СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Программно-аппаратные средства защиты информации***

Блок Б1, базовая часть, Б1.Б.29
цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

10.03.01 ***Информационная безопасность***
код наименование направления

Программа

Безопасность компьютерных систем (по отрасли или в сфере профессиональной деятельности)

Форма обучения

Очная

Для поступивших на обучение в
2020 г.

Разработчик (составитель)
кандидат физико-математических наук, доцент
Беляева М. Б.
ученая степень, должность, ФИО

Стерлитамак 2023

1. Перечень компетенций с указанием этапов их формирования и описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Формируемая компетенция (с указанием кода)	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3				4
		неуд.	удовл.	хорошо	отлично	
Способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1)	1 этап: Знания	Студент демонстрирует незначительное понимание материала. Студент не демонстрирует способность использовать умения в процессе выполнения. Студент демонстрирует непонимание заданий. У студента нет ответа. Не было попытки выполнить задания.	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать умение выражена слабо.	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать умения в процессе выполнения	Студент демонстрирует полное понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать умения в процессе выполнения	Лабораторные работы №3-4
	2 этап: Умения	Студент демонстрирует незначительное	Студент демонстрирует частичное понимание	Студент демонстрирует значительное	Студент демонстрирует полное	Тест №2

		понимание материала. Студент не демонстрирует способность использовать знания в процессе выполнения Студент демонстрирует непонимание заданий. У студента нет ответа. Не было попытки выполнить задания.	материала. Способность студента продемонстрировать знание выражена слабо	понимание материала. Студент демонстрирует способность использовать знания в процессе выполнения	понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать знания в процессе выполнения	
	3 этап: Владения (навыки / опыт деятельности)	Студент демонстрирует незначительное понимание материала. Студент не демонстрирует способность использовать умения в процессе выполнения. Студент демонстрирует непонимание	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать умение выражена слабо	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать умения в процессе выполнения	Студент демонстрирует полное понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать умения в процессе	Проект, Курсовая работа

		заданий. У студента нет ответа. Не было попытки выполнить задания.			выполнения	
Способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)	1 этап: Знания	Студент демонстрирует незначительное понимание материала. Студент не демонстрирует способность использовать умения в процессе выполнения. Студент демонстрирует непонимание заданий. У студента нет ответа. Не было попытки выполнить задания.	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать умение выражена слабо	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать умения в процессе выполнения	Студент демонстрирует полное понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать умения в процессе выполнения	Лабораторные работы №1-2
	2 этап: Умения	Студент демонстрирует незначительное понимание материала.	Студент демонстрирует частичное понимание материала. Способность	Студент демонстрирует значительное понимание материала.	Студент демонстрирует полное понимание учебного	Реферат

		Студент не демонстрирует способность использовать умения в процессе выполнения. Студент демонстрирует непонимание заданий. У студента нет ответа. Не было попытки выполнить задания.	студента продемонстрировать умение выражена слабо	Студент демонстрирует способность использовать умения в процессе выполнения	материала. Студент демонстрирует ярко выраженную способность использовать умения в процессе выполнения	
	3 этап: Владения (навыки / опыт деятельности)	Студент демонстрирует незначительное понимание материала. Студент не демонстрирует способность использовать умения в процессе выполнения. Студент демонстрирует непонимание заданий. У студента нет	Студент демонстрирует частичное понимание материала. Способность студента продемонстрировать умение выражена слабо	Студент демонстрирует значительное понимание материала. Студент демонстрирует способность использовать умения в процессе выполнения	Студент демонстрирует полное понимание учебного материала. Студент демонстрирует ярко выраженную способность использовать умения в процессе выполнения	Тест №1

		ответа. Не было попытки выполнить задания.				

2. Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

ВИДЫ КОНТРОЛЯ ЗНАНИЙ СТУДЕНТОВ И ИХ ОТЧЕТНОСТИ

Видами контроля знаний студентов и их отчетности являются:

1) тесты, реферат – контроль над усвоением теоретического материала;

2) лабораторные работы – контроль над усвоением практического материала; отчет по индивидуальным вариантам лабораторных работ к каждой изученной теме

3) проекты – контроль над усвоением теоретического и практического материала.

Основной формой текущего контроля усвоения материала является защита студентами индивидуальных отчётов по каждой теме лабораторного практикума.

Кроме того, в течение курса предусмотрено проведение практических работ, тестов для проверки усвоения материала лекций и вопросов, вынесенных на самостоятельное изучение. Контрольные работы (тесты), охватывающая практически весь материал, проводятся по завершении изучения разделов.

Перечень тестовых заданий для оценки уровня сформированности компетенции ОПК-7 на этапе «Знания»

Тест №1

1. Под угрозой безопасности информации в компьютерной системе (КС) понимают:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2. Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

3. Атакой на КС называют:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

4. Искусственные угрозы исходя из их мотивов разделяются на:

a) непреднамеренные и преднамеренные

b) косвенные и непосредственные

c) несанкционированные и санкционированные

5. К непреднамеренным угрозам относятся:

a) ошибки в разработке программных средств КС

b) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.

c) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

6. К умышленным угрозам относятся:

a) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

b) воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

c) ошибки пользователей КС;

7. Косвенными каналами утечки называют:

a) каналы, не связанные с физическим доступом к элементам КС

b) каналы, связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

8. К косвенным каналам утечки информации относятся:

a) использование подслушивающих (радиозакладных) устройств;

b) маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.);

c) злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

9. Непосредственными каналами утечки называют:

a) каналы, связанные с физическим доступом к элементам КС.

b) каналы, не связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

10. К непосредственным каналам утески информации относятся:

a) обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.

b) перехват побочных электромагнитных излучений и наводок (ПЭМИН).

c) дистанционное видеонаблюдение;

11. Избирательная политика безопасности подразумевает, что:

a) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

b) все субъекты и объекты системы должны быть однозначно идентифицированы;

c) каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

12. Полномочная политика безопасности подразумевает, что:

a) каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

b) все субъекты и объекты системы должны быть идентифицированы;

c) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

13. Достоверная вычислительная база - это:

a) абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности.

b) активный компонент системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы.

c) пассивный компонент системы, хранящий, принимающий или передающий информацию.

14. Достоверная вычислительная база выполняет задачи:

a) поддерживает реализацию политики безопасности и является гарантом целостности механизмов защиты

b) функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности)

c) представляет собой некоторый соответствующую проверку, организационных мер набор требований, прошедших реализуемых при помощи

15. Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

c) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

16. Идентификация объекта - это:

a) одна из функций подсистемы защиты.

b) взаимное установление подлинности объектов, связывающихся между собой по

линиям связи.

c) сфера действий пользователя и доступные ему ресурсы КС

17. Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:

a) авторизацией

b) аутентификацией

c) Идентификация

18. Авторизация - это:

a) предоставлением полномочий

b) подтверждение подлинности

c) цифровая подпись

19. Аутентификация – это:

a) подтверждение подлинности

b) предоставлением полномочий

c) цифровая подпись

20. Биометрическая идентификация и аутентификация пользователя это:

a) идентификация потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения.

b) схема идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

c) схема идентификации с нулевой передачей знаний.

21. Для чего используется процедура «рукопожатия»:

a) для взаимной проверки подлинности

b) для распределения ключей между подлинными партнерами

c) для безопасного использования интеллектуальных карт

22. Параллельная схема идентификации позволяет увеличить:

a) число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

b) регистрацию времени для каждого сообщения

c) объект-эталон для идентификации и аутентификации пользователей

23. Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть:

a) семантически тождественны

b) модифицированы

c) структурированы

24. Для чего были разработаны протоколы идентификации с нулевой передачей знаний:
a) для безопасного использования интеллектуальных карт
b) для взаимной проверки подлинности
c) для распределения ключей между подлинными партнерами

25. Механизм запроса-ответа используется для:
a) проверки подлинности
b) шифрования
c) регистрации времени для каждого сообщения

26. Кто разработал алгоритм идентификации с нулевой передачей знания:
a) Гиллоу и Ж. Куискуотером
b) У. Фейге
c) А. Фиат и А. Шамир

27. Схему идентификации с нулевой передачей знаний предложили:
a) У. Фейге, А. Фиат и А. Шамир
b) Гиллоу и Ж. Куискуотером
c) А. Фиат и А. Шамир
28. Для чего создается система разграничения доступа к информации:
a) для защиты информации от НСД
b) для осуществления НСДИ
c) определения максимального уровня конфиденциальности документа

29. Какие методы организации разграничения доступа используются в КС:
a) матричный
b) структурированный
c) метод Гиллоу-Куискуотера

30. Мандатный метод основывается на:
a) многоуровневой модели защиты
b) использование матриц доступа
c) криптографическом преобразовании

31. Какой из функциональных блоков должна содержать система разграничения доступа к информации:
a) блок криптографического преобразования информации при ее хранении и передаче;
b) блок контроля среды размещения
c) блок контроля среды выполнения.

32. Диспетчер доступа реализуется в виде:

a) аппаратно-программных механизмов

b) аппаратных механизмов

c) программных механизмов

33. Под ядром безопасности понимают:

a) локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа.

b) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

c) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

34. Главным условием создания ядра безопасности является:

a) обеспечение многоуровневого режима выполнения команд

b) мандатное управление

c) Матричная структура

35. Под организацией доступа к ресурсам понимается

a) весь комплекс мер, который выполняется в процессе эксплуатации КС для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию.

b) хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие.

c) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние

36. При эксплуатации механизмов аутентификации основными задачами являются:

a) генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС.

b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;

c) реализация механизма виртуальной памяти с разделением адресных пространств;

37. В чем заключается правило разграничения доступа

a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.

c) лицо допускается к работе с документом только в том случае, если уровень допуска

субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа,не содержатся все категории, определенные для данного документа.

38. Правильность функционирования ядра безопасности доказывается путем:

a) полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты.

b) использования дополнительных программных или аппаратно- программных средств.

c) использования строго определенного множества программ.

39. Матричное управление доступом предполагает использование:

a) матриц доступа

b) аппаратно-программных механизмов

c) субъекта допуска

40. Основной проблемой создания высокоэффективной защиты от НСД является

a) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние.

b) использования дополнительных программных или аппаратно- программных средств.

c) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

Перечень тестовых заданий для оценки уровня сформированности компетенции ПК-1 на этапе «Знания»

Тест №2

1. Аппаратно-программмные средства криптографической защиты информации выполняют функции:

a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.

b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС.

c) проверяют на отсутствие закладок приборов, устройств.

2. Использование аппаратных средств снимает проблему:

a) обеспечения целостности системы.

b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

c) использования строго определенного множества программ.

3. Криптографические функции плат КРИПТОН образующие ядро системы безопасности

реализуются

a) аппаратно

b) программно

c) аппаратно и программно

4. Безопасность в частично контролируемым компьютерных системамах может быть обеспечена

a) изоляцией от злоумышленника ненадежной компьютерной среды, отдельного ее компонента или отдельного процесса с помощью полностью контролируемых средств.

b) схемой идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации.

c) внешней аутентификацией объекта, не принадлежащего системе;

5. Платы серии КРИПТОН, обеспечивают защиту:

a) ключей шифрования и электронной цифровой подписи (ЭЦП), так и неизменность их алгоритмов.

b) аппаратно-программных механизмов

c) реализации механизма виртуальной памяти с разделением адресных пространств;

6. К основным компонентам сети относятся:

a) центры коммутации пакетов, маршрутизаторы, шлюзы и сетевые экраны;

b) субъекты доступа

c) платы серии КРИПТОН

7. В качестве ключевых носителей устройств криптографической защиты данных серии КРИПТОН используются:

a) дискеты, смарт-карты и Touch-Memory.

b) смарт-карты, Touch-Memory

c) дискеты, смарт-карты

8. Средства серии КРИПТОН независимо от операционной среды обеспечивают:

a) защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП.

b) криптомаршрутизацию

c) функции шифрования и электронной цифровой подписи.

9. В системе Secret Disk используется:

a) смешанная программно-аппаратная схема защиты с возможностью выбора

b) реализация механизма виртуальной памяти с разделением адресных пространств;

c) механизм RUN-файлов позволяет в процессе работы запускать любые программы с предварительной проверкой их целостности.

10. В чем заключается особенность системы Secret Disk:

a) для доступа к защищенной информации необходим не только вводимый пользователем пароль, но и электронный идентификатор.

b) для доступа к защищенной информации необходим только вводимый пользователем пароль.

c) для доступа к защищенной информации необходим только электронный идентификатор.

11. Мастер-ключ в Устройствах криптографической защиты данных серии КРИПТОН загружается:

a) до загрузки операционной системы

b) после загрузки операционной системы

c) вообще не загружается

12. Криптографических функций в устройствах криптографической защиты данных серии КРИПТОН выполняются:

a) внутри платы

b) в операционной системе

c) в блоке загрузки операционной системы

13. Под защитой информации понимается

a) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным.

b) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по реализации механизма виртуальной памяти с разделением адресных пространств;

c) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по разграничению прав пользователей и обслуживающего персонала.

14. Возможные каналы утечки информации по классификации разделяют:

a) человек, аппаратура, программа

b) человек, линия связи

c) коммутационное оборудование, человек

15. К группе каналов утечки информации в которой основным средством является человек, относятся следующие утечки:

a) расшифровка программой зашифрованной информации;

b) несанкционированный доступ программы к информации;

c) копирование программой информации с носителей.

16. К группе каналов утечки информации в которой основным средством является аппаратура, относятся следующие утечки:

a) подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;

b) хищение носителей информации (магнитных дисков, дискет, лент)

c) копирование программой информации с носителей

17. К группе каналов утечки информации в которой основным средством является программа, относятся следующие утечки:

a) несанкционированный доступ программы к информации

b) хищение носителей информации (магнитных дисков, дискет, лент)

c) использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

18. К средствам активной защиты относятся:

a) искаженные программы (программы вирусы, искажение функций)

b) заказное проектирование

c) специальная аппаратура

19. К средствам пассивной защиты относятся:

a) частотный анализ

b) авторская эстетика

c) аппаратура защиты (ПЗУ, преобразователи)

20. К средствам собственной защиты относятся:

a) машинный код

b) сигнатура

c) корреляционный анализ

21. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:

a) организационные и технические

b) технические и коммутационные

c) организационные и объективные

22. Технические мероприятия направлены :

a) на недопущение выхода информативного сигнала за пределы контролируемой территории с помощью сертифицированных технических средств защиты.

b) на использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

c) на защиту ключей шифрования и электронной цифровой подписи (ЭЦП) и неизменность алгоритма шифрования и ЭЦП.

23. Организационными мероприятиями предусматривается

a) исключение нахождения в местах наличия информативного сигнала злоумышленника и контроль за его действиями и передвижением

b) исключение значительной части загрузочных модулей из сферы их досягаемости.

c) исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным

24. Активные способы защиты информации при ее утечке через сеть электропитания направленные на:

a) создание маскирующего шума

b) перехвата информации

c) минимизацию паразитных связей внутри ПЭВМ

25. Пассивные способы защиты информации при ее утечке через сеть электропитания направленные на

a) минимизацию паразитных связей внутри ПЭВМ

b) создание маскирующего шума

c) перехвата информации

26. Для минимизации паразитных связей внутри ПЭВМ используются

a) радиоэкранирующие и радиопоглощающие материалы

b) двигатели-генераторы

c) разомкнутые линии

27. Под системой защиты от несанкционированного использования и копирования понимается

a) комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.

b) комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.

c) комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

28. Под надежностью системы защиты от несанкционированного копирования понимается:

a) способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты.

b) способность систем с открытыми ключами генерировать цифровые подписи, обеспечивающие различные функции защиты, компенсирует избыточность требуемых вычислений.

c) способность к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно- вычислительных сетях и отдельных ЭВМ

29. Методы, затрудняющие считывание скопированной информации основываются на

a) придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС

b) разграничении прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

c) использования дополнительных программных или аппаратно- программных средств.

30. Мероприятия по инженерно-технической защите информации от утечки по электромагнитному каналу подразделяются на:

a) организационные и технические

b) технические и коммутационные

c) организационные и объективные

31. Любая криптографическая система основана на использовании:

a) криптографических ключей

b) разомкнутых линии

c) односторонних функций

32. В симметричной криптосистеме отправитель и получатель сообщения используют

a) один и тот же секретный ключ

b) разные секретных ключи

c) вообще не используют секретных ключей

33. Асимметричная криптосистема предполагает использование

a) двух ключей открытого и личного (секретного)

b) системы разграничения доступа

c) переносных носителей для хранения секретной информации

34. Под ключевой информацией понимают:

a) совокупность всех действующих в АСОИ ключей

b) совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы.

c) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации.

35. Какая из функций не входит в процесс управления ключами?

a) переадресация ключей

b) генерация ключей

c) распределение ключей

36. Модификация ключа - это

a) генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции.

b) генерирование нового ключа из последующего значения ключа с помощью односторонней (однонаправленной) функции.

c) генерирование нового ключа из предыдущего значения ключа с помощью

двусторонней (двунаправленной) функции.

37. Под функцией хранения ключей понимают

a) организацию их безопасного хранения, учета и удаления.

b) организацию их генерации, учета и удаления.

c) организацию их безопасного хранения, учета и сопостовления.

38. Механизм отметки времени позволяет каждому субъекту сети определить:

a) насколько старо пришедшее сообщение, и отвергнуть его, если появится сомнение в его подлинности.

b) были ли внесены изменения в файл.

c) какие информационные потоки в системе являются "легальными", то есть не ведут к утечке информации

39. Модель рукопожатия применяется для:

a) проверки подлинности партнеров

b) для симметричных криптосистем с секретными ключами

c) для асимметричных криптосистем с открытыми ключами

40. Каким из перечисленных способов не реализуется Распределение ключей между пользователями компьютерной сети:

a) документирование алгоритмов обеспечения защиты информации

b) использованием одного или нескольких центров распределения ключей

c) прямым обменом сеансовыми ключами между пользователями сети

41. Задача распределения ключей сводится к

a) построению протокола распределения ключей

b) взаимному подтверждению подлинности участников сеанса

c) использование минимального числа сообщений при обмене ключами

42. Протокол Kerberos основывается на

a) симметричной криптографии

b) ассиметричной криптографии

c) нескольких центров распределения ключей

43. Первым алгоритмом с открытыми ключами был алгоритм:

a) Диффи-Хеллмана

b) А. Фиата

c) А. Шамира

44. SKIP Протокол управления:

a) криптоключами

b) защищенного канала

c) симметричной криптосистемой

45. В каких режимах может выполняться изучение логики работы программы:

a) статическом

b) динамическом

c) и в статическом и в динамическом

46. Сущность статического режима заключается

a) в изучении исходного текста программы

b) в выполнение трассировки программы

c) в использование самогенерирующих кодов

47. Динамический режим изучения алгоритма программы предполагает

a) выполнение трассировки программы

b) изучении исходного текста программы

c) использование самогенерирующих кодов

48. Какой метод может противодействовать дизассемблированию

a) шифрование

b) хэширование

c) изучение

49. Сущность метода, основанного на использовании самогенерируемых кодов, заключается в том что

a) исполняемые коды программы получаются самой программой в процессе ее выполнения.

b) исполняемые коды программы получаются самой программой после процесса ее выполнения.

c) исполняемые коды программы получаются самой программой до процесса ее выполнения.

50. Трассировка программ обычно осуществляется с помощью:

a) программных продуктов, называемых отладчиками

b) шифрования

c) самогенерируемых кодов

51. Под компьютерным вирусом понимается:

a) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно- вычислительных сетях и отдельных ЭВМ.

b) программа имеющая доступ к файлам системы, и имеющая возможность работать с

процессами системы.

c) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы.

52. Резидентные вирусы это:

a) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

b) вирусы, которые выполняются только в момент запуска зараженной программы.

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

53. Транзитные вирусы это:

a) вирусы, которые выполняются только в момент запуска зараженной программы.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

54. Вирусы-мутанты (MtE-вирусы) это

a) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

b) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

55. Stealth-вирусы это

a) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных:

b) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

56. Загрузочные (бутовые) вирусы это:

a) вирусы, заражающие программы, хранящиеся в системных областях дисков.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

c) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

57. Троянские программы это:

a) программы которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям.

b) программы , содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

c) программы которые после активизации постоянно находятся в оперативной памяти

компьютера и контролируют доступ к его ресурсам;

58. Файловые вирусы это:

a) вирусы, заражающие файлы с программами

b) вирусы, заражающие программы, хранящиеся в системных областях дисков.

вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

Темы рефератов и методические рекомендации по их подготовке

Перечень тем рефератов для оценки уровня сформированности компетенции ОПК-7 на этапе «Умения»

Тема выбирается студентом из числа предложенных или может быть определена самостоятельно по рекомендации руководителя. Реферат должен включать в себя оглавление, введение, основную часть, заключение, биографические справки об упоминаемых в тексте ученых и подробный библиографический список, составленный в соответствии со стандартными требованиями к оформлению литературы, в том числе к ссылкам на электронные ресурсы. Работа должна носить самостоятельный характер, в случае обнаружения откровенного плагиата (дословного цитирования без ссылок) реферат не засчитывается. Сдающий реферат студент должен продемонстрировать умение работать с литературой, отбирать и систематизировать материал, увязывать его с существующими математическими теориями и фактами общей истории.

Во введении обосновывается актуальность выбранной темы, определяются цели и задачи реферата, приводятся характеристика проработанности темы в историко-математической литературе и краткий обзор использованных источников.

В основной части, разбитой на разделы или параграфы, излагаются основные факты, проводится их анализ, формулируются выводы (по разделам). Необходимо охарактеризовать современную ситуацию, связанную с рассматриваемой тематикой.

Заключение содержит итоговые выводы и, возможно, предположения о перспективах проведения дальнейших исследований по данной теме.

Биографические данные можно оформлять сносками или в качестве приложения к работе. Список литературы может быть составлен в алфавитном порядке или в порядке цитирования, в полном соответствии с государственными требованиями к библиографическому описанию. Ссылки в тексте должны быть оформлены также в соответствии со стандартными требованиями (с указанием номера публикации по библиографическому списку и страниц, откуда приводится цитата).

Подготовку реферата рекомендуется начинать с библиографического поиска (см. рекомендации к работе с литературой) и составления библиографического списка, а также подготовки плана работы. Каждый из намеченных пунктов плана должен опираться на различные источники, при этом желательно провести сравнительный анализ как результатов, полученных разными специалистами, так и взглядов на эту темы различных

специалистов в области истории науки. Необходимо выявить предпосылки и отметить последствия анализируемых теорий, отметить философские и методологические особенности. Текст реферата должен быть связным, недопустимы повторения, фрагментарный пересказ разрозненных сведений и фактов.

Оформление реферата должно быть аккуратным, при использовании редакторов LaTeX или MS WORD рекомендуется шрифт 12 пт. Ориентировочный объем – не менее 15 страниц, при этом не допускается его искусственное увеличение за счет междустрочных интервалов. Титульный лист готовится в соответствии с требованиями, предъявляемыми к оформлению титульных листов курсовых работ. Ниже представлен примерный перечень тем рефератов по данной дисциплине:

1. Применение привязки к биту и электронной жеребьевки для совместной выработки ключей.
2. Применение схем разделения секрета для безопасной отправки сообщений и депонирования ключей.
3. Идентификация и аутентификация в ОС Windows и Unix.
4. Разновидности цифровых подписей в электронном документообороте.
5. Схемы электронных денег WebMoney и payCash.
6. Схемы электронных денег eCash и PayCash.
7. Криптографические средства в электронном документообороте федеральных и местных органов управления в РФ.
8. Системы управления криптографическими ключами в федеральных и местных органах управления в РФ.
9. Обзор криптографических протоколов, использующих цифровую подпись.
10. Практика электронного голосования на примере ЕС.
11. Применение протокола «Покер по телефону» к раздаче электронных бланков.
12. Идентификация на основе биометрических данных.

Перечень практических и лабораторных заданий для оценки уровня сформированности компетенции ОПК-7 на этапе «Умения» и ПК-1 на этапе «Владения»:

Вопросы к лабораторной работе № 1
«Понятие и виды защищаемой информации»

Предмет и задачи программно-аппаратной защиты информации

Задание 1. Перечень вопросов по теме для устного обсуждения:

1. Предмет и задачи программно-аппаратной защиты информации
2. Уязвимость компьютерных систем
3. Политика безопасности в компьютерных системах. Оценка защищенности.
4. Механизмы защиты

1) Какие параметры области пересылаемых данных должны задаваться?
2) Какие операции передачи данных выполняются симулятором?
3) Какими командами осуществляется пересылка данных?

4) Какие регистры используются в качестве указателей адреса?
5) Что такое регистр порта и какие у него функции?
6) Какие пункты имеет основное меню симулятора?
7) В каком формате вводятся числа?
8) Какие клавиши используются для редактирования команд?
9) Каким образом прекращают автоматическое выполнение программы?

Задание 2. Лабораторные работы

1. Программные средства гарантированного уничтожения информации

Вопросы к лабораторной работе № 2
«Информационная безопасность и информационное противоборство».

Задание 1. Перечень вопросов по теме для устного обсуждения:

1. Защита информации в кс от несанкционированного доступа
2. Система разграничения доступа к информации в кс
3. Концепция построения систем разграничения доступа
4. Организация доступа к ресурсам кс
5. Обеспечение целостности и доступности информации в КС

1) Каким образом проводится инициализация портов контроллера?
2) Какие регистры используются в качестве управляющих?
3) Как наложить маску на используемый регистр?
4) Какие команды используются формирования в регистре вводимых слов?

Задание 2. Лабораторные работы

1. Система контроля разграничения доступа «РЕВИЗОР XP»

Вопросы к лабораторной работе № 3
«Методы и средства обеспечения информационной безопасности».

Задание 1. Перечень вопросов по теме для устного обсуждения:

1. Основные элементы и средства защиты от несанкционированного доступа
2. Системы защиты информации от несанкционированного доступа
3. Комплекс криптон-замок для ограничения доступа к компьютеру
4. Система защиты данных CRYPTON SIGMA

1) Какие разновидности переходов можно выделить в группе команд ветвления?
2) Какой вид имеет регистр состояния микроконтроллера SREG?
3) Назначения битов регистра SREG.
4) Представить двоичную константу, использовавшуюся в программе, в десятичном и стнадцатеричном видах.
5) Где располагаются биты, отвечающие за разрешение прерываний?
6) Какую команду выполнял микроконтроллер большую часть времени

ожиданияпрерывания?

7) Как выбирается источник тактового сигнала таймера? Зачем делится частотавнутреннего источника?

Задание 2. Лабораторные работы

1. Применение криптографических средств защиты информации

Вопросы к лабораторной работе № 4
«Механизмы защиты информации».

Задание 1. Перечень вопросов по теме для устного обсуждения:

1. Методы, затрудняющие считывание скопированной информации

2. Методы, препятствующие использованию скопированной информации

3. Основные функции средств защиты от копирования

4. Основные методы защиты от копирования

5. Методы противодействия динамическим способам снятия защиты программ от копирования

1) Как проводят поиск соединительного пути?
2) Что такое первичный код.
3) Какие действия выполняет для уменьшения вероятности ошибки?
1) Какие особенности организации диспетчеризации?

Зачем делится частота внутреннего
источника?

Задание 2. Лабораторные работы

1. Средства контроля целостности программ «ФИКС»

Темы проектов и методические рекомендации по их подготовке

Перечень тем проектов для оценки уровня сформированности компетенции ПК-1 на этапе «Владения»

В рамках проекта необходимо проанализировать структуры предприятия, угрозы информационной безопасности для выбранного предприятия и выбрать наиболее актуальные, предложить комплекс административных и программно-аппаратных мер защиты данных.

Вариант 1.

Оптовая фирма по продаже продуктов питания в связи с расширением своей деятельности реорганизует свою структуру. Имеется бухгалтерия и отдел продаж. Планируется создание коммерческого отдела, для решения вопросов стратегического планирования. Существующие отделы снабжены компьютерами и несвязанными сегментами локальной сети.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения, с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных.

Вариант 2.

Создается инвестиционная компания.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения, с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных.

Вариант 3.

Крупная торговая фирма производит модернизацию инфраструктуры и существующей информационной системы. Фирма имеет локальную сеть, объединяющую все подразделения. Существует подключение к сети Internet. Основное внимание фирма уделяет развитию сети филиалов и в связи с этим необходимо организовать взаимодействие филиалов и головной компании.

Требуется:

1. Разработать структуру сети, объединяющей все филиалы, с учетом требований информационной безопасности. Разработать типовую схему локальной сети филиала.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных.

Вариант 4.

Создается коммерческий банк.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения, с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных.

Вариант 5.

Сеть розничных магазинов планирует организовать Internet-магазин и объединить локальные сети в одну общую сеть.

Требуется:

1. Разработать структуру сети, объединяющей все магазины, с учетом требований информационной безопасности.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных для сети и электронного магазина.

Вариант 6.

На производственном предприятии принято решение о внедрении информационных технологий и создании локальной сети.

Требуется:

1. Разработать структуру общей локальной сети, объединяющей все подразделения,

с учетом требований информационной безопасности. Предусмотреть возможность подключения к сети Internet.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных.

Вариант 7.

Университет модернизирует локальную сеть и внедряет дистанционное обучение. Требуется:

1. Разработать структуру локальной сети, с учетом требований информационной безопасности. Предусмотреть выход в Internet.

2. Разработать перечень административных мероприятий по защите данных.

3. Осуществить выбор программных и аппаратных средств защиты данных для сети и отделения дистанционного образования.

Критерии оценки (в баллах): В каждой работе студенту предлагается выполнить проект.

Проектная работа считается зачтенной, если студент выполнил задание, продемонстрировал владение методикой, грамотно оформил описание проекта. Ответил на все вопросы, хотя при ответе на вопросы мог допускать ошибки и неточности. В противном случае студенту необходимо заново подготовится, внести исправления проектную работу снова.

За отчет по ппроекту студент может получить максимально 10 баллов. Оценивается весь ответ на все вопросы комплексно, а не на отдельный из них.

- 9-10 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы, продемонстрировал знание и понимание темы проекта.

-6-8 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий и методов. При ответе на дополнительные вопросы допущены небольшие неточности. Хорошо ориентируется в тематике вопроса, однако имеются неточности в описании проекта.

-3-5 балла выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Имеются принципиальные ошибки в логике изложения и оформления проекта.

-0-2 - балла выставляется студенту, если студент плохо ориентируется в вопросе, допускает грубые ошибки.

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Для каждого модуля разработаны задания для лабораторных работ, а также

проектные задания, которые выполняются студентом самостоятельно и в совокупности определяют уровень учебных достижений студента.

№ п/п	Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
				Минимальный	Максимальный
Модуль 1					
Текущий контроль, в том числе				**0**	**20**
1	Лабораторные работы	5	2	0	10
2	Реферат	10	1	0	10
Рубежный контроль, в том числе				**0**	**15**
1.	Тестирование	15	1	0	15
			Итого	**0**	**35**
Модуль 2					
Текущий контроль, в том числе					**20**
1	Лабораторные работы	5	2		10
2	Проект	10	1	0	10
Рубежный контроль, в том числе				**0**	**15**
1.	Тестирование	15	1	0	15
			Итого	**0**	**35**
Поощрительные баллы					**10**
1.	Выступление на семинаре кафедры	5	1	0	5
2.	Публикация статей	5	1	0	5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)					
1.	Посещение лекционных занятий			0	-6
2.	Посещение практических и лабораторных занятий			0	-10
Итоговый контроль					
	Экзамен	10	3	**0**	**30**
			Итого	**0**	**110**

ПЕРЕЧЕНЬ ЭКЗАМЕНАЦИОННЫХ ВОПРОСОВ

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Интересы личности общества и государства в информационной сфере.
4. Виды угроз информационной безопасности Российской Федерации.
5. Методы обеспечения информационной безопасности Российской Федерации
6. Источники понятий в области информационной безопасности.

7. Основные понятия информационной безопасности.
8. Общеметодологические принципы теории информационной безопасности.
9. Понятие и сущность защищаемой информации.
10. Права и обязанности обладателя информации.
11. Виды защищаемой информации.
12. Перечень сведений конфиденциального характера.
13. Понятие интеллектуальной собственности и особенности ее защиты.
14. Понятие угрозы информационной безопасности.
15. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.
16. Классификация и виды угроз информационной безопасности.
17. Внутренние и внешние источники угроз информационной безопасности.
18. Угрозы утечки информации и угрозы несанкционированного доступа.
19. Основные элементы канала реализации угрозы безопасности информации.
20. Субъекты и цели информационного противоборства.
21. Составные части и методы информационного противоборства.
22. Методы нарушения конфиденциальности, целостности и доступности информации.
23. Информационная безопасность критически важных объектов.
24. Основные способы защиты информации.
25. Понятие и классификация средств защиты информации.
26. Характеристика средств защиты информации.
27. Уровни информационной безопасности и их характеристика.
28. Сервисы безопасности программно-технического уровня.
29. Идентификация и аутентификация как сервисы безопасности.
30. Управление доступом и его виды
31. Авторизация как сервис безопасности.
32. Протоколирование и аудит как сервисы безопасности.
33. Криптографические сервисы безопасности.
34. Экранирование как сервис безопасности
35. Анализ защищенности как сервис безопасности.
36. Анализ защищенности как сервис безопасности.
37. Управление как сервис безопасности.
38. Назначение формальных моделей безопасности. Политика безопасности.
39. Модели, стратегии и системы обеспечения информационной безопасности.
40. Общие критерии безопасности информационных технологий.
41. Стандарты по управлению информационной безопасностью ISO/IEC 27000.
42. Технические каналы утечки информации.
43. Электромагнитное воздействие и эффекты его воздействия.
44. Защита систем мобильной связи от внешнего электромагнитноговоздействия.

Примерная тематика курсовых работ

1. Организация безопасного удаленного доступа к ЛВС предприятия.
2. Построение защищенной виртуальной сети на базе специализированного программного обеспечения на предприятии.
3. Автоматизация учета конфиденциальных документов на предприятии.
4. Организация процессов мониторинга конфиденциального документооборота на

предприятии.
5. Автоматизация процесса проверок наличия конфиденциальных документов на предприятии.
6. Разработка комплексной системы защиты информации (КСЗИ) предприятия.
7. Организация системы планирования и контроля функционирования КСЗИ на предприятии.
8. Разработка основных направлений совершенствования КСЗИ предприятия.
9. Организация подсистемы, обеспечивающей управление КСЗИ в условиях чрезвычайной ситуации на предприятии.
10. Разработка методологии проектирования КСЗИ.
11 Разработка моделей процессов защиты информации при проектировании КСЗИ.
12. Анализ методов оценки качества функционирования КСЗИ.
13. Разработка структурно-функциональной модели управления КСЗИ предприятия.
14. Разработка проекта программно-аппаратной защиты информации предприятия.
15. Разработка методов расчета экономической эффективности программно–аппаратной защиты информации предприятия.
16. Криптографические средства защиты информации на основе дискретных носителей.
17. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.
18. Разработка требований по организационной защите конфиденциальной информации, передаваемой и получаемой по сети Интернет.
19. Обоснование и разработка мер организационной защиты конфиденциальной информации при взаимодействии сотрудников предприятия со сторонними организациями.
20. Разработка методов и форм работы с персоналом предприятия, допущенным к конфиденциальной информации.
21. Обоснование и разработка требований и процедур по защите конфиденциальной информации, обрабатываемой средствами вычислительной техники и информационными системами.
22. Организация порядка установления внутри объектного спецрежима на объекте информатизации.
23. Использование институтов правовой защиты интеллектуальной собственности для защиты информации.
24. Организация защиты персональных данных на основе использования правовых мер.
25. Разработка комплексной системы защиты информации на предприятии, осуществляющем изготовление роботов, оснащенных программным обеспечением, представляющем коммерческую тайну.
26. Разработка и анализ эффективности внедрения мер по защите информации торговых автоматов, подключенных к глобальной сети и управляемых удаленно.
27. Разработка организационно-технических мероприятий по обеспечению безопасности функционирующей информационно – вычислительной системы при вводе в эксплуатацию (внедрении) ее
дополнительных очередей (подсистем) сторонними организациями.
28. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада.
29. Разработка систем видеонаблюдения и сигнализации для обеспечения защиты информации на предприятии.
30. Организация автоматизированного пропускного режима на крупном предприятии (на примере).
31. Разработка проекта организационных мер по защите аудиоинформации в локальной сети.

32. Разработка комплексной системы защиты информации в кабинете директора.
33. Обоснование и разработка требований и процедур по защите информации ограниченного доступа на предприятии.
34. Разработка системы защиты информации конфиденциального характера от утечки по техническим каналам.
35. Разработка организационного порядка установления внутри объектного режима для торговой фирмы.
36. Автоматизация обеспечения информационной безопасности группы компаний на базе ОС Unix/Linux.
37. Организация системы контроля доступа и защиты информации на предприятии.
38. Разработка комплексной системы защиты информации в название отдела предприятия.
39. Защита речевой информации в каналах связи коммерческих организаций.
40. Разработка типового проекта комплексной системы защиты информации на предприятии, осуществляющем распределенную продажу продукции с единого склада.
41. Разработка мероприятий организационного характера по обеспечению комплексной защиты информации.
42. Разработка систем видеонаблюдения и контроля доступа к объектам информатизации.
43. Совершенствование системы информационной безопасности в помещениях название организации

Методические указания по выполнению курсовых работ

Целью выполнения курсовых работ является формирование навыков самостоятельного творческого решения профессиональных задач, практическое применение полученных за время обучения студентом знаний путём самостоятельного выполнения работы на заданную тему.

Задачами выполнения курсовых работ являются:

– систематизация, закрепление, углубление и расширение приобретенных студентом знаний, умений, навыков по учебным дисциплинам профессиональной подготовки;

– овладение методами научных исследований;

– формирование навыков решения творческих задач в ходе научного исследования, художественного творчества или проектирования по определенной теме;

– подготовка к написанию ВКР (материалы курсовых работ могут входить в ВКР).

При выполнении курсовых работ студент должен:

– сформулировать цель и задачи исследования, при необходимости выдвинуть научную (рабочую) гипотезу;

– собрать, систематизировать и обобщить имеющуюся информацию по теме;

– изучить и критически проанализировать полученные материалы;

– самостоятельно решить поставленные творческие задачи;

– логически обосновать и сформулировать выводы, предложения и рекомендации.

Курсовая работа имеет следующую структуру:

– титульный лист;

– содержание;

– введение;

– основная часть работы;

– заключение;

– список использованных источников и литературы;

– приложения (при необходимости).

Структура текста курсовой работы устанавливается кафедрой исходя из характера работы и учебной дисциплины, по которой она выполняется.

Изложение материала в курсовой работе должно быть последовательным и логичным. Все разделы работы должны быть связаны между собой. Особое внимание следует обращать на логические переходы от одной главы к другой, от параграфа к параграфу, а внутри параграфа – от вопроса к вопросу.

Текст работы должен демонстрировать:

– знакомство автора с основной литературой по рассматриваемым вопросам;

– умение выделить проблему и определить методы ее решения;

– умение последовательно изложить существо рассматриваемых вопросов;

– владение соответствующим понятийным и терминологическим аппаратом;

– приемлемый уровень языковой грамотности, включая владение функциональным стилем научного изложения.

Общий объем курсовой работы составляет как правило 15-30 страниц.

Текст должен быть отформатирован. Рекомендуемый шрифт Times New Roman, размер – 14, межстрочный интервал – 1,5 пт.

Страницы курсовой работы должны быть пронумерованы сквозной нумерацией.

Оглавление представляет собой составленный в последовательном порядке список всех заголовков разделов работы с указанием страниц, на которых соответствующий раздел начинается.

Введение. Во введении дается обоснование выбора темы, характеризуется ее актуальность и степень научной разработки, общая оценка исследуемой проблемы, формируются цели и задачи исследования, перечисляются подходы и методы анализа.

Основная часть. Основная часть курсовой работы должна быть представлена главами или разделами (не более трех), которые могут быть разбиты на параграфы.

Все части курсовой работы должны быть изложены в строгой логической последовательности и взаимосвязи. Каждая глава, раздел должны иметь определенное

целевое назначение и является базой для последующего изложения. В конце каждой главы или раздела должны быть сформулированы краткие выводы, вытекающие их текста.

Заключение. Заключение содержит в сжатой форме, как теоретические выводы, так и практические предложения, к которым пришел студент в результате выполнения курсовой работы. Они должны быть краткими, конкретными, вытекать из существа работы и отражать предмет защиты.

Список использованных источников и литературы. Список должен содержать перечень источников информации, используемых при выполнении курсовой работы, и их библиографическое описание. Источники следует располагать в алфавитном порядке.

Приложения. Приложения должны включать вспомогательный или дополнительный материал, который загромождает текст основной части работы, но необходим для полноты ее восприятия и оценки практической значимости (копии документов, таблицы вспомогательных и цифровых данных, иллюстрации и т.д.).

Сноски и список использованных источников и литературы рекомендуется оформлять в соответствии с ГОСТ Р 7.0.5.-2008.

Критерии оценки курсовой 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.

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-

100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = k × Максимальный балл,

где k = 0,2 при уровне освоения «неудовлетворительно», k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов УУНиТ:

На экзамене выставляется оценка:

• отлично - при накоплении от 80 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

• хорошо - при накоплении от 60 до 79 рейтинговых баллов,

• удовлетворительно - при накоплении от 45 до 59 рейтинговых баллов,

• неудовлетворительно - при накоплении менее 45 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.