Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Проректор по учебной работе

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

_____ _Василенко В.Н._
(подпись) (Ф.И.О.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Безопасность сетей ЭВМ

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____ _____ _____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой _____информационной безопасности_____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ _____ _____Скрыпников А.В._____
(подпись) (дата) (Ф.И.О.)

1 Цели и задачи дисциплины

Целью дисциплины «Безопасность сетей ЭВМ» является изучение основ построения и эксплуатации вычислительных сетей, принципов и методов защиты информации в компьютерных сетях, навыкам комплексного проектирования, построения, обслуживания и анализа защищенных вычислительных сетей.

Задачами дисциплины «Безопасность сетей ЭВМ» являются:

– организационно-методическое обеспечение информационной безопасности автоматизированных систем;

– организация работ по созданию, внедрению, эксплуатации и сопровождению защищенных автоматизированных систем;

– контроль реализации политики информационной безопасности.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

2 Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОПК-8	Способность к освоению новых образцов программных, технических средств и информационных технологий	Основы архитектуры систем и средств обеспечения безопасности информации в сетях ЭВМ	Осуществлять установку, эксплуатацию и аудит сетевых средств обеспечения БИ	Навыками формирования политики безопасности сети с использованием межсетевых экранов, систем обнаружения вторжений, средств сетевой аутентификации
2	ПК-22	Способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	Перечень организационных мероприятий по обеспечению безопасности информации	Формировать требования к организации защиты информации и требования по технике защиты	Навыками по настройке и эксплуатации межсетевых экранов и систем обнаружения вторжений

3 Место дисциплины в структуре ОП ВО (СПО)

Дисциплина “Безопасность сетей ЭВМ” относится к блоку 1 ОП и ее базовой части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин:

– Компьютерная и инженерная графика;

– Система обнаружения компьютерных атак;

– Учебная практика, практика по получению первичных профессиональных умений;

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

– Мультимедиатехнологии;

– Сети и системы передачи информации;

– Техническая защита информации;

– Виртуальные частные сети;

– Защита конфиденциальной информации;

– Программно-аппаратные средства обеспечения информационной безопасности;

– Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;

– Производственная практика, преддипломная практика;

защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4 Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 7 зачетных единиц.

Виды учебной работы	Всего часов	Семестр	
		5 семестр	6 семестр
	акад. ч	**акад. ч**	**акад. ч**
Общая трудоемкость дисциплины	**252**	**72**	**180**
Контактная работа, в т.ч. аудиторные занятия	**121,85**	**45,85**	**76**
Лекции	51	15	36
в том числе в форме практической подготовки	–	–	–
Лабораторные работы (ЛР)	15	15	–
в том числе в форме практической подготовки	15	15	–
Практические занятия (ПЗ)	51	15	36
в том числе в форме практической подготовки	51	15	36
Консультации текущие	2,55	0,75	1,8
Проведение консультаций перед экзаменом	2	–	2
Виды аттестации – зачет, экзамен	0,3	0,1	0,2
Самостоятельная работа	**96,35**	**26,15**	**70,2**
Проработка материалов по конспекту лекций	26	10	16
Проработка материалов по учебникам, учебным пособиям	26	10	16
Подготовка к тестированию	18,2	–	18,2
Расчетно-практическая работа	6,15	6,15	–
Домашнее задание	20	–	20
Подготовка к экзамену (контроль)	**33,8**		**33,8**

5 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Трудоемкость раздела, час
1	Сетевая архитектура	Постановка задачи распределенной обработки данных. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей	17,65
2	Основы организации и функционирования сетей. Способы представления и преобразования сообщений и сигналов в системах и сетях связи	Основные сетевые стандарты и протоколы. Сетевые операционные системы. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиент-сервер, одноранговые сети, локальные и глобальные сети. Неоднородные вычислительные сети	18,5
3	Типовые угрозы сетевой безопасности	Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендации по построению систем защиты. Влияние человеческого фактора на сетевую безопасность	18,5
4	Защита топологии сети	Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Абонентское шифрование. Виртуальные частные сети	16,5
5	Защита сетевого трафика и компонентов сети	Защита компонентов сети от НСД. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.	22
6	Средства повышения надежности функционирования сетей	Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть.	22
7	Регламентирующие документы в области безопасности вычислительных сетей	Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	16
8	Сетевые операционные системы (ОС) NetWare, Windows, UNIX	Организация сетей на базе операционных систем NetWare. Организация вычислительных сетей на базе операционных систем Windows. Организация вычислительных сетей на базе операционных систем Unix: основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.	16
9	Политика безопасности	Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности	16
10	Критерии оценки безопасности сетевых ОС	Основные критерии анализа сетевой безопасности. Общая процедура анализа. Методика подготовки экспертного заключения	16

11	Стандарты и протоколы Интернет	Глобальная сеть Internet: основные службы и предоставляемые услуги, технологии обеспечения безопасности, основные протоколы, функционирование, разработка и сопровождение приложений, особенности реализации на различных платформах, стандарты. Процесс стандартизации Интернет. Базовые протоколы семейства TCP/IP. Протоколы управления сетью. Прикладные протоколы и службы. Электронный документооборот.	18
12	Защита каналов связи в Интернет	Виды используемых в Интернет каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети. Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты. Безопасность Java.	16,2

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ЛР, час	ПЗ, час	СР, час
1	Сетевая архитектура	3	4	4	6,65
2	Основы организации и функционирования сетей. Способы представления и преобразования сообщений и сигналов в системах и сетях связи	4	4	4	6,5
3	Типовые угрозы сетевой безопасности	4	4	4	6,5
4	Защита топологии сети	4	3	3	6,5
5	Защита сетевого трафика и компонентов сети	6	–	4	12
6	Средства повышения надежности функционирования сетей	6	–	4	12
7	Регламентирующие документы в области безопасности вычислительных сетей	4	–	4	8
8	Сетевые операционные системы (ОС) NetWare, Windows, UNIX	4	–	4	8
9	Политика безопасности	4	–	4	8
10	Критерии оценки безопасности сетевых ОС	4	–	4	8
11	Стандарты и протоколы Интернет	4	–	6	8
12	Защита каналов связи в Интернет	4	–	6	6,2

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, час
1	Сетевая архитектура	Постановка задачи распределенной обработки данных. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей	3
2	Основы организации и функционирования сетей. Способы представления и преобразования сообщений и сигналов в системах и сетях связи	Основные сетевые стандарты и протоколы. Сетевые операционные системы. Средства взаимодействия процессов в сетях. Распределенная обработка информации в системах клиент-сервер, одноранговые сети, локальные и глобальные сети. Неоднородные вычислительные сети	4
3	Типовые угрозы сетевой безопасности	Основы классификации сетевых угроз и атак. Примеры типовых атак и рекомендации по построению систем защиты. Влияние человеческого фактора на сетевую безопасность	4
4	Защита топологии сети	Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Абонентское шифрование. Виртуальные частные сети	4

5	Защита сетевого трафика и компонентов сети	Защита компонентов сети от НСД. Безопасность ресурсов сети: средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевые протоколы. Управление ключами.	6
6	Средства повышения надежности функционирования сетей	Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль и распределение нагрузки на вычислительную сеть.	6
7	Регламентирующие документы в области безопасности вычислительных сетей	Стандарты безопасности вычислительных сетей и их компонентов. Правовые основы защиты информации в сетях.	4
8	Сетевые операционные системы (ОС) NetWare, Windows, UNIX	Организация сетей на базе операционных систем NetWare. Организация вычислительных сетей на базе операционных систем Windows. Организация вычислительных сетей на базе операционных систем Unix: основные протоколы, службы, функционирование, средства обеспечения безопасности, средства управления и контроля, генерация, сопровождение и разработка приложений.	4
9	Политика безопасности	Понятие политики безопасности. Типовые элементы политики безопасности. Рекомендации по построению политики безопасности. Основные шаги по реализации политики безопасности. Поддержание и модификация политики безопасности	4
10	Критерии оценки безопасности сетевых ОС	Основные критерии анализа сетевой безопасности. Общая процедура анализа. Методика подготовки экспертного заключения	4
11	Стандарты и протоколы Интернет	Глобальная сеть Internet: основные службы и предоставляемые услуги, технологии обеспечения безопасности, основные протоколы, функционирование, разработка и сопровождение приложений, особенности реализации на различных платформах, стандарты. Процесс стандартизации Интернет. Базовые протоколы семейства TCP/IP. Протоколы управления сетью. Прикладные протоколы и службы. Электронный документооборот.	4
12	Защита каналов связи в Интернет	Виды используемых в Интернет каналов связи. Особенности их защиты. Использование межсетевых экранов. Виртуальные частные сети. Уязвимости и защита базовых протоколов и служб. Протоколы маршрутизации. Семейство TCP/IP. Службы поиска. Безопасность WWW и электронной почты. Безопасность Java.	4

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Сетевая архитектура	Практическая работа № 1 «Групповые политики Microsoft Windows» Практическая работа № 2 «Межсетевой экран Microsoft Windows»	4
2	Основы организации и функционирования сетей. Способы представления и преобразования сообщений и сигналов в системах и сетях связи	Практическая работа № 3 «Протокол сетевой безопасности IPSec» Практическая работа № 4 «Настройка параметров подключения к сети во FreeBSD»	4
3	Типовые угрозы сетевой	Практическая работа № 5 «Защита электронного	4

	безопасности	документооборота»	
4	Защита топологии сети	Практическая работа № 6 «Разграничение доступа и управление сетевыми ресурсами во FreeBSD. Настройка межсетевого экрана»	3
5	Защита сетевого трафика и компонентов сети	Практическая работа № 7 «Безопасность сетей на прикладном уровне»	4
6	Средства повышения надежности функционирования сетей	Практическая работа № 8 «Использование Центра Сертификации Microsoft Windows»	4
7	Регламентирующие документы в области безопасности вычислительных сетей	Практическая работа № 9 «Регламентирующие документы в области безопасности вычислительных сетей»	4
8	Сетевые операционные системы (ОС) NetWare, Windows, UNIX	Практическая работа № 10 «Защита рабочего места пользователя сети Интернет»	4
9	Политика безопасности	Практическая работа № 11 «Защита программного окружения рабочей станции» Практическая работа № 12 «Защита персональных данных. Защита от вирусов»	4
10	Критерии оценки безопасности сетевых ОС	Практическая работа № 13 «Технология FrameRelay» Практическая работа № 14 «Технология ATM»	4
11	Стандарты и протоколы Интернет	Практическая работа № 15 «Стандарты и протоколы защищенного документооборота»	6
12	Защита каналов связи в Интернет	Практическая работа № 16 «Безопасность различных типов подключений к Интернет» Практическая работа № 17 «Интеграция локальных сетей в региональные и глобальные сети. Контроль и анализ обеспечения безопасности подключения к Интернет»	6

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Сетевая архитектура	Сети Microsoft Windows. Принципы построения. Работа с сетью в графическом режиме	4
2	Основы организации и функционирования сетей. Способы представления и преобразования сообщений и сигналов в системах и сетях связи	Сети Microsoft Windows. Работа в режиме консоли	4
3	Типовые угрозы сетевой безопасности	Сети Microsoft Windows. Настройка подключения рабочей станции к сети	4
4	Защита топологии сети	Разграничение доступа и управление сетевыми ресурсами сети Microsoft Windows. Управление учетными записями пользователей, групп и сетевых ресурсов	3

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Сетевая архитектура	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	3
		Расчетно-практическая работа	1,65
2	Основы организации и функционирования сетей. Способы представления и преобразования сообще-	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	3

	ний и сигналов в системах и сетях связи	Расчетно-практическая работа	1,5
3	Типовые угрозы сетевой безопасности	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	3
		Расчетно-практическая работа	1,5
4	Защита топологии сети	Проработка материалов по конспекту лекций	4
		Проработка материалов по учебникам, учебным пособиям	1
		Расчетно-практическая работа	1,5
5	Защита сетевого трафика и компонентов сети	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Домашнее задание	8
6	Средства повышения надежности функционирования сетей	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Домашнее задание	8
7	Регламентирующие документы в области безопасности вычислительных сетей	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Домашнее задание	4
8	Сетевые операционные системы (ОС) NetWare, Windows, UNIX	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Подготовка к тестированию	4
9	Политика безопасности	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Подготовка к тестированию	4
10	Критерии оценки безопасности сетевых ОС	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Подготовка к тестированию	4
11	Стандарты и протоколы Интернет	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Подготовка к тестированию	4
12	Защита каналов связи в Интернет	Проработка материалов по конспекту лекций	2
		Проработка материалов по учебникам, учебным пособиям	2
		Подготовка к тестированию	2,2

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

Новожилов, Е.О. Компьютерные сети: Учебное пособие / Е.О. Новожилов. М.: Академия, 2018. 176 с

Введение в сетевые технологии: Элементы применения и администрирования сетей. Никифоров С. В. Финансы и статистика 2017 г. – 224 с. http://www.knigafund.ru/books/178313.

Сети и системы телекоммуникаций. Лавров Д. Н. Омский государственный университет 2016 г. – 186 с. http://www.knigafund.ru/books/178954.

6.2 Дополнительная литература

Технологии защиты информации в компьютерных сетях. Национальный Открытый Университет «ИНТУИТ» 2016 г. – 369 с.

Протоколы безопасного сетевого взаимодействия. Лапонина О. Р. Нацио-

нальный Открытый Университет «ИНТУИТ» 2016 г. – 462 с. – http://www.knigafund.ru/books/176152.

Сетевая безопасность на основе серверных продуктов Microsoft. Дюгуров Д. В. Интернет-Университет Информационных Технологий 2014 г. 67 с. – http://www.knigafund.ru/books/175941.

Вычислительные системы, сети и телекоммуникации. Пятибратов А. П., Гудыно Л. П., Кириченко А. А. Финансы и статистика 2015 г. 736 с. http://www.knigafund.ru/books/178860.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Безопасность сетей ЭВМ [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 – «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников**,** Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. Воронеж : ВГУИТ, 2016. 20 с. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1517

6.4 Перечень ресурсов информационно-телекоммуникационной сети Интернет», необходимых для освоения дисциплины

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Методические указания для обучающихся по освоению дисциплины

Зарубежные стандарты в области информационной безопасности [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 – «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, В. А. Хвостов; ВГУИТ, Кафедра информационной безопасности. Воронеж : ВГУИТ, 2016. 10 с. Скрыпников, А. В., Хвостов, В. А. *http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/2548*

6.6 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark);Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007 Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Про-

фессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор)Бесплатное ПО; Adobe Acrobat ReaderБесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec PackБесплатное ПО; Mozilla FirefoxБесплатное ПО; Oracle VM VirtualBoxБесплатное ПО; Sublime TextБесплатное ПО; Symantec Endpoint Protection 12(Заменен на AVP Kaspersky)Бесплатное ПО; VMWare PlayerБесплатное ПО; Антивирус “Зоркий глаз”Бесплатное ПО; Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad)Бесплатное ПО; NanoCAD (аналог Autocad)Бесплатное ПО; Gimp (графичский редактор аналог Photoshop)Бесплатное ПО; Avidemax (видео редактор)Бесплатное ПО; Virtual Dub (видео редактор)Бесплатное ПО; Free PascalБесплатное ПО

Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г. Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.

Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г. Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.

Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г. СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.

СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015 СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013

7 Материально-техническое обеспечение дисциплины

Комплекты мебели для учебного процесса.

ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств

«ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «СонатаАВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замо5к Samsung SHS-2920.

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 **Оценочные материалы** (ОМ) для дисциплины включают:

перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы;

методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формиро-

вания компетенций.

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины**.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
«БЕЗОПАСНОСТЬ СЕТЕЙ ЭВМ»
(наименование дисциплины)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- способностью к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8);
- способностью участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22).

В результате освоения дисциплины студент должен:

Знать

– основы построения систем и сетей электросвязи включая мультисервисные сети связи, типовые модели атак, направленных на преодоление защиты сетевых автоматизированных систем, условия их осуществимости, возможные последствия, способы предотвращения возможности, способы и правила применения основных программных и аппаратных средств защиты информации в сетях

Уметь

– применять защищенные протоколы и межсетевые экраны, необходимые для реализации системы защиты информации в сетях измерять и рассчитывать основные характеристики сигналов и помех реализовывать меры противодействия выявленным угрозам сетевой безопасности с использованием различных программных и аппаратных средств защиты в соответствии с правилами их применения

Владеть

– методами построения и анализа моделей, применяемых в телекоммуникационных системах, навыками проектирования защищенных сетейкомплексного анализа и оценки сетевой безопасности

Содержание разделов дисциплины. Постановка задачи распределенной обработки данных. Классификация сетей по способам распределения данных, сравнительная характеристика различных типов сетей. Основные сетевые стандарты и протоколы. Сетевые операционные системы. Средства взаимодействия процессов в сетях. Маршрутизаторы, межсетевые экраны (МЭ). Основные механизмы применения МЭ. Безопасность ресурсов сети: средства идентификации иаутентификации, методы разделения ресурсов и технологии разграничения доступа. Электронная цифровая подпись и пакетное шифрование. Криптографические сетевыепротоколы. Управление ключами. Защита от сбоев электропитания, аппаратного и программного обеспечения. Контроль ираспределение нагрузки на вычислительную сеть. Организация сетей на базе операционных систем NetWare. Организация вычислительных сетей на базе операционных систем Windows. Организация вычислительных сетей на базе операционных систем Unix: основные протоколы, службы, функционирование, средстваобеспечения безопасности, средства управления и контроля, генерация, сопровождение иразработка приложений.Понятие политики безопасности. Типовые элементы политики безопасности. Глобальная сеть Internet: основные службы и предоставляемые услуги, технологии обеспечения безопасности, основные протоколы, функционирование, разработка и сопровождение приложений, особенности реализации на различных платформах, стандарты. Процесс стандартизации Интернет. Базовые протоколы семейства TCP/IP. Протоколы управления сетью. Прикладные протоколы и службы. Электронных документооборот.Виды используемых в Интернет каналов связи. Особенности их защиты. Использование межсетевых экранов. Безопасность WWW и электронной почты. Безопасность Java.