МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Югорский государственный университет» (ЮГУ)
НЕФТЯНОЙ ИНСТИТУТ
(ФИЛИАЛ) ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «ЮГОРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(НефтИн (филиал) ФГБОУ ВО «ЮГУ»)

РАССМОТРЕНО
На заседании ПЦК ЭТД
Протокол № 7 «31» августа_2022г.
Председатель ПЦК
_____ Тен М.Б.

УТВЕРЖДАЮ
Зам. директора по УВР
НефтИн (филиал) ФГБОУ ВО «ЮГУ»
«31» августа 2022 г.
_____Хайбулина Р.И.

КОМПЛЕКТ КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ ПО МЕЖДИСЦИПЛИНАРНОМУ КУРСУ

МДК.03.03 ФИЗИЧЕСКИЕ ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ/ОСНОВЫ

ИНТЕЛЛЕКТУАЛЬНОГО ТРУДА

программы подготовки специалистов среднего звена (ППССЗ)

по специальности СПО

10.02.05 Обеспечение информационной безопасности автоматизированных систем
базовой подготовки

г. Нижневартовск
-2022-

Комплект контрольно-измерительных материалов по междисциплинарному курсу МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда программы подготовки специалистов среднего звена (ППССЗ) по специальности 10.02.05. Монтаж, наладка и эксплуатация электрооборудования промышленных и гражданских зданий базового уровня разработан на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности среднего профессионального образования (далее – СПО) 10.02.05 Обеспечение информационной безопасности автоматизированных систем, в соответствии с рабочей программой профессионального модуля ПМ.03 Защита информации техническими средствами.

Разработчики:

НефтИн (филиал) ФГБОУ ВО «ЮГУ» преподаватель Д.А. Садиков
(место работы) (занимаемая должность) (инициалы, фамилия)

1. Паспорт комплекта контрольно-измерительных материалов

1.1. Область применения

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения междисциплинарного курса (далее - МДК) МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда программы подготовки специалистов среднего звена (ППССЗ) по специальности (специальностям) СПО 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Комплект контрольно-измерительных материалов позволяет оценивать:

1.1.1. Освоение профессиональных компетенций (ПК) и общих компетенций (ОК)

Профессиональные и общие компетенции	Средства проверки (№ задания)
ПК 3.1. Осуществлять установку, монтаж, настройку и техническое обслуживание технических средств защиты информации в соответствии с требованиями эксплуатационной документации.;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ПК 3.3. Осуществлять измерение параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами обработки информации ограниченного доступа	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ПК 3.4. Осуществлять измерение параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ПК 3.5. Организовывать отдельные работы по физической защите объектов информатизации.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами,	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3

руководством, клиентами.	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 09. Использовать информационные технологии в профессиональной деятельности	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
ОК 10. Пользоваться профессиональной документацией на государственном и иностранных языках.	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3

1.1.2. Освоение умений и усвоение знаний

Освоенные умения, усвоенные знания	№№ заданий для проверки
1	2
У 1. применять технические средства для криптографической защиты информации конфиденциального характера;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
У 2. применять технические средства для уничтожения информации и носителей информации;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
У 3. применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
У 4. применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
У 5. применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
З 1. порядок технического обслуживания технических средств защиты информации;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
З 2. номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3

З 3. физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3
З 4. порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации;	Комплекс ПЗ №1 – №9 Самостоятельная работа №1 – №3

1.2. Система контроля и оценки освоения программы компонента ПМ - междисциплинарного курса

1.2.1. Формы рубежной аттестации по ППССЗ при освоении междисциплинарного курса

Междисциплинарный курс	Формы промежуточной аттестации
1	2
МДК.03.03Физические основы защиты информации / Основы интеллектуального труда	Дифференцированный зачет

1.2.2. Организация контроля и оценки освоения программы междисциплинарного курса

Текущий контроль по междисциплинарному курсу МДК.03.03Физические основы защиты информации / Основы интеллектуального труда осуществляется на учебных занятиях.

Рубежный контроль междисциплинарному курсу МДК.03.03Физические основы защиты информации / Основы интеллектуального труда (7 семестр) осуществляется на дифференцированном зачете. Дифференцированный зачет проводится в виде компьютерного тестирования.

Условием допуска к дифференцированному зачету является положительная оценка по всем практическим занятиям, самостоятельным работам.

Условием положительной аттестации по междисциплинарному курсу является положительная оценка освоения всех умений, знаний, а также формируемых профессиональных и общих компетенций по всем контролируемым показателям.

2 . Задания для оценки освоения умений и усвоения знаний

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

по МДК.03.03Физические основы защиты информации / Основы интеллектуального труда

ПРАКТИЧЕСКАЯ РАБОТА №1

ПРИМЕНЕНИЕ ПРАВОЫХ ОСНОВ ИСПОЛЬЗОВЫНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Цель занятия – закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Практические задания

Задание № 1 Разработать систему защиту информации в информационной системе на предприятии (выбор системы и предприятия произвольно). **Задание № 2** Проанализируйте Доктрину информационной безопасности Российской Федерации, утвержденной Президентом РФ от 5 декабря 2016 г. № 646 и определите основные направления обеспечения информационной безопасности в экономической сфере России.

ПРАКТИЧЕСКАЯ РАБОТА №2

ПРИМЕНЕНИЕ РАЗЛИЧНЫХ МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗПАСНОСТИ В ОПЕРАЦИОННЫХ СИСТЕМАХ

Цель занятия – получение знаний о методах защиты информации, которым подвергаются компьютерные системы и потерях банков.

Порядок выполнения работы:

1. Скопировать папку Y:\ИБ на диск S:\
2. Создать в папке S:\ИБ каталоги 1, 2, 3, 4.
3. Запустить программу ArtMasker.exe
4. В диалоговом режиме выполнить все рекомендации Мастера (в качестве файла-контейнера выбрать) S:\ИБ\фото\Sky_01.bmp, в качестве маскируемого файла выбрать S:\Virus.doc, задайте параметры скрытия как средние
5. Сохраните замаскированный файл с именем Security_1.bmp в папке S:\ИБ\1

6. Выполнить обратные действия ,сохранив размаскированный файл с именем Decod_1.doc в папке S:\ИБ\1
7. Переписать в тетрадь текст по описанию ArtMasker:

ArtMasker - эта программа может прятать информацию в рисунки (BMP 8bit, 16bit, 32bit) и музыкальные файлы(WAV 8bit 16bit). Уникальная возможность этой программы - установка параметров скрытия. Файл-контейнер не меняет своего размера. Имеется поддержка мультиязычности.

1. Запустить программу SimPass. Создать 5 паролей при помощи генератора, количество букв в пароле 10 (использовать специальные символы и латинские буквы). Выбрать любой понравившийся пароль и скопировать его в буфер.
2. Запустить программу Secret BMP (в качестве пароля использовать пароль – результат работы генератора паролей)
3. Создать **небольшой!!!!** растровый рисунок компьютерного вируса в редакторе PAINT, сохранив его с именем S:\ИБ\2\Pic.bmp
4. Скрыть файл Pic.bmp в файле S:\ИБ\фото\Sky_02.bmp, сохранив новый файл с именем Security_2.bmp в папке S:\ИБ\2(использовать сгенерированный пароль)
5. Выполнить обратные действия, сохранив извлеченный файл с именем Decod_2.bmp в папке S:\ИБ\2
6. Переписать в тетрадь текст по описанию Secret BMP и Simple Passwords:

Secret BMP - реализация методов стеганографии и криптографии для защиты данных, хранящихся в файлах любого формата. Методы стеганографии применяются для скрытия секретных данных внутри файла-контейнера. В качестве файла контейнера используются файлы растровых изображений формата bmp. Перед скрытием файла в файле-контейнере (bmp-картинке) файл шифруется с использованием метода гаммирования. Для получения гаммы в работе используется 32-разрядный генератор случайных

чисел, который программно реализуем и позволяет получать псевдослучайное число.

Simple Passwords - программа для генерирования одновременно нескольких паролей из случайных символов. Позволяет выбрать символы, из которых должен состоять пароль - английские и русские, строчные и прописные, цифры и специальные. Можно указать количество символов в пароле и общее количество генерируемых паролей.

1. Запустить программу CriptograFF для реализации криптозащиты из файла в файл
2. Открыть файл для шифрования S:\ИБ\VIP.txt
3. Зашифровать данный файл, присвоив ему имя S:\ИБ\3\Security_3.scr
4. Выполнить обратные действия, сохранив расшифрованный файл с именем Decod_3.txt в папке S:\ИБ\3
5. Выполнить криптозащиту открытых файлов
6. В окне программы набрать текст, где перечислить программно-технические средства защиты информации
7. Зашифровать открытый файл с именем S:\ИБ\3\Metod.txt
8. Переписать в тетрадь текст по описанию CriptograFF

CriptograFF -ш ифрует текстовые файлы криптографическим методом. Предназначена для шифрования текстовых файлов по алгоритму RC4. Особенности данного алгоритма - большая скорость, возможность потокового шифрования, практическая невозможность вскрытия зашифрованного файла.

1. Запустить программу Signature Cryptographer
2. Зашифруйте файл S:\ИБ\фото\Sky_04.bmp, выбрав в качестве файла-ключа любой свой файл
3. Сохраните этот файл с именем S:\ИБ\\4\Security_4
4. Выполнить обратные действия, сохранив извлеченный файл с именем Decod_4.bmp в папке S:\ИБ\\4
5. Переписать в тетрадь текст по описанию Signature Cryptographer:

Signature Cryptographer - программа защиты информации в важных файлах от несанкционированного доступа. Шифровальщик использует в качестве ключа содержимое файлов вместо строки пароля. Таким образом, длина пароля может достигать гигантских размеров или вовсе быть больше длины шифруемого файла, что делает зашифрованный файл теоретически не взламываемым. Вместо длинных строк пароля запомнить нужно только имя файла, используемого для пароля.

1. Показать работу преподавателю, получить оценку, удалить с диска S:\ИБ

ПРАКТИЧЕСКАЯ РАБОТА №3

АУТЕНТИФИКАЦИЯ В ОПЕРАЦИОННЫХ СИСТЕМАХ

Цель занятия - провести идентификацию и аутентификацию

Контрольные вопросы:

1.Перечислить виды паролей

2.От чего зависит надежность пароля?

3. Что такое парольная политика?

ПРАКТИЧЕСКАЯ РАБОТА №4

РАЗГРАНИЧЕНИЕ ДОСТУПА К ЗАЩИЩАЕМЫМ ОБЪЕКТАМ

Цель занятия- ознакомиться с принципами построения VPN на базе программного обеспечения.

Порядок выполнения работы:

1. Загрузить программу "LogMeIn Hamachi" с сайта http://hamachi.ru.softonic.com/ на оба компьютера будущей сети.
2. Создать сеть, пользуясь подсказками на сайте http://hamachiinfo.ru/nastrojka.html

3. Объединить в сеть принтер, камеру или другое устройство либо развернуть в сети какое-либо программное обеспечение (например, игру).

ПРАКТИЧЕСКАЯ РАБОТА №5

АУДИТ СОБЫТИЙ

Цель занятия -

1. получить навыки по планированию аудита, определив какие события необходимо отслеживать;

2. научиться настраивать аудит для файлов, папок и принтеров;

3. научиться использовать оснастку Просмотр событий для выполнения различных заданий, связанных с просмотром журнала аудита и содержимым файлов журнала безопасности, а также для поиска определенных событий в файлах журналов.

Порядок выполнения работы:

Спланируйте политику аудита для вашего компьютера. Затем активизируйте аудит конкретных событий. Назначьте аудит файла и принтера. Просмотрите файл журнала безопасности и задайте параметры в окне Event Viewer (Просмотр событий) для перезаписи журнала событий после его заполнения. Спланируете политику аудита для вашего компьютера. Вы должны определить следующее:

– какие типы событий отслеживать;

– отслеживать успех события, неудачу, или и то, и другое.

Действуйте следующим образом:

– записывайте неудачные попытки регистрации в системе;

– записывайте попытки несанкционированного доступа к файлам из вашей БД;

– отслеживайте использование цветного принтера;

– отслеживайте все попытки вмешательства в аппаратное обеспечение компьютера;

– храните запись действий, выполняемых администратором для отслеживания неразрешенных изменений;

– отслеживайте процедуры резервного копирования для предотвращения кражи данных;

– отслеживайте неразрешенный доступ к важным объектам Active Directory.

Запишите ваши решения в следующую таблицу.

Отслеживаемое действие	**Успешное**	**Неудачное**
Вход в систему		
Управление учетными записями		
Доступ к службе каталогов		
События входа в систему		
Доступ к объектам		
Изменение политики		
Использование привилегий		
Отслеживание процессов		
Системные события		

ПРАКТИЧЕСКАЯ РАБОТА №6

ПРИМЕНЕНИЕ ЗАЩИТНЫХ МЕР БЕЗОПАСНОСТИ ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМ В КОРПОРАТИВНОЙ СЕТИ

Цель занятия- изучить порядок вычисления и проверки ЭЦП (электронной цифровой подписи)

Порядок выполнения работы:

1. Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.
2. На стороне отправителя выполнить следующие действия:
    1. Записать сообщение M (см. вариант).
    2. Сформировать профиль сообщения M’ с помощью упрощенной функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения.
    3. Создать ЭЦП шифрованием профиля сообщения h(M’) закрытым ключом отправителя Da (значение ключа (d, n) см. в таблице с вариантами задания), т.е. Da (h(M’)) (см. вариант).
3. На стороне получателя выполнить следующие действия:
    1. Записать сообщение M (его получает получатель вместе с ЭЦП) и ЭЦП Da (h(M’)).
    2. Сформировать профиль принятого сообщения, M’ с помощью той же функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения (Получателю известен алгоритм хэширования, применяемый на стороне отправителя).
    3. Создать профиль дешифрованием ЭЦП открытым ключем отправителя (Ea (Da (h(M’)) = h(M’)) (значение ключа (e, n) см. в таблице с вариантами задания).
    1. Сравнить два профиля сообщения h(M’) (п.3.2 и 3.3). Убедиться в их совпадении.

Вариант – номер по списку в журнале.

Номер варианта	p	q	e	d	M
1	3	11	7	3	5523
3	17	11	7	23	8866
3	13	7	5	29	3565

4	101	113	3533	6597	6546
5	3	11	7	3	8562
6	17	11	7	23	9795
7	13	7	5	29	8462
8	17	11	7	23	7785
9	13	7	5	29	2123
10	101	113	3533	6597	3145
11	7	11	37	13	2566
12	101	113	3533	6597	3782
13	3	11	7	3	3465
14	17	11	7	23	3895
15	13	7	5	29	4132
16	17	11	7	23	5123
17	13	7	5	29	4416
18	101	113	3533	6597	7895
19	3	11	7	3	7459
20	17	11	7	23	5654
21	13	7	5	29	2456
22	17	11	7	23	3585
23	13	7	5	29	2652
24	101	113	3533	6597	5656
25	3	11	7	3	6685
26	17	11	7	23	5566
27	13	7	5	29	4652
28	17	11	7	23	8666
29	13	7	5	29	4556
30	101	113	3533	6597	9266

ПРАКТИЧЕСКАЯ РАБОТА №7

ОСНОНЫЕ АЛГОРИТМЫ ШИФРОВАНИЯ

Цель занятия - изучить протоколирование и аудит, а также криптографические методы защиты. Показать их место в общей архитектуре безопасности.

Порядок выполнения работы:

Часть 1:

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.
2. Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

1. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).
2. Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m_1, m_2, m_3 (см. вариант).

Вариант – номер по списку в журнале.

Номер варианта	Исходные данные							
	Часть 1	Часть 2						
	Алгоритм шифрования	p	q	e	d	$_1$	m_2	3
1	Простая перестановка	3	1	7	3	9	12	3
3	Одиночная перестановка	7	1	7	3	8	15	5
3	Двойная перестановка	3	7	5	9	3	16	5
4	Магический квадрат	01	13	533	597	6	19	3
5	Шифр Цезаря	7	1	7	3	8	18	1
6	Полибианский квадрат	7	7	5	7	9	11	6
7	Шифр Гронсфельда	3	1	7	3	8	13	5
8	Многоалфавитная замена	7	1	7	3	7	14	7
9	Простая перестановка	3	7	5	9	2	17	5
10	Одиночная перестановка	7	1	7	3	3	20	1
11	Двойная перестановка	3	7	5	9	2	12	5
12	Магический квадрат	01	13	533	597	3	15	6

13	Шифр Цезаря	7	1	7	3	3	16	4
14	Полибианский квадрат	7	7	5	7	3	19	6
15	Шифр Гронсфельда	3	1	7	3	4	18	5
16	Многоалфавитная замена	7	1	7	3	5	11	4
17	Простая перестановка	01	13	533	597	4	13	1
18	Одиночная перестановка	7	1	7	3	7	14	4
19	Двойная перестановка	7	7	5	7	7	17	3
20	Магический квадрат	3	1	7	3	5	20	3
21	Шифр Цезаря	7	1	7	3	2	11	5
22	Полибианский квадрат	3	7	5	9	3	13	7
23	Шифр Гронсфельда	7	1	7	3	2	14	9
24	Многоалфавитная замена	3	7	5	9	5	17	6
25	Простая перестановка	01	13	533	597	6	20	2

ПРАКТИЧЕСКАЯ РАБОТА №8

КРИПТОАНАЛИЗ И АТАКИ КРИПТОСИСТЕМЫ

Цель занятия - изучить методы криптоанализа шифров перестановки.

Порядок выполнения работы:

1.Дешифровать сообщение: Бирои имч еыеес витсч арзки танет есарл лпюсп мотоо еипнф кйаои крслт мн

2. Дешифровать сообщение: тиооско нцрпоед иявдттж афэелиа ткокнбв еапанъг уитриоб

3. Дешифровать сообщение: икинорткелэоидаржделлок

Контрольные вопросы.

1.Оценить надежность шифрования перестановкой

2.От чего зависит возможность успешного проведения криптоанализа шифров перестановки.

3. Насколько увеличивается сложность криптоанализа двойной перестановки.

ПРАКТИЧЕСКАЯ РАБОТА №9

УПРАВЛЕНИЕ КЛЮЧАМИ

Цель занятия - изучить алгоритм Диффи-Хелмана. Освоить методы генерации больших простых чисел и методы проверки больших чисел на простоту. Научиться строить первообразные корни по модулю n.

Порядок выполнения работы:

Произвести расчет ключа.

1.Совместно с удалённой стороной устанавливить открытые параметры p и g (обычно значения p и g генерируются на одной стороне и передаются другой), где p является случайным простым числом (p-1)/2 также должно быть случайным простым числом (для повышения безопасности) g является первообразным корнем по модулю p

2.Вычислить открытый ключ A, используя преобразование над закрытым ключом A = ga mod p для каждого студента.

3.Обменяться открытыми ключами с удалённой стороной

4.Вычислить общий секретный ключ K, используя открытый ключ удаленной стороны B и свой закрытый ключ a K = Ba mod p K получается равным с обеих сторон, потому что: B a mod p = (gb mod p)a mod p = g ab mod p = (ga mod p)b mod p = Ab mod p

5. Сравнить общие ключи.

Контрольные вопросы:

1.Для чего применяется алгоритм Диффи-Хеллмана?

2.Что такое модулярная математика?

3.Чем обеспечивается секретность получаемого ключа?

Критерии оценивания практических занятий

Оценка	Описание оценок
5	Отлично- «5» - содержание материала освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.
4	Хорошо-«4» - содержание материала освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.
3	Удовлетворительно-«3» - содержание материала освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, содержат ошибки.
2	Условно неудовлетворительно- «2» - содержание материала освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.

Составитель _____ / Садиков Д.А. /

подпись Ф.И.О.

«___» _____ 2022 г.

к комплекту КИМ по МДК

ТЕМЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

по междисциплинарному курсу МДК.03.03Физические основы защиты информации / Основы интеллектуального труда

ПЗ	Темы практических занятий	Освоенные умения, усвоенные знания
7 семестр		
	Раздел 1. Обеспечение информационной безопасности	
	Тема 1.1 Правовое обеспечение информационной безопасности	
	Применение правовых основ использования организационных и технических средств защиты информации.	У 1. – У 5. З 1. – З 4.
	Раздел 2. Информационная безопасность в различных системах	
	Тема 2.1 Безопасность операционных систем	
	Применение различных методов обеспечения информационной безопасности в операционных системах	У 1. – У 5. З 1. – З 4.
	Аутентификация в операционных системах.	У 1. – У 5. З 1. – З 4.
	Разграничение доступа к защищаемым объектам.	У 1. – У 5. З 1. – З 4.
	Аудит событий..	У 1. – У 5. З 1. – З 4.
	Тема 2.3 Безопасность вычислительных систем	
	Применение защитных мер безопасности вычислительных систем в корпоративной сети	У 1. – У 5. З 1. – З 4.
	Раздел 3. Методы защиты информации	
	Тема 3.1 Криптографические методы защиты информации	
	Основные алгоритмы шифрования	У 1. – У 5. З 1. – З 4.
	Криптоанализ и атаки на криптосистемы	У 1. – У 5. З 1. – З 4.

	Управление ключами	У 1. – У 5. З 1. – З 4.
Перечень контрольных вопросов для защиты практических работ:		
Раздел 1. Обеспечение информационной безопасности		
Тема 1.1 Правовое обеспечение информационной безопасности		
1. Понятие информационной безопасности. 2. Виды и источники угроз информационной безопасности РФ. 3. Методы обеспечения информационной безопасности РФ. 4. Основные направления обеспечения информационной безопасности. 5. Система защиты информации, содержащейся в информационной системе, защиты информации на предприятие.		
Раздел 2. Информационная безопасность в различных системах		
Тема 2.1 Безопасность операционных систем		
1. Перечислить виды паролей 2. От чего зависит надежность пароля? 3. Что такое парольная политика?		
Раздел 3. Методы защиты информации		
Тема 3.1 Криптографические методы защиты информации		
1. Оценить надежность шифрования перестановкой 2. От чего зависит возможность успешного проведения криптоанализа шифров перестановки. 3. Насколько увеличивается сложность криптоанализа двойной перестановки. 4. Для чего применяется алгоритм Диффи-Хеллмана? Что такое модулярная математика? Чем обеспечивается секретность получаемого ключа?		

Критерии оценки:

- оценка «отлично» выставляется студенту, если ..…90 – 100 %;
- оценка «хорошо» …… ……80 – 89 %;
- оценка «удовлетворительно» ……70 – 79 %;
- оценка «неудовлетворительно» ……..…< 70 %.

Составитель _____ / Садиков Д.А. /

подпись Ф.И.О.

к комплекту КИМ по МДК

КОМПЛЕКТ ЗАДАНИЙ

ДЛЯ ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ №1

по междисциплинарному курсу МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда.

Раздел 1. Обеспечение информационной безопасности

Вариант 1.

1. Кто может проверить электронно-цифровую подпись под документом.
2. Что входит в правовой режим документированной информации.
3. Чем определяется уровень надежности применяемых криптографических преобразований.
4. Кто образует организационную структуру системы государственного лицензирования деятельности предприятий в области защиты информации.
5. Какой закон содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни граждан.

Вариант 2.

1. Какое название носит обособленный объем информации, представленный в электронно-цифровой форме, зафиксированный на электронном носителе и могущий быть представленным в форме, пригодной для восприятия человеком.
2. В отношении каких сведений не устанавливается режим защиты информации
3. Какие функции выполняют государственные органы по лицензированию.
4. Назовите основные источники угроз информационной безопасности.

5. Между кем регулирует правовые отношения Федеральный закон о персональных данных

Вариант 3.

1. Как называется реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации.

2. Чем является информация с точки зрения информационного права.

3. Какие из сервисов реализуются при использовании криптографических преобразований.

4. Какие функции выполняют лицензионные центры.

5. Что такое информационная безопасность.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ..…90 – 100 %;
- оценка «хорошо» …… ……80 – 89 %;
- оценка «удовлетворительно» ……70 – 79 %;
- оценка «неудовлетворительно» ……..…< 70 %.

Составитель _____ / Садиков Д.А. /

подпись Ф.И.О.

к комплекту КИМ по МДК

КОМПЛЕКТ ЗАДАНИЙ

ДЛЯ ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ №2

по междисциплинарному курсу МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда.

Раздел 2. Информационная безопасность в различных системах

Вариант 1

1. Какой из корневых разделов системного реестра хранит информацию об установленных в данный момент аппаратурных средства.
2. Какие традиционные способы защиты имеет база данных.
3. Дать определение термину «защита информации от непреднамеренного воздействия
4. Какой из стандартов аутентификации в WLAN наиболее надежен.
5. Что позволяет получить атакующему высокий уровень риска уязвимости.

Вариант 2

1. Что такое системный реестр.
2. Кто имеет право доступа открытия Базы данных в монопольном режиме.
3. Дать определение термину «защита информации от утечки».
4. Какими способами могут подвергнуться атакам системы шифрования.
5. Что позволяет получить атакующему средний уровень риска уязвимости.

Вариант 3

1. Какой из корневых разделов системного реестра содержит информацию о технологии OLE, отвечает за настройки интерфейса.

2. Кто имеет право доступа для чтения макета.

3. Дать определение термину «защищаемый объект информатизации».

4. Какие основные меры необходимо предпринять для защиты сервера от атак злоумышленника через интернет.

5. Что позволяет получить атакующему низкий уровень риска уязвимости.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ..…90 – 100 %;
- оценка «хорошо» …… ……80 – 89 %;
- оценка «удовлетворительно» ……70 – 79 %;
- оценка «неудовлетворительно» ……..…< 70 %.

Составитель _____ / Садиков Д.А. /

подпись Ф.И.О.

к комплекту КИМ по МДК

КОМПЛЕКТ ЗАДАНИЙ

ДЛЯ ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ №3

по междисциплинарному курсу МДК.03.03 Физические основы защиты информации / Основы интеллектуального труда.

Раздел 3. Методы защиты информации.

Вариант 1

1. Как называется однозначное преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины.
2. Какие требования предъявляются к криптографическим хеш-функциям.
3. Каковы уровни доступа к хранимой, обрабатываемой и защищаемой автоматизированной системе информации. Что является симптомами заражения данных.
4. На что разделяются криптосистемы.

Вариант 2

1. Как называется функция, которая для строки произвольной длины вычисляет некоторое целое значение или некоторую другую строку фиксированной длины.
2. Какие требования предъявляются к криптографическим хеш-функциям.
3. Понятие защищенной системы обработки информации.
4. Что является показателем безопасности информации.
5. Перечислите показатели криптостойкости.

Вариант 3

1. Как называется значение хеш-функции.
2. Какие требования предъявляются к криптографическим хеш-функциям.

3. Что такое ядро безопасности.
4. Перечислить технические средства передачи информации.
5. Что из себя представляет криптографическая система.

Критерии оценки:

- оценка «отлично» выставляется студенту, если ..…90 – 100 %;
- оценка «хорошо» …… ……80 – 89 %;
- оценка «удовлетворительно» ……70 – 79 %;
- оценка «неудовлетворительно» ……..…< 70 %.

Составитель _____ / Садиков Д.А. /

подпись Ф.И.О.