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 /
24 апреля 2018 г.

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

Программно-аппаратные средства обеспечения информационной безопасности

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.

1. **Компетенции обучающегося, формируемые в результате освоения дисциплины и этапы их формирования**

В результате освоения дисциплины «Информационная безопасность распределенных информационных систем» обучающийся должен получить следующие компетенции:

Таблица 1 - Компетенции и уровни их освоения обучающимся

ОПК-8.17**:** 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
Владеть:	
Уровень 1	методикой эксплуатации современные программных технологий.
Уровень 2	методикой эксплуатации современные программных, технических средств
Уровень 3	методикой эксплуатации современные программных, технических средств и информационных технологий.
ПК-1.15**:** 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-3.10**:** способностью проводить анализ защищенности автоматизированных систем	
Знать:	
Уровень 1	методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ
Уровень 2	методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества КСИБ, метод экспертных структурных вопросников
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
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
ПК-4.4**:** 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-5.2**:** способностью проводить анализ рисков информационной безопасности автоматизированной системы	
Знать:	
Уровень 1	методологию оценку риска; оценку ущерба от реализацию угроз; групп оценки риска; этапы оценки риска: определение степени детализации, идентификация и оценка ценностей, идентификация угроз и определение их вероятности
Уровень 2	методологию оценку риска; оценку ущерба от реализацию угроз; групп оценки риска; этапы оценки риска: определение степени детализации, идентификация и оценка ценностей, идентификация угроз и определение их вероятности; измерение риска; выбор мер и средств защиты в соответствии с уровнем риска; внедрение и тестирование средств защиты
Уровень 3	методологию оценку риска; оценку ущерба от реализацию угроз; групп оценки риска; этапы оценки риска: определение степени детализации, идентификация и оценка ценностей, идентификация угроз и определение их вероятности; измерение риска; выбор мер и средств защиты в соответствии с уровнем риска; внедрение и тестирование средств защиты; утверждение остаточного риска; методику оценки потенциально возможных угроз информационной системы и средств защиты: оценка ущерба от угроз безопасности информации, показатели
Уметь:	
Уровень 1	выбирать методику оценки угроз;
Уровень 2	выбирать методику оценки угроз; производить оценку ущерба от угроз безопасности информации;
Уровень 3	выбирать методику оценки угроз; производить оценку ущерба от угроз безопасности информации; производить оценки потенциально возможных угроз информационной системы и средств защиты
Владеть:	
Уровень 1	методикой идентификации и оценки угроз;
Уровень 2	методикой идентификации и оценки угроз; методикой оценки риска; методикой определения вероятности угроз

Уровень 3	методикой идентификации и оценки угроз; методикой оценки риска; методикой определения вероятности угроз; методикой оценки ущерба в зависимости от применяемы средств защиты
ПК-6.6**:** способностью проводить анализ, предлагать и обосновывать выбор решений по обеспечению требуемого уровня эффективности применения автоматизированных систем	
Знать:	
Уровень 1	способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации;
Уровень 2	способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности
Уровень 3	способы определения степени отказоустойчивости автоматизированной системы и системы защиты информации; принципы анализа проблемной области решаемых задач комплексной системы защиты информации, автоматизированных систем защиты информации. методы и средства ограничения доступа к компонентам вычислительных систем; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; методы и средства хранения ключевой информации; защита программ от изучения, способы встраивания средств защиты в программное обеспечение; защита от разрушающих программных воздействий;
Уметь:	
Уровень 1	определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий;

Уровень 2	определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы;
Уровень 3	определять особенности функционирования защищаемой информационной системы; выявлять уязвимости и определять наиболее эффективные способы их устранения; определять целесообразность применения средств привязки программного обеспечения к аппаратному окружению и физическим носителям; определять критерии эффективности работы средств защиты информации; обосновывать целесообразность применения средств защиты программ от изучения, систем защиты от разрушающих программных воздействий; применять средства защиты информации и определять их эффективность в процессе функционирования защищаемой автоматизированной системы; определять эффективность предложенных решений с учетом снижения рисков автоматизированной системы; определять критерии эффективности работы средств защиты информации.
Владеть:	
Уровень 1	методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем;
Уровень 2	методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей;
Уровень 3	методикой определения отказоустойчивости автоматизированных систем; методикой выявления уязвимостей информационных систем; средствами устранения уязвимостей; средствами защиты информации в процессе хранения и передачи данных и методами их тестирования; методикой определения эффективности предложенных решений с учетом снижения рисков
ПК-14.4**:** способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
Знать:	
Уровень 1	принципы поиска и определения уязвимостей сетевых ресурсов при установленной защите сетевых ресурсов; принципы проведения аудита систем передачи данных для проверки проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации

Уровень 2	принципы поиска и определения уязвимостей сетевых ресурсов при установленной защите сетевых ресурсов; принципы проведения аудита систем передачи данных для проверки проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; методы определения стойкости парольной защиты; механизмы активного и пассивного анализа уязвимостей; определять эффективность применяемых программно-аппаратных, криптографических и технических средств защиты информации в зависимости степень риска и вероятность осуществления НСД
Уровень 3	принципы поиска и определения уязвимостей сетевых ресурсов при установленной защите сетевых ресурсов; принципы проведения аудита систем передачи данных для проверки проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; методы определения стойкости парольной защиты; механизмы активного и пассивного анализа уязвимостей; определять эффективность применяемых программно-аппаратных, криптографических и технических средств защиты информации в зависимости степень риска и вероятность осуществления НСД; принципы контроля данных при передачи информации по проводным и беспроводным каналам связи при использовании криптографических протоколов; языки описания уязвимостей и проверок; теоретико-графовые модели комплексной оценки защищенности распределенных ресурсов
Уметь:	
Уровень 1	применять сканеры безопасности в пассивном и активном режиме; производить аудит распределенных систем; анализировать результаты сканирования;
Уровень 2	применять сканеры безопасности в пассивном и активном режиме; производить аудит распределенных систем; анализировать результаты сканирования; использовать снифферы для анализа потока передаваемой информации; рассчитывать степень защищенности передаваемой информации
Уровень 3	применять сканеры безопасности в пассивном и активном режиме; производить аудит распределенных систем; анализировать результаты сканирования; использовать снифферы для анализа потока передаваемой информации; рассчитывать степень защищенности передаваемой информации; определять степень стойкости паролей; применять системы анализа защищенности; системы анализа рисков
Владеть:	
Уровень 1	программным обеспечением сканирования уязвимостей и аудита эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации
Уровень 2	программным обеспечением сканирования уязвимостей и аудита эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; владеть методами сканирования: проверка заголовков, активные зондирующие проверки, имитация атак

Уровень 3	программным обеспечением сканирования уязвимостей и аудита эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения; владеть методами сканирования: проверка заголовков, активные зондирующие проверки, имитация атак; методами и средствами проверки стойкости парольной защиты; программным обеспечением и методиками анализа защищенности распределенных ресурсов; программным обеспечением и методиками анализа рисков
ПК-15.3**:** способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
Знать:	
Уровень 1	принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем
Уровень 2	принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based)
Уровень 3	принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; технологию анализа защищенности распределенных систем обработки информации на сетевом уровне (network-based), уровне операционной системы (host-based) и уровне приложения
Уметь:	
Уровень 1	применять принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем
Уровень 2	применять принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; производить аудит распределенных систем
Уровень 3	применять принципы проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем; производить аудит распределенных систем; анализировать результаты сканирования
Владеть:	
Уровень 1	методиками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем
Уровень 2	методиками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем, аудита распределенных систем
Уровень 3	методиками проведения экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем, аудита распределенных систем; анализа результатов сканирования
ПК-17.4**:** способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
Знать:	

Уровень 1	принципы мониторинга защищенности информации в автоматизированной системе
Уровень 2	принципы мониторинга защищенности информации в автоматизированной системе, выявления каналов утечки информации; механизмы анализа уязвимостей
Уровень 3	принципы мониторинга защищенности информации в автоматизированной системе, выявления каналов утечки информации; механизмы анализа уязвимостей; определять степень риска и вероятность осуществления НСД
Уметь:	
Уровень 1	проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации
Уровень 2	проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; применять сканеры безопасности в пассивном и активном режиме
Уровень 3	проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; применять сканеры безопасности в пассивном и активном режиме; производить аудит информационных систем; анализировать результаты сканирования
Владеть:	
Уровень 1	инструментами мониторинга защищенности информации в автоматизированной системе, средствами выявления каналов утечки информации
Уровень 2	инструментами мониторинга защищенности информации в автоматизированной системе, средствами выявления каналов утечки информации; сканерами безопасности информационных систем
Уровень 3	инструментами мониторинга защищенности информации в автоматизированной системе, средствами выявления каналов утечки информации; сканерами безопасности информационных систем; средствами аудит информационных систем
ПК-23.4**:** способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	
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-24.5**:** 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-25.3**:** 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;
Уровень 2	способы применения средств и систем защиты информационно-технологических ресурсов автоматизированной системы; способы восстановление ресурсов автоматизированной системы работоспособности при возникновении нештатных ситуаций;
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;
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;

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-26.3**:** способностью администрировать подсистему информационной безопасности автоматизированной системы	
Знать:	
Уровень 1	способы администрирования подсистем информационной безопасности;
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	способами администрирования средств защиты информации;
Уровень 2	способами, механизмами администрирования средств защиты информации
Уровень 3	способами, механизмами администрирования средств защиты информации и средств, встроенных в ОС
ПК-27.1**:** способностью выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы	
Знать:	
Уровень 1	виды политик безопасности
Уровень 2	виды политик безопасности, способы мониторинга
Уровень 3	виды политик безопасности, способы мониторинга и аудита
Уметь:	
Уровень 1	настраивать механизмы политик безопасности
Уровень 2	настраивать механизмы политик безопасности, способы мониторинга
Уровень 3	настраивать механизмы политик безопасности, способы мониторинга и аудита в
Владеть:	
Уровень 1	механизмами администрирования, встроенными в ОС

Уровень 2	механизмами администрирования, контроля, встроенными в ОС
Уровень 3	механизмами администрирования, контроля, управления встроенными в ОС
ПК-28.3**:** способностью управлять информационной безопасностью автоматизированной	
Знать:	
Уровень 1	способы управления информационной безопасностью автоматизированной систе-
Уровень 2	способы и механизмы управления информационной АС
Уровень 3	способы и механизмы управления и контроля информационной безопасностью АС
Уметь:	
Уровень 1	применять способы управления информационной безопасностью АС
Уровень 2	применять способы и механизмы управления информационной безопасностью автоматизированной системы АС
Уровень 3	применять способы и механизмы управления и контроля информационной безопасностью АС
Владеть:	
Уровень 1	способами управления информационной безопасностью автоматизированной си-
Уровень 2	способами, механизмами управления информационной безопасностью АС
Уровень 3	способами, механизмами управления информационной безопасностью АС
ПК-11.1**:** способностью разрабатывать политику информационной безопасности автоматизированной системы	
Знать:	
Уровень 1	политику информационной безопасности автоматизированной системы (АС)
Уровень 2	политику и модели информационной безопасности АС
Уровень 3	политику и модели информационной безопасности АС предприятия
Уметь:	
Уровень 1	разрабатывать политику информационной безопасности АС
Уровень 2	разрабатывать политику и модели информационной безопасности АС
Уровень 3	разрабатывать политику и модели информационной безопасности АС предприятия
Владеть:	
Уровень 1	способностью разрабатывать политику информационной безопасности АС
Уровень 2	способностью разрабатывать и модели политику информационной безопасности
Уровень 3	способностью разрабатывать политику информационной безопасности АС предприятия

Таблица 2 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	- методы и средства ограничения доступа к компонентам ВС; - методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям; - методы и средства хранения ключевой информации; - задачи и технологию сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности; - способы встраивания средств защиты в программное обеспече-

	ние; - цели и задачи защиты информации в сетях передачи данных; - основные нормативные правовые акты и методические документы по защите от НСД.
уметь	- организовывать защиту программ от изучения; - производить защиту от разрушающих программных воздействий; - производить защиту программ от изменений; - осуществлять контроль целостности программ и построение изолированной программной среды.
владеть	- средствами контроля информационной целостности; - средствами защиты автоматизированного комплекса от несанкционированного доступа; - средствами борьбы с вирусами и вредоносными закладками.

2. Перечень оценочных средств для проведения поэтапной аттестации обучающихся

В перечень оценочных средств **по данной дисциплине** входят:
- опрос на занятиях,
- выполнение лабораторных работ,
- курсовой проект,
- зачет
- 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
ОПК-8.17	+	+	+	+	+	+	+	+	+	+	+
ПК-1.15	+	+	+	+	+	+	+	+	+	+	+
ПК-3.10	+	+	+	+	+	+	+	+	+	+	+
ПК-4.4	+	+	+	+	+	+	+	+	+	+	+
ПК-5.2	+	+	+	+	+	+	+	+	+	+	+
ПК-6.6	+	+	+	+	+	+	+	+	+	+	+
ПК-11.1	+	+	+	+	+	+	+	+	+	+	+
ПК-14.4	+	+	+	+	+	+	+	+	+	+	+
ПК-15.3	+	+	+	+	+	+	+	+	+	+	+
ПК-17.4	+	+	+	+	+	+	+	+	+	+	+
ПК-23.4	+	+	+	+	+	+	+	+	+	+	+
ПК-24 .5	+	+	+	+	+	+	+	+	+	+	+
ПК-25.3	+	+	+	+	+	+	+	+	+	+	+
ПК-26.3	+	+	+	+	+	+	+	+	+	+	+
ПК-27.1	+	+	+	+	+	+	+	+	+	+	+
ПК-28.3	+	+	+	+	+	+	+	+	+	+	+

Знак «+» означает выполненный этап

2.1 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: 1-18	Этапы: 1 - 9	Этапы: 1-18
	Опрос	Зачет (вопросы)	Экзамен (вопросы)
ОПК-8.17	+	+	+
ПК-1.15	+	+	+
ПК-3.10	+	+	+
ПК-4.4	+	+	+
ПК-5.2	+	+	+
ПК-6.6	+	+	+
ПК-11.1	+	+	+
ПК-14.4	+	+	+
ПК-15.3	+	+	+
ПК-17.4	+	+	+
ПК-23.4	+	+	+
ПК-24 .5	+	+	+
ПК-25.3	+	+	+
ПК-26.3	+	+	+
ПК-27.1	+	+	+
ПК-28.3	+	+	+

3. Критерии оценивания уровня освоения обучающимися компетенций

3.1 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	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«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 разде-	Четко отвечает на вопросы, может точно изобразить графическую часть пройденного материала, увязывает последовательность изучен-

		лами изучаемой дисциплины.	ных разделов дисциплины.

Таблица 6. Шкала оценок уровня освоения дисциплины по зачету

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Правильные ответы даны менее чем на 50% включительно. Материал излагается непоследовательно, сбивчиво, не представляет определенной системы знаний по дисциплине. Имеются заметные нарушения норм литературной речи.	Правильные ответы даны на 51-64% вопросов. Допускаются нарушения в последовательности изложения. Демонстрируются поверхностные знания вопроса. Имеются затруднения с выводами. Допускаются нарушения норм литературной речи.	Правильные ответы даны на 65-94% вопросов. Ответы на поставленные вопросы излагаются систематизировано и последовательно. Материал излагается уверенно. Демонстрируется умение анализировать материал, однако не все выводы носят аргументированный и доказательный характер. Соблюдаются нормы литературной речи.	Правильные ответы даны на 95-100% вопросов. Ответы на поставленные в билете вопросы излагаются логично, последовательно и не требуют дополнительных пояснений. Делаются обоснованные выводы. Демонстрируются глубокие знания предмета. Соблюдаются нормы литературной речи.

Таблица 7. 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 8. 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 9. 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 зачету:

1. Надежность информации.
2. Интегральная информационная безопасность.
3. Основные этапы жизненного цикла информации.
4. Элементы информационной базы АСОД.
5. Уязвимость информации.
6. Типовые структурные компоненты АСОД.
7. Типы дестабилизирующих факторов.
8. Причины нарушения целостности информации.

9. Каналы несанкционированного получения информации без доступа нарушителя к элементам ЭВТ, АСОД.
10. Каналы несанкционированного получения информации с доступом нарушителя к элементам АСОД, но без их изменений.
11. Каналы несанкционированного получения информации с доступом нарушителя к элементам АСОД с их изменением.
12. Классификация угроз безопасности.
13. Основные методы защиты информации в вычислительных системах.
14. Общая схема идентификации и установления подлинности пользователя.
15. Метод проверки подлинности на основе простого пароля.
16. Метод проверки подлинности на основе динамически изменяющегося пароля.
17. Организация контроля информационной целостности.
18. Задачи решаемые аппаратными средствами защиты.
19. Классификация аппаратных средств защиты.
20. Классификация программных средств защиты.
21. Виды программных средств защиты.
22. Средства защиты данных.
23. Средства защиты от копирования.
24. Средства защиты информации о разрушения.
25. Концепция диспетчера доступа.

4.2 Вопросы к экзамену:

1. Методы управления безопасностью сетей.
2. Основные требования защиты сетей и возможные им угрозы.
3. Цели и задачи защиты информации в вычислительных сетях.
4. Перечень и содержание сервисов безопасности.
5. Стандарты сервисов безопасности.
6. Классификация видов услуг механизмов защиты.
7. Сущность методов распределения ключей при использовании механизмов цифровой подписи данных, передаваемых в сетях.
8. Основные положения концепции защиты информации в эталонной модели взаимодействия открытых сетей.
9. Назначение, задачи системы защиты СЗИ AURA.
10. Общее содержание функций подсистемы идентификации и аутентификации СЗИ AURA.
11. Общее содержание функций подсистемы разграничения доступа к ресурсам СЗИ AURA.
12. Общее содержание функций подсистемы контроля целостности СЗИ AURA.
13. Общее содержание функций подсистемы регистрации событий СЗИ AURA.
14. Общее содержание функций подсистемы управления средствами защиты (администрирования) СЗИ AURA.
15. Назначение, задачи, классификация межсетевых экранов.
16. Назначение, задачи прокси-серверов.
17. Характеристика систем активного аудита.
18. Технологии и средства защиты процессов переработки информации в Интернете.
19. Основное содержание информационной безопасности в Интранете.
20. Назначение, состав и возможности системы защиты информации Dallas Lock.
21. Назначение, состав и возможности программно-аппаратного комплекса защиты информации Аккорд.
22. Назначение, состав и возможности программно-аппаратного комплекса защиты информации Соболь – PCI.
23. Назначение, состав и возможности программно-аппаратного комплекса защиты информации Страж NT.
24. Назначение, состав и возможности системы защиты Secret Disk.
25. Методы и средства нейтрализации угроз.

26. Основные нормативные правовые документы по информатизации и защите информации.
27. Основные специальные меры по технической защите информации, обрабатываемой средствами вычислительной техники. (Требования ФСТЭК).
28. Основные принципы защиты от НСД.
29. Основные способы и направления обеспечения защиты от НСД.
30. Основная структура и содержание монитора обращений.
31. Основные модели нарушителей в автоматизированных системах.
32. Порядок обеспечения защиты от НСД к ПК при его оставлении без завершения сеанса работы.
33. Классификация вирусов и методов защиты от них.
34. Классы и виды антивирусных программ.
35. Методы выявления программ-шпионов.

4.2 Комплект тестовых заданий

1.	Для определения доступности хоста может использоваться простейшая команда: a) Ping. b) Wing. c) Ps. д) Tasklist.
2.	1) Под угрозой безопасности информации в компьютерной системе (КС) понимают: a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. b) Событие или действие, которое можетвызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.
3.	2) Уязвимость информации — это: 1) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. 2) Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. 3) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.
4.	Среди множества компонентов, образующих СОВ, отсутствуют: a) данные. b) модуль анализа. c) модуль хранения. d) модуль реакции. e) модуль агрегирования.
5.	Укажете два основных метода анализа, связанных с выявлением атак в СОВ : a) сигнатурный метод и метод, связанный с выявлением аномального поведения. b) сигнальный метод и метод, связанный с выявлением аномального поведения. c) сигнатурный и сигнальный методы. d) структурный и сигнальный методы.
6.	В большинстве случаев обычным типом информации, присутствующим в профилях безопасности, не является:

	a) 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. b) параметры выполнения. Профили также могут устанавливаться в зависимости от предполагаемого типа использования ресурсов, которые должна поддерживать данная вычислительная система. c) доступ к ресурсам. Можно создать профили частоты чтения и записи некоторых файлов, числа отказов на запросы. d) правила определения аномалий.
7.	Существуют три причины использования распределенных атак злоумышленником. Какая из перечисленных лишняя: a) сокрытие. b) мощность. c) сбор информации. d) отсутствие последствий после вторжения.
8.	Распределенные атаки затруднительно обнаружить по следующим указанным причинам. Какая из перечисленных лишняя: a) отсутствие корреляции данных. b) скрытые сигнатуры. c) при блокировании источника обнаруженной атаки на межсетевом экране могут быть заблокированы сети, которые должны быть доступны для атакуемых хостов. d) трудно определить истинного нарушителя безопасности. e) наличие доступных эксплоитов.
9.	Укажите тип троянских утилит удаленного администрирования: a) Backdoor. b) Trojan-Clicker. c) Trojan-Downloader. d) Rootkit. e) Trojan-GameThief.
10.	Укажите тип шпионских программы : a) Backdoor. b) Trojan-Spy. c) Trojan-PSW. d) Rootkit. e) Trojan-SMS.
11.	Укажите тип троянских утилит, с помощью которых осуществляется кража паролей : a) Trojan-PSW. b) Trojan-Downloader. c) Rootkit. d) Trojan-GameThief. e) Trojan-Banker.
12.	Укажите тип троянских утилит несанкционированных обращений к интернет-ресурсам: a) Backdoor. b) Trojan-Spy. c) Trojan-Clicker.

	d) Trojan-Downloader. e) Trojan-Mailfinder.
13.	Укажите троянские утилиты сокрытого присутствия в операционной системе: a) Backdoor. b) Trojan-Spy. c) Trojan-Clicker. d) Rootkit. e) Trojan-Mailfinder.
14.	Укажите тип троянских утилит, предназначенных для кражи пользовательской информации, относящейся к сетевым играм: a) Backdoor. b) Trojan-Clicker. c) Trojan-GameThief. d) Trojan-Banker. e) Trojan-Mailfinder.
15.	Укажите тип троянских утилит, предназначенных для кражи пользовательской информации, относящейся к банковским системам: a) Trojan-PSW. b) Trojan-Clicker. c) Trojan-Downloader. d) Trojan-Banker. e) Trojan-SMS.
16.	Укажите тип троянских утилит, предназначенных для несанкционированного пользователем сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику через электронную почту, HTTP, FTP или другими способами: a) Trojan-Clicker. b) Rootkit. c) Trojan-GameThief. d) Trojan-Banker. e) Trojan-Mailfinder.
17.	Укажите тип троянских утилит, предназначенные для несанкционированной пользователем отсылки SMS-сообщений с пораженных мобильных устройств на дорогостоящие платные номера, которые «жестко» записаны в теле вредоносной программы: a) Trojan-PSW. b) Trojan-Downloader. c) Rootkit. d) Trojan-GameThief. e) Trojan-SMS.
18.	Эксплойт – это: a) приложение или последовательность команд, предназначенная для реализации каких-либо уязвимостей операционной системы или специализированного программного обеспечения. b) приложение или последовательность команд, предназначенная для реализации каких-либо задач операционной системы или специализированного программного обеспечения. c) приложение или последовательность команд, предназначенная для реализации каких-либо функций операционной системы или специализированного программного обеспечения.

	d) утилита настройки безопасности операционной системы.

4.4 Перечень примерных тем курсовых работ.

1. Анализ методов и средств анализа защищенности беспроводных сетей.
2. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.
3. Виброакустические средства современных систем обеспечения информационной безопасности.
4. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.
5. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.
6. Средства обеспечения информационной безопасности банков данных.
7. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).
8. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.
9. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.
10. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.
11. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.
12. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.
13. Инструментальные средства анализа рисков информационной безопасности.
14. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.
15. Оценочный анализ методов и средств тестирования системы защиты информации (аудита информационной безопасности).
16. особенности современной технологии защиты программного обеспечения от исследования средствами отладки
17. особенности современной технологии защиты программного обеспечения от исследования средствами декомпилирования
18. Технологии анализа рисков
19. современные технологии построения изолированных сред
20. Аудит безопасности и анализ рисков
21. Анализ защищенности информационной системы
22. Обнаружение атак и управление рисками
23. использование мандатной политики в современных системах защиты информации.
24. Сигнатуры как основной механизм выявления атак
25. использование ролевой политики в современных системах защиты информации.
26. IDS как средство управления рисками . Типовая и оптимальная архитектура системы выявления атак. Стандарты, определяющие правила взаимодействия между компонентами системы выявления атак.

Сведения о ФОС и его согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины «Программно-аппаратные средства обеспечения информационной безопасности»
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 «28» июня 2018 г. № 6)

Председатель методической комиссии _____ Жестовский.А.Г.

Согласовано

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