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 /
27 июня 2018 г.

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

Безопасность операционных систем

Базовой части образовательной программы
специалитета
10.05.03 Информационная безопасность автоматизированных систем

специализация программы
«Обеспечение информационной безопасности распределенных информационных систем»

Факультет Радиотехнический (РТФ)
(указывается наименование факультета)

Кафедра информационной безопасности
(указывается наименование кафедры)

Калининград
2018 г.

В результате освоения дисциплины «Безопасность операционных систем» обучающийся должен получить следующие компетенции:

Таблица 1 - Компетенции и уровни их освоения обучающимся

ОПК-6.4**:** способностью применять нормативные правовые акты в профессиональной деятельности	
Знать:	
Уровень 1	принципы моделирования поведения злоумышленника при осуществлении несанкционированного доступа в сети; классификация действий злоумышленника в соответствии с законодательством Российской Федерации;
Уровень 2	принципы моделирования поведения злоумышленника при осуществлении несанкционированного доступа в сети; классификация действий злоумышленника в соответствии с законодательством Российской Федерации; способы противодействия действиям злоумышленника допустимые нормами российского законодательства;
Уровень 3	принципы моделирования поведения злоумышленника при осуществлении несанкционированного доступа в сети; классификация действий злоумышленника в соответствии с законодательством Российской Федерации; способы противодействия действиям злоумышленника допустимые нормами российского законодательства; структуру нормативно-технических и нормативно-методических документов по защите информации
Уметь:	
Уровень 1	адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями
Уровень 2	адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями правительства российской федерации; классифицировать злоумышленника в соответствии и определять степень их ответственности за нарушение работы и раскрытие конфиденциальных данных пользователей распределенных систем обработки информации;
Уровень 3	адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями правительства российской федерации; классифицировать злоумышленника в соответствии и определять степень их ответственности за нарушение работы и раскрытие конфиденциальных данных пользователей распределенных систем обработки информации; применять методы обеспечения информационной безопасно-
Владеть:	

Уровень 1	адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями правительства российской федерации;
Уровень 2	адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями правительства российской федерации; классифицировать злоумышленника в соответствии и определять степень их ответственности за нарушение работы и раскрытие конфиденциальных данных пользователей распределенных систем обработки информации;
Уровень 3	адаптировать функционирование служб безопасности распределенных систем обработки информации, параметры криптографической защиты передаваемых данных, определять сферы полномочий пользователей в соответствии с требованиями ФСТЭК и номами законодательства Российской Федерации, нормативными и методическими документы по технической защите информации, постановлениями правительства российской федерации; классифицировать злоумышленника в соответствии и определять степень их ответственности за нарушение работы и раскрытие конфиденциальных данных пользователей распределенных систем обработки информации; применять методы обеспечения информационной безопасности
ПК-1.10**:** способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	
Знать:	
Уровень 1	методики поиска, обобщения и систематизации научно-технической информации
Уровень 2	методики поиска, изучения, обобщения и систематизации научно-технической информации
Уровень 3	методики поиска, изучения, обобщения и систематизации научно-технической информации, виды нормативных и методических материалов в сфере профессиональной деятельности
Уметь:	
Уровень 1	осуществлять поиск, систематизировать научно-техническую информацию в области информационной защиты
Уровень 2	осуществлять поиск и обобщать, систематизировать научно-техническую информацию в области информационной защиты
Уровень 3	осуществлять поиск и обобщать, систематизировать научно-техническую информацию в области информационной защиты, использовать нормативные и методические материалы в сфере профессиональной деятельности
Владеть:	
Уровень 1	методикой поиска и систематизации научно

Уровень 2	методикой поиска, обобщения и систематизации научно
Уровень 3	методикой поиска, изучения, обобщения и систематизации научно
ПК-4.2**:** 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-6.4**:** 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
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-11.3**:** 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
ПК-22.2**:** способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	
Знать:	
Уровень 1	методы формирования политики информационной безопасности организации,
Уровень 2	методы формирования политики информационной безопасности организации, методы формирования политики информационной безопасности информационных систем в организации
Уровень 3	методы формирования политики информационной безопасности организации, методы формирования политики информационной безопасности информационных систем в организации, методы и способы контроля ее реализации
Уметь:	
Уровень 1	формировать политику информационной безопасности организации,
Уровень 2	формировать политику информационной безопасности организации, применять методы и способы контроля ее реализации
Уровень 3	формировать политику информационной безопасности организации, применять методы и способы контроля ее реализации, формировать политики информационной безопасности при эксплуатации информационных систем в организации
Владеть:	
Уровень 1	методами формирования политики информационной безопасности организации
Уровень 2	методами формирования политики информационной безопасности организации, методы и способы контроля ее реализации,
Уровень 3	методами формирования политики информационной безопасности организации, методы и способы контроля ее реализации, методами формирования политики информационной безопасности информационных систем в организации
ПК-24.3**:** способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
Знать:	
Уровень 1	методы применения информационно-технологических ресурсов автоматизированной системы
Уровень 2	методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы
Уровень 3	методы обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
Уметь:	

Уровень 1	обеспечить применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
Уровень 2	обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы
Уровень 3	обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
Владеть:	
Уровень 1	методами формирования политики информационной безопасности организации
Уровень 2	методами формирования политики информационной безопасности организации, методы и способы контроля ее реализации,
Уровень 3	методами обеспечения эффективного применения информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности
ПК-25.1**:** способностью обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций	
Знать:	
Уровень 1	способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; способы восстановление ресурсов автоматизированной системы работоспособности при возникновении нештатных ситуаций
Уровень 2	способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; способы восстановление ресурсов автоматизированной системы работоспособности при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям
Уровень 3	способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; способы восстановление ресурсов автоматизированной системы работоспособности при возникновении нештатных ситуаций; 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; способы защиты программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий.
Уметь:	
Уровень 1	применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы; восстанавливать ресурсы автоматизированной системы, их работоспособность при возникновении нештатных ситуаций;

Уровень 2	применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы; восстанавливать ресурсы автоматизированной системы, их работоспособность при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислительных систем; применять методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям
Уровень 3	применять средства и системы защиты информационно-технологических ресурсов автоматизированной системы; восстанавливать ресурсы автоматизированной системы, их работоспособность при возникновении нештатных ситуаций; методы и средства ограничения доступа к компонентам вычислительных систем; применять методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; применять методы и средства хранения ключевой информации; осуществлять защиту программ от изучения, встраивать средства защиты в программное обеспечение; осуществлять защиту от разрушающих программных воздействий
Владеть:	
Уровень 1	методикой применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы;
Уровень 2	методикой применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; методикой восстановления ресурсов автоматизированной системы, их работоспособности при возникновении нештатных ситуаций; методами и средствами ограничения доступа к компонентам вычислительных систем;
Уровень 3	методикой применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; методикой восстановления ресурсов автоматизированной системы, их работоспособности при возникновении нештатных ситуаций; методами и средствами ограничения доступа к компонентам вычислительных систем; методикой применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; методикой применения методов и средств хранения ключевой информации; методикой защиты программ от изучения, методикой встраивания средств защиты в программное обеспечение; методикой защиты от разрушающих программных воздействий.
ПК-26.1: способностью администрировать подсистему информационной безопасности автоматизированной системы	
Знать:	
Уровень 1	механизмы администрирования подсистем информационной безопасности, критерии эффективности применения СЗИ
Уровень 2	способы и механизмы администрирования подсистем информационной безопасности
Уровень 3	способы и механизмы администрирования подсистем информационной безопасности, критерии эффективности применения СЗИ
Уметь:	

Уровень 1	администрировать подсистем информационной безопасности
Уровень 2	администрировать подсистем информационной безопасности, применять критерии эффективности применения СЗИ
Уровень 3	администрировать подсистем информационной безопасности, применять критерии эффективности применения СЗИ, автоматизировать работу по административной настройке СЗИ от НСД
Владеть:	
Уровень 1	механизмами администрирования средств защиты информации
Уровень 2	механизмами администрирования средств защиты информации и средств, встроенных в ОС
Уровень 3	способами, механизмами администрирования средств защиты информации и средств, встроенных в ОС
ПК-28.1: способностью управлять информационной безопасностью автоматизированной системы	
Знать:	
Уровень 1	способы управления информационной безопасностью
Уровень 2	способы управления информационной безопасностью автоматизированной системы
Уровень 3	способы, средства и механизмы управления информационной безопасностью автоматизированной системы
Уметь:	
Уровень 1	примять способы управления информационной безопасностью автоматизированной системы
Уровень 2	примять способы, средства и механизмы управления информационной безопасностью автоматизированной системы
Уровень 3	примять способы , средства и механизмы управления информационной безопасностью автоматизированной системы
Владеть:	
Уровень 1	способами и механизмами управления информационной безопасностью автоматизированной системы
Уровень 2	способами, механизмами способы и механизмы управления информационной безопасностью автоматизированной системы

Уровень 3	способами, средствами и механизмами способы и механизмы управления информационной безопасностью автоматизированной системы
ПСК-7.4.2: способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	
Знать:	
Уровень 1	знать способы удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах
Уровень 2	знать способы и задачи удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах
Уровень 3	знать способы, правила и задачи удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах
Уметь:	
Уровень 1	применять способы удаленного администрирования операционных систем
Уровень 2	применять способы и правила удаленного администрирования операционных систем
Уровень 3	применять способы и правила удаленного администрирования операционных систем и систем баз данных в распределенных информационных системах
Владеть:	
Уровень 1	способами и механизмами управления информационной безопасностью автоматизированной системы
Уровень 2	способами, механизмами управления информационной безопасностью автоматизированной системы
Уровень 3	способами, средствами и механизмами управления информационной безопасностью автоматизированной системы и систем баз данных в распределенных информационных системах
ПК-3.6: способностью проводить анализ защищенности автоматизированных систем	
Знать:	
Уровень 1	методики определения рисков информационной системы, выявления возможных каналов НСД
Уровень 2	методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ
Уровень 3	методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ, метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана, метод оценки риска Фишера
Уметь:	
Уровень 1	определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники. Оценивать уязвимость информации.
Уровень 2	определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники. Оценивать уязвимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ).

Уровень 3	определять риски информационной системы, возможные каналы НСД, применять экспертные структурные вопросники. Оценивать уязвимость информации. Анализировать пути проникновения в и нарушение работы в комплексных системах информационной безопасности (КСИБ). Создавать модель нарушителя. проводить вероятностный анализ методов и способов воздействия на КСИБ нарушителем
Владеть:	
Уровень 1	методиками определения рисков информационной системы, выявления возможных каналов НСД
Уровень 2	методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы
Уровень 3	методиками определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, средствами автоматизированного расчета рисков информационной системы, методами оценки уязвимости информации, средствами мониторинга и контроля состояния информационный среды КСИБ

Таблица 2 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	принципы построения и функционирования, примеры реализаций современных операционных систем; функции ОС, основные концепции управления процессорами, памятью, вспомогательной памятью, устройствами; критерии оценки эффективности и надежности средств защиты ОС; принципы организации и структуру подсистем защиты ОС семейств UNIX и Windows;
уметь	использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем; оценивать эффективность и надежность защиты операционных систем; планировать политику безопасности операционных систем;
владеть	навыками работы с операционными системами семейств Windows и Unix, восстановления операционных систем после сбоев; навыками установки и настройки операционных систем семейств Windows и Unix с учетом требований по обеспечению информационной безопасности.

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
ОПК-6.4			+	+	+	
ПК-1.10			+	+	+	+
ПК-3.6	+					
ПК-4.2	+			+	+	
ПК-6.4		+	+		+	+
ПК-11.3		+	+		+	+
ПК-13.2		+	+		+	+
ПК-22.2		+	+		+	+
ПК-24.3		+	+		+	+
ПК-25.1		+	+		+	+
ПК-26.1		+	+		+	+
ПК-28.1		+	+		+	+
ПСК-7.4.2		+	+		+	+

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: 1-6	Этапы: 1 - 5	Этапы: 6
	Опрос	Курсовая работа	Экзамен (вопросы)
ОПК-6.4	+	+	
ПК-1.10	+	+	+
ПК-3.6	+	+	
ПК-4.2	+	+	+
ПК-6.4	+	+	+
ПК-11.3	+	+	+
ПК-13.2	+	+	+
ПК-22.2	+	+	+
ПК-24.3	+	+	+
ПК-25.1	+	+	+
ПК-26.1	+	+	+
ПК-28.1	+	+	+
ПСК-7.4.2	+	+	+
ОПК-6.4	+	+	+

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. 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 самостоя-

			тельно 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 курсовой работы.

Оценка			
Неудовлетворитель-ный	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. Пользовательский интерфейс ОС. Классификация программных средств
2. Основные функции ОС. Классификация ОС.
3. Концепция процесса. Типология процессов

4. Концепция ресурсов. Концепция виртуальности.
5. Концепция прерывания. Классы прерываний.
6. Классификация операционных систем. Состав ядра ОС.
7. Модули ядра. Перечислить вспомогательные модули ОС и режимы.
8. Многослойная структура ОС. Микроядерная архитектура.
9. Управление процессами ОС. Понятия задание, задача, поток, нить и процесс.
10. Контекст процесса. Особенности работы нити процесса.
11. Планирование процессов. Концепции планирования процессов. Понятие кванта.
12. Способы организации процесса. Особенности организации процесса. Проблемы выполнения процессов на процессоре.
13. Понятие прерывания. Типы прерывания. Последовательность при обработке прерываний. Способы выполнения прерываний.
14. Особенности управления памятью в ОС.
15. Особенности работы виртуальной памяти и swapping. Алгоритмы распределения памяти. Алгоритмы управления памятью.
16. Механизмы распределения адресов в ОС. Распределение при реальной и виртуальной адресациями.
17. Файловые системы. Общая организация ФС.
18. Особенности ФС FAT и exFAT.
19. Особенности ФС NTFS.
20. Особенности файловых систем ext.
21. Сравнительный анализ файловых систем.
22. Особенности реализации функции безопасности в ОС. Краткие различия организации безопасности Unix и Windows.
23. Организация безопасности в Unix-системах.
24. Аутентификация в Unix-системах.
25. Аспекты механизмов безопасности Windows.
26. Привилегии субъектов в Windows. Маркеры доступа. Дескриптор защиты.
27. Авторизация в ОС Windows.
28. Аудит в ОС
29. Аспекты сетевой безопасности Linux.
30. Основные команды MS-DOS. Особенности создания Bat-файлов
31. Что такое виртуальная память? Каковы свойства различных видов организации виртуальной памяти?
32. Описать способы вычисления адреса при страничной, сегментной и страничносегментной организации виртуальной памяти.
33. Перечислить и охарактеризовать стратегии управления виртуальной памятью.
34. Сформулировать и пояснить принцип локальности.
35. Перечислить и охарактеризовать стратегии вталкивания, размещения и выталкивания.
36. Что такое данные, источник данных, организация данных?
37. Перечислите методы организации данных. В чем их различия?
38. Опишите способы организации файлов.
39. Как можно хранить файлы на носителе?
40. Перечислите основные операции над файлами.
41. Перечислите и опишите уровни многоуровневой модели файловой системы.
42. Каковы основные компоненты архитектуры современных файловых систем?
43. Дайте определения системе ввода-вывода.
44. Что такое драйвер ввода-вывода?
45. Перечислите и охарактеризуйте типы устройств ввода-вывода.
46. На какие слои (уровни) разбито программное обеспечение ввода-вывода, каково их назначение?
47. Сформулируйте список функциональных дефектов с точки зрения защиты в используемой ОС.
48. Какие элементы безопасности содержит ОС Windows NT?
49. Назовите элементы безопасности ОС UNIX?

50. Охарактеризуйте элементы безопасности ОС Novell NetWare?
51. Дайте характеристику задачи активного аудита.
52. Дайте характеристику сигнатурного метода активного аудита.
53. Охарактеризуйте функциональные компоненты активного аудита.

4.2 Комплект тестовых заданий

1.	Что из перечисленного не является основными функциями ОС? a) диспетчеризация (планирование обработки задач); b) распределение памяти между различными задачами; c) распределение задачам необходимых ресурсов ВС; d) обеспечение доверенной загрузки;
2.	Какие режимы обработки данных существуют в ОС? a) однопрограммные b) параллельные c) мультипрограммные д) смешанные
3.	Наличие многоуровневого планирования при организации работы ОС является следствием: a) частотного принципа b) принципа модульности c) принципа функциональной избирательности d) принципа функциональной избыточности
4.	Принцип открытости и наращиваемости ОС предусматривает: a) открытость исходного кода ОС b) модульное построение ОС c) возможность изменения конфигурации ОС и ее мощности без осуществления процессов генерации d) избыточность функций ОС
5.	“Несанкционированный доступ к информации” это: a) доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация b) доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств c) доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация d) доступ к информации, реализуемый путём уничтожения технических средств информационной системы
6.	В состав системы защиты информации от НСД входят: a) подсистема управления доступом b) подсистема контроля за устройствами ввода/вывода информации c) подсистема регистрации и учёта d) подсистема обеспечения целостности

7.	Угроза это: a) совокупность сообщений, направленных на запугивание b) совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу. c) совокупность сообщений, направленных на причинение вреда d) любое действие, направленное на причинение ущерба
8.	Классами защищённости автоматизированных систем от несанкционированного доступа являются: a) 1Е b) 2А c) 2В d) 3Б
9.	Определите класс автоматизированной системы по следующим классификационным признакам: *АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается "Комерческая тайна".* a) 2Б b) 1Г c) 1Д d) 3Б
10.	Определите класс автоматизированной системы по следующим классификационным признакам: *многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. И все пользователи имеют равные права доступа ко всей информации АС, обрабатывается "Служебная тайна" и общедоступная информация:* a) 2Б b) 2А c) 1Г d) 1Д
11.	Методы и средства защиты информации бывают: a) Технические (аппаратные) b) Программные c) Прикладные d) Организационные
12.	Информация по категории доступа классифицируется как: a) Конфиденциальная b) Общедоступная c) Особо конфиденциальная d) Ограниченного доступа
13.	Уязвимость это: a) Совокупность действий, направленная на преодоление системы защиты b) Злонамеренное внедрение специального ПО

	c) Слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации. d) Результат действия вируса
14.	Что из перечисленного не является состоянием процесса? a) порождение b) выполнение c) прерывание d) готовность
15.	Прерывание - это: a) временное прекращение процесса b) остановка процесса c) временное прекращение процесса, вызванное событием, внешним по отношению к этому процессу, и совершенное таким образом, что процесс может быть продолжен d) событие, при котором меняется нормальная последовательность команд, выполняемых процессором
16.	Как соотносятся контекст и дескриптор процесса: a) это одно и то же b) дескриптор включает в себя контекст c) контекст включает в себя дескриптор d) дескриптор содержит более оперативную информацию, которая должна быть легко доступна подсистеме планирования процессов, а контекст используется операционной системой для восстановления прерванного процесса
17.	Что такое тупиковая ситуация для процесса? a) невозможность выделения процессу требуемого ресурса b) ситуация когда процесс ожидает некоторого события, которое никогда не произойдет c) прерывание процесса операционной системой d) критическая системная ошибка во время выполнения процесса
18.	. В системе поблочного отображения адресов виртуальной памяти указываются: a) адрес реальной памяти, в котором расположен указанный элемент b) адрес файла подкачки и номер блока в этом файле, в котором расположен указанный элемент c) блок, в котором расположен этот элемент, и смещение элемента относительно начала блока d) адрес элемента в таблице отображения блоков процесса
19.	В каком порядке задаются права доступа в ОС Linux? a) группа-владелец- остальные b) владелец-группа-остальные c) остальные-владелец-группа d) остальные-группа-владелец
20.	Что такое ACL? a) средство для хранения паролей b) сценарий входа в систему c) список управления доступом d) инструмент мандатного управления доступом в ОС

21.	Что из перечисленного не содержится в маркере доступа пользователя? a) идентификатор пользователя b) привилегии пользователя c) идентификатор сеанса работы пользователя, к которому относится маркер доступа d) уровень доступа пользователя в системе
22.	Кто в ОС может получить доступ к любому объекту по методу ACCESS_SYSTEM_SECURITY: a) все пользователи b) суперпользователь c) администратор d) аудитор
23.	Какова должна быть минимальная длина пароля в случае смены ежеквартально? a) 13 символов b) 12 символов c) 8 символов d) 6 символов
24.	Какая файловая система поддерживает шифрование файлов? a) FAT32 b) NTFS c) EFS d) HPFS
25.	Какая файловая система поддерживает хранение на диске дескрипторов защиты для файлов? a) FAT32 b) NTFS c) FAT16 d) HPFS
26.	Что из перечисленного не является требование к подсистеме регистрации и учета: a) использование идентификационного и аутентификационного механизма b) запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.) c) обеспечение доверенной загрузки ОС d) действия по изменению ПРД
27.	Что такое PAM? a) набор библиотек подключаемых модулей шифрования b) набор открытых библиотек подключаемых модулей аутентификации c) набор открытых библиотек подключаемых модулей резервного восстановления d) набор открытых библиотек подключаемых модулей доверенной загрузки
28.	Что такое домен безопасности? a) собрание участников безопасности, имеющих единый центр, использующий единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров b) виртуальная частная сеть с единым центром управления c) локальная сеть, не имеющая выхода в сети связи общего пользования d) сетевая операционная система

29.	Какое из требований необязательно для операционных систем, сертифицированных по 5 классу РД СВТ? a) Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ b) ОС должна содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа c) Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов) d) В ОС должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа
30.	Присутствуют ли в ОС семейства Windows механизмы, осуществляющие криптографические преобразования? a) нет b) присутствуют механизмы ЭЦП и хеширования c) присутствуют механизмы обмена ключами d) присутствуют механизмы для симметричного шифрования данных

4.3 Темы курсовых работ

1.Идентификация и аутентификация пользователя.
2.Регистрация событий системы.
3.Установка и обновление программного обеспечения в ОС Linux, FreeBSD. Представление о пакете rpm.
4.Сборка ядра ОС Linux
5.Сборка ядра ОС FreeBSD
6.Командные интерпретаторы ОС
7.Создание разделов и файловых систем ОС Linux. Монтирование файловых систем.
8.Журналируемая файловая система.
9.Дисковые квоты в ОС Linux, FreeBSD, Windows.
10.Реализация функций информационной безопасности в файловой системе FAT.
11.Реализация функций информационной безопасности в файловой системе NTFS
12.Реализация функций информационной безопасности в файловой системе FAT 32
13.Реализация функций информационной безопасности в файловой системе ext3
14.Шифрованная файловая система EFS.
15. Ядро и вспомогательные модули ОС Linux
16.Особенности аудита в ОС Windows.
17.Файловая система EXFAT.
18.Управление учетными записями пользователей и групп в ОС Linux, Windows, FreeBSD
19.Планирование процессов ОС Linux
20. Сравнительный анализ функций безопасности Windows 7 и Windows 2003.
21.Настройка модуля безопасности SE в ОС Linux.
22.Особенности аудита в ОС Linux.

Сведения о ФОС и его согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины «Безопасность операционных 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» июня 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./