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 /
21 июня 2018 г.

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

Информационная безопасность автоматизированных информационных систем

вариативной 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 автоматизированных информационных систем» обучающийся должен получить следующие компетенции:

Таблица 1 - Компетенции и уровни их освоения обучающимся

ОК-4.1: способность использовать основы правовых знаний в различных сферах деятельности	
Знать:	
Уровень 1	знать основные руководящие документы РФ в области эксплуатации средств информационной безопасности
Уровень 2	знать основные руководящие документы в области эксплуатации средств информационной безопасности
Уровень 3	знать основные руководящие документы в области эксплуатации средств информационной безопасности, определения угроз и уязвимостей.
Уметь:	
Уровень 1	применять основные руководящие документы РФ в области эксплуатации средств информационной безопасности
Уровень 2	применять основные руководящие документы в области эксплуатации средств информационной безопасности
Уровень 3	применять основные руководящие документы в области эксплуатации средств информационной безопасности, определения угроз и уязвимостей
Владеть:	
Уровень 1	методикой основных руководящие документов РФ в области эксплуатации средств информационной безопасности
Уровень 2	методикой основных руководящие документов в области эксплуатации средств информационной безопасности
Уровень 3	методикой основных руководящие документов в области эксплуатации средств информационной безопасности, определения угроз и уязвимостей.
ПК-3.2: 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 АС
Уровень 3	методики определения рисков информационной системы, выявления возможных каналов НСД, комбинирования средств информационной безопасности, методов оценки качества АС, 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 (АС)
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 (АС); создавать модель нарушителя. проводить вероятностный анализ методов и способов воздействия на АС 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 АС
ПК-4.1**:** 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-11.2**:** 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-17.1**:** способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
Знать:	
Уровень 1	методы инструментального мониторинга защищенности информации
Уровень 2	методы инструментального мониторинга защищенности информации; способы выявления каналов утечки информации
Уровень 3	методы инструментального мониторинга защищенности информации; способы и средства выявления каналов утечки информации
Уметь:	
Уровень 1	проводить инструментальный мониторинг защищенности информации в автоматизированной системе
Уровень 2	проводить инструментальный мониторинг защищенности информации в автоматизированной системе и ОС
Уровень 3	проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации
Владеть:	
Уровень 1	методами инструментального мониторинга защищенности информации
Уровень 2	методами инструментального мониторинга защищенности информации; способами выявления каналов утечки информации
Уровень 3	методами инструментального мониторинга защищенности информации; способами и средствами выявления каналов утечки информации
ПК-24.2**:** 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
ПСК-7.2.2: способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах	
Знать:	
Уровень 1	методики анализа рисков информационной безопасности , способы и методы разработки
Уровень 2	методики анализа рисков информационной безопасности , способы и методы разработки, типы политики безопасности в распределенных информационных систе-
Уровень 3	методики анализа рисков информационной безопасности , способы и методы разработки, типы политики безопасности в распределенных информационных системах, методики разработки политики безопасности в распределенных информационных системах
Уметь:	
Уровень 1	применять методики анализа рисков информационной безопасности , способы и методы разработки
Уровень 2	применять методики анализа рисков информационной безопасности , способы и методы разработки, определять типы политики безопасности в распределенных информационных системах

Уровень 3	применять методики анализа рисков информационной безопасности , способы и методы разработки, определять типы политики безопасности в распределенных информационных системах, применять методики разработки политики безопасности в распределенных информационных системах
Владеть:	
Уровень 1	владеть методиками анализа рисков информационной безопасности
Уровень 2	владеть методиками анализа рисков информационной безопасности, способами и методы разработки, способами внедрения политики безопасности в распределенных информационных системах
Уровень 3	владеть методиками анализа рисков информационной безопасности, способами и методы разработки, способами внедрения политики безопасности в распределенных информационных системах, методиками разработки политики безопасности в распределенных информационных системах

Таблица 2 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	- способы нарушения информационной безопасности при работе автоматизированных систем обработки информации; - определять возможности применения стандартных криптографических решений для зашиты информации; - особенности политики безопасности и способы ее внедрения на предприятии; - методики оценки качества предлагаемых решений в области информационной безопасности.
уметь	- выявлять возможные способы нарушения информационной безопасности при работе автоматизированных систем обработки информации; - определять задачи обеспечения информационной безопасности; - в рамках задач обеспечения информационной безопасности решать вопросы использования средств защиты информации; - определять возможности применения стандартных криптографических решений для зашиты информации; - определять особенности политики безопасности и способы ее внедрения на предприятии; - давать оценку качества предлагаемых решений в области информационной безопасности; - применять системный подход к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс организационных мер.
владеть	- методиками определения задач обеспечения информационной безопасности; - политиками безопасности и способами ее внедрения на предприятии; - методиками оценки качества предлагаемых решений в области информационной безопасности; - применять системный подход к обеспечению информационной безопасности в различных сферах деятельности, включая ком-

	плекс организационных мер.

2. Перечень оценочных средств для проведения поэтапной аттестации обучающихся

В перечень оценочных средств **по данной дисциплине** входят:
- опрос на занятиях,
- выполнение лабораторных работ,
- 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
ОК-4.1	+	+	+	+	+	+	+	+	+
ПК-3.2	+	+	+	+	+	+	+	+	+
ПК-4.1	+	+	+	+	+	+	+	+	+
ПК-11.2	+	+	+	+	+	+	+	+	+
ПК-17.1	+	+	+	+	+	+	+	+	+
ПК-24.2	+	+	+	+	+	+	+	+	+
ПСК-7.2.2	+	+	+	+	+	+	+	+	+

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: 1-9	Этапы: 8
	Опрос/тест	Зачет (вопросы)
ОК-4.1	+	+
ПК-3.2	+	+
ПК-4.1	+	+
ПК-11.2	+	+
ПК-17.1	+	+
ПК-24.2	+	+
ПСК-7.2.2	+	+

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	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 зачету.

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

Таблица 7 - Шкала оценок уровня освоения дисциплины по тесту.

Оценка			
Неудовлетворительный	Пороговый	Углубленный	Продвинутый
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)

Менее 50% правильных ответов.	50-70% правильных ответов.	71-90% правильных ответов.	91-100% правильных ответов.

4. Критерии оценивания для проведения итоговой аттестации

Итоговая аттестация обучающихся проводится **в форме зачета с оценкой**.

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. Сущность, цели и задачи организации защиты информации.
2. Значение основных положений современной теории защиты информации для организации.
3. Значение современной теории систем для организации и обеспечения функционирования АС.
4. Структура угроз для информационных ресурсов АС.
5. Сущность, цели и задачи организации защиты информации.
6. Значение основных положений современной теории защиты информации для организации.
7. Значение современной теории систем для организации и обеспечения функционирования АС.
8. Факторы, оказывающие влияние на организацию защиты АС.
9. Основные принципы организации АС.
10. Роль структуризации объекта в определении требований к защите
11. Основные группы требований к АС.
12. Требования к защите применительно к различным защищаемым элементам АС.
13. Факторы, определяющие состав защищаемой информации.
14. Основные этапы работы по выявлению состава защищаемой информации.
15. Управление рисками.
16. Методы выявления состава защищаемых элементов.
17. Какими факторами определяется состав угроз безопасности предприятия?
18. Какова процедура выявления каналов несанкционированного доступа к информации в АС?
19. Чем определяется состав нарушителей и как осуществляется их категорирование?
20. Каким образом может проводиться оценка степени уязвимости информации в результате действий нарушителей различных категорий?
21. Какие компоненты входят в состав структуры АС?
22. Какие критерии положены в основу классификации каждой группы средств, входящих в состав АС?
23. Какие требования предъявляются к выбору методов и средств защиты при организации и функционировании АС?
24. Как определяются условия функционирования АС?
25. Определите значение моделирования объектов и процессов защиты АС.
26. Какие компоненты входят в состав информационной модели АС?
27. Каково общее содержание схемы технологического и организационного построения АС?
28. Требования, предъявляемые к сотрудникам, обеспечивающим функционирование АС.

29. Нормативные документы, регламентирующие деятельность и взаимодействие персонала с защищенной АС.
30. Особенности контроля деятельности персонала, связанного с защитой информации.

4.2 Комплект тестовых заданий

1.	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
2.	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
3.	1. Открытой распределенной информационной системой (open distributed information system) называется система: a. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики b. располагающая службами, пользование которыми возможно при использовании специальных синтаксиса и семантики c. располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики d. не располагающая службами, пользование которыми возможно при использовании стандартных синтаксиса и семантики
4.	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
5.	Классами защищённости автоматизированных систем от несанкционированного доступа являются: a) 1Е b) 2А c) 2В d) 3Б
6.	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
7.	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
8.	Методы и средства защиты информации бывают: a) Технические (аппаратные) b) Программные c) Прикладные d) Организационные
9.	Информация по категории доступа классифицируется как: a) Конфиденциальная b) Общедоступная c) Особо конфиденциальная d) Ограниченного доступа
10.	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
11.	Что из перечисленного не является состоянием процесса? a) порождение b) выполнение c) прерывание d) готовность
12.	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
13.	. 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

14.	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
15.	Что такое ACL? a) средство для хранения паролей b) сценарий входа в систему c) список управления доступом d) инструмент мандатного управления доступом в ОС
16.	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
17.	Какова должна быть минимальная длина пароля в случае смены ежеквартально? a) 13 символов b) 12 символов c) 8 символов d) 6 символов
18.	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

Сведения о ФОС и его согласовании

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

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

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности

(протокол от «14» 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./