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

УТВЕРЖДАЮ
И.о. декана радиотехнического факультета
_____ / В.А. Баженов /
«14» мая 2018 г.

Фонд оценочных средств для аттестации по дисциплине
(приложение к рабочей программе дисциплины)

Методы проектирования защищенных распределенных информационных систем

Базовой части образовательной программы
по специальности
10.05.03 Информационная безопасность автоматизированных систем

специализация программы
«Обеспечение информационной безопасности распределенных информационных систем»

Факультет Радиотехнический (РТФ)
Кафедра информационной безопасности

Калининград
2018 г.

В результате освоения дисциплины «Методы проектирования защищенных распределенных информационных систем» обучающийся должен получить следующие компетенции:

Таблица 1 - Компетенции и уровни их освоения обучающимся

ОПК-8.19**:** способностью к освоению новых образцов программных, технических средств и информационных технологий	
Знать:	
Уровень 1	принципы построения современных программных, технических средств и информационных технологий
Уровень 2	принципы построения современных программных, технических средств и информационных технологий; принципы эксплуатации и ограничения современных программных, технических средств
Уровень 3	принципы построения современных программных, технических средств и информационных технологий; принципы эксплуатации и ограничения современных программных, технических средств и информационных технологий
Уметь:	
Уровень 1	уметь определять особенности современных программных, технических средств и информационных
Уровень 2	уметь определять особенности современных программных, технических средств и информационных технологий при их изучении
Уровень 3	уметь определять особенности современных программных, технических средств и информационных технологий при их изучении; эксплуатировать современные программных, технических средств и информационных технологий
ПК-2.3**:** способностью создавать и исследовать модели автоматизированных систем	
Знать:	
Уровень 1	модели автоматизированных систем
Уровень 2	модели автоматизированных систем, методики исследования моделей автоматизированных систем
Уровень 3	модели автоматизированных систем, методики исследования моделей автоматизированных систем, способы создания модели автоматизированных систем
Уметь:	
Уровень 1	определять модели автоматизированных систем
Уровень 2	определять модели автоматизированных систем, использовать методики исследования моделей автоматизированных систем
Уровень 3	определять модели автоматизированных систем, использовать методики исследования моделей автоматизированных систем, применять способы создания модели автоматизированных систем
Владеть:	
Уровень 1	методикой составления моделей автоматизированных систем
Уровень 2	методикой составления моделей автоматизированных систем, методиками исследования моделей автоматизированных систем
Уровень 3	методикой составления моделей автоматизированных систем, методиками исследования моделей автоматизированных систем, навыками создания модели автоматизированных систем

ПК-4.7**:** способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	
Знать:	
Уровень 1	классы угроз распределенной системы обработки информации; методику поиска актуальных уязвимостей распределенной системы; порядок создания модели нарушителя;
Уровень 2	классы угроз распределенной системы обработки информации; методику поиска актуальных уязвимостей распределенной системы; порядок создания модели нарушителя; определение базовой модели нарушителя; неформальной модели нарушителя;
Уровень 3	классы угроз распределенной системы обработки информации; методику поиска актуальных уязвимостей распределенной системы; порядок создания модели нарушителя; определение базовой модели нарушителя; неформальной модели нарушителя; типовые модели угроз безопасности персональных данных, обрабатываемых в информационных системах; определение категории нарушителя; типологию нарушителей по характеру поведения
Уметь:	
Уровень 1	установить приоритеты целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект;
Уровень 2	установить приоритеты целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз; создавать модель нарушителя; определять базовой модели нарушителя;
Уровень 3	установить приоритеты целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз; создавать модель нарушителя; определять базовой модели нарушителя; определять категорию нарушителя; составлять содержательную модель нарушителей; создавать сценарии воздействия нарушителей; составлять математическая модель воздействия нарушителей на ресурсы распределенной системы обработки информации
Владеть:	
Уровень 1	навыками установки приоритетов целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей;
Уровень 2	навыками установки приоритетов целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз; системы обработки информации

Уровень 3	навыками установки приоритетов целей безопасности для субъекта отношений; определить перечень актуальных источников угроз; определить перечень актуальных уязвимостей; оценить взаимосвязь угроз, источников угроз и уязвимостей; определить перечень возможных атак на объект; описать возможные последствия реализации угроз; создавать модель нарушителя; определять базовой модели нарушителя; определять категорию нарушителя; составлять содержательную модель нарушителей; создавать сценарии воздействия нарушителей; составлять математическая модель воздействия нарушителей на ресурсы распределенной системы обработки информации
ПК-6.9**:** 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-7.4**:** способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	
Знать:	
Уровень 1	виды научно-технической документации
Уровень 2	виды научно-технической документации; способы разработки научно-технической документации

Уровень 3	виды научно-технической документации; способы разработки научно-технической документации, последовательность подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ
Уметь:	
Уровень 1	разрабатывать научно-техническую документацию
Уровень 2	разрабатывать научно-техническую документацию; готовить научно-технические отчеты; готовить научно-технические отчеты
Уровень 3	разрабатывать научно-техническую документацию; готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ
Владеть:	
Уровень 1	навыками подготовки научно-технических отчетов
Уровень 2	навыками подготовки научно-технических отчетов, обзоров
Уровень 3	навыками подготовки научно-технических отчетов, обзоров, публикаций по результатам выполненных работ
ПК-8.1**:** способностью разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем	
Знать:	
Уровень 1	методы разработки проектных решения по обеспечению безопасности автоматизированных систем
Уровень 2	методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем
Уровень 3	методы разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем
Уметь:	
Уровень 1	разрабатывать проектные решения по обеспечению безопасности автоматизированных систем
Уровень 2	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем
Уровень 3	разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем
Владеть:	
Уровень 1	методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем
Уровень 2	методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем
Уровень 3	методиками разработки и анализа проектных решения по обеспечению безопасности автоматизированных систем

ПК-9.6**:** способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать:	
Уровень 1	методы разработки проектных решения по разработке защищенных автоматизированных систем
Уровень 2	методы разработки и анализа проектных решения по разработке защищенных автоматизированных систем
Уровень 3	методы разработки и анализа проектных решения по разработке защищенных автоматизированных систем, виды проектирования защищенных автоматизированных систем
Уметь:	
Уровень 1	разрабатывать проектные решения по разработке защищенных автоматизированных систем
Уровень 2	разрабатывать и анализировать проектные решения по разработке защищенных автоматизированных систем
Уровень 3	разрабатывать и анализировать проектные решения по разработке защищенных автоматизированных систем, проектировать защищенные автоматизированные системы
Владеть:	
Уровень 1	методами разработки проектных решения по разработке защищенных автоматизированных систем
Уровень 2	методами разработки и анализа проектных решения по разработке защищенных автоматизированных систем
Уровень 3	методами разработки и анализа проектных решения по разработке защищенных автоматизированных систем, методиками проектирования защищенных автоматизированных систем
ПК-10.8**:** способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	
Знать:	
Уровень 1	аспекты применении технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
Уровень 2	аспекты применении электроники технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной
Уровень 3	аспекты применении электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
Уметь:	

Уровень 1	применять знания в области технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
Уровень 2	применять знания в области электроники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
Уровень 3	применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
Владеть:	
Уровень 1	знаниями в области технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
Уровень 2	знаниями в области электроники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
Уровень 3	знаниями в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности
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-12.1**:** способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	
Знать:	
Уровень 1	методы и методики проектирования: методы предотвращения появления каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, предпроектное обследование, техническое задание
Уровень 2	методы и методики проектирования: методы предотвращения появления каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, предпроектное обследование, техническое задание, техническое проектирование
Уровень 3	методы и методики проектирования: методы предотвращения появления каналов НСД, последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию
Уметь:	
Уровень 1	выявлять возможные каналы НСД, определять последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, проводить предпроектное обследование, создавать техническое задание
Уровень 2	выявлять возможные каналы НСД, определять последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, проводить предпроектное обследование, создавать техническое задание, осуществлять техническое и рабочее проектирование с учетом современных технологий формирования КСИБ
Уровень 3	выявлять возможные каналы НСД, определять последовательность работ при проектировании комплексной системы защиты информации от НСД и утечки за счет ПЭМИН, проводить предпроектное обследование, создавать техническое задание, осуществлять техническое и рабочее проектирование с учетом современных технологий формирования КСИБ, осуществлять испытания и внедрение в эксплуатацию, сопровождение КСИБ
Владеть:	
Уровень 1	методиками моделирования и проектирования КСИБ, средствами анализа НСД, знаниями в области
Уровень 2	методиками моделирования и проектирования КСИБ, средствами анализа НСД, знаниями в области, технологией испытания и внедрение в эксплуатацию разработанных систем и подсистем на основе проектных решений

Уровень 3	методиками моделирования и проектирования КСИБ, средствами анализа НСД, знаниями в области, технологией испытания и внедрение в эксплуатацию разработанных систем и подсистем на основе проектных решений; формирования и оформления проекта КСИБ
ПК-13.6**:** 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
ПСК-7.1.2**:** способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать:	
Уровень 1	методы разработки и исследования модели информационно-технологических ресурсов
Уровень 2	методы разработки и исследования модели информационно-технологических ресурсов, модели угроз информационной безопасности в распределенных информационных системах
Уровень 3	методы разработки и исследования модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах
Уметь:	
Уровень 1	разрабатывать и исследовать модели информационно-технологических ресурсов
Уровень 2	разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз информационной безопасности в распределенных информационных системах
Уровень 3	разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах
Владеть:	
Уровень 1	методами исследования информационно-технологических ресурсов

Уровень 2	методами исследования информационно-технологических ресурсов, методами разработки моделей угроз информационной безопасности в распределенных информационных системах
Уровень 3	методами исследования информационно-технологических ресурсов, методами разработки моделей угроз и модели нарушителя информационной безопасности в распределенных информационных системах
ПСК-7.2.7**:** способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	
Знать:	
Уровень 1	способы анализа рисков информационной безопасности и разработки
Уровень 2	методы и способы анализа рисков информационной безопасности и разработки
Уровень 3	методы и способы анализ рисков информационной безопасности и разработки, особенности процесса руководства разработкой политики безопасности в распределенных информационных системах
Уметь:	
Уровень 1	применять способы анализа рисков информационной безопасности и разработки
Уровень 2	применять методы и способы анализа рисков информационной безопасности и разработки
Уровень 3	применять методы и способы анализ рисков информационной безопасности и разработки, руководить0, разработкой политики безопасности в распределенных информационных системах
Владеть:	
Уровень 1	методами исследования информационно-технологических ресурсов
Уровень 2	методами исследования информационно-технологических ресурсов, методами разработки моделей угроз информационной безопасности в распределенных информационных системах
Уровень 3	методами исследования информационно-технологических ресурсов, методами разработки моделей угроз и модели нарушителя информационной безопасности в распределенных информационных системах
ПСК-7.3.3**:** способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем	
Знать:	
Уровень 1	способы аудита защищенности информационно-технологических ресурсов распределенных информационных систем
Уровень 2	методики, способы аудита защищенности информационно-технологических ресурсов распределенных информационных систем, знать приведенные в руководящих документах рекомендации к процессу реализации аудита
Уровень 3	особенности, методики, способы аудита защищенности информационно-технологических ресурсов распределенных информационных систем, знать приведенные в руководящих документах рекомендации к процессу реализации аудита
Уметь:	
Уровень 1	проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем

Уровень 2	проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем, применять приведенные в руководящих документах рекомендации к процессу реализации аудита
Уровень 3	проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем, применять приведенные в руководящих документах рекомендации к процессу реализации аудита и рекомендации по формированию отчетности
Владеть:	
Уровень 1	методикой аудита защищенности информационно-технологических ресурсов информационных систем
Уровень 2	методикой аудита защищенности информационно-технологических ресурсов распределенных информационных систем
Уровень 3	методикой и средствами аудита защищенности информационно-технологических ресурсов распределенных информационных систем

Таблица 2 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	общие принципы построения защищенных распределенных систем, принципы проектирования архитектуры, структуры и основных объектов защищенных систем; основные этапы процесса проектирования и методы, используемые при построении проектируемой сети
уметь	формировать требования к проектируемой сети с учетом анализа угроз и несанкционированных воздействий; составлять функциональные схемы проектируемых распределенных систем
владеть	методами построения распределенных защищенных систем; навыками составления проекта и пониманием содержания основных этапов процесса проектирования

1. Перечень оценочных средств для проведения поэтапной аттестации обучающихся

В перечень оценочных средств **по данной дисциплине** входят:

- опрос на занятиях,
- выполнение лабораторных работ,
- курсовая работа,
- 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	15
ОПК-8.19	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-2.3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-4.7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-6.9	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

ПК-7.4	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-8.1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-9.6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-10.8	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-11	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-12.1	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПК-13.6	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПСК-7.1.2	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПСК-7.2.7	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
ПСК-7.3.3	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

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: 1-15	Этапы: 1 - 14	Этапы: 15
	Опрос	Курсовой проект	Экзамен (вопросы)
ОПК-8.19	+	+	
ПК-2.3	+	+	+
ПК-4.7	+	+	
ПК-6.9	+	+	+
ПК-7.4	+	+	+
ПК-8.1	+	+	+
ПК-9.6	+	+	+
ПК-10.8	+	+	+
ПК-11	+	+	+
ПК-12.1	+	+	+
ПК-13.6	+	+	+
ПСК-7.1.2	+	+	+
ПСК-7.2.7	+	+	+
ПСК-7.3.3	+	+	+

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 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.

3.1.1. 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 или графически 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			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«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 Вопросы к экзамену:

1. Привести и охарактеризовать модель взаимодействия открытых систем, размещение услуг и механизмов защиты на уровнях модели.
2. Привести понятие процесса проектирования. Указать особенности постановки задачи управления процессом проектирования.
3. Характеризовать распределенную информационную систему как объект обеспечения безопасности.
4. Привести и охарактеризовать состав оборудования распределенных информационных систем
5. Привести и охарактеризовать основные протоколы взаимодействия распределенных информационных систем.
6. Трафик и качество функционирования распределенных информационных систем
7. Оптимизация трафика в распределенных информационных системах, типы трафика

8. Привести классификацию угроз безопасности. Дать общую характеристику нарушителей информационной безопасности в распределенных информационных системах. Привести особенности формирование общих требований информационной безопасности к организации.
9. Охарактеризовать общие принципы построения защищенных распределенных информационных систем
10. Указать особенности предпроектного обследование при разработке распределенных защищенных систем
11. Указать особенности формирования технического задания при проектировании распределенных защищенных систем
12. Указать особенности рабочего проектирования распределенных защищенных систем
13. Указать особенности построения защищенного решения для распределенных информационных систем на базе технологий виртуальных частных сетей VPN.
14. Указать и охарактеризовать способы построения сервера безопасности
15. Порядок использования протоколов SSL,TSL ,IPsec, PPP, SSH, S-HTTP. протоколы аутентифицированного распределения ключей.
16. Указать особенности стандарта X.509. Указать особенности протоколов электронной цифровой подписи.
17. Указать и охарактеризовать принципы проектирования VPN, варианты технической реализации
18. Базовые технологии обеспечения качества трафика
19. Указать и охарактеризовать принципы проектирования VPN для сети на базе технологии многопротокольной коммутации по меткам.
20. Указать и охарактеризовать методы криптографической защиты протокола VPN; принципы функционирования протоколов PPTP, L2F.
21. Привести особенности функционирования системы аутентификации Kerberos.
22. Общие принципы расчета нагрузочных и структурных параметров при проектировании сети.
23. Общие принципы автоматизации процесса проектирования
24. Общие требования к применению инструментальных программных средств.
25. Технологические, законодательные и организационные предпосылки организации защиты распределенных информационных систем.
26. Расчет емкости транспортного шлюза и маршрутизатора транспортной сети.
27. Указать и охарактеризовать средства поддержания доступности информации в ИС.
28. Указать и охарактеризовать средства система контроля доступа на объекты и в помещения ИС.
29. Указать и охарактеризовать средства система защиты информации в ИС от НСД.
30. Указать и охарактеризовать средства защиты от разрушающих программных воздействий.
31. Указать и охарактеризовать основные постулаты стандарта ISO 7498-2.

4.2 Комплект тестовых заданий

1.	Функциональная область защиты информации распределенных систем не включает следующую функцию защиты, реализуемую компонентом системы: функции корректирования сетевой нагрузки функции управления данными, реализуемые СУБД функции защиты программных средств, включая средства защиты от вирусов функции защиты информации при обмене данными в распределенных системах, включая криптографические функции

2.	Системы промежуточного уровня (middleware) – это: уровень программного обеспечения, размещаемый между нижним уровнем, на котором находятся операционные системы, и верхним, содержащим пользовательские приложения на терминальных компьютерах уровень программного обеспечения, размещаемый между уровнем API и аппаратным уровнем часть операционной оболочки, предназначенная для создания программных интерфейсов в сети уровень обеспечения маршрутизации, размещаемый между нижним уровнем, на котором находятся операционные системы, и верхним, содержащим пользовательские приложения на терминальных компьютерах
3.	Прозрачность доступа (access transparency) призвана: скрыть разницу в представлении данных и способах доступа пользователя к ресурсам показать разницу в представлении данных и способах доступа пользователя к ресурсам показать параметры данных в ресурсах скрыть параметры данных в ресурсах
4.	Прозрачность местоположения (location transparency) призвана: скрыть от пользователя, где именно физически расположен в системе необходимый ему ресурс показать пользователям, где именно физически расположен в системе необходимый ему ресурс скрыть от пользователя, где именно логически расположен в системе необходимый ему ресурс показать пользователям, где именно логически расположен в системе необходимый ему ресурс
5.	Сокрытие факта наличия нескольких копий ресурса в прозрачности распределенных информационных системах называется: прозрачность репликации прозрачность местоположения прозрачность доступа прозрачность подключения
6.	Прозрачность сохранности (persistence transparency) позволяет: маскировать реальную или виртуальную сохранность ресурсов маскировать только виртуальную сохранность ресурсов маскировать только реальную сохранность ресурсов показывает параметры реальной или виртуальной сохранность ресурсов
7.	Под гибкостью распределенных информационных систем понимается: легкость конфигурирования системы легкость перемещения системы только легкость управления доступом к ресурсам системы легкость взлома системы
8.	Если при этом ни один из пользователей не знает, что одновременно с ним один и тот же ресурс использует еще как минимум один пользователь, то это явление называют: прозрачностью доступа прозрачность репликации прозрачность местоположения прозрачность доступа

9.	Прозрачность отказов (failure transparency) означает, что: пользователей никогда не уведомляют о том, что какой-либо ресурс неработоспособен или выполняет свои функции лишь частично, или с ухудшенным качеством пользователей всегда уведомляют о том, что какой-либо ресурс неработоспособен или выполняет свои функции лишь частично, или с ухудшенным качеством пользователей иногда уведомляют о том, что какой-либо ресурс неработоспособен или выполняет свои функции лишь частично, или с ухудшенным качеством пользователей спрашивают о том, какой ресурс неработоспособен или выполняет свои функции лишь частично, или с ухудшенным качеством
10.	Открытой распределенной информационной системой (open distributed information system) называется система: располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики располагающая службами, пользование которыми возможно при использовании специальных синтаксиса и семантики располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики не располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики
11.	Под оптимизацией сети понимают: некоторый промежуточный вариант, при котором требуется выбрать такие значения параметров сети, чтобы показатели ее эффективности существенно улучшились стандартный вариант, при котором можно выбрать такие значения параметров сети, чтобы показатели ее эффективности существенно улучшились некоторый промежуточный вариант, при котором не требуется выбрать такие значения параметров сети, чтобы показатели ее эффективности существенно улучшились стандартный вариант, при котором не требуется выбрать такие значения параметров сети, чтобы показатели ее эффективности существенно улучшились
12.	Приведение сети в любое работоспособное состояние не включает: отладку пользовательских протколов поиск неисправных элементов сети - кабелей, разъемов, адаптеров, компьютеров проверку совместимости оборудования и программного обеспечения выбор корректных значений ключевых параметров программ и устройств, обеспечивающих прохождение сообщений между всеми узлами сети - адресов сетей и узлов, используемых протоколов, типов кадров Ethernet
13.	Производительность сети измеряется с помощью показателей двух типов: временных показателей и показателей пропускной способности показателей пропускной способности и показателей стойкости к повреждениям показателей пропускной способности и количеству отказов показателей пропускной способности и количеству узлов сети
14.	Время реакции определяется как: интервал времени между возникновением запроса пользователя к какому-либо сетевому сервису и получением ответа на этот запрос

	время реакции определяется временем жизни пакета временем сеанса связи время согласования сетевых служб
15.	При оценке производительности сети не по отношению к отдельным парам узлов, а ко всем узлам в целом используются критерии двух типов: средно-взвешенные и пороговые вероятностные и пороговые вероятностные и средно-взвешенные среднестистические и средно-взвешенные
16.	Если пропускная способность измеряется без деления информации на пользовательскую и служебную, то в этом случае: нельзя ставить задачу выбора протокола или стека протоколов для данной сети можно ставить задачу выбора протокола или стека протоколов для данной сети в некоторых случаях можно ставить задачу выбора протокола или стека протоколов для данной сети в некоторых случаях нельзя ставить задачу выбора протокола или стека протоколов для данной сети
17.	Критерием оценки готовности является коэффициент готовности, который равен: доле времени пребывания системы в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии доле объема трафика системы в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии количеству запросов в системе в работоспособном состоянии и может интерпретироваться как вероятность нахождения системы в работоспособном состоянии количеству отказов в системе в работоспособном состоянии и не может интерпретироваться как вероятность нахождения системы в работоспособном состоянии
18.	Коэффициент готовности вычисляется как: отношение среднего времени наработки на отказ к сумме этой же величины и среднего времени восстановления произведение среднего времени наработки на отказ и суммы этой же величины и среднего времени восстановления разницу среднего времени наработки на отказ и суммы этой же величины и среднего времени восстановления отношение среднего времени наработки на отказ к сумме этой же величины и общего времени восстановления
19.	Основным способом повышения готовности является: избыточность гибкость скорость частота
20.	Протокол, в котором постоянно тестируются физические связи между узлами и концентраторами сети: FDDI TCP UDP SNMP

21.	Непрерывная готовность (continuousavailability) - это свойство систем, которые также обеспечивают время восстановления в пределах: одной секунды одного часа одних суток двух секунд
22.	Распределенная система состоит: из трех частей(клиентское приложение (GUI или Web), сервер приложений и источник данных (СУБД, XML и т.д.)) из двух частей(клиентское приложение (GUI или Web), сервер приложений и источник данных (СУБД, XML и т.д.)) из пяти частей(клиентское приложение (GUI или Web), сервер приложений, сервер безопасности, источник данных (СУБД, XML и т.д.)) из четырех частей(клиентское приложение (GUI или Web), сервер приложений, сервер безопасности, сервер реплицирования, источник данных (СУБД, XML и т.д.))
23.	Технологический процесс функционирования системы защиты информации от несанкционированного доступа, как комплекса программно-технических средств и организационных (процедурных) решений, не предусматривает выполнение следующих процедур: оперативный контроль функционирования систем защиты удаленных узлов смежных сетей учет, хранение и выдачу пользователям информационных носителей, паролей, ключей ведение служебной информации (генерация паролей, ключей, сопровождение правил разграничения доступа) контроль хода технологического процесса обработки информации путем регистрации анализа действий пользователей
24.	В большинстве случаев обычным типом информации, присутствующим в профилях безопасности, не является: описание сессий; для данного пользователя или системы профили могут характеризовать обычное число сессий в данное время в течение дня, предполагаемое самое раннее начало сессии, предполагаемую максимальную длительность сессии и т. д. параметры выполнения. Профили также могут устанавливаться в зависимости от предполагаемого типа использования ресурсов, которые должна поддерживать данная вычислительная система доступ к ресурсам. Можно создать профили частоты чтения и записи некоторых файлов, числа отказов на запросы правила определения аномалий
25.	Существуют три причины использования распределенных атак злоумышленником. Какая из перечисленных лишняя: сокрытие мощность сбор информации отсутствие последствий после вторжения

26.	Эксплойт – это: приложение или последовательность команд, предназначенная для реализации каких-либо уязвимостей операционной системы или специализированного программного обеспечения приложение или последовательность команд, предназначенная для реализации каких-либо задач операционной системы или специализированного программного обеспечения приложение или последовательность команд, предназначенная для реализации каких-либо функций операционной системы или специализированного программного обеспечения утилита настройки безопасности операционной системы
27.	Классификация атак по уровню модели OSI не предполагает: атаки на сетевом уровне атаки на прикладном уровне атаки на транспортном уровне атаки на сеансовом уровне
28.	Атаки типа IP-spoofing – это: атаки на физическом уровне атаки на канальном уровне атаки на сетевом уровне атаки на транспортном уровне
29.	Атаки «отказ в обслуживании» типа TCP flood, UDP flood - это: атаки на физическом уровне атаки на канальном уровне атаки на сетевом уровне атаки на транспортном уровне
30.	Укажите стандартный порт протокола HTTP: 80 443 23 21

4.3 Темы курсовых работ

Задание 1. Проектирование защищенной распределенной информационной системы для организации на базе технологий виртуальных частных сетей VPN.

Задание 2. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов SSL,TSL ,IP sec, S-HTTP

Задание 3. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности.

Задание 4. Проектирование защищенной распределенной информационной системы для организации базе технологий централизованного хранения данных сервера безопасности.

Задание 5. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов TSL

Задание 6. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов IP- sec

Задание 7. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов S-HTTP

Задание 8. Проектирование защищенной распределенной информационной системы для организации на базе технологий протоколов SSL,TSL

Задание 9. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности. базе технологий протоколов SSL,TSL ,IP sec, S-HTTP

Задание 10. Проектирование защищенной распределенной информационной системы для организации на базе технологий децентрализованного хранения данных сервера безопасности. на базе технологий протоколов SSL, IP-sec, S-HTTP

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины «Методы проектирования защищенных распределенных информационных систем»
образовательной программы специалитета по специальности
10.05.03 «Информационная безопасность автоматизированных систем»
утвержденной «27» июня 2018 г.

Автор(ы) фонда – ст. преподаватель кафедры информационной безопасности _____Подтопельный В. В.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности

(протокол от «14» апреля 2018 г. № 9)

Зав. кафедрой информационной безопасности _____ Великите Н.Я.

Фонд оценочных средств рассмотрен и одобрен на заседании методической комиссии радиотехнического факультета БГАРФ

(протокол от «27» июня 2018 г. № 6)

Председатель методической комиссии_____ Жестовский.А.Г.

Согласовано

Начальник отдела мониторинга и контроля БГАРФ _____/Борисевич Ю.В./