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
_____/Баженов В.А./
_____2018 г.

Рабочая программа дисциплины
БЕЗОПАСНОСТЬ СЕТЕЙ ЭЛЕКТРОННЫХ ВЫЧИСЛИТЕЛЬНЫХ МАШИН
(наименование дисциплины)
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 Цель освоения дисциплины

Целью освоения дисциплины «Безопасность сетей электронных вычислительных машин (далее ЭВМ)» является формирование у обучаемых профессиональных компетенций в эксплуатационно-технической и научно-исследовательской областях профессиональной деятельности в соответствии с ОП специальности 10.05.03 – «Информационная безопасность автоматизированных систем», которая достигается:

- изучением базовой инфраструктуры инфокоммуникационных сетей, основных устройств и систем, требований к обеспечению информационной безопасности, соответствующих стандартов, технических спецификаций, протоколов и технологий;
- изучением основных угроз в сетях ЭВМ и методов противодействия им;
- овладением механизмами построения систем безопасности сетей ЭВМ;
- овладением навыками по использованию компонентов защищенных сетей ЭВМ, способностью разрабатывать модели угроз и модели нарушителей ИБ на основе исходных данных о сети;
- приобретением навыков проектирования, построения, обслуживания (эксплуатации) и анализа защищенных сетей ЭВМ.

2 Результаты освоения дисциплины

Таблица 2.1 – 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**.**
<u>ПК-3</u>: 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 систем. **Должен владеть:** • комплексным анализом безопасности распределенных информационных систем; • навыками оценку безопасности сетевого комплекса распределенных информационных систем**;** • Навыками организации службы безопасности вновь вводимых распределенных информационных си-

	стем.
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 защищенно-

	го 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, нормативных и методических материалов в сфере сертификации средств защиты информации автоматизированных	**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; • порядок обработки патентной информации, информации по интеллектуальной собственности. **Должен уметь:**

систем.	• 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 стандартов 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.

3 Место дисциплины в структуре образовательной программы

Дисциплина Б1.Б.22 «Безопасность сетей электронных вычислительных машин» относится к базовой части Блок 1. «Дисциплины (модули)» ОП ВО.

Для успешного освоения данной дисциплины студентам требуются знания по дисциплинам: «Алгебра и геометрия», «Математический анализ», «Математическая логика и теория алгоритмов», «Теория информации», «Информатика», «Языки программирования», «Основы информационной безопасности», «Организация ЭВМ и вычислительных систем».

Знания, умения и навыки, полученные студентами в результате изучения дисциплины «Безопасность сетей ЭВМ», необходимы для успешного освоения следующих дисциплин: «Разработка и эксплуатация защищенных автоматизированных систем», «Безопасность систем баз данных».

4 Содержание дисциплины

Раздел 1. Проблемы информационной безопасности

Тема 1. Общие принципы построения сетей . Сетевое ПО. Сетевые интерфейсы. Доступ к периферийным устройствам через сеть.

Коммутация каналов и пакетов. Передача с установлением логического соединения. Ethernet – технология коммутации пакетов.

Тема 2. Организация и функционирование сетей.

Сетевые стандарты. Инкапсуляция данных. Системы клиент-сервер, одно ранговые сети, локальные и глобальные сети. Модель корпоративной сети. Особенности безопасности инфокоммуникационных сетей.

Основные понятия и анализ угроз информационной безопасности.

Тема 3. Введение в сетевой информационный обмен. Использование сети интернет. Модель ISO/OSI и стек протоколов TCP/IP.
Анализ угроз сетевой безопасности. Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей.
Тема 4. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблемы защиты информации в сетях.
Политика безопасности. Основные понятия. Структура политики безопасности. Процедуры безопасности.
Тема 5. Стандарты информационной безопасности.

Раздел 2. Технологии защиты данных
Тема 6.Принципы криптографической защиты информации.
Технологии аутентификации
Тема 7. Строгая аутентификация
Биометрическая аутентификация

Раздел 3. Технологии защиты межсетевого обмена данных
Тема 8. Обеспечение безопасности операционных систем. Угрозы безопасности ОС. Понятие защищённой ОС.
Архитектура подсистемы защиты ОС. Основные функции подсистемы защиты ОС.
Тема 9. Технологии межсетевых экранов. Фильтрация трафика. Дополнительные возможности МЭ.
Особенности функционирования МЭ. Проблемы безопасности МЭ.
Тема 10. Основы технологии VPN. Концепция построения. Основные понятия и функции.
Средства обеспечения безопасности VPN. VPN решения для построения защищённых сетей.
Тема 11. Защита на канальном уроне. Протоколы формирования защищённых каналов на канальном уровне.
Защита на сеансовом уровне. Протоколы формирования защищённых каналов на сеансовом уровне.
Тема 12. Защита на сетевом уровне. Протокол IPSEC.
Протокол аутентифицирующего заголовка AH. Алгоритмы аутентификации IPSec.
Тема 13. Протокол управления криптоключами IKE. Установление безопасной ассоциации SA.
Особенности реализации средств IPSec. Преимущества и средства безопасности.
Тема 14. Инфраструктура защиты на прикладном уровне. Управление идентификацией и доступом. Функционирование системы управления доступом.
Централизованный контроль удалённого доступа.

Тема 15. Управление доступом по схеме однократного входа с авторизацией SSO.
Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.

Раздел 4. Технологии обнаружения вторжений
Тема 16. Анализ защищённости и обнаружение атак. Концепция адаптивного управления безопасностью.
Технология анализа защищённости. Средства анализа защищённости сетевых протоколов и сервисов. Средства анализа защищённости операционных систем.
Тема 17. Технологии обнаружения атак. Методы реагирования.
Защита от вирусов.

Раздел 5. Управление сетевой безопасностью

Тема 18. Методы управления средствами сетевой безопасности. Задачи управления системой сетевой безопасности.
Архитектура управления средствами сетевой безопасности
Тема 19. Функционирование системы управления средствами безопасности. Аудит и мониторинг безопасности.

5 Объем и структура дисциплины. Форма аттестации по ней

Таблица 5.1 – Структура дисциплины

Номер и наименование раздела, темы	**Объем учебной работы (час.)**					
	Лекции	**ЛЗ**	**ПЗ**	**СРС**	**Контроль**	**Всего**
Семестр – 6 (6 ЗЕТ, 216 час. Из них контроль: 36 час.)						
Раздел 1. Проблемы информационной безопасности	**9**	**14**		**24**	**5**	**52**
Тема 1. Общие принципы построения сетей . Сетевое ПО. Сетевые интерфейсы. Доступ к периферийным устройствам через сеть. Коммутация каналов и пакетов. Передача с установлением логического соединения. Ethernet – технология коммутации пакетов.	2				1	3
Тема 2. Организация и функционирование сетей. Сетевые стандарты. Инкапсуляция данных. Системы клиент-сервер, одно ранговые сети, локальные и глобальные сети. Модель корпоративной сети. Особенности безопасности инфокоммуни-	2	6		10	1	19

кационных сетей. Основные понятия и анализ угроз информационной безопасности.						
Тема 3. Введение в сетевой информационный обмен. Использование сети интернет. Модель ISO/OSI и стек протоколов TCP/IP. Анализ угроз сетевой безопасности. Проблемы безопасности IP-сетей. Угрозы и уязвимости проводных корпоративных сетей. Угрозы и уязвимости беспроводных сетей	2	8			1	11
Тема 4. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблемы защиты информации в сетях. Политика безопасности. Основные понятия. Структура политики безопасности. Процедуры безопасности.	2				1	3
Тема 5. Стандарты информационной безопасности.	1			14	1	16
Раздел 2. Технологии защиты данных	**4**	**16**		**28**	**2**	**50**
Тема 6.Принципы криптографической защиты информации. Технологии аутентификации.	2	8		14	1	25
Тема 7. Строгая аутентификация. Биометрическая аутентификация.	2	8		14	1	25
Раздел 3. Технологии защиты межсетевого обмена данных	**16**	**16**		**24**	**7**	**63**
Тема 8 Обеспечение безопасности операционных систем. Угрозы безопасности ОС. Понятие защищённой ОС. Архитектура подсистемы защиты ОС. Основные функции подсистемы защиты ОС.	2				1	3
Тема 9. Технологии межсетевых экранов. Фильтрация трафика. Дополнительные возможности МЭ. Особенности функционирования МЭ. Проблемы безопасности МЭ.	2	8		10	1	21
Тема 10. Основы технологии VPN. Концепция построения. Основные	2				1	3

понятия и функции. Средства обеспечения безопасности VPN. VPN решения для построения защищённых сетей.						
Тема 11. Защита на канальном уроне. Протоколы формирования защищённых каналов на канальном уровне. . Защита на сеансовом уровне. Протоколы формирования защищённых каналов на сеансовом уровне.	2				1	3
Тема 12. Защита на сетевом уровне. Протокол IPSEC. Протокол аутентифицирующего заголовка AH. Алгоритмы аутентификации IPSec.	2			14	1	17
Тема 13. Протокол управления криптоключами IKE. Установление безопасной ассоциации SA. Особенности реализации средств IPSec. Преимущества и средства безопасности	2				1	3
Тема 14. Инфраструктура защиты на прикладном уровне. Управление идентификацией и доступом. Функционирование системы управления доступом. Централизованный контроль удалённого доступа.	2					2
Тема 15. Управление доступом по схеме однократного входа с авторизацией SSO. Протокол Kerberos. Инфраструктура управления открытыми ключами PKI.	2	8			1	11
Раздел 4. Технологии обнаружения вторжений	**4**			**14**	**1**	**19**
Тема 16. Анализ защищённости и обнаружение атак. Концепция адаптивного управления безопасностью. Технология анализа защищённости. Средства анализа защищённости сетевых протоколов и сервисов. Средства анализа защищённости операционных систем.	2					2
Тема 17. Технологии обнаружения атак. Методы реагирования. Защита	2			14	1	17

от вирусов.						
Раздел 5. . Управление сетевой безопасностью	**3**	**8**			**1**	**12**
Тема 18. Методы управления средствами сетевой безопасности. Задачи управления системой сетевой безопасности. Архитектура управления средствами сетевой безопасности.	2	8			1	11
Тема 19. Функционирование системы управления средствами безопасности. Аудит и мониторинг безопасности	1					1
Подготовка к лабораторным занятиям, оформление отчётов					7	7
Подготовка сообщений, докладов, рефератов, презентаций по вопросам, вынесенным на самостоятельную проработку (по заданию преподавателя)					7	7
Подготовка к сдаче и сдача экзамена по дисциплине					6	6
Итого по дисциплине	**36**	**54**	**0**	**90**	**36**	**216**
	90					

Интерактивные часы: 24 час.

6 Лабораторные работы

Таблица 6.1 – Лабораторные работы по очной форме обучения

Номер ЛР	Номер темы дисциплины	Наименование ЛР	Кол-во часов ЛЗ
Семестр – 6 (весенний)			
1	2	Организация подсетей. Настройка базовой конфигурации маршрутизатора.	6
2	3	Угрозы и уязвимости беспроводных сетей	8
3	6	Принципы криптографической защиты информации. Разработка программы вычисления хэш-функции.	8
4	7	Аутентификация. Цифровая подпись (ЭЦП). Разработка модели системы формирования и проверки ЭЦП. СКЗИ «ПК «Блокхост ЭЦП 2.0» (ПК «Litoria Desktop»)	8
5	8	Скрытые каналы утечки информации, механизмы обеспечения целостности данных Falcongaze SecureTower DALLAS LOCK 8.0-K, C	8
6	9	Исследование реализации аппаратных и программных средств сетевого экрана.	8

7	15	Сети VPN на основе шифрования.	8
Всего			**54**

7 Практические занятия

Практические занятия не предусмотрены.

8 Самостоятельная работа студента

Таблица 8.1 – Самостоятельная работа студента

№	Вид (содержание) СРС, номер темы	Кол-во часов СРС	Форма контроля, аттестации
Семестр – 6 (весенний)			
1	**Тема СРС** включает в себя следующие учебные вопросы по **теме 2**: • сетевые стандарты, инкапсуляция данных; • системы клиент-сервер; • одноранговые сети; • локальные и глобальные сети; • модель корпоративной сети; • особенности безопасности инфокоммуникационных сетей.	10	Конспект лекций, устный опрос
2	**Тема СРС** включает в себя следующие учебные вопросы по **теме 5**: • нормативные документы, действующие в РФ, по метрологии, стандартизации и сертификации программных и аппаратных средств защиты.	14	Конспект лекций, устный опрос
3	**Тема СРС** включает следующие учебные вопросы по **теме 6**: • одна из разновидностей стандарта SHA на основе упрощенного варианта хэш-функции.	14	Конспект лекций, устный опрос
4	**Тема СРС** включает следующие учебные вопросы по **теме 7**: • схема использования сертификатов; • организация сертифицирующих центров; • инфраструктура аутентификации с открытым ключом; • аутентификация программных кодов.	14	Конспект лекций, устный опрос
5	**Тема СРС** включает следующие учебные вопросы по **теме 9**: • организация сети демилитаризованной зоны (DMZ) на базе компьютера и внутреннего маршрутизатора; • организация сетевого экрана на базе прокси-сервера; • организация прокси-серверы прикладного уровня и уровня соединений.	10	Конспект лекций, устный опрос
6	**Тема СРС** включает следующие учебные	14	Конспект лекций,

	вопросы по **теме 12**: • протоколы AH и ESP; • использование баз данных SPD и SAD для защиты сетевого трафика в технологии IPSec.		устный опрос
7	**Тема СРС** включает следующие учебные вопросы по **теме 17**: • троянские программы; • сетевые черви; • вирусы; • шпионские программы; • спам.	14	Конспект лекций, устный опрос
Всего в семестре		**90**	

9 Учебная литература и учебно-методическое обеспечение самостоятельной работы

9.1. Основная литература

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие / В. Г. Олифер, Н. А. Олифер . - 3-е изд. - СПб. : Питер, 2008. - 958 с. : ил. - (Учебник для вузов). - Библиогр.: с. 919-921. - Алф. указ.: с. 922-957. - ISBN 9785469005049 (5 экз.)
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В. Ф. Шаньгин. - М. : ИД "Форум" : ИНФРА-М, 2013. - 416 с. : ил. - (Профессиональное образование). - Библиогр.: с. 401-408. - ISBN 978-5-8199-0331-5. - ISBN 978-5-16-003132-3 : (20 экз.)
3. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях [Электронный ресурс] : учебное пособие / В. Ф. Шаньгин. - М. : ДМК Пресс, 2012. - 592 с. : ил. - ISBN 978-5-94074-637-9
4. Шаньгин, В. Ф. Защита компьютерной информации. Эффективные методы и средства : учебное пособие / В. Ф. Шаньгин. - М. : ДМК Пресс, 2008. - 544 с. : ил. - (Администрирование и защита). - Библиогр.: с. 524-529. - Предм. указ.: с. 530-542. - ISBN 5-94074-383-8 : 468.00 р. (15 экз.)

9.2. Дополнительная литература

1. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие / В. Г. Олифер ; авт. Олифер Н.А. - 2-е изд. - СПб. : Питер, 2003. - 864 с. : ил. - ISBN 5947234785 : (30 экз.).
2. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы : учебник / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2001. - 672 с. : ил. - Библиогр.: с. 641-642. - Алф. указ.: с. 643-668. - ISBN 5804601334 : (71 экз.)

10 Информационные технологии, программное обеспечение и Интернет-ресурсы дисциплины

Программное обеспечение

1. Средство разработки программ с использованием библиотеки Socket. Например, MS Visual Studio с библиотекой WinSock.
2. Программные анализаторы протоколов. Например: WireShark, Iris, Ethereal.
3. Свободно распространяемое средство обнаружения вторжений Snort или другое IDS.
4. Свободно распространяемый пакет IPTABLES в составе Linux или другой МСЭ.
5. Средство построения виртуальных ПЭВМ. Например: VMWare или аналогичный

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины:
http://bgarf.ru/academy/biblioteka/elektronnyj-katalog/ - электронный каталог библиотеки БГАРФ
ЭБС «КГТУ» http://www.klgtu.ru/library/
Университетская библиотека Online (г.Москва) https://biblioclub.ru/
Редакция базы данных POLPRED.COM https://polpred.com/
Научная лицензионная библиотека eLIBRARY.RU
https://elibrary.ru/defaultx.asp
ЭБС "IPRbooks" http://www.iprbookshop.ru/
ЭБС "Лань" https://e.lanbook.com/
ЭБС ИЦ "Академия" http://www.academia-moscow.ru/elibrary
Обучающиеся из числа лиц с ограниченными возможностями здоровья обеспечиваются печатными и (или) электронными образовательными ресурсами в формах, адаптированных к ограничениям их здоровья.

11 Материально-техническое обеспечение дисциплины

г. Калининград, ул. Молодёжная 6, УК-1, ауд. 441 – лекционная аудитория для проведения лекционных и практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Состав оборудования: Специализированная (учебная) мебель - учебная доска, стол преподавателя, парты, стулья экран раздвижной PROJECTA – 1 шт.; доска магнитно-маркерная – 1 шт. меловая доска -1 шт.; мультимедийный проектор TOSHIBA – 1 шт.; ноутбук Acer Extensa – 1 шт.	Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription; Номер контракта 0335100016118000073-0484577-02 от 05.07.2018 Kaspersky Total Space Security Russian Edition госконтракт № 13/18АВ от 23.01.2018 г
г. Калининград, ул.	12 компьютеров, Интернет	Microsoft Desktop Education. Опера-

Молодёжная 6, УК-1, ауд. 250 – лаборатория безопасности сетей ЭВМ	Столы компьютерные – 12 шт. доска меловая – 1 шт. Стол преподавателя – 1 шт. Парта – 1 шт. Стулья – 15 шт. Состав оборудования:	ционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription; Номер контракта 0335100016118000073-0484577-02 от 05.07.2018 Kaspersky Total Space Security Russian Edition госконтракт № 13/18АВ от 23.01.2018 г DALLAS LOCK 8.0-K, C (договор о сотрудничестве № 252-18-ЦЗ/1 от 1.11.2018 г. (3 года)); СЗИ «Блокхост-МДЗ» (договор о сотрудничестве №012 от 14 июня 2018 г. (3 года); Falcongaze SecureTower Лицензионный договор №12/05/2018-1 от 05.12.2018 (1 год)
г. Калининград, ул. Молодёжная 6, УК-1, ауд. 439 – лаборатория безопасности сетей ЭВМ.	Компьютеры AMDAthlon 64 – 8 шт.; Сервер Core 2 DUO – 2 шт.; стол преподавателя – 1 шт. компьютерные столы – 12 шт. стулья – 12 шт. доска маркерная белая – 1 шт. доска-планшет - 2 - Маршрутизатор AC 750 беспроводной, двух-диапазонный TP-LINK, Model Archer C20 IEEE 802.11 ac/n//b/a, 2,4ГГц: 300 Мбит/с, 5ГГц: 433 Мбит/с, № б/н 2017 г.Китай. (1 шт.) - AC450 Wireless Nano USB Adaptor Model NO Archer T1U TP-LINK, IEEE 802.11 ac/n/a, 5ГГц: 433 Мбит/с, № б/н 2017 г., Китай. (10 шт.) - Коммутатор CobiNet, D-Link, DES-2528 PLOA177009242, № 110134040034242 2008 г. Китай (1 шт.)	Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription; Номер контракта 0335100016118000073-0484577-02 от 05.07.2018 Kaspersky Total Space Security Russian Edition госконтракт № 13/18АВ от 23.01.2018 г
г. Калининград, ул. Молодёжная 6, УК-1, ауд. 431 (1)- кабинет для самостоятельной работы	Специализированная (учебная) мебель: - 2 компьютера с подключением к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду организации, комплект лицензионного программного обеспечения, - информационная доска,	Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения: Microsoft Office, по соглашению V9002148 Open Value Subscription; Номер контракта 0335100016118000073-0484577-02 от 05.07.2018 Kaspersky Total Space Security Rus-

	- компьютерные столы (2 шт) -учебные столы (6) -шкаф (1 шт.)	sian Edition госконтракт № 13/18АВ от 23.01.2018 г
г. Калининград, ул. Молодёжная 6, УК-1, ауд. 434 помещение для хранения и профилактического обслуживания учебного оборудования	Демонстрационные материалы: плакаты, учебно-наглядные пособия Сейф: со специализированным оборудованием по безопасности сетей ЭВМ	

12 Фонд оценочных средств для проведения аттестации по дисциплине

Фонд оценочных средств для проведения аттестации по дисциплине представлен в Приложении к рабочей программе.

13 Особенности преподавания и освоения дисциплины

Основными видами учебных занятий по дисциплине являются: лекции и лабораторные занятия, а также 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 тем 1,2,3,5 сопровождается лабораторными занятиями, в ходе которых происходит закрепление теоретических знаний, формирование и совершенствование умений, навыков и компетенций.

Лабораторные занятия проводятся в специализированной лаборатории. Современная учебно-лабораторная база для проведения лабораторных занятий обеспечивает экспериментальное подтверждение теоретического материала, рассматриваемого в теоретической части дисциплины.

Перед началом занятий преподаватель озвучивает тему занятия и его цель, проводит инструктаж по технике электробезопасности и пожарной безопасности.

Формирование знаний обучающихся обеспечивается проведением лекционных занятий в течение шестого семестра обучения.

Лабораторные и лекционные занятия сопровождаются использованием авторских рабочих и демонстрационных программ.

Контроль знаний в ходе изучения дисциплины осуществляется в виде текущих контролей, а также итоговой аттестации в форме экзамена.

Текущие контроли (защита лабораторных работ и контроль выполнения заданий на самостоятельную работу) предназначены для проверки хода и качества усвоения студентами учебного материала и стимулирования их учебной работы. Они могут осуществляться в ходе всех видов занятий в

форме, избранной преподавателем или предусмотренной рабочей программой дисциплины.

Текущие контроли предполагают постоянный контроль преподавателем качества усвоения учебного материала, активизацию учебной деятельности студентов на занятиях, побуждение их к самостоятельной систематической работе. Он необходим обучающимся для самоконтроля на разных этапах обучения. Их результаты учитываются выставлением оценок в журнале учета успеваемости.

К экзамену допускаются студенты, имеющие по всем текущим контролям положительные оценки.

Экзаменационный билет содержит два теоретических вопроса из тематики разделов по дисциплине в данном семестре.

Выбор теоретических вопросов осуществляется из принципа равной сложности всех билетов и наибольшего охвата каждым билетом учебного материала.

Подготовка к экзамену ведется по конспекту лекций, конспектам материалов, запланированных для СРС, а также 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 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 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 билету отводится до 15 минут.

Готовясь к ответу, обучающийся все доказательства, формулы, принципиальные схемы, графики и т.д. записывает и изображает на полученном листе в форме удобной для использования при устном ответе экзаменатору.

Ответ обучающегося должен быть четким, конкретным и кратким. Об окончании ответа на вопрос аттестуемый докладывает. После ответа преподаватель задает вопросы, помогающие ему выявить ход мыслей, логику рассуждений и способность применять полученные знания в практической деятельности. Если требуется уточнить оценку или степень знаний обучающегося 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 экзаменуемого 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 оценка «**неудовлетворительно**», о чем докладывается заведующему кафедрой.

Знания, умения и навыки студентов определяются оценками «**отлично**», «**хорошо**», «**удовлетворительно**», «**неудовлетворительно**». Общая оценка объявляется студенту сразу после окончания его ответа на билет экзамена. Положительная оценка («**отлично**», «**хорошо**», «**удовлетворительно**») заносится в ведомость, зачетную книжку и журнал учета успеваемости учебной группы. Оценка «**неудовлетворительно**» выставляется только в ведомость.

14 Методические указания по освоению дисциплины

Курс разработан таким образом, чтобы дать обучающимся твёрдые знания о теоретических основах и принципах построения защищенных сетей ЭВМ и вычислительных систем. Фундаментальность подготовки достигается путем глубокого и систематического изучения соответствующих тем дисциплины на лекционных занятиях и в ходе изучения материалов при самостоятельной подготовке.

Подготовка к лекционным занятиям

Лекционные занятия проводятся в аудитории, оснащенной техническими средствами обучения. Излагаемый материал иллюстрируется с использованием мультимедийного оборудования и при необходимости классной доски. Познавательная деятельность обучающихся активизируется созданием проблемных ситуаций различного уровня.

При подготовке к лекции рекомендуется повторить ранее изученный материал, это дает возможность получить необходимые разъяснения преподавателя непосредственно в ходе занятия. Большая часть преподаваемого в ходе различных занятий учебного материала не может запечатлеться в памяти. Поэтому рекомендуется вести конспект, главное требование к которому быть систематическим, логически связанным, ясным и кратким. По окончанию занятия обязательно в часы самостоятельной подготовки, по возможности в этот же день, повторить изучаемый материал и доработать конспект.

Подготовка к лабораторным работам

Лабораторные работы имеют целью практическое освоение обучающимися научно-теоретических положений изучаемой учебной дисциплины, овладение ими техникой экспериментальных исследований и анализа полученных результатов, привитие навыков работы с лабораторным оборудованием, контрольно-измерительными приборами и вычислительной техникой.

При подготовке к лабораторным занятиям необходимо получить у преподавателя задание на занятие, уяснить тему, цели, учебные вопросы, повторить теоретический материал, изучить меры безопасности при отра-

ботке учебных вопросов занятия и при работе с контрольно-измерительными приборами и вычислительной техникой. Разобраться в форме отчетности и подготовится к ней. В ходе лабораторного занятия после инструктажа по мерам безопасности отработать учебные вопросы согласно заданию и требованиям преподавателя. По выполнении лабораторной работы обучающиеся представляют отчет и защищают его.

Подготовка к экзамену

При подготовке к экзамену большую роль играют правильно подготовленные заранее записи и конспекты. В этом случае остается лишь повторить пройденный материал, учесть, что было пропущено, восполнить пробелы, закрепить ранее изученный материал.

В ходе самостоятельной подготовки к экзамену при анализе имеющегося теоретического и практического материала студенту также рекомендуется проводить постановку различного рода задач по изучаемой теме, что поможет в дальнейшем выявлять критерии принятия тех или иных решений, причины совершения определенного рода ошибок. При ответе на вопросы, поставленные в ходе самостоятельной подготовки, обучающийся вырабатывает в себе способность логически мыслить, искать в анализе событий причинно-следственные связи.

Формат сведений о РПД и ее согласовании

Рабочая программа дисциплины представляет собой компонент образовательной программы специалитета по специальности 10.05.03 «Информационная безопасность автоматизированных систем» и специализации 7 «Обеспечение информационной безопасности распределенных информационных систем» и соответствует учебному плану, утвержденному 31 января 2018 г. и действующему для студентов, принятых на первый курс, начиная с 2014 года.

Автор, представитель работодателя: директор ООО «Технологии комфорта»
_____ Старикович В.С.
(должность, подпись, Ф.И.О.)

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры информационной безопасности
(протокол № 9 от 14 июня 2018 г.)

Зав. кафедрой _____ /Великите Н.Я./

Рабочая программа дисциплины рассмотрена и одобрена на заседании методической комиссии радиотехнического факультета
(протокол № 6 от 27 июня 2018 г.)

Председатель методической комиссии _____ /Жестовский А.Г./