Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
Балтийская государственная академия рыбопромыслового флота
(ФГБОУ ВО «КГТУ»)
БГАРФ

УТВЕРЖДАЮ
И.о декана РТФ
_____/Баженов В.А./
«27» июня 2018 г.

Фонд оценочных средств для аттестации по дисциплине

(приложение к рабочей программе дисциплины)

Теоретические основы компьютерной безопасности

вариативной части образовательной программы по специальности:

10.05.03 «Информационная безопасность автоматизированных систем ".

(код и наименование специальности)

Специализация программы:

"Обеспечение информационной безопасности распределенных информационных систем".

(наименование специализации)

Факультет радиотехнический (РТФ)

(наименование)

Кафедра информационной безопасности (ИБ)

(наименование)

Калининград 2018

В результате освоения дисциплины «Теоретические основы компьютерной безопасности» обучающийся должен получить следующие компетенции:

Таблица 1 - Компетенции и уровни их освоения обучающимся

ПК-6**:** способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	
Знать:	
Уровень 1	способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации;
Уровень 2	способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности
Уровень 3	способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий;
Уметь:	
Уровень 1	определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий;

Уровень 2	определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы;
Уровень 3	определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации.
Владеть:	
Уровень 1	методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем;
Уровень 2	методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей;
Уровень 3	методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей; средствами защиты информации в процессе хранения и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков
ПК-11**:** способностью разрабатывать политику информационной безопасности автоматизированной системы	
Знать:	
Уровень 1	политику информационной безопасности автоматизированной системы
Уровень 2	политику информационной безопасности автоматизированной системы
Уровень 3	политику информационной безопасности автоматизированной системы
Уметь:	
Уровень 1	разрабатывать политику информационной безопасности автоматизированной системы
Уровень 2	разрабатывать политику информационной безопасности автоматизированной системы
Уровень 3	разрабатывать политику информационной безопасности автоматизированной системы
Владеть:	
Уровень 1	способностью разрабатывать политику информационной безопасности автоматизированной системы

Уровень 2	способностью разрабатывать политику информационной безопасности автоматизированной системы
Уровень 3	способностью разрабатывать политику информационной безопасности автоматизированной системы
ПК-13**:** способностью участвовать в проектировании средств защиты информации	
Знать:	
Уровень 1	методы проектирования средств защиты информации
Уровень 2	методы, средства проектирования средств защиты информации
Уровень 3	методы, порядок, средства проектирования средств защиты информации
Уметь:	
Уровень 1	разрабатывать модели информационно-технологических ресурсов
Уровень 2	разрабатывать модели информационно-технологических ресурсов, проектировать средства защиты информации
Уровень 3	разрабатывать и исследовать модели информационно-технологических ресурсов, проектировать средства защиты информации
Владеть:	
Уровень 1	методами исследования информационно-технологических ресурсов
Уровень 2	методами разработки информационно-технологических ресурсов
Уровень 3	методами исследования информационно-технологических ресурсов, методами проектирования средств защиты информации

Таблица 2 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	- методологические и технологические основы комплексного обеспечения безопасности АС, - угрозы и методы нарушения безопасности АС, - формальные модели, лежащие в основе систем защиты АС, - стандарты по оценке защищенности АС и их теоретические основы, - методы и средства реализации защищенных АС, - методы и средства верификации и анализа надежности защищенных АС
уметь	- проводить анализ АС с точки зрения обеспечения компьютерной безопасности, - разрабатывать модели и политику безопасности, используя известные подходы, методы, средства и их теоретические основы, - применять стандарты по оценке защищенности АС при анализе и проектировании систем защиты информации в АС, - реализовывать системы защиты информации в АС в соответствии со стандартами по оценке защищенности АС
владеть	- навыками работы с АС распределенных вычислений и обработки информации; - навыками работы с документацией АС, - навыками использования критериев оценки защищенности АС, - навыками построения формальных моделей систем защиты ин-

	формации АС

1. Перечень оценочных средств для проведения поэтапной аттестации обучающихся

В перечень оценочных средств **по данной дисциплине** входят:
- опрос на занятиях,
- выполнение лабораторных работ, практических заданий,
-тестовые задания по дисциплине для текущего контроля
- курсовой проект,
- экзамен.

Таблица 3 - Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код компетенции	Этапы формирования компетенций – Разделы/подразделы теоретического обучения (по табл.1)													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14
ПК-6	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-11	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-13	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Знак «+» означает выполненный этап

1.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования

Таблица 4 - Шкала формирования компетенций обучающимися

Код компетенции по ФГОС	Форма оценивания		
	Текущий контроль	Итоговая аттестация	
	Этапы: 1-14	Этапы: 1 - 13	Этап: 14
	Опрос, тестовые задания	Курсовой проект	Экзамен (вопросы)
ПК-6	+	+	+
ПК-11	+	+	+
ПК-13	+	+	+

2. Критерии оценивания уровня освоения обучающимися компетенций

2.1. Текущий контроль

Фонд оценочных средств для проведения текущего контроля успеваемости включает в себя:
- материалы для проведения текущего контроля успеваемости – варианты тестовых заданий;
- перечень компетенций и их элементов, проверяемых на каждом мероприятии текущего контроля успеваемости;
- систему и критерии оценивания по каждому виду текущего контроля успеваемости
- описание процедуры оценивания.

2.1.1. Текущий контроль **в форме опроса**.

Текущий контроль осуществляется путем опроса по материалу, пройденному на предшествующих лекциях.

Оценивается:
- полнота усвоения пройденного материала,

- качество изложения пройденного материала (устно и письменно)

Таблица 5 - Шкала оценок уровня усвоения материала обучающимся

Неудовлетворительный	Пороговый	Углублённый	Продвинутый
«2» (неудовлетв.)	«3» (удовлетвор.)	«4» (хорошо)	«5» (отлично)
Не может ответить на вопросы по пройденному материалу устно или изобразить на доске	Отвечает сбивчиво, путается в определениях и обозначениях, нуждается в помощи других обучающихся	Допускает незначительные ошибки при изложении пройденного материала, не полностью представляет связи между разделами изучаемой дисциплины	Четко отвечает на вопросы, может точно изобразить графическую часть пройденного материала, увязывает последовательность изученных разделов дисциплины

Таблица 6 - Шкала оценок уровня освоения дисциплины по экзамену.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи.	Усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий.	Твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий.	Глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его изложил, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок.

Таблица 7 - Шкала оценок уровня освоения дисциплины по тесту.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Менее 50% правильных ответов.	50-70% правильных ответов.	71-90% правильных ответов.	91-100% правильных ответов.

Таблица 8 - Шкала оценок курсового проекта

Оценка			
Неудовлетворитель-	Пороговый	Углубленный	Продвинутый

ный			
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Работа носит реферативный характер, студент допускает существенные ошибки при защите, с большими затруднениями отвечает на вопросы, оформление работы не соответствует правилам.	Работа носит реферативный характер, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении при защите, оформление работы имеет незначительные отклонения от правил.	В работе углублены теоретические и практические знания, материал излагается грамотно и по существу, не допускается существенных неточностей в ответе на вопрос, оформление работы соответствует правилам.	В процессе выполнения работы приобретены навыки самостоятельного планирования и выполнения научно-исследовательской работы; получен опыт сбора и обработки исходного материала, анализа научно-технической литературы, материал излагается грамотно оформление работы соответствует правилам.

4. Критерии оценивания для проведения итоговой аттестации
Итоговая аттестация обучающихся проводится **в форме экзамена.**
Критерии оценивания:
- уровень усвоения материала, предусмотренного программой
- умение выполнять задания, предусмотренные программой
- уровень знакомства с дополнительной литературой
- уровень раскрытия причинно-следственных связей
- уровень раскрытия междисциплинарных связей
- стиль поведения (культура речи, манера общения, убежденность, готовность к дискуссии)
- качество ответа (полнота, правильность, аргументированность, его общая композиция, логичность)

4.1 Типовые вопросы к экзамену:

1. Методы реализации угроз нарушения конфиденциальности, целостности, отказа доступа, раскрытия параметров системы и методы защиты
2. Основные принципы обеспечения информационной безопасности в автоматизированных системах
3. Структура понятия компьютерная безопасность и основные направления ее обеспечения
4. Понятие защищенности (безопасности) компьютерной информации.
5. Конфиденциальность, целостность и доступность информации.
6. Понятие угроз безопасности компьютерной информации и их классификация
7. Таксонометрия угроз безопасности и изъянов (брешей) систем защиты. ГОСТ Р 51275-99.
8. Человеческий фактор и модель нарушителя безопасности информации
9. Субъектно-объектная модель компьютерной системы. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.
10. Монитор безопасности КС и гарантирование выполнение политики безопасности.
11. Изолированная программная среда.
12. Дискреционные модели безопасности компьютерных систем. Пятимерное пространство Хартсона
13. Модели безопасности на основе матрицы доступа. Способы организации матрицы доступа и управления доступом в компьютерных системах
14. Дискреционные модели распространения прав доступа.
15. Модель и теоремы безопасности Харрисона-Руззо-Ульмана.
16. Модель типизованной матрицы доступа.

17. Модель TAKE-GRANT.
18. Расширенная модель TAKE-GRANT.
19. Основы политики мандатного доступа. Решетка безопасности.
20. Модель Белла-ЛаПадулы и основная теорема безопасности
21. Основные расширения модели Белла-ЛаПадулы.
22. Общая характеристика политики тематического разграничения доступа.
23. Решетки в моделях тематического разграничения доступа.
24. Решетка мультирубрик на иерархических рубрикаторах.
25. Скрытые каналы утечки информации и теоретико-информационные модели безопасности.
26. Технологии "представлений" и "разрешенных процедур".
27. Модели ролевого доступа. Иерархические системы ролей.
28. Принципы наделения ролей полномочиями.
29. Политика и зональная модель безопасности в распределенных КС.
30. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона.
31. Модели обеспечения целостности. Мандатная модель Кена Биба.
32. Объединение мандатных моделей Белла-ЛаПадулы и Кена Биба.
33. Обеспечение целостности данных мониторами транзакций в клиент-серверных системах.
34. Методы, критерии и шкалы оценки эмпирических объектов.
35. Системы многомерного шкалирования защищенности компьютерных систем.
36. Теоретико-графовые модели комплексной оценки защищенности КС.
37. Технико-экономическое обоснование систем обеспечения безопасности.
38. Теоретико-графовые модели комплексной оценки защищенности КС.
39. Тактико-техническое обоснование систем обеспечения безопасности.
40. Теоретико-графовая модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам.
41. Количественные параметры систем индивидуально-группового доступа.
42. Руководящие документы Государственной технической комиссии России
43. Оранжевая книга

4.2 Комплект типовых тестовых заданий

1.	Модель Харрисона-Руззо-Ульмана относится к классу: a) мандатные модели b) дискреционные модели c) ролевые модели
2.	Модель Белла-ЛаПадулы относится к классу: a) мандатные модели b) дискреционные модели c) ролевые модели
3.	Задача проверки безопасности для классической модели Харрисона-Рузо-Ульмана: a) алгоритмически неразрешима b) алгоритмически разрешима c) разрешима только для монооперационных систем d) неразрешима ни для каких систем
4.	Анализ информационных потоков возможен a) в классической модели Take-Grant b) в расширенной модели Take-Grant c) в модели Харрисона-Руззо-Ульмана д) в модели систем военных сообщений
5.	Построение де-факто замыкания позволяет: a) выявить возможные информационные потоки в системе b) проверить истинность предиката возможен доступ c) проверить истинность предиката возможна утечка d) предотвратить утечку прав доступа

6.	Что такое кооперация субъектов? a) возможность сговора инсайдеров b) дружба между сотрудниками c) передача прав доступа при возможности d) непередача прав доступа при возможности
7.	Какая из перечисленных моделей не относится к моделям информационных потоков: a) программная b) вероятностная c) автоматная d) изолированной программной среды
8.	Какая из перечисленных моделей не относится к моделям информационных потоков: e) программная f) вероятностная g) автоматная h) изолированной программной среды
9.	Какие из перечисленных моделей относятся к классу дискреционных: a) Харрисона-Руззо-Ульмана b) Белла-ЛаПадулы c) Take-Grant d) модель систем военных сообщений e) ролевая модель
10.	Какие из перечисленных моделей относятся к классу мандатных: a) Харрисона-Руззо-Ульмана b) Белла-ЛаПадулы c) Take-Grant d) модель систем военных сообщений e) ролевая модель
11.	Какая из перечисленных моделей позволяет проконтролировать целостность объектов: a) Харрисона-Руззо-Ульмана b) Белла-ЛаПадулы c) Take-Grant d) модель систем военных сообщений e) модель Биба
12.	Как звучит основная аксиома компьютерной безопасности: a) все сущности в компьютерной системе идентифицированы b) все сущности в компьютерной системе однозначно делятся на субъекты и объекты c) все вопросы безопасности в компьютерной системе описываются доступами субъектов к сущностям d) все вопросы безопасности в компьютерной системе описываются матрицей доступа
13.	Для какого вида типизированных матриц доступа возможна проверка безопасности? a) монотонных типизированных матриц доступа b) ациклических монотонных типизированных матриц доступа c) канонической формы монотонных типизированных матриц доступа d) монооперационных типизированных матриц доступа
14.	Сколько существует де-юре правил модели Take-Grant? a) 3 b) 4 c) 5 d) 6
15.	Сколько существует де-факто правил расширенной модели Take-Grant? a) 3 b) 4

	c) 5 d) 6
16.	Какой из перечисленных алгоритмов не используется для проверки безопасности в модели Take-Grant? a) алгоритм построения де-юре замыкания b) алгоритм построения де-факто замыкания c) алгоритм построения t-g замыкания d) алгоритм построения мостов
17.	Какой элемент характерен для модели изолированной программной среды? a) монитор безопасности объектов b) монитор безопасности субъектов c) монитор обращений
18.	Сколько смыслов безопасности функции переходов модели СВС существует? a) 3 b) 5 c) 8 d) 10
19.	Какое понятие определено ниже? «преобразование данных в сущности- приемнике, реализуемое субъектами КС и зависящее от данных, содержащихся в сущности-источнике» a) субъект b) объект c) контейнер d) информационный поток
20.	Какое понятие определено ниже? «в произвольном графе доступа его максимальный tg-связный подграф, состоящий из вершин-субъектов» a) мост b) остров c) начальный пролет моста d) конечный пролет моста
21.	Какому условию удовлетворяет компьютерная система, если для $p(H) > 0$, $p(L) > 0$ справедливо равенство $p(L\|H)=p(L)$? a) информационного невлияния b) информационной невыводимости c) информационной независимости d) информационной изолированности
22.	Можно ли описать в терминах модели Харрисон-Руззо-Ульмана задачу об останове машины Тьюринга? a) нельзя b) можно c) можно, но только в случае типизированных матриц доступа
23.	Какое понятие определено ниже? «субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту» a) монитор безопасности субъектов b) монитор безопасности объектов c) монитор безопасности системы d) монитор обращений
24.	Сколько условий необходимо выполнить для функции переходов в СВС, чтобы она была безопасна в смысле базовой теоремы безопасности: a) 3 b) 5 c) 6 d) 8

25.	Какими свойствами должна обладать система Белла-ЛаПадулы, чтобы соответствовать требованиям базовой теоремы безопасности: a) ss b) ds c) sd d) *
26.	Что такое CCR? a) метка конфиденциальности b) защитный атрибут субъектов c) атрибут контейнеров, определяющий порядок обращения к его содержимому d) уровень допуска сущности
27.	Какие виды ограничений бывают при ролевом разграничении доступа? a) временные b) статические c) сессионные d) динамические
28.	Существуют ли модели управления доступом, позволяющие исключить администратора безопасности из числа потенциальных нарушителей? a) нет b) да c) только дискреционные модели d) только мандатные модели
29.	Возможны ли информационные потоки по времени в модели Белла-ЛаПадулы? a) нет b) да c) только при невыполнении *-свойства d) только при невыполнении **-свойства
30.	Инверсией какой модели является модель Кена Биба? a) Харрисона-Руззо-Ульмана b) Белла-ЛаПадулы c) Take-Grant d) модель систем военных сообщений
31.	Сколько свойств присутствует в неформальном описании модели СВС? a) 5 b) 8 c) 10 d) 12

Пример варианта промежуточного контроля по дисциплине (тестовое задание)

Фамилия_____ **Кол-во правильных ответов**_____

Оценка_____

Тестовые задания

Вариант 1

Дисциплина:	Теоретические основы компьютерной безопасности	Специальность:	10.05.03 - ИБАС
Семестр:	7		
Кафедра:	Информационная безопасность		

1.	Модель Харрисона-Руззо-Ульмана относится к классу: d) мандатные модели e) дискреционные модели f) ролевые модели

2.	Задача проверки безопасности для классической модели Харрисона-Рузо-Ульмана: e) алгоритмически неразрешима f) алгоритмически разрешима g) разрешима только для монооперационных систем h) неразрешима ни для каких систем
3.	Построение де-факто замыкания позволяет: e) выявить возможные информационные потоки в системе f) проверить истинность предиката возможен доступ g) проверить истинность предиката возможна утечка h) предотвратить утечку прав доступа
4.	Какая из перечисленных моделей не относится к моделям информационных потоков: i) программная j) вероятностная k) автоматная l) изолированной программной среды
5.	Какие из перечисленных моделей относятся к классу мандатных: f) Харрисона-Руззо-Ульмана g) Take-Grant h) Белла-ЛаПадулы i) модель систем военных сообщений j) ролевая модель
6.	Какая из перечисленных моделей позволяет проконтролировать целостность объектов: f) Харрисона-Руззо-Ульмана g) Белла-ЛаПадулы h) Take-Grant i) модель систем военных сообщений j) модель Биба
7.	Для какого вида типизированных матриц доступа возможна проверка безопасности? e) монотонных типизированных матриц доступа f) ациклических монотонных типизированных матриц доступа g) канонической формы монотонных типизированных матриц доступа h) монооперационных типизированных матриц доступа i)
8.	Сколько существует де-факто правил расширенной модели Take-Grant? e) 3 f) 4 g) 5 h) 6
9.	Какой из перечисленных алгоритмов не используется для проверки безопасности в модели Take-Grant? e) алгоритм построения де-юре замыкания f) алгоритм построения де-факто замыкания g) алгоритм построения t-g замыкания h) алгоритм построения мостов
10.	Сколько смыслов безопасности функции переходов модели СВС существует? e) 3 f) 5 g) 8 h) 10
11.	Какому условию удовлетворяет компьютерная система, если для $p(H) > 0$, $p(L) > 0$ справедливо равенство $p(L\|H)=p(L)$? e) информационного невлияния f) информационной невыводимости g) информационной независимости h) информационной изолированности

12.	Какое понятие определено ниже? «субъект, активизирующийся при возникновении потока от любого субъекта к любому объекту» e) монитор безопасности субъектов f) монитор безопасности объектов g) монитор безопасности системы h) монитор обращений
13.	Сколько условий необходимо выполнить для функции переходов в СВС, чтобы она была безопасна в смысле базовой теоремы безопасности: e) 3 f) 6 g) 5 h) 8
14.	Что такое CCR? e) уровень допуска сущности f) защитный атрибут субъектов g) атрибут контейнеров, определяющий порядок обращения к его содержимому h) метка конфиденциальности
15.	Какие виды ограничений бывают при ролевом разграничении доступа? e) временные f) статические g) сессионные h) динамические

Критерий оценки теста. Результаты теста оценивается следующим образом: «отлично» - если студент ответил верно на 13 и более вопросов; «хорошо» - если студент отвел верно на 10-12 вопросов; «удовлетворительно» - на 6-9 вопросов; при верном ответе менее чем на 6 вопросов ставится оценка «неудовлетворительно».

4.3 Типовые темы теоретической части курсового проекта.

1. Человеческий фактор и модель нарушителя безопасности информации
2. Субъектно-объектная модель компьютерной системы.
3. Понятие потока, доступа и правил разграничения доступа. Основные типы политик разграничения доступа.
4. Монитор безопасности КС и гарантирование выполнение политики безопасности.
5. Изолированная программная среда.
6. Использование дискреционной модели доступа в ОС. Модели безопасности на основе матрицы доступа.
7. Способы организации матрицы доступа и управления доступом в компьютерных системах
8. Дискреционные модели распространения прав доступа. Модель и теоремы безопасности Харрисона-Руззо-Ульмана.
9. Модель типизованной матрицы доступа. Модель TAKE-GRANT. Расширенная модель TAKE-GRANT.
10. Использование политики мандатного доступа в ОС. Решетка безопасности.
11. Модель Белла-ЛаПадулы и основная теорема безопасности. Основные расширения модели Белла-ЛаПадулы.
12. Особенности политики тематического разграничения доступа. Решетки в моделях тематического разграничения доступа. Решетка мультирубрик на иерархических рубрикаторах.
13. Скрытые каналы утечки информации и теоретико-информационные модели безопасности. Технологии "представлений" и "разрешенных процедур".
14. Особенности использования модели ролевого доступа. Иерархические системы ролей. Принципы наделения ролей полномочиями.
15. Политика и зональная модель безопасности в распределенных КС.
16. Модели обеспечения целостности. Дискреционная модель Кларка-Вильсона.
17. Модели обеспечения целостности. Мандатная модель Кена Биба. Объединение мандатных моделей Белла-ЛаПадулы и Кена Биба.
18. Обеспечение целостности данных мониторами транзакций в клиент-серверныхс системах.

19. Методы, критерии и шкалы оценки эмпирических объектов. Системы многомерного шкалирования защищенности компьютерных систем.
20. Применение теоретико-графовой модели комплексной оценки защищенности КС. Технико-экономическое обоснование систем обеспечения безопасности.
21. Применение теоретико-графовой модели комплексной оценки защищенности КС. Тактико-техническое обоснование систем обеспечения безопасности.
22. Применение теоретико-графовой модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Итоговые права доступа.
23. Применение теоретико-графовой модель систем индивидуально-группового доступа к иерархически организованным информационным ресурсам. Количественные параметры систем индивидуально-группового доступа.
24. Темы предложенные студентами, отражающие тематику дисциплины «Теоретические основы компьютерной безопасности».

4.3 Типовые темы практической части курсового проекта (пример одного из вариантов)
Вариант № 1
1. Разработать элементы информационной технологии, выполняющей следующие функции:
- Заполнение матрицы доступа.
- Моделирование механизма идентификации и аутентификации.

При разработке механизма идентификации и аутентификации
- проверить пароль (пароль должен содержать пять символов);
- для шифрования пароля использовать шифр *Перестановки (*вектор размерности n=5).
- Моделирование политики безопасности МБО.

При разработке политики безопасности МБО использовать формальную модель Харрисона-Руззо-Ульмана (добавление субъекта в матрицу прав доступа с учетом критерия безопасности).
- Определение субъекта, имеющего наибольшее количество доступов типа *read* к объектам матрицы доступа.
- Формирование данных о пользователе, имя которого задается администратором системы (имя и количество его входов в систему).

2. Проанализировать состояния компьютерной системы при выполнении следующих процессов:
- пользователь *Л1* разрабатывает на языке программирования C++ код приложения *Структура Развилка* и запускает его на выполнение, затем текст кодов приложения *Структура Развилка* и *Структура Следование* записывает в файл, созданный текстовым процессором Word, и выводит их текст на печатающее устройство;
- пользователь *П7* запускает на выполнение код приложения *Структура Развилка* и *Структура Следование*, разрабатывает на языке программирования C++ код приложения и записывает его в файл D5, выводит на печатающее устройство файлы F9 и F5 и с помощью субъекта A3 запускает на выполнение файл D5.

Данные для отладки кодов приложений:
Объекты: печатающее устройство – Printer_206
диск H: файлы F1, F5, F9
диск C: файлы C1, C5
диск D: коды приложений *Структура Следование, Структура Развилка*,
текстовый процессор Word, Visual C++
Пользователи: Л1, П7
Права доступа:
Л1 *read* F1, C5, код приложения Структура Следование
write F1, C5, F9
execute код приложения Следование, F9, C1, C5, Visual C++, текстовый процессор Word

П7 *read* F9, C1, код приложения Развилка,
write код приложения Структура Развилка, F5
execute код приложения Структура Развилка, F1, C5, Visual C++, текстовый процессор Word.

Формат сведений о ФОС и ее согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины «**Теоретические основы компьютерной безопасности**» образовательной программы специалитета по специальности
10.05.03 Информационная безопасность автоматизированных систем

утвержденной «27» июня 2018 г.

Автор фонда – Великите Н.Я.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры «Информационная безопасность»

(протокол № 9 от 24 июня 2018 г.)

Заведующий кафедрой _____ /Великите Н.Я./

Фонд оценочных средств рассмотрен и одобрен на заседании методической комиссии РТФ

(протокол №6 от 27.06 2018 г.)

Председатель методической комиссии РТФ _____ /А.Г. Жестовский/

Согласовано
начальник отдела
мониторинга и контроля _____ /Ю.В. Борисевич/