МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе
_____ / О.В. Юсупова
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.01.20 «Компьютерная вирусология»

Код и направление подготовки (специальность)	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Вычислительные машины, комплексы, системы и сети
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра "Вычислительная техника"
Кафедра-разработчик	кафедра "Вычислительная техника"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

Самара 2022

Б1.В.01.20 «Компьютерная вирусология»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **09.03.01 Информатика и вычислительная техника**, утвержденного приказом Министерства образования и науки РФ от № 929 от 19.09.2017 и соответствующего учебного плана.

Разработчик РПД:

Доцент, кандидат химических наук, доцент	А.В Чуваков
(должность, степень, ученое звание)	(ФИО)

Заведующий кафедрой	А.В. Иващенко, доктор технических наук, профессор
	(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	Я.Г Стельмах, кандидат педагогических наук
	(ФИО, степень, ученое звание)
Руководитель образовательной программы	С.П. Орлов, доктор технических наук, профессор
	(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы 4
2. Место дисциплины (модуля) в структуре образовательной программы 4
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 5
4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 5
4.1 Содержание лекционных занятий 6
4.2 Содержание лабораторных занятий 7
4.3 Содержание практических занятий 9
4.4. Содержание самостоятельной работы 9
5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю) 9
6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения 10
7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 10
8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю) 11
9. Методические материалы 12
10. Фонд оценочных средств по дисциплине (модулю) 13

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-5 Способность обеспечивать информационную безопасность информационно-вычислительных систем	ПК-5.1 Знает методики обеспечения информационной безопасности информационно-вычислительных систем.	Знать методики обеспечения информационной безопасности информационно-вычислительных систем.
		ПК-5.2 Умеет обеспечивать информационную безопасность информационно-вычислительных систем	Владеть обеспечивать информационную безопасность информационно-вычислительных систем
			Уметь обеспечивать информационную безопасность информационно-вычислительных систем
	ПК-6 Владение навыками использования различных технологий разработки программного обеспечения	ПК-6.7 Знает методики использования различных технологий разработки программного обеспечения для защиты информации	Знать методики использования различных технологий разработки программного обеспечения для защиты информации
		ПК-6.8 Умеет использовать различные технологии разработки программного обеспечения для защиты информации	Уметь использовать различные технологии разработки программного обеспечения для защиты информации
		ПК-6.9 Имеет навыки использования различных технологий разработки программного обеспечения для защиты информации.	Владеть навыки использования различных технологий разработки программного обеспечения для защиты информации.

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **часть, формируемая участниками образовательных отношений**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
ПК-5	Программирование интернета вещей; Производственная практика: технологическая (проектно-технологическая) практика; Производственная практика: эксплуатационная практика	Выполнение и защита выпускной квалификационной работы	
ПК-6	Алгоритмы и структуры данных; Базы данных; Планирование эксперимента; Программирование на языке Java; Разработка интернет-приложений; Системное программное обеспечение	Выполнение и защита выпускной квалификационной работы; Производственная практика: преддипломная практика	

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	8 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	48	48
Лабораторные работы	32	32
Лекции	16	16
Внеаудиторная контактная работа, КСР	4	4
Самостоятельная работа (всего), в том числе:	56	56
выполнение творческого задания (групповых, индивидуальных)	10	10
подготовка к лабораторным работам	42	42
подготовка к участию в собеседовании	4	4
Контроль	36	36
Итого: час	144	144
Итого: з.е.	4	4

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

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	4	8	0	16	28
2	Криптографические модели, алгоритмы и протоколы.	6	8	0	20	34
3	Защита информации в компьютерных сетях, оборудование защиты информации	6	16	0	20	42
	КСР	0	0	0	0	4
	Контроль	0	0	0	0	36
	Итого	16	32	0	56	144

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
8 семестр				
1	Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	Основные понятия компьютерной безопасности.	Основные виды компьютерных вирусов: черви, троянские кони, логические бомбы. Основные криптографические термины и определения. Механизмы и виды угроз на информацию.	2
2	Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	Стандарты и законодательные акты в области компьютерной безопасности.	Национальные стандарты, законодательные акты и постановления. Правительства РФ Международные стандарты в области компьютерной безопасности и защиты информации.	2
3	Криптографические модели, алгоритмы и протоколы.	Структура загрузочных модулей и аппаратно-программные прерывания	Структура загрузочных модулей. Аппаратные и программные прерывания. Структурная модель многоуровневого доступа. Защита программных модулей от модификации	2
4	Криптографические модели, алгоритмы и протоколы.	Криптографические алгоритмы. История развития	Шифры замены. Шифр Люцифер как прообраз алгоритма DES	2
5	Криптографические модели, алгоритмы и протоколы.	Симметричные алгоритмы. Ассиметричные алгоритмы	Алгоритм DES, 3DES. Режимы шифрования алгоритма DES. Подмена шифра в режиме OFB. Алгоритм ГОСТ 28147-89. АлгоритмДиффи-Хелмана. Алгоритм RSA.	2
6	Защита информации в компьютерных сетях, оборудование защиты информации	. Защита информации в компьютерных сетях	Программирование межсетевых экранов. Средства обнаружения вторжений.	2
7	Защита информации в компьютерных сетях, оборудование защиты информации	Программные средства антивирусной защиты.	Организационные меры антивирусной защиты. Отечественные и зарубежные антивирусные программы.	2
8	Защита информации в компьютерных сетях, оборудование защиты информации	Аппаратные средства защиты информации	Использование HSM в платёжных системах. Виды ключей и их назначение в HSM	2
			Итого за семестр:	**16**

Итого:	**16**

4.2 Содержание лабораторных занятий

№ занятия	Наименование раздела	Тема лабораторного занятия	Содержание лабораторного занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
8 семестр				
1	Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	Программная реализация шифра Виженера и шифра полиалфавитной замены	Анализ частотных характеристик открытого и шифртекста.	2
2	Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	Программная реализация шифра Виженера и шифра полиалфавитной замены	Анализ частотных характеристик открытого и шифртекста.	2
3	Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	Исследование ассиметричных алгоритмов.	Программная реализация алгоритма RSA. Реализация операции "возведение в степень по модулю"	2
4	Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	Исследование ассиметричных алгоритмов.	Программная реализация алгоритма RSA. Реализация операции "возведение в степень по модулю"	2
5	Криптографические модели, алгоритмы и протоколы.	Исследование HASH - функций	Программная реализация электронной цифровой подписи.	2
6	Криптографические модели, алгоритмы и протоколы.	Исследование HASH - функций	Программная реализация электронной цифровой подписи.	2
7	Криптографические модели, алгоритмы и протоколы.	Программная реализация генератора псевдослучайных чисел	Неприводимые многочлены высокой степени.	2

8	Криптографические модели, алгоритмы и протоколы.	Программирование межсетевых экранов	Составление стандартных списков доступа (accesslist)	2
9	Защита информации в компьютерных сетях, оборудование защиты информации	Реализация программной модели использования устройств аппаратной защиты HSM.	Межцентровая защита информации в платёжных системах.	2
10	Защита информации в компьютерных сетях, оборудование защиты информации	Реализация программной модели использования устройств аппаратной защиты HSM.	Межцентровая защита информации в платёжных системах.	2
11	Защита информации в компьютерных сетях, оборудование защиты информации	Программирование межсетевых экранов.	Составление именованных списков доступа (accesslist)	2
12	Защита информации в компьютерных сетях, оборудование защиты информации	Программирование межсетевых экранов.	Составление именованных списков доступа (accesslist)	2
13	Защита информации в компьютерных сетях, оборудование защиты информации	Программирование межсетевых экранов.	Составление расширенных списков доступа (accesslist)	2
14	Защита информации в компьютерных сетях, оборудование защиты информации	Программирование межсетевых экранов.	Составление расширенных списков доступа (accesslist)	2
15	Защита информации в компьютерных сетях, оборудование защиты информации	Программирование межсетевых экранов	Составление стандартных списков доступа (accesslist)	2
16	Защита информации в компьютерных сетях, оборудование защиты информации	Программирование межсетевых экранов	Составление стандартных списков доступа (accesslist)	2
			Итого за семестр:	**32**

Итого:	**32**

4.3 Содержание практических занятий

Учебные занятия не реализуются.

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
8 семестр			
Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности	Подготовка к лабораторной работе № 1	Программная реализация шифра Виженера и шифра полиалфавитной замены.	16
Криптографические модели, алгоритмы и протоколы.	Подготовка к лабораторным работам № 2 – 4	Исследование ассиметричных алгоритмов. Программная реализация генератора псевдослучайных чисел Исследование HASH - функций.	10
Криптографические модели, алгоритмы и протоколы.	Индивидуальные задания	Индивидуальные задания	10
Защита информации в компьютерных сетях, оборудование защиты информации	Подготовка к лабораторным работам № 5 – 8	Программирование межсетевых экранов. Реализация программной модели использования устройств аппаратной защиты HSM.	16
Защита информации в компьютерных сетях, оборудование защиты информации	Подготовка к тестированию	Подготовка к тестированию	4
		Итого за семестр:	**56**
		Итого:	**56**

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	**Библиографическое описание**	**Ресурс НТБ СамГТУ** (ЭБС СамГТУ, IPRbooks и т.д.)
Основная литература		

1	Буканов, Ф.Ф. Организационное обеспечение информационной безопасности : Учеб.пособие / Ф. Ф. Буканов, В. М. Кузнецов; Гос.образоват.учреждение высш.проф.образования Самар.гос.техн.ун-т.- Самара, 2007.- 344 с.	Электронный ресурс
2	Гайдамакин, Н.А. Разграничение доступа к информации в компьютерных системах / Н. А. Гайдамакин.- Екатеринбург, Изд-во Урал.ун-та, 2003.- 327 с.	Электронный ресурс
3	Девянин, П.Н. Модели безопасности компьютерных систем : Учеб.пособие / П. Н. Девянин.- М., Academia, 2005.- 143 с.	Электронный ресурс
4	Казанцев, С.Я. Правовое обеспечение информационной безопасности : Учеб.пособие / Под ред.С.Я.Казанцева .- 3-е изд.,стер..- М., Academia, 2008.- 239 с.	Электронный ресурс
5	Мельников, В.П. Информационная безопасность : учеб.пособие / В. П. Мельников, С. А. Клейменов, А. М. Петраков .- 3-е изд.,стер..- М., Академия, 2008.- 332 с.	Электронный ресурс
6	Одинцов, А.А. Экономическая и информационная безопасность : Справ.:Учеб.пособие / А. А. Одинцов.- М., Экзамен, 2005.- 575 с.	Электронный ресурс
7	Хисамутдинов, В.Р. Автоматизированная система информационного обеспечения разработок / В.Р.Хисамутдинов,В.С.Авраменко,В.И.Легоньков.- М., Наука, 1980.- 209 с.	Электронный ресурс
8	Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : Учеб.пособие / П. Б. Хорев.- М., Academia, 2005.- 255 с.	Электронный ресурс
Дополнительная литература		
9	Вендров, А.М. Практикум по проектированию программного обеспечения экономических информационных систем : Учеб.пособие / А. М. Вендров .- 2-е изд.,перераб.и доп..- М., Финансы и статистика, 2006.- 191 с.	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	ОС MS Windows 10	Microsoft (Зарубежный)	Лицензионное
2	Microsoft Windows 7 Pro-fessional операционная системат	Microsoft (Зарубежный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Национальный открытый университет ИНТУИТ	http://www.intuit.ru	Ресурсы открытого доступа
2	Государственная публичная научно-техническая библиотека России (ГПНТБ)	http://www.gpntb.ru/win/ntb/	Ресурсы открытого доступа
3	РОСПАТЕНТ	http://www1.fips.ru/wps/wcm/connect/content_ru/ru	Ресурсы открытого доступа
4	Поисковая система SciVerse	http://www.scopus.com	Ресурсы открытого доступа
5	Научная электронная библиотека «Киберленинка»	https://cyberleninka.ru	Ресурсы открытого доступа
6	Библиотека учебно-методической литературы системы "Единое окно"	http://window.edu.ru/	Ресурсы открытого доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Аудитории для лекционных занятий укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории (наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия, тематические иллюстрации).

Практические занятия

не предусмотрены

Лабораторные занятия

Для лабораторных занятий используются аудитория №314, корпус № 8, оснащенная следующим оборудованием:

компьютерами iRU i3-4160/4 GB с мониторами Samsung S20D300NH (11 шт.) с выходом в сеть Интернет. с лицензионным программным обеспечением, коммутатором D-Link DES? мультимедийным проектором DS 1700 , экраном переносным.

Для лабораторных занятий используются аудитория №309, корпус № 8, оснащенная следующим оборудованием:

компьютерами Intel Core 2 Duo E6300 с мониторами LG Flatron L1752S – SF17 (11 шт). с выходом в Интернет, с лицензионным программным обеспечением, коммутатором HUB Compex PS16, мультимедийным проектором NEC, экраном настенным проекционным.

Самостоятельная работа

Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интеренет» и доступом к электронной информационно-образовательной среде СамГТУ:

- читальный зал НТБ СамГТУ (ауд. 200 корпус № 8; ауд. 125 корпус № 1; ауд. 41, 31, 34, 35 Главный корпус библиотеки, ауд. 83а, 414, 416, 0209 АСА СамГТУ; ауд. 401 корпус №10);

- компьютерные классы (ауд. 208, 210 корпус № 8).

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при работе на лабораторном занятии

Проведение лабораторной работы делится на две условные части: теоретическую и практическую.

Необходимыми структурными элементами занятия являются проведение лабораторной работы, проверка усвоенного материала, включающая обсуждение теоретических основ выполняемой работы.

Перед лабораторной работой, как правило, проводится технико-теоретический инструктаж по использованию необходимого оборудования. Преподаватель корректирует деятельность обучающегося в процессе выполнения работы (при необходимости). После завершения лабораторной работы подводятся итоги, обсуждаются результаты деятельности.

Возможны следующие формы организации лабораторных работ: фронтальная, групповая и индивидуальная. При фронтальной форме выполняется одна и та же работа (при этом возможны различные варианты заданий). При групповой форме работа выполняется группой (командой). При индивидуальной форме обучающимися выполняются индивидуальные работы.

По каждой лабораторной работе имеются методические указания по их выполнению, включающие необходимый теоретический и практический материал, содержащие элементы и последовательную инструкцию по проведению выбранной работы, индивидуальные варианты заданий, требования и форму отчетности по данной работе.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения

дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.01.20 «Компьютерная вирусология»

Фонд оценочных средств
по дисциплине
Б1.В.01.20 «Компьютерная вирусология»

Код и направление подготовки (специальность)	09.03.01 Информатика и вычислительная техника
Направленность (профиль)	Вычислительные машины, комплексы, системы и сети
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2022
Институт / факультет	Институт автоматики и информационных технологий
Выпускающая кафедра	кафедра "Вычислительная техника"
Кафедра-разработчик	кафедра "Вычислительная техника"
Объем дисциплины, ч. / з.е.	144 / 4
Форма контроля (промежуточная аттестация)	Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-5 Способность обеспечивать информационную безопасность информационно-вычислительных систем	ПК-5.1 Знает методики обеспечения информационной безопасности информационно-вычислительных систем.	Знать методики обеспечения информационной безопасности информационно-вычислительных систем.
		ПК-5.2 Умеет обеспечивать информационную безопасность информационно-вычислительных систем	Владеть обеспечивать информационную безопасность информационно-вычислительных систем
			Уметь обеспечивать информационную безопасность информационно-вычислительных систем
	ПК-6 Владение навыками использования различных технологий разработки программного обеспечения	ПК-6.7 Знает методики использования различных технологий разработки программного обеспечения для защиты информации	Знать методики использования различных технологий разработки программного обеспечения для защиты информации
		ПК-6.8 Умеет использовать различные технологии разработки программного обеспечения для защиты информации	Уметь использовать различные технологии разработки программного обеспечения для защиты информации
		ПК-6.9 Имеет навыки использования различных технологий разработки программного обеспечения для защиты информации.	Владеть навыки использования различных технологий разработки программного обеспечения для защиты информации.

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Основные понятия безопасности информации, источники угроз, стандарты и законодательные акты по информационной безопасности				
ПК-5.1 Знает методики обеспечения информационной безопасности информационно-вычислительных систем.	**Знать** методики обеспечения информационной безопасности информационно-вычислительных систем.	Отчеты по лабораторным работам	Да	Да
ПК-5.2 Умеет обеспечивать информационную безопасность информационно-вычислительных систем	**Уметь** обеспечивать информационную безопасность информационно-вычислительных систем	Отчеты по лабораторным работам	Да	Да
	Владеть обеспечивать информационную безопасность информационно-вычислительных систем	Отчеты по лабораторным работам	Да	Да

ПК-6.7 Знает методики использования различных технологий разработки программного обеспечения для защиты информации	**Знать** методики использования различных технологий разработки программного обеспечения для защиты информации	Отчеты по лабораторным работам	Да	Да
ПК-6.8 Умеет использовать различные технологии разработки программного обеспечения для защиты информации	**Уметь** использовать различные технологии разработки программного обеспечения для защиты информации	Отчеты по лабораторным работам	Да	Да
ПК-6.9 Имеет навыки использования различных технологий разработки программного обеспечения для защиты информации.	**Владеть** навыки использования различных технологий разработки программного обеспечения для защиты информации.	Отчеты по лабораторным работам	Да	Да
Криптографические модели, алгоритмы и протоколы.				
ПК-5.1 Знает методики обеспечения информационной безопасности информационно-вычислительных систем.	**Знать** методики обеспечения информационной безопасности информационно-вычислительных систем.	Отчеты по лабораторным работам	Да	Да
ПК-5.2 Умеет обеспечивать информационную безопасность информационно-вычислительных систем	**Владеть** обеспечивать информационную безопасность информационно-вычислительных систем	Отчеты по лабораторным работам	Да	Да
	Уметь обеспечивать информационную безопасность информационно-вычислительных систем	Отчеты по лабораторным работам	Да	Да
ПК-6.7 Знает методики использования различных технологий разработки программного обеспечения для защиты информации	**Знать** методики использования различных технологий разработки программного обеспечения для защиты информации	Отчеты по лабораторным работам	Да	Да
ПК-6.8 Умеет использовать различные технологии разработки программного обеспечения для защиты информации	**Уметь** использовать различные технологии разработки программного обеспечения для защиты информации	Отчеты по лабораторным работам	Да	Да
ПК-6.9 Имеет навыки использования различных технологий разработки программного обеспечения для защиты информации.	**Владеть** навыки использования различных технологий разработки программного обеспечения для защиты информации.	Отчеты по лабораторным работам	Да	Да
Защита информации в компьютерных сетях, оборудование защиты информации				
ПК-5.1 Знает методики обеспечения информационной безопасности информационно-вычислительных систем.	**Знать** методики обеспечения информационной безопасности информационно-вычислительных систем.	Отчеты по лабораторным работам	Да	Да

ПК-5.2 Умеет обеспечивать информационную безопасность информационно-вычислительных систем	**Владеть** обеспечивать информационную безопасность информационно-вычислительных систем	Отчеты по лабораторным работам	Да	Да
	Уметь обеспечивать информационную безопасность информационно-вычислительных систем	Отчеты по лабораторным работам	Да	Да
ПК-6.7 Знает методики использования различных технологий разработки программного обеспечения для защиты информации	**Знать** методики использования различных технологий разработки программного обеспечения для защиты информации	Отчеты по лабораторным работам	Да	Да
ПК-6.8 Умеет использовать различные технологии разработки программного обеспечения для защиты информации	**Уметь** использовать различные технологии разработки программного обеспечения для защиты информации	Отчеты по лабораторным работам	Да	Да
ПК-6.9 Имеет навыки использования различных технологий разработки программного обеспечения для защиты информации.	**Владеть** навыки использования различных технологий разработки программного обеспечения для защиты информации.	Отчеты по лабораторным работам	Да	Да

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Проверка достижения индикаторов компетенций в части «Знать» выполняется с помощью тестирования.

1. Что из следующего является типом программы, которая либо не скрывает своего присутствия, либо описывается как имеющая набор полезных или желательных функций, но на самом деле содержит вредоносный код.
A) Трояны
B) Вирусы
C) Червь
D) Рекламное ПО
E) Боты
Ответ A

2. Что из перечисленного относится к типу программного обеспечения, в котором есть самовоспроизводящееся программное обеспечение, которое вызывает повреждение файлов и системы?
A) Вирусы
B) Троянские кони
C) Боты
D) Черви
E) Бэкдоры
Ответ D

3. Что из перечисленного является программой, способной непрерывно воспроизводиться с минимальным вмешательством пользователя или без него?
A) Вирус
B) Троянские кони
C) Руткит
D) Черви
E) Боты
Посмотреть ответ
Ответ A

4. Что из перечисленного представляет собой программное обеспечение, которое после установки на ваш компьютер отслеживает ваши привычки просмотра Интернета и отправляет вам всплывающие окна с рекламой, связанной с сайтами и темами, которые вы посещали?
A) Бэкдоры
B) Рекламное ПО
C) Вредоносное ПО
D) Боты
E) шпионское ПО
Ответ B

5. Как называется программное обеспечение, предназначенное для применения пользователем компьютера, и которое включаеткомпьютерные вирусы, черви,

трояны, рекламное ПО и т. д.?
A) Бэкдоры
B) Кейлоггер
C) Вредоносное ПО
D) Боты
E) шпионское ПО
Ответ C

6. Как называется программное обеспечение, которое при загрузке на компьютер сканирует ваш жесткий диск в поисках личной информации и ваших привычек просмотра Интернета?
A) Бэкдоры
B) Кейлоггер
C) Вредоносное ПО
D) Антивирус
E) шпионское ПО
Ответ E

7. _____ - компьютерные программы, разработанные злоумышленниками для получения доступа с правами суперпользователя или администратора (root) к вашему компьютеру.
A) Бэкдоры
B) Руткиты
C) Вредоносное ПО
D) Антивирус
E) шпионское ПО
Посмотреть ответ
Ответ B

8. Атака, направленная на перехват небольших пакетов из сети, передаваемых другими компьютерами, и чтение содержимого данных в поисках любого типа информации, ____
A) Фишинг
B) Прослушивание
C) Мошенничество
D) Эксплойты
E) Отказ в обслуживании
Ответ B

9. _____ - это действие по записи нажатий клавиш на клавиатуре, обычно скрытое, так что человек, использующий клавиатуру, не подозревает, что их действия отслеживаются.
A) Отказ в обслуживании
B) Эксплойты
C) Мошенничество
D) Кейлоггинг
E) Спам
Ответ D

10. Для чего из следующего используется прокси-сервер?

(a) Для обеспечения безопасности от неавторизованных пользователей
(b) Для обработки запросов клиентов на веб-страницы
(c) Обработка клиентских запросов на доступ к базе данных
(d) Обеспечить TCP / IP
Ответ (b)

11. Пароли позволяют пользователям
(a) быстро войти в систему
(b) эффективно использовать время
(c) сохранять конфиденциальность файлов
(d) упростить файловые структуры
Ответ (c)

12. Технологией, более не защищенной авторским правом, доступной каждому, считается:
(a) проприетарный
(b) открытый
(c) экспериментальный
(d) в общественном достоянии.
Ответ a)

13. Что такое бэкап?
(a) Восстановление резервной копии информации
(b) Точная копия информации о системе.
(c) Возможность запустить систему в случае сбоя или сбоя системы.
(d) Все эти
Ответ (b)

14. Перед предоставлением доступа компьютер проверяет _____ имен пользователей и паролей на совпадение
(a) сайт
(b) Сеть
(c) Резервный файл
(d) Базу данных
Ответ (d)

15. Все нижеперечисленное является примерами реальных рисков для безопасности и конфиденциальности, ЗА ИСКЛЮЧЕНИЕМ:
(a) Хакеры
(b) Спам
(c) Вирусы
(d) Кража личных данных
Ответ (b)

16. Что из перечисленного, скорее всего, НЕ будет признаком вируса?
(a) Исчезают существующие программные файлы и значки
(b) CD-ROM перестает работать.
(c) Веб-браузер открывает необычную домашнюю страницу.
(d) На экране отображаются нечетные сообщения или изображения.
Ответ (b)

17. Все нижеперечисленное является примерами реальных рисков для безопасности и

конфиденциальности, ЗА ИСКЛЮЧЕНИЕМ:
(a) хакеры
(b) спам
(c) вирусы
(d) кража личных данных
Ответ (b)

18. Все нижеприведенные примеры реальных рисков для безопасности и конфиденциальности, кроме?
(a) хакеры
(b) спам
(c) вирусы
(d) выявление кражы
Ответ (b)

19. __ - это компьютерное преступление, при котором преступник взламывает компьютерную систему для изучения подробной информации и т. д.
(a) Взлом
(b) Спуфинг
(c) Подслушивание
(d) Фишинг
Ответ (a)

20. ____ - это вирусы, которые запускаются с течением времени или в определенную дату.
(a) Вирусы загрузочного сектора
(b) Макровирусы
(c) Бомбы замедленного действия
(d) Черви
Ответ (c)

21. Проверка имени пользователя и пароля называется:
(a) конфигурация
(b) доступность
(c) аутентификация
(d) вход в систему
Ответ (c)

22. __ - протокол безопасности, основанный на цифровых сертификатах.
(a) Цифровая подпись
(b) Протокол уровня защищенных сокетов
(c) Безопасные электронные транзакции
(d) Ни один из этих
Ответ (c)

23. Способность восстанавливать и читать удаленные или поврежденные файлы с компьютера преступника является примером специальности правоохранительных органов, которая называется:
a) робототехника
(b) моделирование
(c) компьютерная криминалистика
(d) анимация

Ответ (c)

24. Межсетевые экраны используются для защиты от __
(a) несанкционированные атаки
(b) вирусные атаки
(c) Атаки на основе данных
(d) Огневые атаки
Ответ a)

25. __ - это электронный файл, который однозначно идентифицирует людей и веб-сайты в Интернете и обеспечивает безопасную конфиденциальную связь.
(a) Цифровая подпись
(b) Цифровые сертификаты
(c) Безопасные электронные транзакции
(d) Ни один из этих
Ответ (b)

26. В наши дни фишинг превратился в преступную практику использования социальной инженерии в отношении чего из перечисленного?
(a) Сайты социальных сетей
(b) Мобильные телефоны
(c) Электронная почта
(d) Интернет-кафе
Ответ (b)

27. Технологией, более не защищенной авторским правом, доступной каждому, считается:
(a) проприетарная
(b) открытая
(c) экспериментальная
(d) в общественном достоянии
Ответ (a)

27. Что такое резервное копирование?
(a) Добавление дополнительных компонентов в вашу сеть
(b) Защита данных путем их копирования из исходного источника в другое место назначения.
(c) Фильтрация старых данных из новых.
(d) Доступ к данным на ленте
Ответ (b)

28. __ может использоваться для минимизации риска нарушения безопасности или вирусов.
(a) Брандмауэр
(b) Резервные копии
(c) Шифрование
(d) Цифровая подпись
Ответ (a)

29. Программное обеспечение, такое как вирусы, черви и троянские кони, имеющее злой умысел, известно как:

(a) шпионское ПО
(b) рекламное ПО
(c) спам
(d) вредоносное ПО
Ответ (d)

30. __, иногда называемый вирусом загрузочного сектора, запускается при загрузке компьютера, поскольку он находится в основной загрузочной записи жесткого диска.
(a) системный вирус
(b) Вирус троянского коня
(c) файловый вирус
(d) Ни один из этих
Ответ (d)

31. В результате компьютерный вирус не может привести к __
(a) Сбою диска
(b) Сбою материнской платы
(c) Коррупции программы
(d) Удалению файлов
Ответ (b)

32. Личное содержимое транзакции, если она не защищена, может быть перехвачено, когда она проходит по маршруту через Интернет, называется __.
(a) Спуфинг
(b) Несанкционированное раскрытие
(c) Прослушивание
(d) Фишинг
Ответ (c)

33. _____ - это наука, которая пытается создать машины, демонстрирующие тот же тип интеллекта, что и люди.
(a) Нанонаука
(b) Нанотехнологии
(c) Моделирование
(d) Искусственный интеллект
Ответ (d)

34. Что делать, если вы получили письмо от незнакомого человека?
(a) Немедленно отправьте его в полицию
(b) Удалить его, не открывая
(c) Откройте его и ответьте им, что вы их не знаете.
(d) Ответить и попросить их предоставить личную информацию.
Ответ (b)

35. Все нижеперечисленное является примерами реальных рисков для безопасности и конфиденциальности, кроме ___
(a) хакеры
(b) спам
(c) вирусы
(d) выявить кражу
Ответ (b)

36. __ Это специализированная форма кражи личных данных в Интернете.
(a) Спуфинг
(b) Несанкционированное раскрытие
(c) Подслушивание
(d) Фишинг
Ответ (d)

37. __ предполагает, что кто-то маскируется под кого-то другого.
(a) Спуфинг
(b) Несанкционированные действия
(c) Подслушивание
(d) Фишинг
Ответ (a)

38. Когда информация о транзакциях передается прозрачным образом, хакеры могут перехватить передачу, чтобы получить конфиденциальную информацию о клиентах. Это известно как __
(a) Спуфинг
(b) Несанкционированное вскрытие
(c) Прослушивание
(d) Фишинг
Ответ (b)

39. Конкурент или недовольный клиент могут изменить веб-сайт так, чтобы он отказывался от услуг потенциальным клиентам. Это известно как __
(a) Несанкционированные действия
(b) Несанкционированное раскрытие
(c) Подслушивание
(d) Фишинг
Ответ (a)

40. __ - это кража личных данных в Интернете.
(a) Подслушивание
(b) Фишинг
(c) Спуфинг
(d) Ни один из этих
Ответ (b)

41. Что из нижеперечисленного не является риском для транзакций через Интернет
(a) прослушивание
(b) спуфинг
(c) шифрование
(d) несанкционированные действия
Ответ (c)

42. Инструмент безопасности для проверки подлинности сообщения и заявленной личности отправителя, а также проверки целостности сообщения.
(a) шифрование
(b) межсетевые экраны
(c) цифровые сертификаты
(d) цифровая подпись

Ответ (d)

43. Что такое кибербезопасность?
a) Кибербезопасность обеспечивает защиту от вредоносных программ.
b) Кибербезопасность обеспечивает безопасность от кибертеррористов
c) Кибербезопасность защищает систему от кибератак.
d) Все вышеперечисленное
Ответ: d

44. Что защищает кибербезопасность?
a) Кибербезопасность защищает преступников
b) Кибербезопасность защищает системы, подключенные к Интернету
c) Кибербезопасность защищает хакеров
d) Ничего из вышеперечисленного
Ответ: b

45. Кто отец компьютерной безопасности?
a) Август Керкхоффс
b) Боб Томас
c) Роберт
d) Чарльз
Посмотреть ответ
Ответ: a

46. Что из перечисленного является целью сетевой безопасности?
a) Конфиденциальность
b) Целостность
c) Доступность
d) Все вышеперечисленное
Ответ: d

47. Что из нижеперечисленного определяется как попытка кражи, шпионажа, повреждения или уничтожения компьютерных систем, сетей или связанной с ними информации?
a) Кибератака
b) Компьютерная безопасность
c) Криптография
d) Цифровой взлом
Ответ: a

48. Что из перечисленного является типом кибербезопасности?
a) Облачная безопасность
b) Сетевая безопасность
c) Безопасность приложений
d) Все вышеперечисленное
Ответ: d

49. Каковы особенности кибербезопасности?
a) Соответствие
b) Защита от внутренних угроз
c) Предотвращение угроз

d) Все вышеперечисленное
Ответ: d

50. Что из перечисленного не является киберпреступлением?
угроза?
a) Отказ в обслуживании
b) Взлом пароля
c) Вредоносное ПО
d) AES (Advanced Encryption Standard)
Ответ: d

51. Что из перечисленного является компонентом кибербезопасности?
a) Интернет вещей
b) AI
c) База данных
d) Атаки
Ответ: a

52. Что из перечисленного является типом кибератаки?
a) Фишинг
b) SQL-инъекции
c) Атака на пароль
d) Все вышеперечисленное
Ответ: d

53. Что из перечисленного не является преимуществом кибербезопасности?
a) замедляет работу системы
b) Минимизирует зависание компьютера и сбои
c) Обеспечивает конфиденциальность пользователей
d) Защищает систему от вирусов
Ответ: a

54. «Киберпространство» было придумано _____
a) Ричард Столмен
b) Уильям Гибсон
c) Эндрю Танненбаум
d) Скотт Фальман
Ответ: b

55. В _____ хакерство стало практическим преступлением и поводом для беспокойства в области кибер-технологий.
a) 1991 г.
b) 1983 г.
c) 1970 г.
d) 1964 г.
Ответ: c

56. Правительства наняли несколько высококвалифицированных хакеров для обеспечения кибербезопасности страны или штата. Эти типы хакеров называются _____
a) Хакеры, спонсируемые нацией/государством
b) ЦРУ

c) Особые хакеры
d) Правительственные хакеры
Ответ: a

57. Закон о компьютерном мошенничестве и злоупотреблениях был принят в Соединенных Штатах _____.
a) 1985 г.
b) 1987 г.
c) 1989 г.
d) 1984 г.
Ответ: d

58. Какое из следующих действий нарушает кибербезопасность?
a) Использование
b) Атака
c) Угроза
d) Уязвимость
Ответ: b

59. Какие из следующих действий ставят под угрозу кибербезопасность?
a) Уязвимость
b) Атака
c) Угроза
d) использовать
Ответ: c

60. Что из перечисленного является хакерским подходом, при котором киберпреступники создают поддельные веб-сайты или страницы для обмана или получения дополнительного трафика?
a) Фарминг (Pharming)
b) Веб-сайт-дублирование
c) подражание
d) рассылка спама
Ответ: a

61. Что из перечисленного не относится к киберпреступлениям в одноранговых сетях?
a) MiTM
b) Внедрение троянских программ целевой жертве
c) Утечка данных кредитной карты в глубокой сети
d) Фишинг
Ответ: c

62. Получение доступа к Wi-Fi нечестным путем не является киберпреступлением.
a) Ложь
b) Верно
Ответ: a

63. Киберпреступник или тестировщик на проникновение использует дополнительные данные, которые хранят в памяти определенные специальные инструкции для действий по взлому системы, в какой из следующих атак?
a) Кликджекинг
b) Переполнение буфера

c) Фишинг
d) MiTM
Ответ: b

64. Что такое легальная форма взлома?
a) Активизм
b) Растрескивание
c) Неэтичный взлом
d) Этичный взлом
Ответ: d

65. Лица с криминальными взглядами, которые работают на террористические организации и крадут информацию о государствах и других секретных разведданных, совершая киберпреступления, являются _____
a) Хакеры Red Hat
b) Кибертеррористы
c) Хакеры, спонсируемые государством
d) Хакеры Blue Hat
Ответ: b

66. Что из нижеперечисленного является интернет-мошенничеством, совершаемым киберпреступниками, когда пользователя убеждают в цифровом виде предоставить конфиденциальную информацию.
a) Атака MiTM
b) Фишинговая атака
c) Атака на веб-сайт
d) DoS-атака
Ответ: b

67. _____ - это не шаг киберпреступников в утечке данных.
a) Эксфильтрация
b) Исследования и сбор информации
c) атаковать систему
d) Исправление ошибок
Ответ: d

68. Что представляет собой полная форма вредоносного ПО?
a) Неисправность системы безопасности
b) Вредоносное программное обеспечение
c) Неисправное программное обеспечение
d) Многоцелевое программное обеспечение
Ответ: b

69. Филип Циммерман выпустил _____ в 1991 году, и это сложный инструмент шифрования.
a) Data Encryption Standard
b) Pretty Good Privacy
c) Protected Good Privacy
d) Advanced Encryption Standard
Ответ: b

70. Термин _____ относится к группе хакеров, которые носят одновременно

белые и черные шляпы.
a) Yellow Hat hackers
b) Grey Hat hackers
c) Red Hat Hackers
d) White-Black Hat Hackers
Ответ: b

71. _______ широко известно как триада ЦРУ.
a) AIC (подлинность, целостность, конфиденциальность)
b) AIN (доступность, целостность, отсутствие отказа от авторства)
c) NIC (безотказность, целостность, конфиденциальность)
d) AIC (доступность, целостность, конфиденциальность)
Ответ: d

72. Какой из следующих этических приемов взлома используется для определения того, какая операционная система (ОС) работает на удаленном компьютере?
a) дактилоскопия ОС
b) тестирование ОС на проникновение
c) Цифровая печать
d) След
Ответ: a

73. Что из нижеперечисленного является типом сбора разведданных, который не мешает и является незаметным по своей природе?
a) AI
b) бетон
c) конкурентоспособный
d) познавательный
Ответ: c

74. _____ не является инструментом для взлома электронной почты.
a) Mail Password
b) Email Finder Pro
c) Mail PassView
d) Sendinc
Ответ: d

75. Какие из следующих DDoS-атак в мобильных системах ждут, пока владелец инициирует кибератаку?
a) ботнеты
b) программы
c) вирус
d) черви
Ответ: a

76. Наименее надежный стандарт шифрования - _____
a) WPA3
b) WPA2
c) WPA
d) WEP
Ответ: d

77. Что из нижеперечисленного определяется как количество подключенных к Интернету систем, в каждой из которых работает один или несколько ботов?
a) Вирус
b) Ботнет
c) троян
d) Черви
Ответ: b

78. _____ не является примером перехвата DNS.
a) Взлом DNS на основе HTTP
b) Захват DNS-провайдера
c) Перехват DNS для фишинга
d) Перехват DNS для фарминга
Ответ: a

79. Что из перечисленного может снизить вероятность утечки данных?
a) Стеганография
b) Хорография
c) Криптография
d) Томография
Ответ: a

80. Что такое полная форма TOR.
a) The Onion Router
b) Tactical Onion Router
c) The Onion Reader
d) The Open Router
Ответ: a

81. Что такое полная форма AES?
a) Расширенный стандарт шифрования
b) Стандарт активного шифрования
c) Расширенная безопасность шифрования
d) Расширенный стандарт шифрования
Ответ: d

82. Что из следующего можно сделать функциональным для различных аспектов деятельности по разработке программного обеспечения и совершенствованию оборудования?
a) Социальная инженерия
b) Обратный инжиниринг
c) Обратный взлом
d) Растрескивание
Ответ: b

83. Электронный файл, который однозначно идентифицирует людей и веб-сайты в Интернете и обеспечивает безопасную конфиденциальную связь.
(a) Цифровая подпись
(b) Цифровые сертификаты
(c) Шифрование
(d) Межсетевые экраны
Ответ (b)

84. В чем из нижеперечисленного за человеком постоянно следит/преследует другой человек или группа из нескольких людей?

1. Фишинг
2. Буллинг
3. Преследование
4. Кража личных данных

Ответ (3)

Задания к лабораторным работам

Проверка достижения индикаторов компетенций в части «Уметь» и «Владеть» выполняется по следующим заданиям к лабораторным работам.

Результаты обучения	Задания к лабораторным работам
ПК-1 Владение навыками моделирования, анализа и использования формальных методов конструирования программного обеспечения	
ПК-1.7 Знает основные методы защиты информации.	
Знает основные методы защиты информации.	Анализ частотных характеристик открытого и шифртекста.
ПК-1.8 Умеет использовать основные методы защиты информации.	
Уметь использовать основные методы защиты информации.	Программная реализация алгоритма RSA. Реализация операции "возведение в степень по модулю"
ПК-1.9 Владеет основными методами защиты информации	
Владеть основными методами защиты информации	Неприводимые многочлены высокой степени.
ПК-6 Владение концепциями и атрибутами качества программного обеспечения (надежности, безопасности, удобства использования), в том числе роли людей, процессов, методов, инструментов и технологий обеспечения качества	
ПК-6.4 Знает концепции и атрибуты безопасности программного обеспечения	
Знать концепции и атрибуты безопасности программного обеспечения	Межцентровая защита информации в платёжных системах.
ПК-6.5 Умеет определять атрибуты безопасности программного обеспечения	
Уметь определять атрибуты безопасности программного обеспечения	Составление именованных списков доступа (accesslist)
ПК-6.6 Имеет навыки в использовании методов, инструментов и технологий обеспечения безопасности программного обеспечения	
Владеть навыками в использовании методов, инструментов и технологий обеспечения безопасности программного обеспечения	Составление стандартных списков доступа (accesslist)

Форма промежуточной аттестации

Промежуточная аттестация проходит в форме экзамена.

Перечень вопросов для подготовки к экзамену.

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
2. Основные составляющие и аспекты информационной безопасности.
3. Классификация угроз информационной безопасности: для личности, для общества, для государства.
4. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
5. Концепция «информационной войны» по оценкам российских спецслужб.
6. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?
7. Сфера применения информационного оружия.
8. Особенности информационного оружия. Организация защиты.
9. Основные задачи в сфере обеспечения информационной безопасности.
10. Отечественные стандарты в области информационной безопасности
11. Зарубежные стандарты в области информационной безопасности
12. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?
13. Основные критерии оценки надежности: политика безопасности и гарантированность.
14. Понятие государственной тайны. Понятие профессиональной тайны.
15. Понятие коммерческой тайны. Понятие служебной тайны. Понятие банковской тайны.
16. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.
17. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.
18. Уязвимость информации в автоматизированных системах обработки данных.
19. Элементы и объекты защиты в автоматизированных системах обработки данных.
20. Методы защиты информации от преднамеренного доступа.
21. Защита информации от исследования и копирования.
22. Опознавание с использованием простого пароля. Метод обратимого шифрования.
23. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
24. Использование динамически изменяющегося пароля. Метод «запрос-ответ»
25. Использование динамически изменяющегося пароля. Функциональные методы
26. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.
27. Электронная (цифровая) подпись. Цели применения электронной подписи.
28. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.
29. Классификация методов криптографического закрытия.

30. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.
31. Угрозы информации в персональных ЭВМ.
32. Обеспечение целостности информации в ПК. Физическая зашита ПК и носителей информации.
33. Защита ПК от несанкционированного доступа.
34. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.
35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.
36. Программные закладки. Классификация критериев вредоносного воздействия закладок.
37. Общие характеристики закладок.
38. Методы и средства защиты от закладок.
39. Компьютерный вирус. Какая программа считается зараженной.
40. По каким признакам классифицируются вирусы?
41. Способы заражения программ. Стандартные методы заражения.
42. Как работает вирус?
43. Методы защиты от вирусов.
44. Антивирусные программы. Программы-детекторы. Программы-доктора.
45. Антивирусы-полифаги. Эвристические анализаторы.
46. Программы-ревизоры. Программы-фильтры.
47. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
48. В чём заключаются задачи защиты в сетях передачи данных?
49. Проблемы защиты информации в вычислительных сетях.
50. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.
51. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
52. Архитектура механизмов защиты информации в сетях ЭВМ.

Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Процедура оценивания представлена в табл. 1 и реализуется поэтапно:

1-й этап процедуры оценивания: оценивание уровня достижения каждого из запланированных результатов обучения – дескрипторов (знаний, умений, владений) в соответствии со шкалами и критериями, установленными картами компетенций ОПОП (Приложение 1 ОПОП). Экспертной оценке преподавателя подлежит сформированность отдельных индикаторов достижения компетенций, для оценивания которых предназначена данная оценочная процедура текущего контроля и промежуточной аттестации согласно матрице соответствия оценочных средств результатам обучения, представленная в ОПОП.

2-й этап процедуры оценивания: интегральная оценка достижения обучающимся запланированных результатов обучения по итогам отдельных видов текущего контроля и промежуточной аттестации.

Таблица 1

Характеристика процедур текущего и итогового контроля по дисциплине:

№	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Методы оценивания (экспертный, самооценка, групповая оценка, взаимооценка)	Виды выставляемых оценок (по пятибалльной шкале, зачтено /не зачтено, баллы)	Способ учета индивидуальных достижений обучающихся
1	Контрольная точка 1 (тест)	1 раз в семестр	экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости, контрольная точка в АИС ВУЗа
2	Контрольная точка 2 (тест)	1 раз в семестр	экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости, контрольная точка в АИС ВУЗа
3	Отчет по лабораторной работе 1, 2	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
4	Отчет по лабораторной работе 3, 4	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
5	Отчет по лабораторной работе 5, 6	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
6	Отчет по лабораторной работе 7, 8	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
7	Отчет по лабораторной работе 9, 10	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости

8	Отчет по лабораторной работе 11 - 14	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
№	Наименование оценочного средства	Периодичность и способ проведения процедуры оценивания	Методы оценивания (экспертный, самооценка, групповая оценка, взаимооценка)	Виды выставляемых оценок (по пятибалльной шкале, зачтено /не зачтено, баллы)	Способ учета индивидуальных достижений обучающихся
9	Отчет по лабораторной работе 15, 16	На лабораторных занятиях, письменно и устно	Экспертный	Зачтено / не зачтено	Журнал учета посещаемости и успеваемости
10	Экзамен	По окончании семестра, письменно	Экспертный	По пятибалльной шкале	Зачетная ведомость, зачетные книжки и учебные карточки, портфолио, АИС вуза

Шкала и процедура оценивания сформированности компетенций На этапе промежуточной аттестации используется система оценки успеваемости обучающихся, которая позволяет преподавателю оценить уровень освоения материала обучающимися. Критерии оценивания сформированности планируемых результатов обучения (дескрипторов) представлены в карте компетенции ОПОП.

Форма оценки знаний: оценка - 5 «отлично»; 4 «хорошо»; 3 «удовлетворительно»; 2 «неудовлетворительно». Лабораторные работы, практические занятия, практика оцениваются: «зачет», «незачет». Возможно использование балльно-рейтинговой оценки. **Шкала оценивания**:

«Отлично» – выставляется, если сформированность заявленных дескрипторов компетенций на 80 % и более (в соответствии с картами компетенций ОПОП) оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно»: студент показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи повышенной сложности, свободно использовать справочную литературу, делать обоснованные выводы из результатов анализа конкретных ситуаций;

«Хорошо» – выставляется, если сформированность заявленных дескрипторов компетенций на 50% и более (в соответствии с картами компетенций ОПОП) оценивается критериями «хорошо» и «отлично», при условии отсутствия оценки «неудовлетворительно», допускается оценка «удовлетворительно»: обучающийся показал прочные знания основных положений фактического материала, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты анализа конкретных ситуаций;

«Удовлетворительно» – выставляется, если сформированность заявленных дескрипторов компетенций 50 % и более (в соответствии с картами компетенций ОПОП) оценивается критериями «удовлетворительно», «хорошо» и «отлично»: обучающийся

показал знание основных положений фактического материала, умение получить с помощью преподавателя правильное решение конкретной практической задачи из числа предусмотренных рабочей программой, знакомство с рекомендованной справочной литературой;

«Неудовлетворительно», «Незачет» – выставляется, если сформированность заявленных дескрипторов компетенций менее чем 50 % (в соответствии с картами компетенций ОПОП) оценивается критериями «удовлетворительно», «хорошо» и «отлично»: при ответе обучающегося выявились существенные пробелы в знаниях основных положений фактического материала, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

Ответы и решения обучающихся оцениваются по следующим общим критериям: распознавание проблем; определение значимой информации; анализ проблем; аргументированность; использование стратегий; творческий подход; выводы; общая грамотность.

Соответствие критериев оценивания сформированности планируемых результатов обучения (дескрипторов) системам оценок представлено в табл. 2.

Таблица 2

Интегральная оценка

Критерии	Традиционная оценка	Балльно-рейтинговая оценка
5	5	86 - 100
4	4	61-85
3	3	51-60
2 и 1	2, Незачет	0-50
5, 4, 3	Зачет	51-100

Обучающиеся обязаны сдавать все задания в сроки, установленные преподавателем. Оценка «Удовлетворительно» по дисциплине, может выставляться и при неполной сформированности компетенций в ходе освоения отдельной учебной дисциплины, если их формирование предполагается продолжить на более поздних этапах обучения, в ходе изучения других учебных дисциплин.