

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



И.о. декана радиотехнического факультета  
/ В.А. Баженов /  
21.10.2018 г.

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

**Информационная безопасность распределенных информационных систем**

Базовой части образовательной программы  
по специальности

10.05.03 Информационная безопасность автоматизированных систем

специализация программы

«Обеспечение информационной безопасности распределенных информацион-  
ных систем»

Факультет Радиотехнический (РТФ)  
Кафедра информационной безопасности

Калининград  
2018 г.

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

Таблица 1 - Компетенции и уровни их освоения обучающимся

<b>ОПК-8.18:</b> способностью к освоению новых образцов программных, технических средств и информационных технологий	
<b>Знать:</b>	
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
<b>Уметь:</b>	
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
<b>Владеть:</b>	
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.
<b>ПК-1.17:</b> способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке	
<b>Знать:</b>	
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
<b>Уметь:</b>	
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
<b>Владеть:</b>	
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-3.1: способностью проводить анализ защищенности автоматизированных систем	
<b>Знать:</b>	
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
<b>Уметь:</b>	
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
<b>Владеть:</b>	
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 информационной среды КСИБ
ПК-14.1: способностью проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных, криптографических и технических средств защиты информации	
<b>Знать:</b>	
Уровень 1	принципы поиска и определения уязвимостей сетевых ресурсов при установленной защите сетевых ресурсов; принципы проведения аудита систем передачи данных для 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 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 от степени риска и вероятности осуществления НСД

Уровень 3	принципы поиска и определения уязвимостей сетевых ресурсов при установленной защите сетевых ресурсов; принципы проведения аудита систем передачи данных для 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 от степени риска и вероятности осуществления НСД; принципы контроля данных при передаче информации по проводным и беспроводным каналам связи при использовании криптографических протоколов; языки описания уязвимостей и проверок; теоретико-графовые модели комплексной оценки защищенности распределенных ресурсов
<b>Уметь:</b>	
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
<b>Владеть:</b>	
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

<b>ПК-15.4:</b> способностью участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем	
<b>Знать:</b>	
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
<b>Уметь:</b>	
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
<b>Владеть:</b>	
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
<b>ПК-17.5:</b> способностью проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	
<b>Знать:</b>	
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

<b>Уметь:</b>	
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
<b>Владеть:</b>	
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-24.1: способностью обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности	
<b>Знать:</b>	
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
<b>Уметь:</b>	
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
<b>Владеть:</b>	
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-7.1.1: способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах	
Знать:	
Уровень 1	методы разработки и исследования модели информационно-технологических ресурсов
Уровень 2	методы разработки и исследования модели информационно-технологических ресурсов, модели угроз
Уровень 3	методы разработки и исследования модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах
Уметь:	
Уровень 1	разрабатывать и исследовать модели информационно-технологических ресурсов
Уровень 2	разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз
Уровень 3	разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах
Владеть:	
Уровень 1	методами исследования информационно-технологических ресурсов
Уровень 2	методами исследования информационно-технологических ресурсов, методами разработки моделей угроз
Уровень 3	методами исследования информационно-технологических ресурсов, методами разработки моделей угроз и модели нарушителя информационной безопасности в распределенных информационных системах
ПСК-7.4.4: способностью проводить удаленное администрирование операционных систем и систем баз данных в распределенных информационных системах	
Знать:	
Уровень 1	модели политик безопасности
Уровень 2	модели политик безопасности; протоколы и сетевые службы, используемые при организации политики безопасности
Уровень 3	модели политик безопасности; протоколы и сетевые службы, используемые при организации политики безопасности и отладке удаленного соединения: архитектуры распределенных систем; методы доступа операционных систем
Уметь:	
Уровень 1	применять модели политик безопасности в соответствии с предъявляемыми требованиями
Уровень 2	применять модели политик безопасности в соответствии с предъявляемыми требованиями; использовать протоколы и сетевые службы при организации политики безопасности и отладке удаленного соединения



Уровень 3	применять модели политик безопасности в соответствии с предъявляемыми требованиями; использовать протоколы и сетевые службы при организации политики безопасности и отладке удаленного соединения; определять и выстраивать архитектуры распределенных систем; использовать методы доступа операционных систем
Владеть:	
Уровень 1	инструментами настройки политик безопасности
Уровень 2	инструментами настройки политик безопасности; инструментами управления протоколами и сетевыми службами
Уровень 3	инструментами настройки политик безопасности; инструментами управления протоколами и сетевыми службами, используемыми при организации политики безопасности, средствами отладки удаленного соединения
ПСК-7.5.3: способностью координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении	
Знать:	
Уровень 1	особенности координирования деятельности подразделений и специалистов по защите информации в организациях
Уровень 2	особенности и способы координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов
Уровень 3	особенности, методы и способы координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов
Уметь:	
Уровень 1	осуществлять отбор методов и способов координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов
Уровень 2	осуществлять отбор и применять методы координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов
Уровень 3	осуществлять отбор и применять методы и способы координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов
Владеть:	
Уровень 1	методами координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении
Уровень 2	методами и способами координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов
Уровень 3	методами и способами координирования деятельности подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении с учетом специфики сетевой защиты ресурсов

Таблица 2 - Результаты обучения по дисциплине

В результате изучения дисциплины студент должен:	Результаты
знать	<ul style="list-style-type: none"> <li>- концепцию диспетчера доступа;</li> <li>- методы и средства ограничения доступа к ресурсам распределенной ВС;</li> <li>- методы и средства обнаружения уязвимостей распределенной ВС;</li> <li>- методы и средства обнаружения атак на ресурсы распределенной ВС;</li> <li>- методы и средства противодействия атакам на ресурсы распределенной ВС.</li> </ul>
уметь	<ul style="list-style-type: none"> <li>- организовывать защиту распределенной ВС;</li> <li>- производить защиту от атак на ресурсы распределенной ВС;</li> <li>- производить защиту программ от изменений в распределенной ВС;</li> <li>- осуществлять контроль трафика в рамках распределенной ВС.</li> </ul>
владеть	<ul style="list-style-type: none"> <li>- средствами защиты в распределенной ВС от несанкционированного доступа и нарушения функциональности ее подсистем;</li> <li>- средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных.</li> <li>- методикой контроля информационной целостности в распределенной ВС;</li> </ul>

### 1. 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	10	11
ОПК-8.18	+	+	+	+	+	+					
ПК-1.17	+	+	+	+	+	+	+	+	+	+	+
ПК-3.1	+	+	+	+	+	+	+	+	+	+	+
ПК-14.1	+	+	+	+	+	+	+	+	+	+	+
ПК-15.4	+	+	+	+	+	+	+	+	+	+	+
ПК-17.5	+	+	+	+	+	+	+	+	+	+	+
ПК-24.1	+	+	+	+	+	+	+	+	+	+	+
ПСК-7.1.1							+	+	+	+	+
ПСК-7.4.1							+	+	+	+	+
ПСК-7.5.3							+	+	+	+	+

Знак «+» означает выполненный этап

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

Таблица 4 - Шкала формирования компетенций обучающимися

Код компетенции по ФГОС	Форма оценивания	
	Текущий контроль	Итоговая аттестация
	Этапы: 1-11	Этапы: 11
	Опрос	Экзамен (вопросы)
ОПК-8.18	+	+
ПК-1.17	+	+
ПК-3.1	+	+
ПК-14.1	+	+
ПК-15.4	+	+
ПК-17.5	+	+
ПК-24.1	+	+
ПСК-7.1.1	+	+
ПСК-7.4.1	+	+
ПСК-7.5.3	+	+

## 2. Критерии оценивания уровня освоения обучающимися компетенций

### 2.1. Текущий контроль

Фонд оценочных средств для проведения текущего контроля успеваемости включает в себя:

- материалы для проведения текущего контроля успеваемости – варианты заданий;
- перечень компетенций и их элементов, проверяемых на каждом мероприятии текущего контроля успеваемости;
- систему и критерии оценивания по каждому виду текущего контроля успеваемости
- описание процедуры оценивания.

### 3. Текущий контроль в форме опроса.

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

Оценивается:

- полнота усвоения пройденного материала,
- качество изложения пройденного материала (устно и письменно)

Таблица 5 - Шкала оценок уровня усвоения материала обучающимся

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

Таблица 6 - Шкала оценок уровня освоения дисциплины по экзамену.

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

Таблица 7 - Шкала оценок уровня освоения дисциплины по тесту.

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

#### 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. Раскрыть структурные особенности системы обнаружения вторжений
2. Раскрыть особенности защиты интрасетей
3. Раскрыть особенности политики безопасности интрасети
4. Раскрыть особенности сетевого аудита

5. Раскрыть особенности определения места систем обнаружения вторжений в защите ин-трасетей
6. Охарактеризовать особенности функционирования и организации межсетевых экранов
7. Привести порядок развертывания систем обнаружения вторжений
8. Назвать и охарактеризовать методы отражения вторжений
9. Привести классификация методов отражения вторжений
10. Привести причины, способствующие атакам
11. Привести ошибки в программном обеспечении используемые для сетевых атак.
12. Привести особенности конфигурирования системы защиты сети
13. Привести особенности атаки «перехват паролей»
14. Привести особенности атаки «перехват незащищенного трафика»
15. Привести недостатки ос unix и протоколов
16. Привести слабости системных утилит, команд и сетевых служб
17. Раскрыть принципы проведения и указать особенности удаленных атак на интрасети
18. Указать способы проникновения нарушителей в интрасети и проанализировать их
19. Указать типичные сценарии и уровни атак
20. Указать методы, используемые нападающими для сканирование карты сети
21. Указать особенности проведения и блокирования атаки на переполнение буфера и rdist
22. Указать и охарактеризовать нападения с использованием сетевых протоколов
23. Указать особенности проведения и блокирования атаки «летучая смерть»
24. Указать особенности проведения и блокирования атаки «Syn-бомбардировка»
25. Указать особенности проведения и блокирования атаки «спуффинг»
26. Указать особенности «нападений на основе протокола icmp и методы противодействия данным нападениям
27. Указать особенности проведения и блокирования атаки «arp-spoofing»
28. Указать особенности проведения и блокирования атаки «атака ip hijacking»
29. Указать особенности проведения и блокирования атаки XSS-атак
30. Указать особенности проведения и блокирования атаки SQL- инъекций
31. Указать особенности распределенных атак "отказ в обслуживании"
32. Указать особенности обнаружения прослушивающих приложений в Windows XP
33. Раскрыть методы и охарактеризовать средства нейтрализации угрозы атаки.
34. Раскрыть методы управления безопасностью сетей
35. Охарактеризовать основные модели нарушителей.

#### 4.2 Комплект тестовых заданий

1.	Для определения доступности хоста может использоваться простейшая команда: <b>a) Ping.</b> b) Wing. c) Ps. д) Tasklist.
2.	Для определения доступности UDP порта необходимо получить отклик в ответ на посылку UDP пакета соответствующему порту. Если в ответ пришло сообщение ICMP PORT UNREACHEBLE, то: <b>a) соответствующий сервис не доступен.</b> b) соответствующий сервис доступен. c) соответствующий сервис неизвестен. соответствующий сервис известен.
3.	Системы обнаружения вторжений обеспечивают: <b>a) обнаружение внешних нарушителей.</b> b) обнаружение внешних и внутренних нарушителей.

	<p>с) обнаружение внутренних нарушителей. обнаружение вирусных программ.</p>
4.	<p>Среди множества компонентов, образующих СОВ, отсутствуют:</p> <ul style="list-style-type: none"> <li>a) данные.</li> <li>b) модуль анализа.</li> <li>c) модуль хранения.</li> <li>d) модуль реакции.</li> <li>e) <b>модуль агрегирования.</b></li> </ul>
5.	<p>Укажите два основных метода анализа, связанных с выявлением атак в СОВ :</p> <ul style="list-style-type: none"> <li>a) <b>сигнатурный метод и метод, связанный с выявлением аномального поведения.</b></li> <li>b) сигнальный метод и метод, связанный с выявлением аномального поведения.</li> <li>c) сигнатурный и сигнальный методы.</li> <li>d) структурный и сигнальный методы.</li> </ul>
6.	<p>В большинстве случаев обычным типом информации, присутствующим в профилях безопасности, не является:</p> <ul style="list-style-type: none"> <li>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.</li> <li>b) параметры выполнения. Профили также могут устанавливаться в зависимости от предполагаемого типа использования ресурсов, которые должна поддерживать данная вычислительная система.</li> <li>c) доступ к ресурсам. Можно создать профили частоты чтения и записи некоторых файлов, числа отказов на запросы.</li> <li>d) <b>правила определения аномалий.</b></li> </ul>
7.	<p>Существуют три причины использования распределенных атак злоумышленником. Какая из перечисленных лишняя:</p> <ul style="list-style-type: none"> <li>a) сокрытие.</li> <li>b) мощность.</li> <li>c) сбор информации.</li> <li>d) <b>отсутствие последствий после вторжения.</b></li> </ul>
8.	<p>Распределенные атаки затруднительно обнаружить по следующим указанным причинам. Какая из перечисленных лишняя:</p> <ul style="list-style-type: none"> <li>a) отсутствие корреляции данных.</li> <li>b) скрытые сигнатуры.</li> <li>c) при блокировании источника обнаруженной атаки на межсетевом экране могут быть заблокированы сети, которые должны быть доступны для атакуемых хостов.</li> <li>d) трудно определить истинного нарушителя безопасности.</li> <li>e) <b>наличие доступных эксплоитов.</b></li> </ul>
9.	<p><u>Укажите тип троянских утилит удаленного администрирования:</u></p> <ul style="list-style-type: none"> <li>a) <b>Backdoor.</b></li> <li>b) Trojan-Clicker.</li> <li>c) Trojan-Downloader.</li> <li>d) Rootkit.</li> <li>e) Trojan-GameThief.</li> </ul>

10.	<p><u>Укажите тип шпионских программы :</u></p> <ul style="list-style-type: none"> <li>a) Backdoor.</li> <li>b) <a href="#">Trojan-Spy.</a></li> <li>c) <a href="#">Trojan-PSW.</a></li> <li>d) Rootkit.</li> <li>e) Trojan-SMS.</li> </ul>
11.	<p><u>Укажите тип троянских утилит, с помощью которых осуществляется кража паролей :</u></p> <ul style="list-style-type: none"> <li>a) <b>Trojan-PSW.</b></li> <li>b) Trojan-Downloader.</li> <li>c) Rootkit.</li> <li>d) Trojan-GameThief.</li> <li>e) Trojan-Banker.</li> </ul>
12.	<p>Укажите тип троянских утилит несанкционированных обращений к интернет-ресурсам:</p> <ul style="list-style-type: none"> <li>a) Backdoor.</li> <li>b) <a href="#">Trojan-Spy.</a></li> <li>c) <b>Trojan-Clicker.</b></li> <li>d) Trojan-Downloader.</li> <li>e) Trojan-Mailfinder.</li> </ul>
13.	<p>Укажите троянские утилиты сокрытого присутствия в операционной системе:</p> <ul style="list-style-type: none"> <li>a) Backdoor.</li> <li>b) <a href="#">Trojan-Spy.</a></li> <li>c) Trojan-Clicker.</li> <li>d) <b>Rootkit.</b></li> <li>e) Trojan-Mailfinder.</li> </ul>
14.	<p>Укажите тип троянских утилит, предназначенных для кражи пользовательской информации, относящейся к сетевым играм:</p> <ul style="list-style-type: none"> <li>a) Backdoor.</li> <li>b) Trojan-Clicker.</li> <li>c) <b>Trojan-GameThief.</b></li> <li>d) Trojan-Banker.</li> <li>e) Trojan-Mailfinder.</li> </ul>
15.	<p>Укажите тип троянских утилит, предназначенных для кражи пользовательской информации, относящейся к банковским системам:</p> <ul style="list-style-type: none"> <li>a) <a href="#">Trojan-PSW.</a></li> <li>b) Trojan-Clicker.</li> <li>c) Trojan-Downloader.</li> <li>d) <b>Trojan-Banker.</b></li> <li>e) Trojan-SMS.</li> </ul>
16.	<p>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:</p> <ul style="list-style-type: none"> <li>a) Trojan-Clicker.</li> <li>b) Rootkit.</li> <li>c) Trojan-GameThief.</li> <li>d) Trojan-Banker.</li> <li>e) <b>Trojan-Mailfinder.</b></li> </ul>

17.	<p>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:</p> <ul style="list-style-type: none"> <li>a) <a href="#">Trojan-PSW.</a></li> <li>b) Trojan-Downloader.</li> <li>c) Rootkit.</li> <li>d) Trojan-GameThief.</li> <li>e) <b>Trojan-SMS.</b></li> </ul>
18.	<p>Эксплойт – это:</p> <ul style="list-style-type: none"> <li>a) <b>приложение или последовательность команд, предназначенная для реализации каких-либо уязвимостей операционной системы или специализированного программного обеспечения.</b></li> <li>b) приложение или последовательность команд, предназначенная для реализации каких-либо задач операционной системы или специализированного программного обеспечения.</li> <li>c) приложение или последовательность команд, предназначенная для реализации каких-либо функций операционной системы или специализированного программного обеспечения.</li> <li>d) утилита настройки безопасности операционной системы.</li> </ul>
19.	<p>Классификация атак по уровню модели OSI не предполагает:</p> <ul style="list-style-type: none"> <li>a) атаки на физическом уровне.</li> <li>b) атаки на канальном уровне.</li> <li>c) атаки на сетевом уровне.</li> <li>d) атаки на прикладном уровне.</li> <li>e) <b>атаки на сеансовом уровне.</b></li> </ul>
20.	<p>Атаки типа IP-spoofing – это:</p> <ul style="list-style-type: none"> <li>a) атаки на физическом уровне.</li> <li>b) атаки на канальном уровне.</li> <li>c) <b>атаки на сетевом уровне.</b></li> <li>d) атаки на транспортном уровне.</li> </ul>
21.	<p>Атаки «отказ в обслуживании» типа TCP flood, UDP flood - это:</p> <ul style="list-style-type: none"> <li>a) атаки на физическом уровне.</li> <li>b) атаки на канальном уровне.</li> <li>c) атаки на сетевом уровне.</li> <li>d) <b>атаки на транспортном уровне.</b></li> </ul>
22.	<p>Атаки TCP Hijacking - это:</p> <ul style="list-style-type: none"> <li>a) атаки на физическом уровне.</li> <li>b) атаки на канальном уровне.</li> <li>c) атаки на сетевом уровне.</li> <li>d) атаки на транспортном уровне.</li> </ul>
23.	<p>Сканирование с целью выявления открытых портов происходит на:</p> <ul style="list-style-type: none"> <li>a) физическом уровне.</li> <li>b) канальном уровне.</li> <li>c) сетевом уровне.</li> <li>d) <b>транспортном уровне.</b></li> </ul>



24.	Атака ICMP - Redirect – это: a) атаки на физическом уровне. b) атаки на канальном уровне. c) атаки на сетевом уровне. d) атаки на транспортном уровне.
25.	Атака «отказ в обслуживании» типа ICMP flood происходит: a) на физическом уровне. b) на канальном уровне. c) на сетевом уровне. d) на транспортном уровне.
26.	Атака на протоколы маршрутизации происходит: a) на физическом уровне. b) на канальном уровне. c) на сетевом уровне. d) на транспортном уровне. e) на прикладном уровне.
27.	Атака на веб-приложения типа XSS происходит: a) на физическом уровне. b) на канальном уровне. c) на сетевом уровне. d) на транспортном уровне. e) на прикладном уровне.
28.	Атака SQL Injection происходит: a) на физическом уровне. b) на канальном уровне. c) на сетевом уровне. d) на транспортном уровне. e) на прикладном уровне.
29.	Атака IP-spoofing – это: a) подмена реального IP-адреса ложным в отправляемых пакетах. b) добавление реального IP-адреса в отправляемых пакетах. c) расширение реального IP-адреса ложным в отправляемых пакетах. d) извлечение реального IP-адреса в отправляемых пакетах.
30.	Укажите стандартный порт протокола HTTP: a) 80 b) 443 c) 21 d) 23

### Сведения о ФОС и его согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины «Информационная безопасность распределенных информационных систем»

образовательной программы специалитета по специальности

10.05.03 «Информационная безопасность автоматизированных систем»

утвержденной «27» июня 2018 г.

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

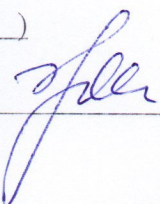
Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности

(протокол от «14» июня 2018 г. № 3 )

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./