должно соответствовать номеру

источника в списке использованных источников, который размещается в конце работы. Второе число – номер страницы.

В некоторых случаях, когда ссылки отражают не конкретный вывод автора, а его концепцию, изложенную во всей работе, указывать номера страниц источника нецелесообразно.

Подстраничные и внутритекстовые сноски в работе делать не рекомендуется.

Смысловое содержание введения и заключения не предполагают наличия ссылок: эти разделы являются личным умозаключением студента.

Структура списка использованных источников выглядит следующим образом: нормативная литература в порядке убывания юридического статуса, затем все остальные источники в алфавитном порядке. Количество их должно быть не менее 20.

После списка использованных источников размещаются «Приложения».

Каждое приложение следует начинать с новой страницы, по правому краю слово «ПРИЛОЖЕНИЕ». Нумеруются приложения последовательно арабскими цифрами (без знака №), например, «ПРИЛОЖЕНИЕ 1».

Работа вкладывается в папку. Электронная версия курсовой работы также сдается научному руководителю для рецензирования.