Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве РФ»
КОЛЛЕДЖ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ И ОФОРМЛЕНИЮ КУРСОВОГО ПРОЕКТА ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ 02 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

МДК 02.01 Программные и программно-аппаратные средства защиты информации

специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем

Рассмотрен
предметной (цикловой) комиссией
Информационная безопасность
«23» апреля 2020г.
Протокол № 6
Председатель цикловой комиссии:
_____/С.М. Володин/

Преподаватель _____/ Е.В. Поколодина /

Москва 2020

Содержание

Введение

В условиях цифровой трансформации общества острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Это, прежде всего, связано с расширением сферы применения средств вычислительной техники и возросшим уровнем доверия к автоматизированным системам управления и обработки информации.

Проблема защиты вычислительных систем становится еще более серьезной и в связи с развитием и распространением вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам. Доступность средств вычислительной техники, персональных ЭВМ и мобильных устройств, приводит к увеличению числа попыток неправомерного вмешательства в работу государственных и коммерческих автоматизированных систем. К сожалению, многие из этих попыток имеют успех и наносят значительный урон всем заинтересованным субъектам информационных отношений. Это обуславливают все возрастающее значение защиты информации, хранящейся в компьютерных системах. Причем при проектировании систем безопасности корпоративных систем необходимо учитывать вопросы защиты информации, как от внешних атак, так и от внутренних злоумышленников.

Курсовой проект является составной частью учебного МДК 02.01 Программные и программно-аппаратные средства защиты информации и предназначена для практического закрепления и расширения полученных теоретических знаний. Задачей курсового проекта является приобретение студентом навыков проектирования программных и аппаратных средств защиты компьютерной информации в персональных компьютерах.

1. Цели и задачи курсового проектирования

Выполнение студентом курсового проекта по профессиональному модулю (ПМ) проводится с целью

1. Формирование умений

Применять программно-аппаратные средства обеспечения информационной безопасности

-диагностировать, устранять отказы и обеспечивать работоспособность программно- аппаратных средств обеспечения информационной безопасности

-оценивать эффективность применяемых программно-аппаратных средств обеспечения информационной безопасности;

участвовать в обеспечении учета, обработки, хранения и передачи конфиденциальной информации;

-решать частные технические задачи, возникающие при аттестации объектов, помещений, программ, алгоритмов;

-использовать типовые криптографические средства и методы защиты информации, в том числе и электронную цифровую подпись;

-применять нормативные правовые акты, нормативные методические документы по обеспечению информационной безопасности программно-аппаратными средствами

2. Формирование профессиональных компетенций:

Название ПК	**Основные показатели оценки результата (ПК)**
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	**Практический опыт:** установка, настройка программных средств защиты информации в автоматизированной системе **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	**Практический опыт:** обеспечение защиты автономных автоматизированных систем программными и программно-аппаратными средствами; использование программных и программно-аппаратных средств для защиты информации в сети **Умения:** устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; **Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации	**Практический опыт:** тестирование функций, диагностика, устранение отказов и восстановление работоспособности программных и программно-аппаратных средств защиты информации **Умения:** диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; **Знания:** методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	**Практический опыт:** решение задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных **Умения:** применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для вы-

	полнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись **Знания:** особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	**Практический опыт:** учёт, обработка, хранение и передача информации, для которой установлен режим конфиденциальности **Умения:** применять средства гарантированного уничтожения информации **Знания:** особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	**Практический опыт:** работа с подсистемами регистрации событий; выявление событий и инцидентов безопасности в автоматизированной системе **Умения:** устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак **Знания:** типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа

3. Форматирования общих компетенций по специальности:

Код компетенции	Формулировка компетенции	Знания, умения
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	**Умения:** распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника).
		Знания: актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	**Умения:** определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.
		Знания номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие	**Умения**: определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития
		Знания: содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования

ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	**Умения**: организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами
		Знания: психология коллектива; психология личности; основы проектной деятельности
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	**Умения:** излагать свои мысли на государственном языке; оформлять документы.
		Знания: особенности социального и культурного контекста; правила оформления документов.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей	**Умения:** описывать значимость своей профессии Презентовать структуру профессиональной деятельности по специальности
		Знания: сущность гражданско-патриотической позиции Общечеловеческие ценности Правила поведения в ходе выполнения профессиональной деятельности
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	**Умения:** соблюдать нормы экологической безопасности; определять направления ресурсосбережения в рамках профессиональной деятельности по специальности.
		Знания: правила экологической безопасности при ведении профессиональной деятельности; основные ресурсы, задействованные в профессиональной деятельности; пути обеспечения ресурсосбережения.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности	**Умения:** использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; применять рациональные приемы двигательных функций в профессиональной деятельности; пользоваться средствами профилактики перенапряжения характерными для данной специальности
		Знания: роль физической культуры в общекультурном, профессиональном и социальном развитии человека; основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; средства профилактики перенапряжения.
ОК 09		**Умения: п**рименять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение

	Использовать информационные технологии в профессиональной деятельности	**Знания:** современные средства и устройства информатизации; порядок их применения и программное обеспечение в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках	**Умения:** понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы
		Знания: правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности

Задачи курсового проекта

-поиск, анализ необходимой информации

-разработка материалов в соответствии с заданием на курсовую работу

-выполнение расчетной, графической или демонстрационной части курсового проекта;

-подготовка и защита курсового проекта

2. Теоретическая часть

При проектировании систем защиты информации (СЗИ) необходимо решить задачи алгоритмического, логического и конструктивного синтеза. Алгоритмический синтез предполагает определение основных характеристик разрабатываемой системы, выбора и обоснования решаемых задач, формулирования технического задания к разрабатываемой системе. Затем производится разработка математического описания решаемых задач, формулировка общего алгоритма, описанного на математическом языке, выбор структуры системы.

Программные и аппаратные СЗИ должны проектироваться исходя из предъявляемых требований к показателям защищенности средств вычислительной техники и автоматизированных систем от несанкционированного доступа [1-3].

На втором этапе производится разработка рабочего алгоритма (методики). Логический синтез предполагает разработку функциональной и на ее основе принципиальной схемы устройства, наилучшим образом удовлетворяющей основным характеристикам, полученным на этапе алгоритмического синтеза. На этапе логического синтеза осуществляется выбор архитектуры и элементной базы. Важное место при проектировании системы занимает распределение функций между аппаратной и программной частями системы.

Аппаратная реализация ряда функций позволяет увеличить быстродействие, степень защиты от изучения и взлома, но ценой аппаратных затрат. Программная реализация обеспечивает большую универсальность и компактность, но более уязвима к взлому.

При разработке СЗИ необходимо понимание физических принципов, лежащих в основе их работы – методам модификации загрузочных областей винчестера, перехвата прерываний, использования специальных драйверов и т.д. В курсовой работе должен быть четко показан и обоснован выбранный метод защиты информации.

При разработке СЗИ необходимо ознакомиться с существующими системами защиты типа семейства Криптон, Аккорд, Верба, *Secret Net, Dallas Lock*, Страж, продукцией фирм Лан-Крипто, Сигнал-КОМ [1–10].

При создании СЗИ значительное внимание уделяется методам идентификации. Большую перспективу имеют биометрические методы идентификации: как статические на основе идентификации по отпечаткам пальцев, рук, лицу, радужной оболочке и сетчатке глаза, так и динамические на основе клавиатурного почерка, росписи мыши, голосу. Получить информацию о различных аспектах биометрической идентификацией, уже существующих системах и продуктах вы можете в [1,8,32].

Популярным методом идентификации является использование магнитных и смарт карт, а также электронных таблеток *ibutton*, номенклатура и возможности которых растут с каждым годом. Принципы, особенности, виды магнитных и смарт карточек, других электронных идентификаторов рассмотрены в [1-10].

Важной проблемой в условиях киберугроз является реализация защита программ и данных от несанкционированного копирования. Для защиты программ после их размещения на компьютере используется различные технологии активации, использующие идентификацию компьютера на основе особенностей аппаратной среды и по программным особенностям среды. Также достаточно широко различные виды электронных ключей. Их разновидности, методы защиты, состав системы защиты раскрыты в [19-26].

Для защиты данных в последнее время все шире используется *DRM* системы. В их основе лежит шифрование информации [19-26]. Доступ к информации может получить лишь купивший соответствующую лицензию.

Все большую популярность для защиты от внутренних угроз получают *DLP* системы [1.31,32].

3. Типовые задания к курсовому проекту

1. Анализ систем видеонаблюдения, применяемые в рамках программы «Умный город»
2. Исследование программно-аппаратных средств защиты DNS
3. Анализ систем банковской безопасности
4. Анализ современных программных средств антивирусной защиты
5. Программно-аппаратные средства перехвата управлением беспилотными летательными аппаратами
6. Технические средства обеспечения информационной безопасности
7. Защита информации в электронных платежных системах
8. Методы организации информационной безопасности бизнеса
9. ПО для защиты информации в государственных информационных системах.
10. Программно-аппаратные средства обеспечения безопасности продуктовых сетей
11. Нормативно правовая база и стандарты в области программно-аппаратных средств защиты информации
12. Анализ троянских программ
13. Биометрическая идентификация как средство обеспечения безопасности организации
14. Защита информации в сфере социальной инженерии
15. Информационная безопасность интернет-сайтов
16. Анализ троянских программ
17. Анализ антивирусных средств защиты информации
18. Анализ программных средств систем распознавания лиц
19. Разработка защиты от программ слежения за набором на клавиатуре
20. Программные средства в банковской безопасности
21. Исследование сетевых атак на Web-серверы
22. Анализ уязвимостей IP-камер

23. Организация защиты персональных данных в КИП
24. Анализ атак на службу DNS
25. Анализ систем банковской безопасности
26. Система защиты персональных данных сотрудников коммерческого предприятия
27. Анализ уязвимостей камер видеонаблюдения
28. Разработка мероприятий по защите информации интернет портала
29. Метода организации информационной безопасности бизнес
30. Защита информации в электронных платежных системах
31. Биометрическая идентификация как средство обеспечения безопасности организации
32. Нормативно правовая база и стандарты в области программно-аппаратных средств защиты информации
33. Системы защиты персональных данных клиентов коммерческого предприятия
34. Анализ троянских программ
35. Анализ уязвимости IP камеры
36. Анализ систем безопасности аэропорта
37. Защита данных в области социальной инженерии
38. Организация защиты персональных данных в КИП
39. Анализ атак на службу ДНС
40. Анализ программных средств систем распознавания лиц
41. Эпоха интернет вещей вопроса безопасности
42. Исследование вопроса безопасности интернет вещей
43. Исследование программ для USB аутентификации
44. Программные средства банковской безопасности
45. Анализ программно-аппаратных средств безопасности аэропорта
46. Уязвимости UNIX систем
47. Межсетевые экраны и их роли в защите АИС

48. Информационная безопасность интернет-сайтов
49. Анализ систем банковской безопасности
50. Анализ атак на службу DNS
51. Программные средства в банковской безопасности
52. Технические средства обеспечения информационной безопасности
53. Исследование программно-аппаратных средств защиты беспроводных сетей
54. Анализ уязвимостей камер видеонаблюдения
55. Методы организации информационной безопасности бизнеса или социальная инженерия
56. Анализ троянских программ
57. Система охранной сигнализации
58. Межсетевые экраны и их роль в защите АИС
59. Защита информации в электронных платежных системах
60. Система пожарной безопасности
61. Системы защиты персональных данных сотрудников коммерческого предприятия
62. Анализ троянских программ
63. Защита информации в сфере социальной инженерии.
64. Программные средства в банковской безопасности
65. Биометрическая идентификация как средство обеспечения безопасности организации
66. Информационная безопасность интернет сайтов
67. Анализ уязвимостей камер наблюдения
68. Организация защиты персональных данных в КИП
69. Эпоха интернет вещей: вопрос безопасности
70. Анализ методов идентификации и аутентификации
71. Анализ программных закладок
72. Анализ уязвимостей ip камер

73. Технические средства защиты информационной безопасности
74. Анализ алгоритмов целостности файлов
75. Методы противодействия взлому в информационных системах с помощью технологий подбора паролей «brute force».
76. Анализ программно-аппаратных средств защиты автомобилей
77. Анализ программно-аппаратных средств для системы контроля управления доступа
78. Защита информации в электронных платежных системах
79. Информационная безопасность интернет сайтов
80. Системы защиты персональных данных сотрудников банка
81. Методы организации информационной бизнеса
82. Анализ программных средств систем распознавания лиц
83. Анализ программно-аппаратных средств защиты государственных учреждений
84. Программно-аппаратные средства обеспечения безопасности продуктовых сетей
85. Анализ систем банковской безопасности

4. Требования к структуре курсового проекта

Курсовой проект должен состоять из пояснительной записки и электронного приложения к ней на носителе.

Пояснительная записка курсового проекта должна включать в себя:

-теоретические основы разрабатываемой темы

-анализ существующих проблем в сфере информационной безопасности по теме проекта

-обоснование выбора алгоритма (методики) для решения поставленной задачи из известных алгоритмов (методик) или создание оригинального алгоритма с описанием его правильности;

-подробное описание алгоритма (методики);

-обоснования выбора языка программирования (если он задан) или математического метода;

-руководство для пользователя в котором описывается как применять созданную программу (методику);

-описание тестирования программы (методики);

-результаты применения программы (методики) для решения поставленной задачи;

-листинги разработанных программ, помещаемые обычно в приложении.

Пояснительная записка должна содержать графическую часть, которая может содержать схемы применяемых алгоритмов, структуры исходных и обработанных в программе данных, графические результаты работы программы.

Объем пояснительной записки курсового проекта должен быть не менее 20 страниц печатного текста, объем графической части – не менее 4 страниц.

Студент должен предоставить преподавателю для проверки копию своего курсового проекта на электронном носителе, а также презентацию.

5. Организация выполнения курсового проекта

5.1 Общее руководство и контроль за ходом выполнения курсового проекта осуществляет преподаватель соответствующего МДК.

5.2 На время выполнения курсового проекта составляется расписание консультаций, утверждаемое заместителем директора по учебной работе колледжа.

Консультации проводятся за счет объема времени, отведенного в рабочем учебном плане на дисциплину или МДК.

В ходе консультаций преподавателем разъясняются назначение и задачи, структура и объем, принципы разработки и оформления, примерное распределение времени на выполнение отдельных частей курсового проета, даются ответы на вопросы студентов.

5.3 Основными функциями преподавателя – руководителя курсового проекта являются:

-консультирование по вопросам содержания и последовательности выполнения работы;

-оказание помощи студенту при подборе необходимой литературы;

-контроль хода выполнения курсовой работы;

-подготовка письменного отзыва на курсовую работу.

5.4 По завершении студентом курсового проекта руководитель, подписывает ее и вместе с письменным отзывом передает студенту для ознакомления.

5.5 Письменный отзыв должен включать:

-заключение о соответствии курсового проекта заявленной теме;

-оценку качества выполнения работы;

-оценку полноты разработки поставленных вопросов, теоретической и практической значимости курсового проекта;

-оценку курсового проекта.

Проверку и составление письменного отзыва и прием курсового проекта осуществляет руководитель курсового проекта вне расписания учебных занятий. На выполнение этой работы отводится один час на каждый курсовой проект.

5.6 Защита курсового проекта является обязательной и проводится за счет объема времени, предусмотренного на изучение МДК.

5.7 Курсовой проект оценивается по пятибальной системе. Положительная оценка по МДК, по которому предусматривается курсовой проект, выставляется только при условии успешной сдачи курсовой работы на оценку не ниже “удовлетворительно”

5.8 Студентам, получившим неудовлетворительную оценку по курсовому проекту, предоставляется право выбора новой темы курсового проекта, или по решению преподавателя, доработки прежней темы и определяется новый срок для ее выполнения.

6. Критерий оценки курсового проекта

«Отлично» выставляется за курсовой проект, если:

1. Работа выполнена в полном соответствии с требованиями, изложенными в методических указаниях.

2. При защите курсового проекта показано отличное знание и владение современными методами защиты компьютерной информации.

3. Работа безукоризненна в отношении оформления (пояснительная записка выполнена в соответствии с требованиями ЕСКД и ЕСПД).

4. Все этапы выполнены в отведенный срок и в соответствии с методическими указаниями по выполнению курсового проекта.

5. Даны правильные ответы на все теоретические и практические вопросы, заданные членами комиссии.

«Хорошо» выставляется в случае, если:

1. Работа выполнена с несущественными недостатками по отношению к требованиям, изложенным в методических указаниях к курсовому проекту.

2. При защите курсового проекта показано хорошее знание и владение современными методами защиты компьютерной информации.

3. Работа оформлена с небольшими недостатками в пояснительной записке и электронном варианте курсового проекта.

4. Все этапы выполнены в отведенный срок и в соответствии с методическими указаниями по выполнению курсового проекта.

5. Даны правильные ответы на все теоретические и практические вопросы, заданные членами комиссии.

«Удовлетворительно» выставляется, если:

1. Работа выполнена с определенными недостатками по отношению к требованиям, изложенным в методических указаниях к курсовому проекту.

2. При защите курсового проекта показано удовлетворительное знание и владение современными методами защиты компьютерной информации.

3. Работа оформлена неряшливо, с нарушениями стандартов в пояснительной записке и электронном варианте курсового проекта.

4. Работа представлена в срок.

5. Даны неполные и неточные ответы на ряд теоретических и практических вопросов, заданных членами комиссии.

«Неудовлетворительно» выставляется, если:

1. Работа выполнена с грубыми недочетами по отношению к требованиям, изложенным в методических указаниях к курсовому проекту.

2. При защите курсового проекта показано неудовлетворительное знание и владение современными методами защиты компьютерной информации.

3. Работа оформлена с грубыми нарушениями требований ЕСКД и ЕСПД в пояснительной записке и имеются грубые ошибки в электронном варианте курсового проекта.

4. Работа представлена не в срок.

5. Работа содержит заимствования из научно-технических источников литературы без соблюдения авторских прав (плагиат).

6. Даны неправильные ответы на теоретические и практические вопросы, заданные членами комиссии.

7. Организация и график выполнения курсового проекта

Каждый студент выполняет индивидуальное задание, которое выдается ему преподавателем. Список типовых заданий на курсовой проект приведен в главе 3.

График выполнения каждого этапа курсового проекта с определенной трудоемкостью отражается в выдаваемом студенту плане (Приложение 1) и устанавливается в соответствии с требованиями положения УГАТУ о курсовом проектировании (10 недель). Содержание отдельных этапов и сроки их выполнения

устанавливаются таким образом, чтобы в течение всего периода работы обеспечивалась равномерная недельная нагрузка (Приложение 1).

На пятой и восьмой неделе проводится контрольный просмотр состояния дел с курсовым проектированием.

Проектирование и моделирование работы защищенной компьютерной системы может производиться с помощью ПО создания и управления виртуальными машинами (например, *Virtual PC* или фирмы *VMWare*).

Внимание! Не допускается распространение исходников, описаний и самих программ, которые могут использоваться для атак на компьютерные системы.

По результатам курсового проекта студентом в соответствии с требованиями, изложенными в разделе 8, оформляется пояснительная записка и сдается преподавателю на проверку в электронном виде. Срок проверки 3 – 7 дней. После проверки работы преподавателем и устранения студентом выявленных недостатков и недочетов курсовой проект в электронном виде сдается на повторную проверку. При этом в виде отдельного файла должен прилагаться список имевших место замечаний, краткие ответы на них и ссылки на разделы и страницы курсовой работы, где они учтены. В тексте курсового проекта цветом должны быть выделены все произведенные изменения. Также студентом сдается в электронном виде:

а) анализируемое (за исключением, выданного преподавателем) ПО;

б) написанное ПО;

в) электронные материалы, используемые при выполнении курсового проекта;

г) образы виртуальных машин, используемых при моделировании спроектированной системы защиты, список учетных записей и паролей, используемых в виртуальных машинах;

д) различные отчеты, сформированные исследуемым и написанным ПО.

После положительных результатов проверки пояснительной записки, она распечатывается и сдается преподавателю, студент защищает курсовой проект, по результатам защиты выставляется итоговая оценка.

Если студент не представил завершенную работу в установленный срок по неуважительной причине, то руководитель согласно положению «О курсовом проектировании» вправе не проверять материалы курсовой работы. В этом случае студент имеет право представить свою работу непосредственно комиссии в соответствии с графиком защит.

8. Требования к оформлению курсового проекта

8.1 Общие требования к оформлению

Страницы текста пояснительной записки, а также иллюстрации и таблицы должны соответствовать формату А4 и быть выполнены с использованием компьютера и принтера на одной стороне листа белой бумаги формата А4 через полтора интервала.

Цвет шрифта должен быть черным. Высота и стиль букв, цифр и других знаков должны соответствовать кеглю 14, шрифту Times New Roman.

Текст пояснительной записки должен быть выровнен по ширине, начертание обычное.

Текст пояснительной записки следует печатать, соблюдая следующие размеры полей:

- правое–10 мм;
- верхнее и нижнее – 20 мм;
- левое– 30 мм.

Абзацный отступ (красная строка) должен составлять10 мм.

Разрешается использовать компьютерные возможности акцентирования внимания на определенных терминах, формулах, теоремах, применяя шрифты разной гарнитуры.

Фамилии, названия учреждений, организаций, фирм, название изделий и другие имена собственные в пояснительной записке приводят на языке оригинала. Допускается транслитерировать имена собственные и приводить названия организаций в переводе на язык пояснительной записки с добавлением (при первом упоминании) оригинального названия.

8.2 Требования к построению пояснительной записки

Наименования структурных элементов пояснительной записки «СОДЕРЖАНИЕ», «ВВЕДЕНИЕ», «ЗАКЛЮЧЕНИЕ», «СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ», «ПРИЛОЖЕНИЕ» служат заголовками структурных элементов. Заголовки структурных элементов следует располагать в середине строки без точки в конце и печатать прописными буквами, не подчеркивая.

Каждый структурный элемент пояснительной записки, а также каждый новый раздел следует начинать с нового листа (страницы).

Основную часть пояснительной записки следует делить на разделы, подразделы и пункты. Пункты, при необходимости, могут делиться на подпункты. При делении текста на пункты и подпункты необходимо, чтобы каждый пункт содержал законченную информацию.

Разделы, подразделы должны иметь заголовки. Пункты, как правило, заголовков не имеют. Заголовки должны четко и кратко отражать содержание разделов, подразделов.

Заголовки разделов, подразделов и пунктов следует печатать с абзацного отступа с прописной буквы без точки в конце, не подчеркивая. Если заголовок состоит из двух предложений, их разделяют точкой.

Заголовок раздела отделяется от заголовка подраздела одной пустой строкой. Текст подраздела отделяется от заголовка подраздела также одной строкой.

8.3 Требования к нумерации страниц

Страницы пояснительной записки следует нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту пояснительной записки. Номер страницы проставляют в центре нижней части листа без точки.

Титульный лист включают в общую нумерацию страниц пояснительной записки. Номер страницы на титульном листе не проставляют.

Иллюстрации и таблицы, расположенные на отдельных листах, включают в общую нумерацию страниц.

8.4 Требования к нумерации разделов, подразделов, пунктов, подпунктов

Разделы пояснительной записки должны иметь порядковые номера в пределах всей пояснительной записки, обозначенные арабскими цифрами без точки и записанные с абзацного отступа.

Подразделы должны иметь нумерацию в пределах каждого раздела. Номер подраздела состоит из номеров раздела и подраздела, разделенных точкой. В конце номера подраздела точка не ставится, например:

3 Методы испытаний

3.1 Аппараты, материалы и реактивы

3.1.1
3.1.2
3.1.3 } Нумерация пунктов первого подраздела третьего раздела

3.2 Подготовка к испытанию

3.2.1
3.2.2
3.2.3 } Нумерация пунктов второго подраздела третьего раздела

Если раздел состоит из одного подраздела, то подраздел не нумеруется. Если подраздел состоит из одного пункта, то пункт не нумеруется.

Если текст пояснительной записки подразделяется только на пункты, то они нумеруются порядковыми номерами в пределах всей записки. Пункты, при необ-

ходимости, могут быть разбиты на подпункты, которые должны иметь порядковую нумерацию в пределах каждого пункта, например, 4.2.1.1, 4.2.1.2, 4.2.1.3 и т.д.

Внутри пунктов или подпунктов могут быть приведены перечисления. Перед каждым элементом перечисления следует ставить дефис. При необходимости ссылки в тексте пояснительной записки на один из элементов перечисления вместо дефиса ставятся строчные буквы в порядке русского алфавита, начиная с буквы а (за исключением букв ё, з, й, о, ч, ъ, ы, ь).

Для дальнейшей детализации перечислений необходимо использовать арабские цифры, после которых ставится скобка, а запись производится с абзацного отступа.

8.5 Требования к оформлению иллюстраций

Иллюстрации (чертежи, графики, схемы, компьютерные распечатки, диаграммы, фотоснимки) следует располагать в пояснительной записке непосредственно после текста, в котором они упоминаются впервые, или на следующей странице, с выравниванием по центру.

Иллюстрации, за исключением иллюстрации приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Если рисунок один, то он обозначается «Рисунок 1». Слово «Рисунок» и его наименование располагают посередине строки.

Допускается нумеровать иллюстрации в пределах раздела. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой. Например, Рисунок 1.1.

Допускается использование цветных иллюстраций. На все иллюстрации должны быть даны ссылки в тексте пояснительной записки. При ссылках на иллюстрации следует писать «...в соответствии с рисунком 2» при сквозной нумерации и «...в соответствии с рисунком 1.2» при нумерации в пределах раздела.

Иллюстрации, при необходимости, могут иметь наименование и пояснительные данные (подрисуночный текст). Слово «Рисунок» и наименование рисунка при этом помещают под рисунком по центру, например,:

Рисунок 1 – Детали прибора

Иллюстрации каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения. Например, Рисунок А.3.

8.6 Требования к оформлению таблиц

Таблицы применяют для лучшей наглядности и удобства сравнения показателей. Наименование таблицы, при его наличии, должно отражать ее содержание, быть точным, кратким. Наименование таблицы следует помещать над таблицей слева, без абзацного отступа в одну строку с ее номером через тире.

Таблицу следует располагать в пояснительной записке непосредственно после текста, в котором она упоминается впервые, или на следующей странице.

Таблицы следует располагать по ширине документа. Заголовки столбцов должны быть центрированы, а остальной текст должен быть выровнен по левому краю. Шрифт в таблице должен быть таким же, как и во всей пояснительной записке, однако размер шрифта может быть при необходимости уменьшен до кегля 12.

На все таблицы должны быть ссылки в тексте пояснительной записки. При ссылке следует писать слово «таблица» с указанием ее номера, например:

«В таблице 1 представлены специальные символы» или «Для явного преобразования типов существуют функции, которые приведены в таблице 2.»

Если две и более таблиц располагаются последовательно, то они разделяются одной пустой строкой.

Не должно быть пустых строк между названием таблицы и самой таблицей, а также между таблицей и последующим текстом.

Таблицу с большим числом строк допускается переносить на другой лист (страницу). При переносе части таблицы на другой лист (страницу) слово «Таблица», ее номер и наименование указывают один раз слева над первой частью таблицы, а над другими частями также слева пишут слова «Продолжение таблицы» и указывают номер таблицы.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Допускается нумеровать таблицы в пределах раздела. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой.

Таблицы каждого приложения обозначают отдельной нумерацией арабскими цифрами с добавлением перед цифрой обозначения приложения.

8.7. Требования к оформлению примечаний и сносок

Примечания приводят, если необходимы пояснения или справочные данные к содержанию текста пояснительной записки, таблиц или графического материала. Слово «Примечание» следует печатать с прописной буквы с абзаца и не подчеркивать.

Примечания следует помещать непосредственно после текстового, графического материала или в таблице, к которым относятся эти примечания.

Если примечание одно, то после слова «Примечание» ставится тире и примечание печатается с прописной буквы. Одно примечание не нумеруют. Несколько примечаний нумеруют по порядку арабскими цифрами без проставления точки. Примечание к таблице помещают в конце таблицы над линией, обозначающей окончание таблицы.

При необходимости дополнительного пояснения в пояснительной записке его допускается оформлять в виде сноски. Знак сноски ставят непосредственно после того слова, числа, символа, предложения, к которому дается пояснение.

Знак сноски выполняют надстрочно арабскими цифрами со скобкой. Допускается вместо цифр выполнять сноски звездочками «*». Применять более трех звездочек на странице не допускается.

Сноску располагают в конце страницы с абзацного отступа, отделяя от текста короткой горизонтальной линией слева. Сноску к таблице располагают в конце таблицы над линией, обозначающей окончание таблицы.

8.8. Требования к оформлению формул и уравнений

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено по одной пустой строке.

Если уравнение не умещается в одну строку, то оно должно быть перенесено после знака равенства или после знаков плюс, минус, умножения, деления или других математических знаков, причем знак в начале следующей строки повторяют.

Расчетные формулы должны записываться в общем виде. Пояснения значений символов и числовых коэффициентов из формулы следует приводить непосредственно под формулой в той же последовательности, в какой они даны в формуле. Первую строку пояснений начинают без абзацного отступа со слова «где» без двоеточия после него. Значение каждого символа и числового коэффициента следует давать с новой строки, располагая символы один под другим.

Формулы в пояснительной записке следует нумеровать порядковой нумерацией в пределах всей пояснительной записки арабскими цифрами в круглых скобках в крайнем правом положении на строке.

Ниже приведен пример оформления формулы.

$$ОС = \frac{(ЗП_О + ЗП_Д) \cdot \%ОС}{100\%}, \qquad (1)$$

где $ОС$ – отчисления на социальные нужды, руб.;

$\%ОС$ – процент отчислений на социальные нужды, %;

$ЗП_{о}$ –заработная плата основная, руб.;

$ЗП_{д}$ –заработная плата дополнительная, руб.;

Формулы, помещаемые в приложения, должны нумероваться отдельной нумерацией арабскими цифрами в пределах каждого приложения с добавлением перед каждой цифрой обозначения приложения.

Ссылки в тексте на порядковые номера формул дают в скобках, например, ... в формуле (1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой.

8.9. Требования к оформлению ссылок и списка использованных источников

Ссылки на использованные источники в тексте пояснительной записки следует указывать порядковым номером библиографического описания источника в списке использованных источников. Порядковые номера ссылок указываются арабскими цифрами и заключаются в квадратные скобки, например [5].

Список использованных источников оформляется согласно ГОСТ 7.1. – 2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления» и ГОСТ 7.82 – 2001 «Библиографическая запись. Библиографическое описание электронных ресурсов. Общие требования и правила составления».

Пример оформления списка использованных источников приведен в Приложении 3.

8.10. Требования к оформлению приложений

Приложения оформляют как продолжение основного документа на последующих его листах.

В тексте пояснительной записки на все приложения должны быть даны ссылки. Приложения располагают в порядке ссылок на них в тексте пояснительной записки.

Каждое приложение следует начинать с новой страницы с указанием наверху посередине страницы слова «Приложение», его обозначения.

Приложение должно иметь заголовок, который записывают посередине страницы с прописной буквы отдельной строкой.

Приложения обозначают заглавными буквами русского алфавита, начиная с А, за исключением букв Ё, З, Й, О, Ч, Ъ, Ы, Ь. После слова «Приложение» следует буква, обозначающая его последовательность. Допускается обозначение приложений буквами латинского алфавита, за исключением букв I и О.В случае полного использования букв русского и латинского алфавитов допускается обозначать приложения арабскими цифрами.

Если в пояснительной записке одно приложение, оно обозначается «Приложение А».

Текст каждого приложения, при необходимости, может быть разделен на разделы, подразделы, пункты, подпункты, которые нумеруют в пределах каждого приложения. Перед номером ставится обозначение текущего приложения.

Приложения должны иметь общую с остальной частью пояснительной записки сквозную нумерацию страниц.

Список литературы

1. Программно-аппаратные средства обеспечения информационной безопасности: учеб. Пособие. – Душкин А.В., Барсуков О.М., Кравцов Е.В., Славнов К.В. М.: Горячая линия – Телеком, 2016. - 248 с.

2. 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

3. Основы современной криптографии: учеб. Пособие. – Баричев С.Г., Гончаров В.В., Серов Р.Е. М.: Горячая линия – Телеком, 2017. - 175 с.

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

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

6. 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».

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

8. 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.

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

10. 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.

11. 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.

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

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

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

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

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

16. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 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.

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

18. 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

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

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

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

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

23. 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

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

25. 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

Интернет-ресурсы

26. Федеральная служба по техническому и экспортному контролю (ФСТЭК России). – [Электронный ресурс]. – Режим доступа www.fstec.ru

27.Образовательные порталы по различным направлениям образования и тематике. – [Электронный ресурс]. – Режим доступа http://depobr.gov35.ru/

28.Справочно-правовая система «Консультант Плюс». – [Электронный ресурс]. – Режим доступа www.consultant.ru

29. Справочно-правовая система «Гарант»». – [Электронный ресурс]. – Режим доступа www.garant.ru

30. Федеральный портал «Российское образование. – [Электронный ресурс]. – Режим доступа www.edu.ru

31.Федеральный правовой портал «Юридическая Россия». – [Электронный ресурс]. – Режим доступа http://www.law.edu.ru/.

32.Российский биометрический портал. – [Электронный ресурс]. – Режим доступа www.biometrics.ru

33.Федеральный портал «Информационно- коммуникационные технологии в образовании». – [Электронный ресурс]. – Режим доступа htpp//:www.ict.edu.ru

34. Сайт Научной электронной библиотеки. – [Электронный ресурс]. – Режим доступа www.elibrary.ru

35. Приказ Финансового университета от 14.03.2013 № 416/о "Об утверждении Положения о курсовой о работе (проекте) студентов, обучающихся в колледжах-филиалах (подразделениях)Финуниверситета" – [Электронный ресурс]. – Режим доступа www.elibrary.ruhttp://www.fa.ru/org/spo/mfc/uch/VKR/Pologenie%20o%20kursovoi.PDF

Приложение 1

Федеральное государственное образовательное бюджетное учреждение высшего образования
«Финансовый университет при Правительстве Российской Федерации»
КОЛЛЕДЖ ИНФОРМАТИКИ И ПРОГРАММИРОВАНИЯ

МДК 02.01 Программные и программно-аппаратные средства защиты информации

УТВЕРЖДАЮ
Председатель цикловой комиссии информационной безопасности

Володин С.М.

___- _____2020

Группа: ЗОИБАС-ХХХ

ПРОЕКТ КУРСОВОЙ
На тему: Название темы

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Руководитель курсового проекта:
Поколодина Е.В.

Исполнитель курсового проекта:
Иванов И.И.

Оценка за проект: _____
____/____/2020

Москва 2020

Приложение 3

Нормативные документы

1. ГОСТ 34.003-90. Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения действующий Настоящий стандарт устанавливает термины и определения основных понятий в области автоматизированных систем (АС) и распространяется на АС, используемые в различных сферах деятельности (управление, исследования, проектирование и т. п., включая их сочетание), содержанием которых является переработка информации.
2. ГОСТ Р ИСО/МЭК 90003-2014 Разработка программных продуктов. Руководящие указания по применению ИСО 9001:2008 при разработке программных продуктов.

Монографии, учебники, учебные пособия

3. Зиборов В.В. Visual C++ 2012 на примерах. – СПб.: БХВ-Петербург, 2013. – 480 с.
4. Павловская Т.А. C++. Программирование на языке высокого уровня: учебник для вузов. – СПб.: Питер, 2009. – 432 с.

Интернет-ресурсы

5. Язык программирования C++: учебный курс А. Фридмана. – [Электронный ресурс]. – Режим доступа: http://www.intuit.ru/studies/courses/17/17/info