МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины (модуля)

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2025

Форма обучения
очная

Владивосток 2025

Рабочая программа дисциплины (модуля) «Безопасность вычислительных сетей» составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем (утв. приказом Минобрнауки России от 26.11.2020г. №1457) и Порядком организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры (утв. приказом Минобрнауки России от 06.04.2021 г. N245).

Составитель(и):

Клюев А.С., старший преподаватель, Кафедра информационной безопасности

Шумик Е.Г., кандидат экономических наук, заведующий кафедрой, Кафедра информационной безопасности, Ekaterina.Shumik1@vvsu.ru

Утверждена на заседании кафедры информационной безопасности от «____»_____20__г. , протокол № _____

СОГЛАСОВАНО:

Заведующий кафедрой (разработчика)

Шумик Е.Г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат	eg_1575874368
Номер транзакции	0000000000EA7BF9
Владелец	Шумик Е.Г.

1 Цель, планируемые результаты обучения по дисциплине (модулю)

Целью изучения дисциплины «Безопасность вычислительных сетей» является теоретическая и практическая подготовка специалистов в области обеспечения безопасности при эксплуатации вычислительных сетей; 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».

Задачи дисциплины:

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

Планируемыми результатами обучения по дисциплине (модулю), являются знания, умения, навыки. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы, представлен в таблице 1.

Таблица 1 – Компетенции, формируемые в результате изучения дисциплины (модуля)

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине		
			Код результата	Формулировка результата	
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-12 : Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1к : оценивает эффективность и надёжность защиты вычислительных сетей, операционных систем и баз данных	РД1	Знание	особенностей безопасности распределенных информационных систем; методов оценки угроз безопасности и стандарты информационной безопасности;
			РД2	Умение	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
			РД3	Навык	проектирования безопасности распределенных информационных систем; навыками оценки угроз безопасности в соответствии со стандартами информационной безопасности;
	ОПК-5 : Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.2к : использует нормативные документы, регламентирующих работу по защите информации, а также положения, инструкции и другие организационно-распорядительных документы для решения поставленных задач	РД4	Навык	разработки эксплуатационной документации по системам обеспечения информационной безопасности в соответствии с действующими стандартами.
	ОПК-9 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1к : Применяет современную эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации	РД4	Навык	разработки эксплуатационной документации по системам обеспечения информационной безопасности в соответствии с действующими стандартами.
			РД6	Умение	использовать средства противодействия атакам на сетевой комплекс, применять симметричные и асимметричные алгоритмы шифрования;
			РД7	Знание	комплексов вредоносных программ, внедряемых в компьютеры сетевого комплекса

					автоматизированных систем: троянские программы, сетевые черви, вирусы, шпионские программы, спам; методов защиты от вирусов; сетевые экраны и системы обнаружения вторжений.
			РД8	Умение	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
			РД9	Навык	эксплуатации инструментальными программами обнаружения атак на сетевой комплекс; проектирования симметричных и асимметричных криптосистем;

В процессе освоения дисциплины решаются задачи воспитания гармонично развитой, патриотичной и социально ответственной личности на основе традиционных российских духовно-нравственных и культурно-исторических ценностей, представленные в таблице 1.2.

Таблица 1.2 – Целевые ориентиры воспитания

Воспитательные задачи	**Формирование ценностей**	**Целевые ориентиры**
Формирование гражданской позиции и патриотизма		
Воспитание уважения к Конституции и законам Российской Федерации	Гражданственность	Внимательность к деталям
Формирование духовно-нравственных ценностей		

Воспитание чувства долга и ответственности перед семьей и обществом	Гражданственность	Коммуникабельность
Формирование научного мировоззрения и культуры мышления		
Развитие познавательного интереса и стремления к знаниям	Патриотизм	Активная жизненная позиция
Формирование коммуникативных навыков и культуры общения		
Воспитание культуры диалога и уважения к мнению других людей	Служение Отечеству и ответственность за его судьбу	Настойчивость и упорство в достижении цели

2 Место дисциплины (модуля) в структуре ОПОП

Дисциплина «Безопасность вычислительных сетей» относится к базовой части дисциплин учебного плана направления «Информационная безопасность автоматизированных систем».

Входными требованиями, необходимыми для освоения дисциплины, является наличие у обучающихся компетенций, сформированных при изучении дисциплин и/или прохождении практик «Информатика и основы программирования», «Основы информационной безопасности», «Сети ЭВМ и телекоммуникации». На данную дисциплину опираются «Программно-аппаратные средства защиты информации»,

«Разработка и эксплуатация защищенных автоматизированных систем».

3. Объем дисциплины (модуля)

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу с обучающимися (по видам учебных занятий) и на самостоятельную работу, приведен в таблице 2.

Таблица 2 – Общая трудоемкость дисциплины

Название ОПОП ВО	Форма обуче-ния	Часть УП	Семестр (ОФО) или курс (ЗФО, ОЗФО)	Трудо-емкость	Объем контактной работы (час)						СРС	Форма аттес-тации
				(З.Е.)	Всего	Аудиторная			Внеауди-торная			
						лек.	прак.	лаб.	ПА	КСР		
10.05.03 Информационная безопасность автоматизированных систем	ОФО	С1.Б	6	5	91	36	36	0	1	18	89	Э

4 Структура и содержание дисциплины (модуля)

4.1 Структура дисциплины (модуля) для ОФО

Тематический план, отражающий содержание дисциплины (перечень разделов и тем), структурированное по видам учебных занятий с указанием их объемов в соответствии с учебным планом, приведен в таблице 3.1

Таблица 3.1 – Разделы дисциплины (модуля), виды учебной деятельности и формы текущего контроля для ОФО

№	Название темы	Код результата обучения	Кол-во часов, отведенное на				Форма текущего контроля
			Лек	Практ	Лаб	СРС	
1	Технологии фильтрации информационного обмена	РД1, РД2, РД3, РД4, РД5, РД6, РД7, РД8, РД9	12	12	0	6	Тестовые задания, практические работы
2	Технологии изолирования информационного обмена	РД1, РД2, РД3, РД4, РД5, РД6, РД7, РД8, РД9	12	12	0	6	Тестовые задания, практические работы
3	Контроль сетевой безопасности и разработка политик сетевой безопасности.	РД1, РД2, РД3, РД4, РД5, РД6, РД7, РД8, РД9	12	12	0	6	Тестовые задания, практические работы
Итого по таблице			**36**	**36**	**0**	**18**	

4.2 Содержание разделов и тем дисциплины (модуля) для ОФО

Тема 1 Технологии фильтрации информационного обмена.

Содержание темы: Принципы и уровни фильтрации трафика в вычислительных сетях. Списки доступа (ACL) и их роль в политике безопасности сетевого обмена. Работа сетевого оборудования со списками доступа (ACL). Списки управления доступом (ACL) интеллектуальных коммутаторов локальных вычислительных сетей. Принципы и уровни фильтрации трафика в вычислительных сетях. Списки доступа (ACL) и их роль в политике безопасности сетевого обмена. Работа сетевого оборудования со списками доступа (ACL). Маршрутизаторы и межсетевые экраны (МСЭ). Многоуровневые МСЭ и принципы их применения в вычислительных сетях. Понятие границы сети и пограничного контроля. Технология NAT и PAT для фильтрации и контроля информационного обмена на границе. Демилитаризованная зона. Проксирование информационного обмена, обеспечение контроля и защиты передаваемых данных. Маршрутизаторы и межсетевые экраны (МСЭ). Многоуровневые МСЭ и принципы их применения в вычислительных сетях. Понятие границы сети и пограничного контроля. Технология NAT и PAT для фильтрации и контроля информационного обмена на границе. Демилитаризованная зона. Проксирование информационного обмена, обеспечение контроля и защиты передаваемых данных. Демилитаризованная зона. Проксирование информационного обмена, обеспечение контроля и защиты передаваемых данных. Маршрутизаторы и межсетевые экраны (МСЭ). Многоуровневые МСЭ и принципы их применения в вычислительных сетях. Понятие границы сети и пограничного контроля. Технология NAT и PAT для фильтрации и контроля информационного обмена на границе. Демилитаризованная зона. Проксирование информационного обмена, обеспечение контроля и защиты передаваемых данных.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекции- дискусии, выполнение практического задания.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 2 Технологии изолирования информационного обмена.

Содержание темы: Принципы шифрования информационного обмена. Туннелирование сетевого трафика. Протоколы туннелирования GRE и PPTP. Принцип построения виртуальных частных сетей (VPN) на основе туннелей. Построение защищенной виртуальной частной сети VPN на базе протокола PPTP. Протоколы защищенного информационного обмена IPSec. Протоколы AH и ESP. Режимы работы, принципы обмена ключами (ISAKMP). Протокол SSL/TLS. Принципы работы, аутентификация сторон и особенности шифрования данных. Протокол защищенного туннелирования IPSec. Практическая реализация IPSec туннеля на базе маршрутизаторов CISCO. Протоколы защищенного информационного обмена IPSec. Протоколы AH и ESP. Режимы работы, принципы обмена ключами (ISAKMP). Протокол SSL/TLS. Принципы работы, аутентификация сторон и особенности шифрования данных.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекции- дискусии, выполнение практического задания.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

Тема 3 Контроль сетевой безопасности и разработка политик сетевой безопасности.

Содержание темы: Сетевые сканеры. Принципы и методики сканирования. Способы построения политик сетевой безопасности и обеспечения надежности функционирования вычислительных сетей и сетевых служб. Сетевые сканеры. Принципы и методики сканирования. Способы построения политик сетевой безопасности и обеспечения надежности функционирования вычислительных сетей и сетевых служб.

Формы и методы проведения занятий по теме, применяемые образовательные технологии: лекции- дискусии, выполнение практического задания.

Виды самостоятельной подготовки студентов по теме: Изучение рекомендованной литературы.

5 Методические указания для обучающихся по изучению и реализации дисциплины (модуля)

5.1 Методические рекомендации обучающимся по изучению дисциплины и по обеспечению самостоятельной работы

Самостоятельная работа студентов (СРС) — это деятельность учащихся, которую они совершают без непосредственной помощи и указаний преподавателя, руководствуясь сформировавшимися ранее представлениями о порядке и правильности выполнения операций. Цель СРС в процессе обучения заключается, как в усвоении знаний, так и в формировании умений и навыков по их использованию в новых условиях на новом учебном материале. Самостоятельная работа призвана обеспечивать возможность осуществления студентами самостоятельной познавательной деятельности в обучении, и является видом учебного труда, способствующего формированию у студентов самостоятельности. Вданной учебной программе приведен перечень основных и дополнительных источников, которые предлагается изучить в процессе облучения по дисциплине. Кроме того, для расширения и углубления знаний по данной дисциплине целесообразно использовать: научные публикации в тематических журналах; полнотекстовые базы данных библиотеки; имеющиеся в библиотеках вуза и региона публикаций на электронных и бумажных

носителях. Успешное освоение дисциплины предполагает активную работу студентов на всех занятиях аудиторной формы: лекций и практических занятий, выполнение аттестационный мероприятий, эффективную самостоятельную работу. В процессе изучения дисциплины студенту необходимо ориентироваться на самостоятельную проработку лекционного материала, подготовку к практическим занятиям, выполнение тестов, самостоятельное изучение некоторых разделов курса Для проведения занятий лекционного типа используются учебно-наглядные пособия в форме презентационных материалов, обеспечивающих тематические иллюстрации, соответствующие темам лекций, представленным в пункте 5 настоящей

5.2 Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости обучающимся из числа лиц с ограниченными возможностями здоровья и инвалидов (по заявлению обучающегося) предоставляется учебная информация в доступных формах с учетом их индивидуальных психофизических особенностей:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания, консультации и др.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; индивидуальные задания, консультации и др.

6 Фонд оценочных средств для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

В соответствии с требованиями ФГОС ВО для аттестации обучающихся на соответствие их персональных достижений планируемым результатам обучения по дисциплине (модулю) созданы фонды оценочных средств. Типовые контрольные задания, методические материалы, определяющие процедуры оценивания знаний, умений и навыков, а также критерии и показатели, необходимые для оценки знаний, умений, навыков и характеризующие этапы формирования компетенций в процессе освоения образовательной программы, представлены в Приложении 1.

7 Учебно-методическое и информационное обеспечение дисциплины (модуля)

7.1 Основная литература

1. Басан, Е.С. Безопасность сетей ЭВМ : учеб. пособие / О.Ю. Пескова; Южный федер. ун-т; Е.С. Басан .— Ростов-на-Дону : Изд-во ЮФУ, 2024 .— 183 с. : ил. — ISBN 978-5-9275-4634-3 .— URL: https://lib.rucont.ru/efd/909306 (дата обращения: 04.08.2025)

2. Пятибратов, А. П., Вычислительные системы, сети и телекоммуникации : учебное пособие / А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко, ; под ред. А. П. Пятибратова. — Москва : КноРус, 2021. — 372 с. — ISBN 978-5-406-08157-0. — URL: https://book.ru/book/939116 (дата обращения: 26.10.2025). — Текст : электронный.

3. Толстобров, А. П. Архитектура ЭВМ : учебное пособие для вузов / А. П. Толстобров. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 162 с. — (Высшее образование). — ISBN 978-5-534-16839-6. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/531870 (дата обращения: 06.09.2023).

7.2 Дополнительная литература

1. Клашанов, Ф. К. Вычислительные системы и сети, облачные технологии : учебно-методическое пособие / Ф. К. Клашанов. — Москва : МИСИ – МГСУ, 2020. — 40 с. — ISBN 978-5-7264-2187-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/145093 (дата обращения: 27.10.2025). — Режим доступа: для авториз. пользователей.
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. —Москва : ФОРУМ : ИНФРА-М, 2023. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1910870 (Дата обращения - 22.10.2025)

7.3 Ресурсы информационно-телекоммуникационной сети "Интернет", включая профессиональные базы данных и информационно-справочные системы (при необходимости):

1. Образовательная платформа "ЮРАЙТ"
2. Электронно-библиотечная система "BOOK.ru"
3. Электронно-библиотечная система "ZNANIUM.COM"
4. Электронно-библиотечная система "ЛАНЬ"
5. Электронно-библиотечная система "РУКОНТ"
6. Open Academic Journals Index (OAJI). Профессиональная база данных - Режим доступа: http://oaji.net/
7. Президентская библиотека им. Б.Н.Ельцина (база данных различных профессиональных областей) - Режим доступа: https://www.prlib.ru/
8. Информационно-справочная система "Консультант Плюс" - Режим доступа: http://www.consultant.ru/

8 Материально-техническое обеспечение дисциплины (модуля) и перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

Основное оборудование:

- Компьютеры
- Проектор

Программное обеспечение:

- VMware Horizon ViewStandard
- Microsoft OfficeProffessionalPlus 2019 Russian
- Microsoft Windows 8 - MAK

МИНОБРНАУКИ РОССИИ

ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фонд оценочных средств
для проведения текущего контроля
и промежуточной аттестации по дисциплине (модулю)

БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

Специальность и специализация
10.05.03 Информационная безопасность автоматизированных систем. Безопасность открытых информационных систем

Год набора на ОПОП
2025

Форма обучения
очная

Владивосток 2025

1 Перечень формируемых компетенций

Название ОПОП ВО, сокращенное	Код и формулировка компетенции	Код и формулировка индикатора достижения компетенции
10.05.03 «Информационная безопасность автоматизированных систем» (ИБ)	ОПК-12 : Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	ОПК-12.1к : оценивает эффективность и надёжность защиты вычислительных сетей, операционных систем и баз данных
	ОПК-5 : Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации	ОПК-5.2к : использует нормативные документы, регламентирующих работу по защите информации, а также положения, инструкции и другие организационно-распорядительных документы для решения поставленных задач
	ОПК-9 : Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	ОПК-9.1к : Применяет современную эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации

Компетенция считается сформированной на данном этапе в случае, если полученные результаты обучения по дисциплине оценены положительно (диапазон критериев оценивания результатов обучения «зачтено», «удовлетворительно», «хорошо», «отлично»). В случае отсутствия положительной оценки компетенция на данном этапе считается несформированной.

2 Показатели оценивания планируемых результатов обучения

Компетенция ОПК-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации»

Таблица 2.1 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-5.2к : использует нормативные документы, регламентирующих работу по защите информации, а также положения, инструкции и другие организационно-распорядительных документы для решения поставленных задач	РД 4	Навык	разработки эксплуатационной документации по системам обеспечения информационной безопасности в соответствии с действующими стандартами.	выполнение практических работ

Компетенция ОПК-9 «Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации»

Таблица 2.2 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	
ОПК-9.1к : Применяет современную эталонную модель взаимодействия открытых систем; принципы построения и функционирования систем и сетей передачи информации	РД 4	Навык	разработки эксплуатационной документации по системам обеспечения информационной безопасности в соответствии с действующими стандартами.	выполнение практических работ
	РД 6	Умение	использовать средства противодействия атакам на сетевой комплекс, применять симметричные и асимметричные алгоритмы шифрования;	выполнение практических работ
	РД 7	Знание	комплексов вредоносных программ, внедряемых в компьютеры сетевого комплекса автоматизированных систем: троянские программы, сетевые черви, вирусы, шпионские программы, спам; методов защиты от вирусов; сетевые экраны и системы обнаружения вторжений.	ответы на тестовые задания
	РД 8	Умение	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	выполнение практических работ
	РД 9	Навык	эксплуатации инструментальными программами обнаружения атак на сетевой комплекс; проектирования симметричных и асимметричных криптосистем;	выполнение практических работ

Компетенция ОПК-12 «Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем»

Таблица 2.3 – Критерии оценки индикаторов достижения компетенции

Код и формулировка индикатора достижения компетенции	Результаты обучения по дисциплине			Критерии оценивания результатов обучения
	Код рез-та	Тип рез-та	Результат	

ОПК-12.1к : оценивает эффективность и надёжность защиты вычислительных сетей, операционных систем и баз данных	РД 1	Знание	особенностей безопасности распределенных информационных систем; методов оценки угроз безопасности и стандарты информационной безопасности;	ответы на тестовые задания
	РД 2	Умение	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	выполнение практических работ
	РД 3	Навык	проектирования безопасности распределенных информационных систем; навыками оценки угроз безопасности в соответствии со стандартами информационной безопасности;	выполнение практических работ

Таблица заполняется в соответствии с разделом 1 Рабочей программы дисциплины (модуля).

3 Перечень оценочных средств

Таблица 3 – Перечень оценочных средств по дисциплине (модулю)

Контролируемые планируемые результаты обучения		Контролируемые темы дисциплины	Наименование оценочного средства и представление его в ФОС	
			Текущий контроль	Промежуточная аттестация
Очная форма обучения				
РД1	Знание : особенностей безопасности распределенных информационных систем; методов оценки угроз безопасности и стандарты информационной безопасности;	1.1. Технологии фильтрации информационного обмена	Тест	Экзамен в устной форме
		1.2. Технологии изолирования информационного обмена	Тест	Экзамен в устной форме
		1.3. Контроль сетевой безопасности и разработка политик сетевой безопасности.	Тест	Экзамен в устной форме
РД2	Умение : проводить оценку проектных решений распределенных информационных систем на предмет обеспечения их безопасности; анализировать все угрозы безопасности в соответствии со стандартами информационной безопасности; анализировать проектные ре	1.1. Технологии фильтрации информационного обмена	Практическая работа	Экзамен в устной форме
		1.2. Технологии изолирования информационного обмена	Практическая работа	Экзамен в устной форме
		1.3. Контроль сетевой безопасности и разработка политик сетевой безопасности.	Практическая работа	Экзамен в устной форме

	шения систем на соотве тствие методам обеспеч ения информационной б езопасности			
РД3	Навык : проектирования безопасности распредел енных информационных систем; навыками оценк и угроз безопасности в с оответствии со стандарт ами информационной бе зопасности;	1.1. Технологии фильтра ции информационного о бмена	Практическая рабо та	Экзамен в устной форме
		1.2. Технологии изолиро вания информационного обмена	Практическая рабо та	Экзамен в устной форме
		1.3. Контроль сетевой бе зопасности и разработка политик сетевой безопас ности.	Практическая рабо та	Экзамен в устной форме
РД4	Навык : разработки эксп луатационной документ ации по системам обесп ечения информационно й безопасности в соотве тствии с действующими стандартами.	1.1. Технологии фильтра ции информационного о бмена	Практическая рабо та	Экзамен в устной форме
		1.2. Технологии изолиро вания информационного обмена	Практическая рабо та	Экзамен в устной форме
		1.3. Контроль сетевой бе зопасности и разработка политик сетевой безопас ности.	Практическая рабо та	Экзамен в устной форме
РД5	Знание : основных напр авлений развития инфор мационно- коммуникац ионных технологий объ екта защиты, методов и проблемы оценивания у гроз безопасности; осно вных угроз информацио нной безопасности; осно вных методов обеспечен ия информационной без опасности;	1.1. Технологии фильтра ции информационного о бмена	Тест	Экзамен в устной форме
		1.2. Технологии изолиро вания информационного обмена	Тест	Экзамен в устной форме
		1.3. Контроль сетевой бе зопасности и разработка политик сетевой безопас ности.	Тест	Экзамен в устной форме
РД6	Умение : использовать с редства противодействи я атакам на сетевой ком плекс, применять симме тричные и асимметричн ые алгоритмы шифрова ния;	1.1. Технологии фильтра ции информационного о бмена	Практическая рабо та	Экзамен в устной форме
		1.2. Технологии изолиро вания информационного обмена	Практическая рабо та	Экзамен в устной форме
		1.3. Контроль сетевой бе зопасности и разработка политик сетевой безопас ности.	Практическая рабо та	Экзамен в устной форме
РД7	Знание : комплексов вре доносных программ, вне дряемых в компьютеры сетевого комплекса авто матизированных систем : троянские программы, сетевые черви, вирусы, шпионские программы, спам; методов защиты о т вирусов; сетевые экра ны и системы обнаруже ния вторжений.	1.1. Технологии фильтра ции информационного о бмена	Тест	Экзамен в устной форме
		1.2. Технологии изолиро вания информационного обмена	Тест	Экзамен в устной форме
		1.3. Контроль сетевой бе зопасности и разработка политик сетевой безопас ности.	Тест	Экзамен в устной форме
РД8	Умение : использовать методы защиты автомат изированных систем от	1.1. Технологии фильтра ции информационного о бмена	Практическая рабо та	Экзамен в устной форме

	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	1.2. Технологии изолирования информационного обмена	Практическая работа	Экзамен в устной форме
		1.3. Контроль сетевой безопасности и разработка политик сетевой безопасности.	Практическая работа	Экзамен в устной форме
РД9	Навык : эксплуатации инструментальными программами обнаружения атак на сетевой комплекс ; проектирования симметричных и асимметричных криптосистем;	1.1. Технологии фильтрации информационного обмена	Практическая работа	Экзамен в устной форме
		1.2. Технологии изолирования информационного обмена	Практическая работа	Экзамен в устной форме
		1.3. Контроль сетевой безопасности и разработка политик сетевой безопасности.	Практическая работа	Экзамен в устной форме

4 Описание процедуры оценивания

Качество сформированности компетенций на данном этапе оценивается по результатам текущих и промежуточных аттестаций при помощи количественной оценки, выраженной в баллах. Максимальная сумма баллов по дисциплине (модулю) равна 100 баллам.

Вид учебной деятельности	Оценочное средство			
	Тест 1-5	Практическая работа	Экзамен	Итого
Лекционные занятия	22			22
Практические занятия		58		58
Промежуточная аттестация			20	20
Итого	22	58	20	100

Сумма баллов, набранных студентом по всем видам учебной деятельности в рамках дисциплины, переводится в оценку в соответствии с таблицей.

Сумма баллов по дисциплине	Оценка по промежуточной аттестации	Характеристика качества сформированности компетенции
от 91 до 100	«зачтено» / «отлично»	Студент демонстрирует сформированность дисциплинарных компетенций, обнаруживает всестороннее, систематическое и глубокое знание учебного материала , усвоил основную литературу и знаком с дополнительной литературой, рекомендованной программой, умеет свободно выполнять практические задания, предусмотренные программой, свободно оперирует приобретенными знаниями, умениями, применяет их в ситуациях повышенной сложности.
от 76 до 90	«зачтено» / «хорошо»	Студент демонстрирует сформированность дисциплинарных компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
от 61 до 75	«зачтено» / «удовлетворительно»	Студент демонстрирует сформированность дисциплинарных компетенций: в ходе контрольных мероприятий допускаются значительные ошибки, проявляется отсутствие отдельных знаний, умений, навыков по некоторым дисциплинарным компетенциям, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.
от 41 до 60	«не зачтено» /	У студента не сформированы дисциплинарные компетенции, проявляется недостаточность знаний, умений, навыков.

	«неудовлетворительно»	
от 0 до 40	«не зачтено» / «неудовлетворительно»	Дисциплинарные компетенции не сформированы. Проявляется полное или практически полное отсутствие знаний, умений, навыков.

5 Примерные оценочные средства

5.1 Контрольный тест

1. Под информационной безопасностью понимается…

А) защищенность информации и поддерживающей инфраструктуры от случайных или

преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

2. Защита информации – это..

А) комплекс мероприятий, направленных на обеспечение информационной безопасности.

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?

А) от компьютеров

Б) от поддерживающей инфраструктуры

В) от информации

4. Основные составляющие информационной безопасности:

А) целостность

Б) достоверность

В) конфиденциальность

5. Доступность – это…

А) возможность за приемлемое время получить требуемую информационную услугу.

Б) логическая независимость

В) нет правильного ответа

6. Целостность – это..

А) целостность информации

Б) непротиворечивость информации

В) защищенность от разрушения

7. Конфиденциальность – это..

А) защита от несанкционированного доступа к информации

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

8. Для чего создаются информационные системы?

А) получения определенных информационных услуг

Б) обработки информации

В) все ответы правильные

9. Целостность можно подразделить:

А) статическую

Б) динамичную

В) структурную

10. Где применяются средства контроля динамической целостности?

А) анализе потока финансовых сообщений

Б) обработке данных

В) при выявлении кражи, дублирования отдельных сообщений

11. Какие трудности возникают в информационных системах при конфиденциальности?

А) сведения о технических каналах утечки информации являются закрытыми

Б) на пути пользовательской криптографии стоят многочисленные технические проблемы

В) все ответы правильные

12. Угроза – это…

А) потенциальная возможность определенным образом нарушить информационную безопасность

Б) система программных языковых организационных и технических средств, предназначенных

для накопления и коллективного использования данных

В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

13. Атака – это…

А) попытка реализации угрозы

Б) потенциальная возможность определенным образом нарушить информационную безопасность

В) программы, предназначенные для поиска необходимых программ.

14. Источник угрозы – это..

А) потенциальный злоумышленник

Б) злоумышленник

В) нет правильного ответа

Краткие методические указания

Тестовые задания состоят из вопроса и нескольких вариантов ответа. Решение представляет собой указание номера вопроса и букву, которой обозначен правильный, по мнению студента, вариант ответа.

Шкала оценки

Оценка	Баллы	Описание
5	9-11	Студент не допустил ошибок
4	7-10	Студент совершил от 2 до 4 ошибок в ответах на тест
3	3-6	Студент совершил от 5 до 7 ошибок в ответах на тест
2	0-2	Студент совершил 8 и более ошибок в ответах на тест

5.2 Примеры заданий для выполнения практических работ

Практическая работа 1

Списки управления доступом (ACL) интеллектуальных коммутаторов локальных

вычислительных сетей. Принципы и уровни фильтрации трафика в вычислительных сетях. Списки доступа (ACL) и их роль в политике безопасности сетевого обмена. Работа сетевого оборудования со списками доступа (ACL).

Практическая работа 2

Построение защищенной виртуальной частной сети VPN на базе протокола PPTP.

Практическая работа 3

Протоколы защищенного информационного обмена IPSec. Протоколы AH и ESP. Режимы работы, принципы обмена ключами (ISAKMP).

Практическая работа 4

Протокол SSL/TLS. Принципы работы, аутентификация сторон и особенности шифрования данных.

Практическая работа 5

Протокол защищенного туннелирования IPSec. Практическая реализация IPSec туннеля на базе маршрутизаторов CISCO.

Практическая работа 6

Сетевые сканеры. Принципы и методики сканирования. Способы построения политик сетевой безопасности и обеспечения надежности функционирования вычислительных сетей и сетевых служб.

Краткие методические указания

На выполнение одной практической работы отводится не менее трех двухчасовых занятий. После выполнения каждой практической работы студент должен представить отчет о ее выполнении, а также, по указаниям преподавателя, выполнить дополнительные задания по теме.

Шкала оценки

Оценка	Баллы	Описание
5	8-10	Оценка «отлично» выставляется, если студент выполнил задание, правильно применил методы.
4	5-7	Оценка «хорошо» выставляется, если студент выполнил задание, правильно применил методы, но совершил логические ошибки.
3	2-4	Оценка «удовлетворительно» выставляется, если студент выполнил задание, но применил методы не все необходимые методы для его выполнения.
2	0-1	Оценка «неудовлетворительно» выставляется в случае, если студент не выполнил задание и/или неверно применил методы необходимые его выполнения.

5.3 Вопросы к экзамену

1. Охарактеризуйте основные угрозы безопасности вычислительных сетей и приведите примеры наиболее распространенных атак.
2. Какие существуют методы и средства защиты информации в вычислительных сетях? Раскройте их суть и приведите примеры.
3. Какие механизмы защиты применяют для обеспечения конфиденциальности и целостности данных при передаче по сетям? Каково их назначение?
4. Дайте определение понятию «брандмауэр» (межсетевой экран) и расскажите о видах межсетевых экранов. Когда и зачем они применяются?
5. Что такое VPN (Virtual Private Network)? Какие преимущества и недостатки у VPN имеются?
6. Какие виды сетевого сканирования существуют? Приведите примеры утилит и объясните, какую информацию они могут собирать.
7. В чём разница между пассивными и активными методами сетевой разведки? Приведите примеры методов и инструментов для каждого случая.
8. Что такое «DNS poisoning» (отравление DNS-кеша)? Опишите данную атаку и меры защиты от нее.
9. Объясните, почему важно применять криптографические методы защиты информации при обмене данными в сети? Какие криптографические алгоритмы широко распространены и рекомендуются для использования?

10. Какие меры и технологии применяют для защиты от атак типа «отказ в обслуживании» (DDoS)? Опишите хотя бы одну технологию и объясните принцип её работы.

Краткие методические указания

Для подготовки к экзамену студенту необходимо изучить лекционный материал, а так же материал представленный в дополнительных источниках.

Шкала оценки

Оценка	Баллы	Описание
5	14-20	Оценка «отлично» выставляется студенту, если он глубоко и прочно усвоил программный материал исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой.
4	8-12	Оценка «хорошо» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач.
3	2-6	Оценка «удовлетворительно» выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки.
2	0-2	Оценка «неудовлетворительно» выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки.