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

УТВЕРЖДАЮ
И.о декана РТФ
_____ /Баженов В.А./
27 _____ 2018 г.

Фонд оценочных средств для аттестации по дисциплине

(приложение к рабочей программе дисциплины)

Безопасность сетей электронных вычислительных машин

Базовой части образовательной программы по специальности:

10.05.03 «Информационная безопасность автоматизированных систем ".

(код и наименование специальности)

Специализация программы:

"Обеспечение информационной безопасности распределенных информационных систем".

(наименование специализации)

Факультет радиотехнический (РТФ)

(наименование)

Кафедра информационной безопасности (ИБ)

(наименование)

Калининград 2018

1. Результаты освоения дисциплины

В результате освоения дисциплины «Безопасность сетей электронных вычислительных машин (далее – ЭВМ)» обучающийся должен:

Знать:

- основные направления развития информационно-коммуникационных технологий объекта защиты;
- современные методы и проблемы оценивания угроз безопасности, стандарты информационной безопасности;
- типовые структуры, принципы организации, средства и технологии обеспечения информационной безопасности инфокоммуникационных сетей;
- требования к архитектуре информационных систем и их компонентам для обеспечения безопасности функционирования;
- основные угрозы информационной безопасности и методы противодействия им;
- нормативные документы по метрологии, стандартизации и сертификации программных и аппаратных средств защиты;
- типовые аппаратные и программные средства обеспечения информационной безопасности.

Уметь

- проектировать и администрировать компьютерные телекоммуникационные сети, реализовывать политику безопасности инфокоммуникационных сетей;
- эффективно использовать различные методы и средства защиты информации для инфокоммуникационных сетей;
- проводить мониторинг угроз безопасности инфокоммуникационных сетей и разрабатывать методы;
- применять нормативные документы по метрологии, стандартизации и сертификации на практике.

Владеть:

- навыками разработки, документирования инфокоммуникационных сетей с учетом требований по обеспечению;
- навыками использования аппаратно-программных средств обеспечения безопасности с инфокоммуникационных сетей;
- навыками эксплуатации и администрирования баз данных, локальных компьютерных сетей, программных систем с учетом требований по обеспечению информационной безопасности (в части, касающейся разграничения доступа, аутентификации и аудита).

1.1 Компетенции, формируемые в результате освоения дисциплины

Таблица 1.1 - Компетенции, формируемые в результате изучения дисциплины

Компетенции выпускника ОП ВО и этапы их формирования в результате изучения дисциплины	**Знания, умения и навыки, характеризующие этапы формирования компетенций**
1	2
ОПК-8: способность к освоению новых образцов программных, технических средств и информационных технологий. **Этап 6:** способность к освоению новых образцов программных, технических средств компьютерных систем и средств их защиты.	**Должен знать:** • методы и способы поиска информации и средства их приобретения для формирования представления о проблемной области компьютерных систем, методы поиска информации об актуальных угрозах и средствах защиты информации при построении аппаратной части компьютерных систем; • методы и способы поиска информации и средства их приобретения для формирования представления о проблемной области в смежных областях; методы поиска информации об актуальных угрозах и

	средствах защиты информации. • методы и способы поиска информации и средства их приобретения для формирования представления о проблемной области и способах ее создания с учетом фактора влияния знаний смежных областей науки; методы средства интеллектуального анализа данных. **Должен уметь:** • осуществлять поиск и приобретать новые знания в области компьютерных систем; • осуществлять поиск и приобретать новые знания по предметной области и из смежных областей ИБ, познания для формирования представления о проблемной области ИБ; выявлять наиболее важные для решения поставленных задач факты проблемных и смежных областей знаний; • применять методы и способы поиска информации и средства познания для формирования представления о проблемной области информационной безопасности; выявлять наиболее важные для решения поставленных задач факты проблемных и смежных областей знаний; определять границы проблемной области; определять наиболее эффективные решения в области анализа данных и прогнозирования в области информационной безопасности; использовать методы интеллектуального анализа данных на ЭВМ. **Должен владеть:** • методами и средствами познания, обучения и самоконтроля для приобретения новых знаний и умений, связанных с предметной областью; • методами и средствами познания, связанными с предметной областью: обобщать и систематизировать новые знания в предметной области, используя первоисточники, периодические издания, исследовательские сайты в сети Internet**;** • предметами и объектами в областях науки и техники, непосредственно примыкающих к теории построения и защиты процессорных систем и информационных сетей; способами расчета надежности, эффективности, быстродействия и построения таких систем**.**
ПК-3: способность проводить анализ защищенности автоматизированных систем. Этап 2: способность проводить анализ защищенности сетевого комплекса распределенных информационных систем.	**Должен знать:** • концепцию информационной безопасности распределенных информационных систем**;** • схемы безопасности сетевого комплекса распределенных информационных систем**;** • организацию службы безопасности распределенных информационных систем**.** **Должен уметь:** • учитывать концептуальные положения безопасности распределенных информационных систем в целях анализа безопасности объектов их инфраструктуры; • производить оценку безопасности сетевого комплекса распределенных информационных систем; • планировать структуру службы безопасности вновь вводимых распределенных информационных си-

	стем. **Должен владеть:** • комплексным анализом безопасности распределенных информационных систем; • навыками оценку безопасности сетевого комплекса распределенных информационных систем; • Навыками организации службы безопасности вновь вводимых распределенных информационных систем.
ПК-5: способностью проводить анализ рисков информационной безопасности автоматизированной системы. Этап 1: способностью проводить анализ рисков информационной безопасности сетевого комплекса распределенных информационных систем.	**Должен знать:** • особенности безопасности распределенных информационных систем; • методы оценки угроз безопасности и стандарты информационной безопасности; • методы обеспечения информационной безопасности. **Должен уметь:** • проводить оценку проектных решений распределенных информационных систем на предмет обеспечения их безопасности; • анализировать все угрозы безопасности в соответствии со стандартами информационной безопасности; • анализировать проектные решения систем на соответствие методам обеспечения информационной безопасности. **Должен владеть:** • методами проектирования безопасности распределенных информационных систем; • навыками оценки угроз безопасности в соответствии со стандартами информационной безопасности; • навыками разработки эксплуатационной документации по системам обеспечения информационной безопасности в соответствии с действующими стандартами.
ПК-9: способностью участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности. Этап 2: способностью участвовать в разработке защищенных сетевых комплексов распределенных информационных систем.	**Должен знать:** • типичные атаки на сетевой комплекс распределенных информационных систем: атаки отказа в обслуживании (DDoS), перехват и перенаправление трафика. Средства обеспечения конфиденциальности данных: симметричные и асимметричные криптосистемы; • комплексы вредоносных программ, внедряемых в компьютеры сетевого комплекса автоматизированных систем: троянские программы, сетевые черви, вирусы, шпионские программы, спам; Методы защиты от вирусов; • сетевые экраны и системы обнаружения вторжений. **Должен уметь:** • использовать средства противодействия атакам на сетевой комплекс, применять симметричные и асимметричные алгоритмы шифрования; • использовать методы защиты автоматизированных систем от вирусов и других вредоносных программ; • применять корпоративные и персональные сетевые

	экраны для организации демилитаризованной зоны автоматизированных систем, создавать подсистему защиты сетевого трафика автоматизированной системы на основе компонент протокола защищенного канала IPsec. **Должен владеть:** • инструментальными программами обнаружения атак на сетевой комплекс. Методами проектирования симметричных и асимметричных криптосистем; • способами использования антивирусных программ и инструментами обнаружения нарушений целостности данных; • навыками применения корпоративных и персональных сетевых экранов в автоматизированных системах, проектирования защиты сетевого трафика автоматизированной системы на основе компонент протокола защищенного канала IPsec, а также методологией построения VPN – сети на основе шифрования .
ПК-11: способностью разрабатывать политику информационной безопасности автоматизированной системы. Этап 2: способностью разрабатывать политику информационной безопасности сетевого комплекса распределенных информационных систем.	**Должен знать:** • основные направления развития информационно-коммуникационных технологий объекта защиты, методы и проблемы оценивания угроз безопасности; • основные угрозы информационной безопасности; • основные методы обеспечения информационной безопасности. **Должен уметь:** • анализировать направления развития информационно-коммуникационных технологий объекта защиты, прогнозировать эффективность функционирования систем информационной безопасности, а также применять нормативные документы по метрологии, стандартизации и сертификации на практике; • анализировать угрозы информационной безопасности объектов; • разрабатывать методы противодействия угрозам информационной безопасности объектов. **Должен владеть:** • навыками организации комплекса средств и технологий обеспечения информационной безопасности объектов защиты; • навыками анализа угроз информационной безопасности объектов; • нёавыками разработки соответствующих методов противодействия угрозам информационной безопасности.
ПК-15: Способность участвовать в проведении экспериментально-исследовательских работ при сертификации средств защиты информации автоматизированных систем. Этап 1**:** способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации,	**Должен знать:** • классификацию и характеристики информационных баз и хранилищ информации по сертификации средств защиты информации автоматизированных систем; • информационные базы и хранилища информации по сертификации средств защиты информации АС, порядок обращения к ним и поиска информации;

нормативных и методических материалов в сфере сертификации средств защиты информации автоматизированных систем.	• порядок обработки патентной информации, информации по интеллектуальной собственности. **Должен уметь:** • определить пути получения научно-технической информации, обобщать и систематизировать информацию; • использовать ресурсы информационных баз и хранилищ для поиска, систематизации и обобщения материала в области сертификации средств защиты информации автоматизированных систем; • разрабатывать проекты нормативных материалов, регламентирующих работу по сертификации средств защиты информации, а также положений, инструкций и других организационно-распорядительных документов; проводить патентный поиск по ключевым словам, выявлять аналоги и прототипы, обобщать и систематизировать научную информацию. **Должен владеть:** • навыками систематизации, обобщения справочной, нормативно-технической информации; • навыками поиска, обобщения, систематизации научно-технической информации, составления кратких отчетов, рефератов; • навыками разработки и использования нормативно-методическими материалами по регламентации вопросов сертификации средств защиты информации при построении вычислительных систем.
ПК-19: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы.	**Должен знать:** • современные действующие стандарты информационной безопасности; • вновь вводимые отечественные и международные стандарты информационной безопасности; • правоприменительную практику использования действующих и вновь вводимых стандартов информационной безопасности. **Должен уметь:** • оперировать действующими стандартами информационной безопасности в целях анализа и создания безопасных распределенных информационных систем; • анализировать возможные области применения вновь вводимых отечественных и международных стандартов информационной безопасности; • использовать правоприменительную практику действующих и вновь вводимых стандартов информационной безопасности в целях анализа безопасности инфокоммуникационных сетей. **Должен владеть:** • навыками внедрения на объекты защиты действующих отечественных и международных стандартов; • навыками анализа возможности использования вновь вводимых отечественных и международных стандартов информационной безопасности на объектах защиты; • навыками использования правоприменительной практики действующих и вновь вводимых стандар-

	тов информационной безопасности в целях анализа безопасности объектов инфокоммуникационных сетей.
ПСК-7.2: способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах. Этап 1: способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в сетевом комплексе распределенных информационных систем.	**Должен знать:** • модель угроз сетевой безопасности; • влияние человеческого фактора на сетевую безопасность; • характерные признаки сетевых угроз и атак. **Должен уметь:** • определять характерные угрозы и риски, направленные на нарушение информационной безопасности систем; • разрабатывать политику информационной безопасности на основе базовых принципов; • проводить анализ сетевых угроз и атак. **Должен владеть:** • навыками анализа модели угроз сетевой безопасности; • экономически обоснованными принципами разработки политики информационной безопасности систем; • навыками анализа сетевых угроз и атак.

1.2 Этапы формирования компетенций в результате освоения дисциплины

Таблица 1.2 – Этапы формирования компетенции в результате изучения дисциплины

Этап формирования	Код формируемой компетенции			
	ОПК-8 Этап 6: способность к освоению новых образцов программных, технических средств компьютерных систем и средств их защиты.	**ПК 3 Этап 2:** способность проводить анализ защищенности сетевого комплекса распределенных информационных систем.	**ПК-5 Этап 1**: способностью проводить анализ рисков информационной безопасности сетевого комплекса распределенных информационных систем.	**ПК-9 Этап 2**: способностью участвовать в разработке защищенных сетевых комплексов распределенных информационных систем.
Раздел 1. Проблемы информационной безопасности	+	+	+	+
Раздел 2. Технологии защиты данных	+	+	+	+
Раздел 3. Технологии защиты межсетевого обмена данных	+	+	+	+
Раздел 4. Технологии обнаружения вторжений	+	+	+	+
Раздел 5. Управление сетевой безопасностью	+	+	+	+

Продолжение таблицы 1.2

Этап формирования	Код формируемой компетенции			
	ПК-11Этап 2: способностью разрабатывать политику информационной безопасности сетевого комплекса распределенных информационных систем.	**ПК 15 Этап 1:** способностью осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере сертификации средств защиты информации автоматизированных систем.	**ПК-19**: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью распределенных информационных систем.	**ПСК-7.2 Этап 1**: способностью проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в сетевом комплексе распределенных информационных систем.
Раздел 1. Проблемы информационной безопасности	+	+	+	+
Раздел 2. Технологии защиты данных	+	+	+	+
Раздел 3. Технологии защиты межсетевого обмена данных	+	+	+	+
Раздел 4. Технологии обнаружения вторжений	+	+	+	+
Раздел 5. Управление сетевой безопасностью	+	+	+	+

2. Перечень оценочных средств поэтапного формирования результатов освоения дисциплины

2.1 Текущий контроль

Текущая промежуточная (семестровая) аттестация студентов осуществляется по результатам контроля уровня знаний в ходе проведения лекционных и лабораторных занятий. Промежуточная (семестровая) аттестация проводится в форме устного опроса по лекционному курсу и курсу лабораторных занятий данной дисциплины. Контроль знаний слушателей проводится в виде письменной аттестации в форме теста.

Оценивается:
- полнота усвоения пройденного материала.

Таблица 2.1 - Шкала оценок уровня усвоения материала обучающимся

Неудовлетворительный	Пороговый	Углублённый	Продвинутый
«2» (неудовлетв.)	«3» (удовлетвор.)	«4» (хорошо)	«5» (отлично)
Полнота ответа на вопросы задания менее 50%	Полнота ответа на вопросы задания 50 - 70%	Полнота ответа на вопросы задания 70 - 90%	Полнота ответа на вопросы задания 90-100%

Результаты оценок уровня усвоения учитываются в назначении рейтинговых баллов и оценки по этапам контрольных мероприятий (таблицы 3.1 и 3.2).

Фонд оценочных средств для проведения текущего контроля успеваемости включает в себя варианты вопросов для формирования заданий на тестирование **(ОПК-8, ПК-3, ПК-5, ПК-9, ПК-11, ПК-15, ПК-19, ПСК-7.2)**.

Текущий контроль в форме опроса (тестирования) студентов осуществляется по результатам контроля уровня знаний в ходе проведения лекционных занятий.

2.2 Задания и контрольные вопросы по лабораторным работам

Степень освоения обучающимися компетенций подвергается оценке в ходе проведения лабораторных занятий при защите лабораторных работ из следующего перечня:

1. Лабораторная работа №1 «Организация подсетей. Настройка базовой конфигурации маршрутизатора» (О**ПК-8 этап 6, ПК-9 этап 2**);
2. Лабораторная работа №2 «Угрозы и уязвимости беспроводных сетей» (О**ПК-8.13, ПК-3.7, ПК-11.4, , ПК-19.1, ПСК-7.2.1**);
3. Лабораторная работа №3 «Принципы криптографической защиты информации. Разработка программы вычисления хэш-функции» (О**ПК-8 этап 6, ПК-3 этап 7, ПК-9 этап 2, ПК-19, ПСК-7.2 этап 1**);
4. Лабораторная работа №4 «Аутентификация. Цифровая подпись (ЭЦП). Разработка модели системы формирова-ния и проверки ЭЦП. СКЗИ «ПК «Блокхост ЭЦП 2.0» (ПК «Litoria Desktop»)» (О**ПК-8 этап 6, ПК-3 этап 2, ПК-5 этап 1, ПК-9 этап 2, ПК-11 этап 2, ПК-15 этап 1, ПК-19, ПСК-7.2 Этап 1**);
5. Лабораторная работа №5 «Скрытые каналы утечки информации, механизмы обеспечения целостности данных Falcongaze SecureTower, DALLAS LOCK 8.0-K, С» (О**ПК-8 этап 6, ПК-3 этап 2, ПК-9 этап 2, ПК-19 , ПСК-7.2 этап 1**);
6. Лабораторная работа №6 «Исследование реализации аппаратных и программных средств сетевого экрана» (О**ПК-8 этап 6, ПК-3 этап 2, ПК-9 этап 2, ПК-19 , ПСК-7.2 этап 1**);
7. Лабораторная работа №7 «Сети VPN на основе шифрования» (О**ПК-8 этап 6, ПК-3 этап 2, ПК-9 этап 2, ПК-15 этап 1**);

2.3 Вопросы, выносимые на экзамен (ОПК-8 Этап 6, ПК-3 этап 2, ПК-5 этап 1, ПК-9 этап 2, ПК-11 этап 2, ПК-15 этап 1, ПК-19, ПСК-7.2 этап 1).

3. Оценочные средства поэтапного формирования результатов освоения дисциплины

3.1 Образцы вопросов для формирования заданий на тестирование

Образцы заданий на тестирование

Типовые варианты

Вариант XX

№	Задание		Варианты ответа
1	В каких средствах обеспечения безопасности используется шифрование?	**a** **b** **c** **d** **e** **f**	аутентификация и авторизация; антивирусные системы; защищенный канал; сетевой экран прикладного уровня; фильтрующий маршрутизатор; цифровая подпись
2	Какие из антивирусных методов способны обнаружить еще неизвестный вирус?	**a** **b** **c** **d**	сканирование сигнатур; метод контроля целостности; отслеживание поведения команд; эмуляция тестируемых программ.

3	К числу базовых функций сетевого экрана относятся:	**a** **b** **c** **d** **e** **f** **g**	аудит; шифрование трафика; фильтрация трафика; антивирусная защита; функция прокси-сервера; авторизация; повышение пропускной способности канала.
4	Существует ли угроза похищения пароля при использовании аппаратного ключа?	**a** **b**	да нет (почему?)
5	Справедливо ли утверждение «Поскольку открытый ключ не является секретным, то его не нужно защищать?»	**a** **b**	да нет (почему?)
6	Что содержится в электронном сертификате?	**a** **b** **c** **d**	секретный ключ владельца данного сертификата; данные о владельце сертификата; информация о сертифицирующем центре; зашифрованные открытым ключом сертифицирующего центра данные, содержащиеся в сертификате.
7	Правила доступа узлов сети периметра к ресурсам внутренней сети часто бывают более строгими, чем правила, регламентирующие доступ к этим ресурсам внешних пользователей.		Как вы думаете, почему?
8	Какие из следующих утверждений верны:	**a** **b** **c**	любое приложение после соответствующего конфигурирования имеет возможность работать через прокси-сервер; для работы через прокси-сервер приложение, изначально не рассчитанное на работу через прокси-сервер, требует изменения исходного кода; каждое приложение, построенное в архитектуре клиент-сервер, непременно должно работать через прокси-сервер.
9	Почему в семействе протоколов IPsec функции обеспечения целостности и аутентичности данных дублируются в двух протоколах: AH и ESP?		
10	Отметьте в таблице все возможные комбинации режимов работы протокола IPsec		**Режимы** / *Хост-хост* / *Шлюз-шлюз* / *Хост-шлюз* **Транспортный** **Туннельный**

3.2 Методические материалы, определяющие процедуры использования оценочных средств

Изучение дисциплины «Безопасность сетей ЭВМ» сопровождается рейтинговой системой контроля знаний обучающихся.

3.2.1 Методика подготовки и проведения занятий

Основными видами учебных занятий по дисциплине являются: лекции, лабораторные и самостоятельная работа студентов.
В ходе изучения дисциплины предусматривается применение эффективных методик обучения, которые предполагают постановку вопросов проблемного характера с разрешением их, как непосредственно в ходе занятий, так и в ходе самостоятельной работы.
Изучение разделов 1,2,3,5 сопровождается лабораторными занятиями, в ходе которых происходит закрепление теоретических знаний, формирование и совершенствование умений, навыков и компетенций.
Лабораторные занятия проводятся циклическим методом в специализированной лаборатории. Учебно-лабораторная база для проведения лабораторных занятий обеспечивает экспериментальное подтверждение теоретического материала, рассматриваемого в дисциплине.
Перед началом занятий преподаватель проводит инструктаж по технике электробезопасности и пожарной безопасности.
Формирование знаний обучающихся, по основам безопасности сетей ЭВМ, обеспечивается проведением лекционных занятий в течение шестого семестра обучения. Закрепление теоретических знаний и приобретение умений, навыков и компетенций осуществляется в ходе лабораторных занятий в шестом семестре обучения.
Контроль знаний в ходе изучения дисциплины осуществляется в виде текущих и рубежного контролей, а также итоговой аттестации в форме экзамена.
Текущий и рубежный контроли предназначены для проверки хода и качества усвоения студентами учебного материала и стимулирования учебной работы студентов. Они могут осуществляться в ходе всех видов занятий в форме, избранной преподавателем или предусмотренной рабочей программой дисциплины.
Текущий и рубежный контроли предполагают постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим студентам для самоконтроля на разных этапах обучения. Их результаты учитываются выставлением оценок в журнале учета успеваемости.
Практически на всех занятиях может применяться выборочный контроль, который имеет целью убедиться, в какой степени усвоен материал студентами.
Преподавателем в ходе лекций проверяется, как правило, качество ведения конспектов и выполнение тестовых заданий.
Допуск к экзаменам выдается студенту, имеющему по всем текущим и рубежным контролям за шестой семестр положительные оценки.
Билет на экзамен содержит два теоретических вопроса из тематики разделов по всей дисциплине.
Выбор теоретических вопросов осуществляется из принципа равной сложности всех билетов и наибольшего охвата каждым билетом учебного материала.
Подготовка к экзамену ведется по конспекту лекций, рекомендуемым к изучению в начале курса учебникам и учебным пособиям. В ходе подготовки к экзамену преподаватель проводит консультацию, на которой доводится порядок проведения экзамена и даются ответы на вопросы, вызвавшие наибольшие затруднения у студентов в процессе подготовки.
Экзамен проводится в день, указанный в расписании занятий.
Студент, прибывший для сдачи экзамена, докладывает экзаменатору, принимающему экзамен, сдает ему зачетную книжку, получает экзаменационный билет на бланке установленной формы и занимает указанное ему место для подготовки. После получения билета в

течение 45 минут студент имеет право готовиться к ответу. На ответ по экзаменационному билету отводится до 15 минут.
Готовясь к ответу, студент обязан все доказательства, формулы, принципиальные схемы, графики и т.д. записывать и изображать на полученном листе так, чтобы по письменным записям можно было бы оценить уровень знаний без устных пояснений.
Ответ студента должен быть четким, конкретным и кратким. Об окончании ответа на вопрос аттестуемый докладывает. После ответа преподаватель задает вопросы, помогающие ему выявить ход мыслей студента, логику его рассуждений и способность применять полученные знания в практической деятельности. Если требуется уточнить оценку или степень знаний студента по тому или иному вопросу, задаются дополнительные вопросы.
Во время экзамена должна соблюдаться дисциплина и порядок, разговоры студентов между собой не допускаются. Если во время экзамена у студента возникает необходимость обратиться к преподавателю, то он поднимает руку и просит подойти к нему преподавателя. Кроме авторучки, калькулятора, билета и бланка для ответа на столе не должно быть ничего. Пользоваться конспектами, учебниками, учебными пособиями и иными дополнительными материалами, раскрывающими содержание вопросов, не разрешается.
Студентам, пользующимся на экзамене материалами, различного рода записями, техническими средствами, не указанными в перечне разрешенных, выставляется в ведомости «неудовлетворительно».

3.2.2 Система контроля знаний

Рейтинговая система контроля и оценки знаний обучающихся – это комплекс учебных, организационных и методических мероприятий, направленных на обеспечение систематической творческой работы студентов, повышение самостоятельности и состязательности учебы. Она обеспечивает реализацию принципов обратной связи в процессе учебы и включает в себя:

1. Схему контрольных мероприятий;
2. Критерии оценки знаний, умений и навыков.

Максимальное количество баллов (рейтинг), которое может получить студент, определяется количеством часов, отводимых на изучение данной дисциплины – 216.

Схема контрольных мероприятий приведена в таблице 3.1.
Таблица 3.1 - Схема контрольных мероприятий

Вид контрольного мероприятия	Этапы контрольных мероприятий					
	ТК1*	ТК2	ТК3	РК	ПА	Итого
Экзамены	-	-	-	-	54	54
Лабораторные работы	14	14	14	12	-	54
Посещение занятий	9	9	9	9	-	36
Компонент своевременности	18	18	18	18	-	72
Итого	41	41	41	39	54	216

*ТК – текущий контроль (ТК1-ТК3), включающий тестирование (Таблица 2.1);
РК – рубежный контроль, включающий выполнение индивидуальных письменных тестов;
ПА – промежуточная аттестация по ООП, включающая сдачу экзаменов по дисциплине.

В таблице 3.2 представлено соответствие рейтинговых баллов и оценки по 4-х балльной шкале, выставляемых за каждый этап контрольного мероприятия.
Таблица 3.2 - соответствие рейтинговых баллов и оценки по 4-х балльной шкале

Оценка	Этапы контрольных мероприятий					
	ТК1	ТК2	ТК3	РК	Итого до ПА	ПА
неудовлетворительно	0-23	0-23	0-23	0-22	0-91	0-30
удовлетворительно	24-27	24-27	24-27	23-26	95-107	31-36
хорошо	28-35	28-35	28-35	27-33	111-138	37-46
отлично	36-41	36-41	36-41	34-39	142-162	47-54

Критерии выставления оценок за лабораторные работы:

Оценка «отлично» выставляется, если студент показал глубокие знания и понимание программного материала по теме лабораторной работы, умело увязывает лекционный материал с практикой, грамотно и логично строит ответ на контрольные вопросы.

Оценка «хорошо» выставляется, если студент твердо знает программный материал по теме лабораторной работы, грамотно его излагает, не допускает существенных неточностей в ответе на контрольные вопросы. Правильно применяет полученные знания при решении практических вопросов.

Оценка «удовлетворительно» выставляется, если студент имеет знания только основного материала по поставленным контрольным вопросам, но не усвоил его деталей, для принятия правильного решения требует наводящих вопросов, допускает отдельные неточности или недостаточно четко излагает учебный материал по теме лабораторной работы.

Оценка «неудовлетворительно» выставляется, если студент допускает грубые ошибки в ответе на контрольные вопросы, не может применять полученные знания на практике.

4 Перечень типовых вопросов, выносимых на экзамен по дисциплине «Безопасность сетей ЭВМ»

ФГБОУ ВО «КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
БАЛТИЙСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ РЫБОПРОМЫСЛОВОГО ФЛОТА

Вопросы на экзамен

Дисциплина:	Безопасность сетей ЭВМ	Специальность:	10.05.03
Семестр:	VI		
Кафедра:	Информационная безопасность		

1.	Сетевое ПО. Назначение, принцип работы.
2.	Сетевая операционная система
3.	Активные атаки. Определение, краткий обзор видов активных атак.
4.	Пассивные атаки. Определение, краткий обзор видов пассивных атак
5.	Межсетевой экран. Назначение, виды межсетевых экранов.
6.	Межсетевой экран канального уровня. Назначение, принцип работы.
7.	Межсетевой экран сетевого уровня. Назначение, принцип работы.

8.	Межсетевые экраны сеансового и прикладного уровней. Назначение, принцип работы.
9.	Прокси сервер. Назначение, виды. Принцип работы.
10.	Вредоносное ПО. Определение, типы вредоносных ПО.
11.	Компьютерные вирусы. Определение, виды.
12.	Пути заражения компьютерными вирусами. Признаки заражения компьютерными вирусами.
13.	Антивирусные программы. Назначение, методы защиты от вирусов.
14.	Сканирование сигнатур. Назначение, принцип работы.
15.	Эвристический анализ. Назначение, принцип работы.
16.	Идентификация. Назначение, сущность.
17.	Аутентификация. Назначение, сущность.
18.	Авторизация. Назначение, сущность.
19.	Модели информационной безопасности. Определение, назначение. Модель КЦД.
20.	Модели информационной безопасности. Определение, назначение. Гексада Паркера.
21.	Модели информационной безопасности. Определение, назначение. Модель STRIDE
22.	Уязвимость. Определение, сущность.
23.	Угроза. Определение, сущность.
24.	Атака. Определение, сущность.
25.	Средства защиты от информационных угроз. Уровни ИБ. Законодательный уровень. Определение, сущность.
26.	Средства защиты от информационных угроз. Уровни ИБ. Административный уровень. Определение, сущность.

27.	Средства защиты от информационных угроз. Уровни ИБ. Процедурный уровень. Определение, сущность.
28.	Средства защиты от информационных угроз. Уровни ИБ. Программно-технический уровень. Определение, сущность.
29.	Средства защиты от информационных угроз. Политика безопасности.
30.	Безопасность операционных систем. Угрозы. Защищённая операционная система.
31.	Защита на канальном уровне. Протоколы.
32.	Защита на сетевом уровне. Протоколы.
33.	VPN. Назначение. Принцип работы.
34.	Клиентский VPN.
35.	Операторский VPN.
36.	Вирус. Определение, сущность.
37.	Root Kit. Определение, сущность.
38.	Червь. Определение, сущность.
39.	Шпионские программы. Определение, сущность.
40.	Эксплойт. Определение, сущность
41.	Классификация источников угроз ИБ.
42.	DoS атака.
43.	DDoS атака.
44.	PPTP протокол. Назначение, сущность.
45.	L2TP протокол. Назначение, сущность.

46.	Протокол IPSec. Назначение, сущность.
47.	Типичные атаки на ОС.
48.	Защищённая ОС. Объект доступа, определение, сущность
49.	Защищённая ОС. Субъект доступа, определение, сущность
50.	Защищённая ОС. Метод доступа, определение, сущность

Вопросы рассмотрены и утверждены на заседании кафедры	Дата: __.__. __ г.	Протокол № __
Заведующий кафедрой	подпись	Великите Н.Я.

Формат сведений о ФОС и ее согласовании

Фонд оценочных средств для аттестации по дисциплине представляет собой приложение к рабочей программе дисциплины

Безопасность сетей электронных вычислительных машин
(наименование дисциплины)

образовательной программы специалитета по специальности
10.05.03 Информационная безопасность автоматизированных систем
(код и наименование специальности)

утвержденной 27 июня 2018 г.

Автор фонда, представитель работодателя, директор ООО «Технологии комфорта»_____Старикович В.С.

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности
(протокол № 9 от 14 июня 2018 г.)

Заведующий кафедрой _____ /Н.Я. Великите/

Фонд оценочных средств рассмотрен и одобрен на заседании методической комиссии радиотехнического факультета
(протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ /А.Г. Жестовский/

Согласовано
начальник отдела
мониторинга и контроля _____ /Ю.В. Борисевич/