Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Агабекян Раиса Левоновна
Должность: ректор
Дата подписания: 06.02.2024 14:53:52
Уникальный программный ключ:
4237c7ccb9b9e111bbaf1f4fcda9201d015c4dbaa123ff774747307c89b5beb8e

Негосударственное аккредитованное некоммерческое частное образовательное учреждение высшего образования
«Академия маркетинга и социально-информационных технологий – ИМСИТ»
(г. Краснодар)

(НАН ЧОУ ВО Академия ИМСИТ)

УТВЕРЖДАЮ
Проректор по учебной работе, доцент

_____Н.И. Севрюгина

20.11.2023

Б1.В.04
Защита информационных процессов в компьютерных системах
рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Кафедра математики и вычислительной техники**

Учебный план 10.03.01 Информационная безопасность

Квалификация **бакалавр**
Форма обучения **очная**
Общая трудоемкость **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 64
самостоятельная работа 44
контактная работа во время промежуточной аттестации (ИКР) 0
часов на контроль 34,7

Виды контроля в семестрах:
экзамены 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	15 5/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	32	32	32	32
Контактная работа на аттестации (в период экз. сессий)	0,3	0,3	0,3	0,3
Консультации перед экзаменом	1	1	1	1
В том числе в форме практ.подготовки	10	10	10	10
Итого ауд.	64	64	64	64
Контактная работа	65,3	65,3	65,3	65,3
Сам. работа	44	44	44	44
Часы на контроль	34,7	34,7	34,7	34,7
Итого	144	144	144	144

Программу составил(и):
к.т.н., доцент кафедры математики и вычислительной техники, Капустин С.А.

Рецензент(ы):
д.т.н., профессор кафедры информатики и вычислительной техники КубГТУ, Хисамов Ф.Г.;директор АО «ЮГ-СИСТЕМА ПЛЮС», Глебов О.В.

Рабочая программа дисциплины
Защита информационных процессов в компьютерных системах

разработана в соответствии с ФГОС ВО:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 10.03.01 Информационная безопасность (приказ Минобрнауки России от 17.11.2020 г. № 1427)

составлена на основании учебного плана:
10.03.01 Информационная безопасность
утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры
Кафедра математики и вычислительной техники

Протокол от 13.10.2023 г. № 3

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью преподавания дисциплины «Защита информационных процессов в компьютерных системах» является изложение основ методики комплексной защиты информационных систем на основе программных и программно-аппаратных средств, а также требований к системам защиты информации

Задачи: - изучение принципов действия основных видов сетевых атак и методов борьбы с ними;
- изучение структуры политики безопасности организации и основных этапов ее разработки;
- изучение методов аутентификации на основе паролей, на основе PIN-кода, принципов работы аппаратно-программных систем
идентификации и аутентификации;
- изучение классификации межсетевых экранов, функций межсетевых экранов, схем подключения межсетевых экранов;
- изучение классификации компьютерных вирусов, методов обнаружения компьютерных вирусов, обзор современных антивирусных программ;
- изучение средств анализа защищенности и обнаружения сетевых атак;
- изучение основных требований и рекомендаций по защите информации в компьютерных системах;
- изучение методов и программных средств анализа рисков;
- изучение принципов разработки и защиты Web-сайтов.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Системы охраны и инженерной защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика: Преддипломная практика
2.2.2	Выполнение и защита выпускной квалификационной работы

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ПК-1: Способен эксплуатировать средства обеспечения информационной безопасности автоматизированных систем	
ПК-1.1: Производит внедрение в состав автоматизированных систем средств обеспечения информационной безопасности	
Знать	
Уровень 1	Минимальный необходимый уровень внедрения в состав автоматизированных систем средств обеспечения информационной безопасности
Уровень 2	Уровень знаний внедрения в состав автоматизированных систем средств обеспечения информационной безопасности в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний внедрения в состав автоматизированных систем средств обеспечения информационной безопасности в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-1.2: Соотносит функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности	
Уметь	
Уровень 1	Продемонстрированы основные умения соотношения функционала автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности , решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения соотношения функционала автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами

Уровень 3	Продемонстрированы все основные умения соотношения функционал автоматизированных систем средств обеспечения информационной безопасности с реализуемыми процедурами обеспечения информационной безопасности, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-1.3: Выполняет регламентные работы по эксплуатации средств защиты информации	
Владеть	
Уровень 1	Имеется минимальный набор навыков выполнения регламентных работ по эксплуатации средств защиты информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки выполнения регламентных работ по эксплуатации средств защиты информации области с некоторыми недочётами
Уровень 3	Продемонстрированы навыки выполнения регламентных работ по эксплуатации средств защиты информации без ошибок и недочётов
ПК-1.4: Устраняет неисправности при эксплуатации средств защиты информации	
Знать	
Уровень 1	Минимальный необходимый набор знаний устранения неисправностей при эксплуатации средств защиты информации
Уровень 2	Уровень знаний для устранения неисправностей при эксплуатации средств защиты информации
Уровень 3	Уровень знаний для устранения неисправностей при эксплуатации средств защиты информации
Уметь	
Уровень 1	Продемонстрированы основные умения устранять неисправности при эксплуатации средств защиты информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения устранять неисправности при эксплуатации средств защиты информации , решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения устранять неисправности при эксплуатации средств защиты информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков устранения неисправностей при эксплуатации средств защиты информации
Уровень 2	Продемонстрированы базовые навыки устранения неисправностей при эксплуатации средств защиты информации
Уровень 3	Продемонстрированы навыки устранения неисправностей при эксплуатации средств защиты информации

ПК-2: Способен реализовывать политики безопасности с использованием инструментальных средств обеспечения информационной безопасности	
ПК-2.1: Формулирует критерии безопасности обработки информации в автоматизированных системах	
Знать	
Уровень 1	Минимальный необходимый уровень знаний критериев безопасности обработки информации в автоматизированных системах
Уровень 2	Уровень знаний критериев безопасности обработки информации в автоматизированных системах в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний критериев безопасности обработки информации в автоматизированных системах в объёме, соответствующем программе подготовки, без ошибок
ПК-2.2: Выполняет мероприятия для реализации политики информационной безопасности	
Уметь	
Уровень 1	Продемонстрированы основные умения проведения мероприятия для реализации политики информационной безопасности, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения проведения мероприятия для реализации политики информационной безопасности, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения проведения мероприятия для реализации политики информационной безопасности, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
ПК-2.3: Определяет состав средств, необходимый для управления автоматизированными системами и средствами их защиты от НСД	
Владеть	
Уровень 1	Имеется минимальный набор навыков определения состава средств, необходимых для управления автоматизированными системами и средствами их защиты от НСД с негрубыми ошибками и некоторыми недочётами

Уровень 2	Продемонстрированы базовые навыки определения состава средств, необходимых для управления автоматизированными системами и средствами их защиты от НСД с некоторыми недочётами
Уровень 3	Продемонстрированы навыки определения состава средств, необходимых для управления автоматизированными системами и средствами их защиты от НСД без ошибок и недочётов
ПК-2.4: Определяет порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД	
Знать	
Уровень 1	Минимальный необходимый уровень знаний порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД
Уровень 2	Уровень знаний порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД в объёме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НСД в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения определять порядок настройки технических средств для устранения автоматизированными системами и средствами их защиты от НСД, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения определять порядок настройки технических средств для устранения автоматизированными системами и средствами их защиты от НСД, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения определять порядок настройки технических средств для устранения автоматизированными системами и средствами их защиты от НСД, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме
Владеть	
Уровень 1	Имеется минимальный набор навыков определять порядок настройки технических средств для управления автоматизированными системами и средствами их защиты от НДС с негрубыми ошибками и некоторыми недочетами
Уровень 2	Продемонстрированы базовые навыки определения порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НДС с некоторыми недочетами
Уровень 3	Продемонстрированы навыки определения порядка настройки технических средств для управления автоматизированными системами и средствами их защиты от НДС без ошибок и недочетов
ПК-2.5: Устанавливает программное обеспечение в соответствии с требованиями по защите информации	
Знать	
Уровень 1	Минимальный необходимый уровень знаний установления программного обеспечения в соответствии с требованиями по защите информации
Уровень 2	Уровень знаний установления программного обеспечения в соответствии с требованиями по защите информации в объеме, соответствующем программе подготовки, допущено несколько негрубых ошибок
Уровень 3	Уровень знаний установления программного обеспечения в соответствии с требованиями по защите информации в объёме, соответствующем программе подготовки, без ошибок
Уметь	
Уровень 1	Продемонстрированы основные умения установки программного обеспечения в соответствии с требованиями по защите информации, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объёме
Уровень 2	Продемонстрированы все основные умения установки программного обеспечения в соответствии с требованиями по защите информации, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объёме, но некоторые с недочётами
Уровень 3	Продемонстрированы все основные умения установки программного обеспечения в соответствии с требованиями по защите информации, решены все основные задачи с отдельными несущественными недочётами, выполнены все задания в полном объёме
Владеть	
Уровень 1	Имеется минимальный набор навыков установки программного обеспечения в соответствии с требованиями по защите информации с негрубыми ошибками и некоторыми недочётами
Уровень 2	Продемонстрированы базовые навыки установки программного обеспечения в соответствии с требованиями по защите информации с некоторыми недочётами
Уровень 3	Продемонстрированы навыки установки программного обеспечения в соответствии с требованиями по защите информации без ошибок и недочётов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов**	**Компетен-ции**	**Литература и эл. ресурсы**	**Практ. подг.**
	Раздел 1. Раздел 1					
1.1	Основы защищенной ОС Windows /Лек/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.2	Основы защищенной ОС Windows /Пр/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	2
1.3	Основы защищенной ОС Windows /Ср/	7	8	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.4	Отладка и перехват процессов /Лек/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.5	Отладка и перехват процессов /Пр/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	2
1.6	Отладка и перехват процессов /Ср/	7	10	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.7	Защита компьютерной сети в Windows /Лек/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.8	Защита компьютерной сети в Windows /Пр/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	2
1.9	Защита компьютерной сети в Windows /Ср/	7	8	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.10	Внутреннее строение защищенной ОС Windows /Лек/	7	8	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	

1.11	Внутреннее строение защищенной ОС Windows /Пр/	7	8	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	2
1.12	Внутреннее строение защищенной ОС Windows /Ср/	7	10	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.13	Безопасность в ОС Windows /Лек/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.14	Безопасность в ОС Windows /Пр/	7	6	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	2
1.15	Безопасность в ОС Windows /Ср/	7	8	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Промежуточная аттестация					
2.1	/КАЭ/	7	0,3	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
2.2	/Консл/	7	1	ПК-1.1 ПК-1.2 ПК-1.3 ПК-1.4 ПК-2.1 ПК-2.2 ПК-2.3 ПК-2.4 ПК-2.5	Л1.1 Л1.2 Л1.3Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Информация как объект защиты. Цели защиты информации.
2. Информационная безопасность. Понятие. Аспекты. Угрозы информационной безопасности.
3. Меры по формированию режима информационной безопасности. Принципы системы защиты.
4. Аппаратно-программные средства защиты информации. Подробнее о системах шифрования дисковых данных и данных, передаваемых по сетям.
5. Аппаратно-программные средства защиты информации. Подробнее о системах аутентификации электронных данных и средствах управления криптографическими ключами.
6. Причины взлома систем защит информации и способы заинтересовать пользователя в лицензионном ПО.
7. Каналы утечки информации.
8. Виды криптографического закрытия информации. Подробно два способа шифрования.
9. DES. Определение. Основные положения. Общая схема алгоритма.
10. Виды DES.
11. IDEA. Определение. Основные положения. Основные отличия от DES.
12. Что такое однонаправленные функции? Привести примеры.
13. Система распределения ключей Диффи-Хелмана.
14. RSA. Основные принципы.
15. Электронная подпись в системах с открытым ключом.
16. Группы отладочных средств. Групповые характеристики. Слабые места для каждой группы.
17. Способы борьбы с отладчиком.

18. Дополнительные возможности процессора при работе в защищенном режиме. Отладочные регистры.
19. Способы борьбы с дизассемблером.
20. Способы борьбы с "хакером".
21. Способы привязки к дискете.
22. Способы привязки к компьютеру.
23. Общее представление о классах безопасности, определенных в "Оранжевой книге".
24. Функции систем защиты информации от несанкционированного доступа.
25. Идентификация и аутентификация пользователя. Определения. Формы хранения данных о пользователе. Структура данных о пользователе.
26. Две типовые схемы идентификации и аутентификации.
27. Биометрические методы идентификации и аутентификации пользователя.
28. Взаимная проверка подлинности пользователей.
29. Программы с потенциально опасными последствиями. Определение. Классификация.
30. Компьютерные вирусы. Классификация вирусов по способу заражения среды обитания.
31. Компьютерные вирусы. Классификация вирусов по деструктивным действиям.
32. Что такое "Люк", "Троянский конь", "Логическая бомба", "Атака салями"?
33. Программные закладки. Условия срабатывания. Основные группы деструктивных функций закладок.
34. Основные методы воздействия программных закладок на ЭЦП.
35. Задачи и методы борьбы с программными закладками.
36. Защита от вирусов и программных закладок. Организационно-технические меры. Общие способы защиты. Средства, учитывающие специфику работы фрагментов системы.
37. Брандмауэр. Определение. Типы.
38. Пакетные фильтры и сервера прикладного уровня. Достоинства и недостатки.
39. Компьютерные атаки. Определение. Модели.
40. Этапы реализации компьютерной атаки. Подробно - сбор информации.
41. Этапы реализации компьютерной атаки. Подробно - реализация и завершение.
42. Классификация компьютерных атак.
43. Основные задачи и дополнительные функции средств обнаружения компьютерных атак.
44. Безопасность электронной коммерции. Протокол SSL.
45. Безопасность электронной коммерции. Протокол SET.
46. Безопасность электронной коммерции. Сравнительная характеристика протоколов SSL и SET. Протокол 3D Secure.
47. ЭЦП. Проблема аутентификации данных.
48. ЭЦП. Однонаправленные хэш-функции
49. ЭЦП. Алгоритм безопасного хэширования SHA
50. ЭЦП. Однонаправленные хэш-функции на основе симметричных блочных алгоритмов
51. ЭЦП. Отечественный стандарт хэш-функции
52. Алгоритм ЭЦП "RSA"
53. Алгоритм ЭЦП "Эль Гамаля (EGSA)"
54. Алгоритм ЭЦП "DSA"
55. Отечественный стандарт ЭЦП
56. Безопасность электронных платежных систем. Пластиковые карты.

5.2. Темы письменных работ

1. Анализ уязвимостей сетей и защита от них
2. Программные средства обеспечения безопасности веб-приложений
3. Защита персональных данных в социальных сетях
4. Использование криптографических методов для защиты данных
5. Разработка алгоритмов шифрования информации
6. Создание системы шифрования и расшифровки сообщений
7. Разработка антивирусных программ и антихакерских средств
8. Обеспечение безопасности при передаче данных через интернет
9. Методы защиты от DDoS-атак и фишинга
10. Безопасность в облачных вычислениях
11. Защита от межсетевых атак
12. Анализ и предотвращение кибератак на компьютерные сети
13. Защита локальных сетей от внешних угроз
14. Использование биометрических технологий в системах безопасности
15. Разработка системы контроля доступа к информации в сетях
16. Анализ и прогнозирование угроз безопасности информации
17. Разработка методов обнаружения уязвимостей в операционных системах
18. Защита от хакерских атак на мобильные устройства
19. Создание системы резервного копирования и восстановления данных
20. Кибербезопасность государственных органов и крупных корпораций
21. Создание безопасной среды для онлайн-игр
22. Обнаружение и предотвращение внутренних угроз безопасности информации
23. Программное обеспечение для мониторинга безопасности сетей
24. Программное обеспечение для защиты от шпионского ПО

25. Методы обнаружения скрытых угроз в сети интернет
26. Разработка средств защиты от вредоносных программ
27. Защита банковской информации от кибератак
28. Использование технологии блокчейн для обеспечения безопасности данных
29. Разработка системы обнаружения и предотвращения взломов серверов
30. Программное обеспечение для защиты от кражи личных данных

5.3. Фонд оценочных средств

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

Разработка аппаратных средств обеспечения правовых данных
Разработка и установка во всех компьютерных правовых сетях журналов учета действий
Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

Хищение жестких дисков, подключение к сети, инсайдерство
Перехват данных, хищение данных, изменение архитектуры системы
Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

Персональная, корпоративная, государственная
Клиентская, серверная, сетевая
Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:

несанкционированного доступа, воздействия в сети
инсайдерства в организации
чрезвычайных ситуаций

5) Основные объекты информационной безопасности:

Компьютерные сети, базы данных
Информационные системы, психологическое состояние пользователей
Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:

Искажение, уменьшение объема, перекодировка информации
Техническое вмешательство, выведение из строя оборудования сети
Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:

Экономической эффективности системы безопасности
Многоплатформенной реализации системы
Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:

руководители, менеджеры, администраторы компаний
органы права, государства, бизнеса
сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:

Установление регламента, аудит системы, выявление рисков
Установка новых офисных приложений, смена хостинг-компании
Внедрение аутентификации, проверки контактных данных пользователей

тест 10) Принципом информационной безопасности является принцип недопущения:

Неоправданных ограничений при работе в сети (системе)
Рисков безопасности сети, системы
Презумпции секретности

11) Принципом политики информационной безопасности является принцип:

Невозможности миновать защитные средства сети (системы)
Усиления основного звена сети, системы
Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:

Усиления защищенности самого незащищенного звена сети (системы)
Перехода в безопасное состояние работы сети, системы
Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:

Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Одноуровневой защиты сети, системы
Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:

Компьютерный сбой
Логические закладки («мины»)
Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:

Прочитать приложение, если оно не содержит ничего ценного – удалить
Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:

Секретность ключа определена секретностью открытого сообщения
Секретность информации определена скоростью передачи данных
Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:

Электронно-цифровой преобразователь
Электронно-цифровая подпись
Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:

Покупка нелицензионного ПО
Ошибки эксплуатации и неумышленного изменения режима работы системы
Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:

Распределенный доступ клиент, отказ оборудования
Моральный износ сети, инсайдерство
Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:

Слабый трафик, информационный обман, вирусы в интернет
Вирусы в сети, логические мины (закладки), информационный перехват
Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:

Потерей данных в системе
Изменением формы информации
Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

Целостность
Доступность
Актуальность

23) Угроза информационной системе (компьютерной сети) – это:

Вероятное событие
Детерминированное (всегда определенное) событие
Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:

Регламентированной
Правовой
Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:

Программные, технические, организационные, технологические
Серверные, клиентские, спутниковые, наземные
Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:

Владелец сети
Администратор сети
Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:

Руководств, требований обеспечения необходимого уровня безопасности
Инструкций, алгоритмов поведения пользователя в сети
Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

Аудит, анализ затрат на проведение защитных мер
Аудит, анализ безопасности
Аудит, анализ уязвимостей, риск-ситуаций

5.4. Перечень видов оценочных средств

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых верный(ые). Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Дергачев К. В., Титарев Д. В.	Защита информации: лабораторный практикум: Учебное пособие	Москва: Русайнс, 2021, URL: https://book.ru/book/940250
Л1.2	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2021, URL: https://book.ru/book/938255
Л1.3	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020, URL: http://znanium.com/catalog/document?id=358722

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Трофимец И. А.	Государственные информационные системы учета населения: Монография	Москва: Русайнс, 2022, URL: https://book.ru/book/942744

	Авторы, составители	Заглавие	Издательство, год
Л2.2	Морозова О. А.	Информационные системы управления портфелями и программами проектов. (Магистратура). Учебное пособие: Учебное пособие	Москва: КноРус, 2019, URL: https://book.ru/book/932061
Л2.3	Ищейнов В. Я.	Информационная безопасность и защита информации: словарь терминов и понятий: Словарь	Москва: Русайнс, 2018, URL: https://book.ru/book/931784

6.2. Электронные учебные издания и электронные образовательные ресурсы	
Э1	Национальный открытый университет "ИНТУИТ" . - Режим доступа: https://www.intuit.ru/studies/courses%20
Э2	Электронно-библиотечная система . - Режим доступа: http://znanium.com/%20
Э3	ЭИОС. - Режим доступа: http://eios.imsit.ru/
Э4	ЭБС Айбукс. - Режим доступа: http://www.ibooks.ru/
Э5	РПД. - Режим доступа: http://rpd.eios.imsit.ru:8080/RPD/Index/1636711/%20http://www.book.ru
6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства	
6.3.1.1	Windows 10 Pro RUS Операцинная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL
6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Кодекс – Профессиональные справочные системы https://kodeks.ru
6.3.2.2	Консультант Плюс http://www.consultant.ru

7. МТО (оборудование и технические средства обучения)			
Ауд	Наименование	ПО	Оснащение
114а	Лаборатория программно-аппаратных средств защиты информации	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack MS Office Standart 2010 Traffic inspector Special Unlimited Ramus Educational	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение Коммутатор LincSys SR224G – 1 шт., проектор ViewSonic PJD5232 – 1 шт., проекционный экран Luma – 1 шт., шкаф телекоммуникационный – 1 шт., ИБП SMART UPS 2000 – 1 шт., коммутатор Cisco Catalist 2960 – 3 шт., концентратор AlterPath 16 port – 1 шт., маршрутизатор Cisco-2800 – 4 шт., маршрутизатор Cisco-2811 – 2 шт., модуль 2-port – 6 шт., панель коммутационная 2 шт., Шнур V.35 Cable – 12 шт., витая пара, коннектор RJ-45, инструмент для зачистки кабеля UTP – 2 шт., протяжка кабельная, d=3,5 мм 10 м – 1 шт., тестер МЕГЕОН 40060/Шт. – 1 шт., инструмент для обжима витой пары – 5 шт., Тестер кабельный – 5 шт., инструмент для заделки кабеля витая пара тип Krone с крючками – 3 шт., Р телефон GrandStream GXP1610 – 2 шт., комплект для монтажа СКС (патч-панель 1U kat.5e UTP 24 порта-1 шт., инструмент обжимной для RJ-45 1 шт., инструмент для зачистки кабеля 1 шт., инструмент для разделки контактов - 1 шт., LAN тестер 1 шт.) – 2 шт., роутер Wi-Fi роутер Keenetic – 2 шт., сервер GA-870A-USB3/AMD-Phenom(tm)-II-X4-945/ DDR3-1333-4Гб/SSD Flexis 120Gb/WD5000AAKX/Radeon HD-5800/Realtek PCIe GBE – 1 шт., аппаратные средства аутентификации пользователя: Соболь – 3 шт., эмуляторы активного сетевого оборудования в составе: Cisco Packet Tracer, Minine, Line Network Emulator, Marionnet – 21 шт., стенды для исследования параметров сетевого трафика в составе: WireShark, Snort, Colasoft Capsa Free, Ostinato, Suricata, Hping – 21 шт., средства антивирусной защиты: Kaspersky

		Micro-Cap Evaluation vGate Secren Net Studio Secren Net LSP Astra Linux Special Edition	Endpoint Security для бизнеса, Dr.Web Security Space, средства защиты информации: ОС Astra Linux SE 1.7 «Смоленск» – 21 шт., Secret Net Studio – 21 шт., Secret Net LSP – 21 шт., vGate – 21 шт., стенд «Континент» – 21 шт., средства криптографической защиты информации: PGP – 21 шт., КриптоПро УЦ, – 21 шт., КриптоАРМ – 21 шт., КриптоПро CSP – 21 шт., межсетевые экраны: встроенные в ОС, стенд «Континент» – 21 шт., IPTables – 21 шт., Colasoft Capsa Free – 21 шт., средства обнаружения компьютерных атак: XSpider – 21 шт., MaxPatrol VM – 21 шт.
121	Компьютерный класс	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclips Adobe Reader DC Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate ПО ЛИНКО v8.2 демо-версия Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	Стол - 20 шт., стул - 21 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., соответствующее программное обеспечение
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., многофункциональное устройство – 2 шт.

		PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

В соответствии с требованиями ФГОС ВО по направлению подготовки реализация компетентностного подхода предусматривает использование в учебном процессе активных и интерактивных форм проведения занятий (разбор конкретных задач, проведение блиц-опросов, исследовательские работы) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся.
Лекционные занятия дополняются ПЗ и различными формами СРС с учебной и научной литературой В процессе такой работы студенты приобретают навыки «глубокого чтения» - анализа и интерпретации текстов по методологии и методике дисциплины.
Учебный материал по дисциплине «Защита информационных процессов в компьютерных системах». разделен на логически завершенные части (модули), после изучения, которых предусматривается аттестация в форме письменных тестов, контрольных работ.
Работы оцениваются в баллах, сумма которых дает рейтинг каждого обучающегося. В баллах оцениваются не только знания и навыки обучающихся, но и их творческие возможности: активность, неординарность решений поставленных проблем. Каждый модуль учебной дисциплины включает обязательные виды работ – лекции, ПЗ, различные виды СРС (выполнение домашних заданий по решению задач, подготовка к лекциям и практическим занятиям).
Форма текущего контроля знаний – работа студента на практическом занятии, опрос. Форма промежуточных аттестаций – контрольная работа в аудитории, домашняя работа. Итоговая форма контроля знаний по модулям – контрольная работа с задачами по материалу модуля.
Методические указания по выполнению всех видов учебной работы размещены в электронной образовательной среде академии.
Методические указания и материалы по видам учебных занятий по дисциплине:
Вид учебных занятий, работ - Организация деятельности обучающегося
Лекция - Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения, отмечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, попытаться найти ответ в рекомендуемой литературе, если самостоятельно не удаётся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на консультации, на практическом занятии.
Практические занятия - Конспектирование источников. Работа с конспектом лекций, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с текстом. Выполнение практических задач в инструментальных средах. Выполнение проектов. Решение расчётно-графических заданий, решение задач по алгоритму и др.
Самостоятельная работа - Знакомство с основной и дополнительной литературой, включая справочные издания, зарубежные источники, конспект основных положений, терминов, сведений, требующихся для запоминания и являющихся основополагающими в этой теме. Составление аннотаций к прочитанным литературным источникам и др

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Методические указания по выполнению самостоятельной работы по дисциплине «Защита информационных процессов в компьютерных системах».
Формой осуществления контроля выполнения самостоятельной работы является подготовки рефератов на актуальные темы,
т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.
Цель реферата – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.
Основой разработки каждой темы является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно исследовательской задачи.
Процесс подготовки реферата состоит из следующих основных этапов:
1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных
средств анализа.
4. Сбор фактического материала.
5. Обработка и анализ полученной информации с применением современных методов анализа.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы в соответствии с установленными требованиями