

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ



УТВЕРЖДАЮ
Декан ФИиВТ

УТВЕРЖДАЮ /А.А. Кречетов/
(Ф.И.О. декана (директора института))

01.03.2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б.1.1.25 Защита информации в вычислительных сетях

(код и наименование дисциплины по учебному плану)

Направление подготовки
(специальность)

09.03.01 Информатика и вычислительная техника

Квалификация выпускника

Бакалавр

(бакалавр/магистр/специалист)

Направленность

Вычислительные машины, комплексы, системы и сети

Курс 4
Семестр 8

Распределение учебного времени

Трудоемкость по учебному плану	108 / 3	часов/зачетных единиц
Лекции	16	часов
Лабораторные работы	-	часов
Практические занятия	24	часов
Иная контактная работа	-	часов
Всего контактной работы (без учета экз.)	40	часов
Контактная работа по экзамену	-	часов
Курсовой проект (работа)	-	семестр
Самостоятельная работа обучающихся (без учета экз.)	68	часов
Самостоятельная работа по подготовке к экзамену	-	часов
Экзамен	-	семестр
Зачет	-	семестр
БРК, ДЗ	8	семестр

(год)

Программа составлена в соответствии с требованиями ФГОС ВО направления подготовки (специальности) 09.03.01 Информатика и вычислительная техника

Программу составили:

заведующий кафедрой с ученой степенью доктора наук и ученым званием "профессор"	ИБ	СОГЛАСОВАНО	И.Г. Сидоркина
(должность)	(кафедра)		(И.О. Фамилия)

РАССМОТРЕНА и ОДОБРЕНА на заседании кафедры, за которой закреплена дисциплина
Кафедра информационной безопасности

(наименование кафедры)		
17.01.2023	протокол №	10
(дата)		

Заведующий кафедрой	СОГЛАСОВАНО	И.Г. Сидоркина
		(И.О. Фамилия)

Рабочая программа СОГЛАСОВАНА с факультетом (институтом), выпускающей(ими)
кафедрой(ами).

СООТВЕТСТВУЕТ действующей ОП.

Заведующий кафедрой	СОГЛАСОВАНО	Д.В. Морохин
		(И.О. Фамилия)

Председатель методической комиссии факультета (института), в который входит
выпускающая кафедра

СОГЛАСОВАНО	А.А. Кречетов
	(И.О. Фамилия)

Эксперт(ы): Чернов Михаил Павлович, Заместитель генерального директора по
производству ЗАО СКБ "Хроматэк"

Рабочая программа проверена и зарегистрирована в УМЦ 06.03.2023 г.

Специалист учебно-методического центра СОГЛАСОВАНО /Т.А. Смирнова/

Раздел 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является достижение планируемых результатов обучения, соответствующих установленным в ОПОП индикаторам достижения компетенций:

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения
1. ОПК-2 Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ОПК-2.1. Знать: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	знания: современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности умения: навыки:
	ОПК-2.2. Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности	знания: умения: выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности навыки:
	ОПК-2.3. Владеть: навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности	знания: умения: навыки: применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

2. ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знания: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности умения: навыки:
	ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	знания: умения: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности навыки:
	ОПК-3.3. Владеть: навыками подготовки обзоров, аннотаций, проектов информационных систем с учетом требований информационной безопасности	знания: умения: навыки: подготовка обзоров, аннотаций, проектов информационных систем с учетом требований информационной безопасности

Раздел 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части ОПОП.

Дисциплина является обязательной

Для продолжения формирования заявленных компетенций необходимы знания предшествующих дисциплин: Операционные системы (ОПК-2), Сети и телекоммуникации (ОПК-2), Сети и телекоммуникации (ОПК-3); практик: Учебная практика. Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы) (ОПК-2)

Изучаемая дисциплина является основой для продолжения формирования указанных компетенций в следующих практиках: Преддипломная практика (ОПК-2); государственной

итоговой аттестации в форме: Подготовка к сдаче и сдача государственного экзамена (ОПК-2), Подготовка к сдаче и сдача государственного экзамена (ОПК-3)

Раздел 3. ОПИСАНИЕ ОБРАЗОВАТЕЛЬНЫХ ТЕХНОЛОГИЙ

Для формирования заявленных компетенций используются методологические технологии, реализующие деятельностный, личностно-ориентированный, практико-ориентированный подходы.

Основными стратегическими технологиями являются: лекционные занятия, практические занятия, процедуры самообучения

На достижение конкретных целей обучения направлены применяемые тактические технологии: задания, информационные, классическая лекция

Раздел 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

8 семестр

Виды и темы занятий	Количество часов	Формируемые компетенции
Основы защиты информации в вычислительных системах и сетях	28	ОПК-3
Лекция. Основные понятия защиты информации и информационной безопасности. Основные законодательные положения защиты информации	2	
Лекция. Обеспечение безопасности телекоммуникационных связей и административный контроль. Основные понятия и терминология	2	
Лекция. Типовые угрозы сетевой безопасности. Основы классификации сетевых угроз и атак. Влияние человеческого фактора на сетевую безопасность	2	
Практическое занятие. Сравнительный анализ понятийных аппаратов различных источников в области защиты информации в вычислительных системах и сетях	8	
Задания для самостоятельной работы, в том числе выполнение	14	
Подготовка к лекциям, повторение учебного материала прошлых лекций, выполнение домашних заданий Подготовка к практическим занятиям		
Методы защиты информации в вычислительных системах и сетях	44	ОПК-2, ОПК-3
Лекция. Политика безопасности. Основные типы моделей управления доступом	2	
Лекция. Идентификация и аутентификация. Современные методы аутентификации	2	
Лекция. Криптографические методы защиты	2	
Практическое занятие. Средства идентификации и аутентификации, методы разделения ресурсов и технологии разграничения доступа	8	
Практическое занятие. Криптографическая защита информации в компьютерных сетях	4	

Задания для самостоятельной работы, в том числе выполнение реферата Подготовка к лекциям, повторение учебного материала прошлых лекций, выполнение домашних заданий Подготовка к практическим занятиям Выполнение реферата	26	ОПК-2, ОПК-3
Обеспечение безопасности межсетевого взаимодействия	36	
Лекция. Основные механизмы обеспечения безопасности и управления распределенными ресурсами. Уязвимости и защита базовых протоколов и служб. Обеспечение надежности инфраструктуры Интернет	2	
Лекция. Защита каналов связи в Интернет. Виды используемых в Интернет каналов связи. Использование межсетевых экранов. Виртуальные частные сети	2	
Практическое занятие. Методы управления средствами сетевой безопасности	4	
Задания для самостоятельной работы, в том числе выполнение Подготовка к лекциям, повторение учебного материала прошлых лекций, выполнение домашних заданий Подготовка к практическим занятиям Выполнение контрольной работы Консультации БРК	28	
Иная контактная работа: выполнение контрольной работы, выполнение реферата, дифференцированный зачет (БРК), консультации	0	

Раздел 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины "Защита информации в вычислительных сетях" рекомендуется начать с ознакомления с рабочей программой, ее структурой и содержанием разделов. Учебный материал структурирован, изучение дисциплины осуществляется в тематической последовательности.

Занятия лекционного типа дают систематизированные знания по дисциплине, концентрируют внимание на наиболее сложных и важных вопросах. Во время лекционных занятий рекомендуется вести конспектирование учебного материала; обращать внимание на формулировки и категории, раскрывающие суть проблемы, явления или процесса; зафиксировать выводы и практические рекомендации. Подготовка к **занятиям семинарского типа** включает ознакомление с планом практического занятия; работу с конспектом лекций, выполнение домашнего задания, работу с учебной и учебно-методической литературой, научными изданиями и электронными образовательными ресурсами, рекомендованными рабочей программой дисциплины.

Содержание **самостоятельной работы** определяется рабочей программой дисциплины, оценочными и методическими материалами, заданиями и указаниями преподавателя. Самостоятельная работа может осуществляться в аудиторной и внеаудиторной формах. Эффективным средством осуществления самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к образовательной программе, рабочей программе дисциплины, к электронным библиотечным системам, профессиональным базам данных и информационным справочным системам.

Изучение дисциплины включает выполнение контрольной работы, практической работы и подготовку реферата.

Краткие требования к написанию реферата:

– Реферат состоит из введения, основного текста, заключения и списка литературы. Реферат при необходимости может содержать приложение. Каждая из частей начинается с новой страницы. Первой страницей реферата является титульный лист.

– Заголовки должны четко и кратко отражать содержание разделов. Заголовки следует печатать с прописной буквы. Переносы слов не допускаются. Если заголовок состоит из двух предложений, их разделяют точкой. В конце заголовка точку не ставят.

– Во введении реферата указываются актуальность темы реферата, цель реферата, задачи, которые необходимо решить, чтобы достигнуть указанной цели. Кроме того, во введении реферата дается краткая характеристика структуры работы и использованной литературы. Объем введения для реферата – 1-1,5 страницы.

– Основной текст разделён на главы. Главы и параграфы реферата нумеруются. Точка после номера не ставится. Обычно в реферате 3-4 главы. Каждая новая глава начинается с новой страницы. На основную часть реферата приходится до 16 страниц.

– В заключении формируются выводы. В заключении должны быть представлены ответы на поставленные во введении задачи, сформулирован общий вывод и дано заключение о достижении цели реферата. Заключение должно быть кратким, четким.

– При составлении списка литературы следует придерживаться общепринятых стандартов. Список литературы должен включать от 4 до 12 позиций. Работы, указанные в списке литературы, должны быть относительно новыми (за последние 5-10 лет). Более старые источники можно использовать лишь при условии их уникальности. Периодичность проведения, формы текущего контроля успеваемости, система оценивания хода освоения дисциплин представлены в рабочей программе. Формой промежуточной аттестации по дисциплине является балльно-рейтинговый контроль (БРК).

Раздел 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-методическое обеспечение

№№ п/п	Список используемой литературы	Количество экземпляров печатных изданий, имеющихся в библиотеке, или электронный адрес издания (ресурса) в сети Интернет
УЧЕБНЫЕ, УЧЕБНО-МЕТОДИЧЕСКИЕ И НАУЧНЫЕ ИЗДАНИЯ		
1.	Нестеров, С. А. Основы информационной безопасности [Электронный ресурс] / Нестеров С. А. Санкт-Петербург: Лань, 2024. - 324 с. ISBN 978-5-8114-6738-9.	https://e.lanbook.com/book/370967
2.	Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений [Электронный ресурс] : учебное пособие для вузов / Никифоров С. Н. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 96 с. ISBN 978-5-507-45868-4.	https://e.lanbook.com/book/288974
3.	Никифоров, С. Н. Методы защиты информации. Защищенные сети [Электронный ресурс] / Никифоров С. Н. 2-е изд., стер. Санкт-Петербург: Лань, 2021. - 96 с. ISBN 978-5-8114-8123-1.	https://e.lanbook.com/book/171868
4.	Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование [Электронный ресурс] / Никифоров С. Н. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 124 с.	https://e.lanbook.com/book/338018

	ISBN 978-5-507-47181-2.	
5.	Никифоров, С. Н. Методы защиты информации. Шифрование данных [Электронный ресурс] : учебное пособие / Никифоров С. Н. 2-е изд., стер. Санкт-Петербург: Лань, 2022. - 160 с. ISBN 978-5-8114-4042-9.	https://e.lanbook.com/book/206285
6.	Прохорова, О. В. Информационная безопасность и защита информации [Электронный ресурс] : учебник для вузов / Прохорова О. В. 5-е изд., стер. Санкт-Петербург: Лань, 2023. - 124 с. ISBN 978-5-507-46010-6.	https://e.lanbook.com/book/293009

6.2. Материально-техническая база и программное обеспечение

№№ п/п	Аудитории для проведения учебных занятий, самостоятельной работы и проведения государственной итоговой аттестации	Перечень основного оборудования	Программное обеспечение
1.	510 (III)	Экран настенный рулонный 200x200 см (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
2.	518 (III)	Системный блок CEL D-341 FAN/ASUS S-775/512 M/160.0G/DVD+-RW (1), ПК 5 - ICL RAY P222.3 ,клавиат.,мышь.,монитор LG E2251T-BN (14), Сист. блок CE 331/256*2/PC 3200/80 Gb/FDD/DVD-ROM/КЛАВ+МЫШЬ+коврик (1), Комплект учебной мебели (1)	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Microsoft Access, Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
3.	519 (III)	Системный блок CEL D-341 FAN/ASUS S-775/512 M/160.0G/DVD+-RW (7), Монитор 15" Samsung 510 M (1), Монитор 17" BenQ FP 71G (1), Монитор TET 20" Samsung SIM 2043W (1), ПК ICL RAY H494.1	Microsoft Windows Enterprise, Справочная правовая система "Консультант Плюс", Microsoft Office Standard, Агент Dr.Web, Microsoft Access,

		сист.блок,клавиат,мышь,монитор View Sonic VA2231 WLED WZ1218) (14), Сист. блок CE 331/256*2/PC 3200/80 Gb/FDD/DVD- ROM/КЛАВ+МЫШЬ+коврик (1), Комплект учебной мебели (1)	Microsoft Visio Professional, Microsoft Project Professional, Microsoft Visual Studio Enterprise, Комплект ПО для решения основных пользовательских задач
--	--	--	---

Раздел 7. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ/ ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Критерии оценивания индикаторов достижения компетенций направлены на:

- усвоение теоретического материала (объем знаний, глубина усвоения), предусмотренного рабочей программой;
- умение излагать материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания при решении практических заданий.

Шкала оценивания представлена ниже.

Уровень сформированности элементов компетенции	Критерии оценивания	Шкала оценивания
Пороговый уровень	Обучающийся имеет знания основного материала, проявляет умение логично его излагать, но может допускать неточности в изложении материала, недостаточно правильные формулировки, испытывает затруднения в выполнении практических заданий.	удовлетворительно
Продвинутый уровень	Обучающийся твердо знает программный материал, излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения	хорошо
Высокий уровень	Обучающийся глубоко и прочно усвоил программный материал, грамотно и логически стройно его излагает, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с задачами, вопросами и другими видами применения знаний, показывает знакомство с монографической литературой, периодическими изданиями, правильно обосновывает принятые решения, свободно владеет разносторонними навыками, приемами выполнения практических работ	отлично

7.1. Текущий контроль успеваемости

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля) и производится с применением технологии рейтингового контроля в соответствии с технологической картой дисциплины. Порядок составления технологической карты и алгоритм проведения процедуры оценивания видов деятельности обучающихся, направленных на освоение знаний, умений, навыков и/или опыта деятельности, по

накопительной системе в баллах устанавливается положением о системе РИТМ в ФГБОУ ВО «ПГТУ»

7.2. Промежуточная аттестация обучающихся

Промежуточная аттестация обучающихся направлена на оценивание результатов обучения по дисциплине (модулю) и проводится с использованием фондов оценочных средств.

Примеры типовых контрольных заданий из базы фонда оценочных средств по образовательной программе.

1. По масштабу компьютерные сети подразделяются на

- a) звездообразные, кольцевые, шинные
- b) одноранговые и сети "клиент-сервер"
- c) проводные и беспроводные
- d) локальные и глобальные

2. Задачей какого уровня модели OSI является управление доступом к среде в сетях, построенных на основе разделяемой среды?

- a) прикладного
- b) сетевого
- c) канального
- d) физического

3. Какое минимальное количество уровней протоколов (в терминах модели OSI) должны поддерживать маршрутизаторы сетей с коммутацией пакетов?

- a) 1
- b) 2
- c) 3
- d) 4

4. К транспортному уровню модели OSI относятся протоколы:

- a) IP, RIP, OSPF
- b) SSL, TLS
- c) SMTP, IMAP, POP3
- d) UDP, TCP

5. По какой причине в протоколе RIP расстояние в 16 хопов между сетями полагается недостижимым?

- a) поле, отведенное для хранения значения расстояния, имеет длину 4 двоичных разряда
- b) для получения приемлемого времени сходимости алгоритма
- c) сети, в которых работает RIP, редко бывают большими
- d) таблицы маршрутизации не могут хранить больше 16 записей

6. Что нужно сделать на DHCP сервере чтобы исключить выдачу определенного IP адреса из существующего диапазона?

- a) создать диапазон IP адресов
- b) создать параметр DHCP
- c) создать область DHCP
- d) создать исключение для IP адреса

7. Как называется объект Active Directory, который хранит информацию об учетных записях, общих ресурсах, подразделениях?

- a) сетевой доступ
- b) каталог
- c) папка
- d) домен

8. Какой протокол используется для доступа к службе каталогов AD?

- a) LDAP

- b) ShareDiscovery
- c) ADSL
- d) UDP

9. Компьютер, занимающийся обслуживанием сети, управлением передачей сообщений, и предоставляющий удаленный доступ к своим ресурсам, называется

- a) хабом
- b) сервером
- c) рабочей станцией
- d) хостом

10. Метод передачи данных, при котором данные пересылаются в двух направлениях одновременно, называется ...

- a) симплексным
- b) дуплексным
- c) синхронным
- d) полудуплексным

11. Анализ защищенности - это ...

- a) выбор обоснованного набора контрмер, позволяющих снизить уровень рисков до приемлемой величины
- b) независимая экспертиза отдельных областей функционирования предприятия
- c) процедура учета действий, выполняемых пользователем на протяжении сеанса доступа
- d) поиск уязвимых мест информационной системы

12. Воздействие на систему с целью создания условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднен.

- a) DoS-атака
- b) несанкционированный доступ
- c) незаконное использование привилегий
- d) программная закладка

13. Программное средство для удаленной или локальной диагностики различных элементов сети на предмет выявления в них различных уязвимостей.

- a) агент безопасности
- b) политика безопасности
- c) средство делегирования административных полномочий
- d) сканер безопасности

14. ... - процесс блокировки выявленных вторжений.

- a) анализ защищенности
- b) обнаружение атак
- c) предотвращение атак
- d) аудит безопасности

15. В журнале аутентификации обнаружено несколько записей неуспешных попыток войти в систему под учетными записями пользователей. Возможно была попытка подбора паролей.

Какоестандартное средство следует использовать для уменьшения риска такого рода атак?

- a) использовать систему обнаружения вторжений
- b) переименовать учетную запись администратора
- c) использовать мультифакторную аутентификацию
- d) включить блокировку учетных записей при определенном количестве неуспешных попыток регистрации

16. Политика безопасности требует сокрытия схемы IP-адресации, используемой во внутренней сети. Какая из перечисленных технологий позволит решить поставленную задачу?

- a) система обнаружения вторжений
- b) персональный межсетевой экран
- c) NAT

d) антивирусное программное обеспечение

17. Технология, которая для обнаружения атак использует, например, образец IP-пакета, характерного для какой-нибудь определенной атаки.

a) монитор регистрационных файлов

b) контроль целостности

c) выявление аномальной деятельности

d) анализ сигнатур

18. Согласно классификации ФСТЭК России, межсетевой экран применяемый на логической границе ИС или между логическими границами сегментов ИС, это МЭ ...

a) типа А

b) типа Б

c) типа В

d) типа Г

19. Согласно классификации ФСТЭК России системы обнаружения вторжений делятся на

a) уровня узла и уровня сети

b) внешние и внутренние

c) симметричные и асимметричные

d) коммутируемые и некоммутируемые

20. Согласно профилю защиты средства антивирусной защиты типа «Б» устанавливаются на ... информационной системы, функционирующей на базе вычислительной сети.

a) рабочие станции пользователей

b) серверы

c) рабочую станцию администратора

d) серверы и рабочие станции

21. Защита ресурсов сети от несанкционированного использования - это

a) охрана оборудования сети

b) защита ядра безопасности

c) контроль доступа

d) защита периметра безопасности

22. Средство защиты, обеспечивающее защищенность информации от угроз нелегитимной передачи данных из защищенного сегмента системы путем анализа и блокирования исходящего трафика

a) межсетевой экран

b) средство антивирусной защиты

c) DLP-система

d) сканер безопасности

23. Средство, решающее задачи консолидации и хранения журналов событий от различных источников, а также имеющее инструменты для анализа событий и разбора инцидентов на основе их корреляции и обработки по правилам – это ...

a) DLP-система

b) система обнаружения вторжений

c) SIEM-система

d) сканер безопасности

24. Способ перехвата информации, при котором на машину устанавливается программное средство, собирающее и передающее информацию – это ...

a) перехват в разрыв

b) сетевой перехват

c) агентский перехват

d) перехват путем интеграции со сторонними продуктами

25. Программное или аппаратное средство, которое осуществляет мониторинг сети в реальном времени с целью выявления, предотвращения и блокировки вредоносной активности.

a) межсетевой экран

- b) система обнаружения вторжений
 - c) система предотвращения вторжений
 - d) средство антивирусной защиты
26. К каким методам сбора данных, использующихся при аудите информационной безопасности, относится MaxPatrol?
- a) анализ документации
 - b) предоставление опросных листов
 - c) использование специализированных программных средств
 - d) интервьюирование
27. Какой из методов проверки направлен на определение наличия уязвимости по косвенным признакам?
- a) активные зондирующие проверки
 - b) проверка заголовков и активные зондирующие проверки
 - c) проверка заголовков
 - d) имитация атак
28. В каком режиме сканирования системы анализа защищенности MaxPatrol можно произвести подбор паролей?
- a) Audit
 - b) Compliance
 - c) PenTest
 - d) Pentest и Compliance
29. В каком режиме функционирования IPsec шифруется весь исходный IP-пакет, а затем он вставляется в поле данных нового пакета?
- a) транспортном
 - b) туннельном
 - c) в обоих режимах
 - d) IPsec не использует шифрование
30. Процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности организации в соответствии с определёнными критериями показателями безопасности – это ...
- a) выявление аномальной деятельности
 - b) анализ защищённости
 - c) аудит информационной безопасности
 - d) установка системы защиты

Перечень вопросов для проведения промежуточной аттестации

Вопросы по балльно-рейтинговому контролю

1. Типовые конфигурации информационных систем. Влияние конфигурации информационной системы на безопасность хранимых, обрабатываемых и передаваемых по сети данных.
2. Угроза. Уязвимость. Атака. Взаимосвязь между этими понятиями.
3. Классификация угроз информационной безопасности вычислительных сетей.
4. Классификация уязвимостей.
5. Классификация атак.
6. Перехват информации в сети. Инструменты. Способы противодействия перехвату.
7. Spoofing. Способы подделки идентификаторов. Способы противодействия.
8. DOS-атаки. Особенности реализации. Способы противодействия DOS-атакам.
9. Универсальные методы обеспечения информационной безопасности компьютеров и компьютерных сетей.
10. Специализированные методы обеспечения информационной безопасности компьютерных сетей.

11. Идентификация и аутентификация. Особенности аутентификации пользователей в компьютерных сетях.
12. Протокол Kerberos. Назначение. Особенности функционирования.
13. Разграничение доступа к информационным ресурсам компьютерных сетей.
14. Криптографическая защита информации в компьютерных сетях. Достоинства и недостатки. Способы преодоления криптографической защиты информации.
15. Электронная подпись. Назначение. Применение для защиты сетевого взаимодействия. Примеры.
16. Сканеры безопасности. Способы выявления уязвимостей в информационных системах.
17. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
18. Системы обнаружения вторжений. Системы предотвращения вторжений. Методики выявления сетевых атак.
19. Сетевые и хостовые системы обнаружения и предотвращения вторжений. Достоинства и недостатки.
20. Межсетевые экраны. Классификация. Варианты размещения межсетевого экрана. Достоинства и недостатки.
21. Демилитаризованные зоны. Назначение. Способы выделения.
22. Классификация межсетевых экранов по уровням защищенности. Показатель защищенности, применяемые для классификации. Применение межсетевых экранов различных классов.
23. Технология VPN (Виртуальные частные сети). Назначение. Достоинства и недостатки.
24. Основные компоненты технологии виртуальных частных сетей (VLAN).
25. Вредоносные программы. Классификация. Каналы распространения. Влияние на информационные системы.
26. Антивирусные средства. Классификация. Методики выявления вредоносного кода.
27. Средства обеспечения информационной безопасности в ОС семейства Windows. Разграничение доступа к данным. Групповая политика. Область действия групповых политик.
28. Основные этапы разработки защищенной компьютерной сети.
29. Проблемы обеспечения безопасности прикладных сервисов (Веб, почта, FTP) и их решения.
30. Физические средства обеспечения информационной безопасности.