МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Брянский государственный аграрный университет»

УТВЕРЖДАЮ
Проректор по учебной работе
_____ Г.П. Малявко
17 июня 2021г.

Информационная безопасность
(Наименование дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Закреплена за кафедрой	информатики, информационных систем и технологий
Направление подготовки	09.03.03 Прикладная информатика
Направленность (профиль)	Программно-технические средства информатизации
Квалификация	Бакалавр
Форма обучения	очная, заочная
Общая трудоемкость	4 з.е.

Брянская область
2020

Программу составил(и):

к.т.н., доцент Никулин В.В._____

Рецензент(ы):

к.э.н., доцент Лысенкова С.Н._____

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с ФГОС ВО – бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утверждённого приказом Министерства образования и науки РФ от 19 сентября 2017 г., №922.

составлена на основании учебных планов 2021 года поступления:

направление подготовки 09.03.03 Прикладная информатика направленность (профиль) Программно-технические средства информатизации

утверждённых учёным советом вуза от «17» июня 2021г. протокол №11

Рабочая программа одобрена на заседании кафедры информатики, информационных систем и технологий

Протокол от «17» июня 2021г. №12

Зав. кафедрой, к.э.н., доцент Ульянова Н.Д. _____

(подпись)

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Цель дисциплины – является формирование основополагающих знаний в области защиты информации и обеспечения информационной безопасности защищаемому объекту.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок ОПОП ВО: Б1.О.20

2.1 Требования к предварительной подготовке обучающегося:

Для успешного освоения дисциплины необходимы знания, умения и навыки, полученные в результате изучения дисциплин: «Информатика и программирование», «Вычислительные системы, сети и телекоммуникации» «Теория систем и системный анализ», «Информационные системы и технологии».

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Знания, полученные при изучении дисциплины, необходимы при освоении дисциплин, «Web-программирование», «Информационные системы мобильных устройств», «Web-дизайн».

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ИНДИКАТОРАМИ ДОСТИЖЕНИЯ КОМПЕТЕНЦИЙ

Достижения планируемых результатов обучения, соотнесенных с общими целями и задачами ОПОП, является целью освоения дисциплины.

Для дисциплин обязательной части

Освоение дисциплины направлено на формирование следующих компетенций:

Компетенция (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Результаты обучения**
Общепрофессиональные компетенции		
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*ОПК-3.2. Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности*	***Знать:*** *стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности* ***Уметь****: использовать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности* ***Владеть:*** *навыками использования стандартных задач профессиональной деятельности на основе*

		информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

***Этапы формирования компетенций в процессе освоения образовательной* программы**: в соответствии с учебным планом и планируемыми результатами освоения ОПОП.

4. РАСПРЕДЕЛЕНИЕ ЧАСОВ ДИСЦИПЛИНЫ ПО СЕМЕСТРАМ (очная форма)

Вид занятий	1		2		3		4		5		6		7		8		Итого	
									УП	РПД							УП	РПД
Лекции									32	32							32	32
Лабораторные									32	32							32	32
КСР									2	2							2	2
Консультация									1	1							1	1
Прием экзамена									0,25	0,25							0,25	0,25
Контактная работа обучающихся с преподавателем (аудиторная)									67,25	67,25							67,25	67,25
Сам. работа									60	60							60	60
Контроль									16,75	16,75							16,75	16,75
Итого									144	144							144	144

РАСПРЕДЕЛЕНИЕ ЧАСОВ ДИСЦИПЛИНЫ ПО КУРСАМ (заочная форма)

Вид занятий	1		2		3		4		5		6		7		8		Итого	
					УП	РПД	УП	РПД									УП	РПД
Лекции					2	2	4	4									6	6
Лабораторные					2	2	4	4									6	6
КСР																		
Консультация							1	1									1	1
Прием экзамена							0,25	0,25									0,25	0,25
Прием зачета																		
Контактная работа обучающихся с преподавателем (аудиторная)					4	4	9,25	9,25									13,25	13,25
Сам. работа					32	32	92	92									124	124
Контроль							6,75	6,75									6,75	6,75
Итого					36	36	108	108									144	144

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (очная форма)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часов	Индикаторы достижения компетенций
	Раздел 1. Основные положения теории информационной безопасности.			
1.1	Основные понятия и определения курса Информационная безопасность /Лек/	5	4	ОПК-3.2
1.2	Сбор данных об информационной системе с помощью средств администрирования Windows (оснасток ММС) /Лаб/	5	4	

1.3	Освоить приёмы работы с виртуальной машиной. Создать и настроить виртуальную машину /Ср/	5	6	
1.4	Проблемы информационной безопасности сетей /Лек/	5	4	ОПК-3.2
1.5	Сбор данных о топологии сети с помощью средства администрирования сетей 3Com Network Supervisor /Лаб/	5	4	ОПК-3.2
1.6	С помощью 3Com Network Supervisor постройте карту сети учебной лаборатории. Опишите узлы сети, используемые типы соединений, доступные средства удаленного администрирования. /Ср/	5	6	ОПК-3.2
1.7	Безопасность компьютерных сетей /Лек/	5	4	ОПК-3.2
1.8	выявление уязвимостей с помощью Microsoft Baseline Security Analyzer. Настройка локальной политики паролей /Лаб/	5	4	ОПК-3.2
1.9	Опишите действующую на вашем компьютере политику паролей. /Ср/	5	6	ОПК-3.2
1.10	Политики безопасности. Основные понятия политики безопасности /Лек/	5	4	ОПК-3.2
1.11	Использование сканеров безопасности для получения информации о сети. /Лаб/	5	4	ОПК-3.2
1.12	Проведите сканирование указанных компьютеров в учебной лаборатории. Охарактеризуйте уровень безопасности проверенных компьютеров. /Ср/	5	6	ОПК-3.2
	Раздел 2. Криптографическая защита информации. Криптография и криптоалгоритмы			
1.13	Принципы криптографической защиты информации /Лек/	5	4	ОПК-3.2
1.14	Использование Microsoft Security Assessment Tool (MSAT) /Лаб/	5	4	ОПК-3.2
1.15	Использование цифровых сертификатов. /Ср/	5	6	ОПК-3.2
	Раздел 3. Законы и стандарты в области Информационной безопасности			
1.16	Законодательный уровень обеспечения Информационной безопасности /Лек/	5	4	ОПК-3.2
1.17	Использование цифровых сертификатов. Посмотрите параметры сертификата «электронной сберкассы» Сбербанка – https://esk.sbrf.ru Опишите, кем на какой срок и для какого субъекта сертификат был выдан. /Лаб/	5	4	ОПК-3.2
1.18	Запросите сертификат в Thawte и настройте почтовый клиент для использования S/MIME. /Ср/	5	6	ОПК-3.2
1.19	Стандарты и спецификации в области информационной безопасности /Лек/	5	4	ОПК-3.2
1.20	Создание центра сертификации (удостоверяющего центра) в Windows Server 2008/12. /Лаб/	5	4	ОПК-3.2
1.21	На учебном сервере или виртуальной машине установите роль Active Directory Certificate Services с настройками /Ср/	5	6	ОПК-3.2
1.22	Криптографические алгоритмы шифрования /Лек/	5	4	ОПК-3.2
1.23	Шифрование данных при хранении - EFS. Шифрующая файловая система (Encrypting File System – EFS) /Лаб/	5	4	ОПК-3.2
1.24	Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с тестовым файлом, который не жалко потерять. Проверьте, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NFTS на том же компьютере, копировании папки на сетевой диск или диск с FAT /Ср/	5	6	ОПК-3.2
	Раздел 4. Несанкционированный доступ (НСД) к информации и методы защиты от НСД			
1.25	Несанкционированный доступ (нсд) к информации. Комплекс программно - технических средств и организационных мер по защите информации от НСД /Ср/	5	6	ОПК-3.2

1.26	Управление разрешениями на файлы и папки. /Ср/	5	6	ОПК-3.2
	Контроль /К/	5	16,75	ОПК-3.2
	Консультация перед экзаменом /К/	5	1	ОПК-3.2
	Контактная работа при приеме экзамена /К/	5	67,25	ОПК-3.2

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (заочная форма)

Код занятия	Наименование разделов и тем /вид занятия/	Курс	Часов	Индикаторы достижения компетенций
	Раздел 1. Основные положения теории информационной безопасности.			
1.1	Основные понятия и определения курса Информационная безопасность /Лек/	3	2	ОПК-3.2
1.2	Сбор данных об информационной системе с помощью средств администрирования Windows (оснасток MMC) /Лаб/	3	2	
1.3	Освоить приёмы работы с виртуальной машиной. Создать и настроить виртуальную машину /Ср/	3	4	
1.4	Проблемы информационной безопасности сетей /Ср/	3	4	ОПК-3.2
1.5	Сбор данных о топологии сети с помощью средства администрирования сетей 3Com Network Supervisor /Ср/	3	4	ОПК-3.2
1.6	С помощью 3Com Network Supervisor постройте карту сети учебной лаборатории. Опишите узлы сети, используемые типы соединений, доступные средства удаленного администрирования. /Ср/	3	4	ОПК-3.2
1.7	Безопасность компьютерных сетей /Ср/	3	4	ОПК-3.2
1.8	выявление уязвимостей с помощью Microsoft Baseline Security Analyzer. Настройка локальной политики паролей /Ср/	3	4	ОПК-3.2
1.9	Опишите действующую на вашем компьютере политику паролей. /Ср/	3	4	ОПК-3.2
1.10	Политики безопасности. Основные понятия политики безопасности. Проведите сканирование указанных компьютеров в учебной лаборатории. Охарактеризуйте уровень безопасности проверенных компьютеров. /Ср/	3	4	ОПК-3.2
	Раздел 2. Криптографическая защита информации. Криптография и криптоалгоритмы			
1.13	Принципы криптографической защиты информации /Лек/	4	2	ОПК-3.2
1.14	Использование Microsoft Security Assessment Tool (MSAT) /Лаб/	4	2	ОПК-3.2
1.15	Использование цифровых сертификатов. /Ср/	4	10,2	ОПК-3.2
	Раздел 3. Законы и стандарты в области Информационной безопасности			
1.16	Законодательный уровень обеспечения Информационной безопасности /Лек/	4	2	ОПК-3.2
1.17	Использование цифровых сертификатов. Посмотрите параметры сертификата «электронной сберкассы» Сбербанка – https://esk.sbrf.ru Опишите, кем на какой срок и для какого субъекта сертификат был выдан. /Лаб/	4	2	ОПК-3.2
1.18	Запросите сертификат в Thawte и настройте почтовый клиент для использования S/MIME. /Ср/	4	10,2	ОПК-3.2
1.19	Стандарты и спецификации в области информационной безопасности /Ср/	4	10,2	ОПК-3.2
1.20	Создание центра сертификации (удостоверяющего центра) в Windows Server 2008/12. /Ср/	4	10,2	ОПК-3.2
1.21	На учебном сервере или виртуальной машине установите роль Active Directory Certificate Services с настройками /Ср/	4	10,2	ОПК-3.2
1.22	Криптографические алгоритмы шифрования /Лек/	4	10,2	ОПК-3.2

1.23	Шифрование данных при хранении - EFS. Шифрующая файловая система (Encrypting File System – EFS) /Ср/	4	10,2	ОПК-3.2
1.24	Работая под первой учетной записью, запросите сертификат (если он не был получен ранее), после чего зашифруйте папку с тестовым файлом, который не жалко потерять. Проверьте, что будет происходить при добавлении файлов, переименовании папки, копировании ее на другой диск с файловой системой NFTS на том же компьютере, копировании папки на сетевой диск или диск с FAT /Ср/	4	10,2	ОПК-3.2
	Раздел 4. Несанкционированный доступ (НСД) к информации и методы защиты от НСД			
1.25	Несанкционированный доступ (нсд) к информации. Комплекс программно - технических средств и организационных мер по защите информации от НСД. Управление разрешениями на файлы и папки. /Ср/	4	10,2	ОПК-3.2
	Контроль /К/	4	6,75	ОПК-3.2
	Консультация перед экзаменом /К/	4	1	ОПК-3.2
	Контактная работа при приеме экзамена /К/	4	13,25	ОПК-3.2

Реализация программы предполагает использование традиционной, активной и интерактивной форм обучения на лекционных и лабораторных занятиях.

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Приложение №1

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

6.1. Рекомендуемая литература

	Авторы, составители	Заглавие	Издательство, год	Количество
6.1.1. Основная литература				
Л.1.1	А.В. Бабаш, Е.К. Баранова, Ю.Н.	Информационная безопасность: Лабораторный практикум -	М.: КноРус, 2019	ЭБС «BOOK.RU»
Л.1.2	Шаньгин, В. Ф..	Информационная безопасность и защита информации 2-е изд.	Саратов : Профобразование, 2019.	ЭБС «IPRbooks»
Л.1.3	Бахаров, Л. Е.	Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум . — 59 с. — ISBN 978-5-906953-94-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS :	Москва : Издательский Дом МИСиС, 2019	ЭБС «IPRbooks»
Л1.4	Шаньгин В.Ф.	Защита компьютерной информации. Эффективные методы и средства [Электронный ресурс]/ — Электрон. текстовые данные. — 544 с.— Режим доступа:	Саратов: Профобразование, 2017	ЭБС «IPRbooks»
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Количество
Л 2.1	Никулин В. В.	Информационная безопасность : электронное учебно-метод. пособие [Электронный ресурс] Режим доступа - http://moodle.bgsha.com/course/view.php?id=27	Брянск: БГСХА, 2010.	ЭИОС «Moodle»

Л2.2	Исаев А.С., Хлюпина Е.А.	Правовые основы организации защиты персональных данных: Учебное пособие. - [Электронный ресурс] Режим доступа - http://window.edu.ru/resource/482/80482	СПб.: НИУ ИТМО 2014	ЭБС «Единое окно»
Л 2.3	Камышев Э.Н.	Информационная безопасность и защита информации: Учебное пособие. [Электронный ресурс] Режим доступа - http://window.edu.ru/resource/033/75033	Томск: ТПУ, 2009.	ЭБС «Единое окно»
Л 2.4	Оголюк А.А.	Защита приложений от модификации [Электронный ресурс]: учебное пособие/— Электрон. текстовые данные. — Режим доступа: http://www.iprbookshop.ru/66450.html.	СПб.: Университет ИТМО, 2013.	ЭБС «IPRbooks»
Л 2.5	Нестеров С.А.	Информационная безопасность и защита информации: Учебное пособие. - [Электронный ресурс] Режим доступа - http://window.edu.ru/resource/462/67462	СПб.: Изд-во Политехн. ун-та, 2009.	ЭБС «Единое окно»
Л 2.6	Цуканова О.А., Смирнов С.Б.	Экономика защиты информации: Учебное пособие. - [Электронный ресурс] Режим доступа - http://window.edu.ru/resource/588/41588	СПб.: СПб ГУИТМО, 2007.	ЭБС «Единое окно»
Л 2.7	Каторин Ю.Ф., Разумовский А.В., Спивак А.И.	Техническая защита информации: Лабораторный практикум - [Электронный ресурс] Режим доступа - http://window.edu.ru/resource/351/80351	СПб: НИУ ИТМО, 2013	ЭБС «Единое окно»
	Ш.Т. Ишмухаметов, Р.Г. Рубцова	Математические основы защиты информации: Электронное учебное пособие - [Электронный ресурс] Режим доступа - http://window.edu.ru/resource/128/78128	Казань: Казанский федеральный университет, 2012	ЭБС «Единое окно»
	Каторин Ю.Ф., Разумовский А.В., Спивак А.И.	Защита информации техническими средствами: Учебное пособие - http://window.edu.ru/resource/565/78565	СПб: НИУ ИТМО, 2012	ЭБС «Единое окно»
	Гатченко Н.А., Исаев А.С., Яковлев А.Д.	Криптографическая защита информации: Учебное пособие. – [Электронный ресурс] Режим доступа - - http://window.edu.ru/resource/614/78614	СПб.: НИУ ИТМО, 2012.	ЭБС «Единое окно»

6.1.3. Методические разработки

	Авторы	Заглавие	Издательство, год	Количество
Л3.1	Никулин В. В.	Методические указания к лабораторно-практическим занятиям по дисциплинам «Информационная безопасность», «Безопасность и защита информации»	Брянск: Издательство Брянский ГАУ, 2015	100
Л3.1	Никулин В. В.	Безопасность и защита информации. Электронное учебно-методическое пособие. http://moodle.bgsha.com	Брянск: Издательство Брянский ГАУ,	ЭИОС БГАУ

6.2. Перечень современных профессиональных баз данных и информационных справочных систем

1.Компьютерная информационно-правовая система «КонсультантПлюс»

2.Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru/

3.Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru/

4.Портал "Информационно-коммуникационные технологии в образовании" http://www.ict.edu.ru/

5.Полнотекстовый архив «Национальный Электронно-Информационный Консорциум» (НЭИКОН) https://neicon.ru/

6.3. Перечень программного обеспечения

1. Операционная система Microsoft Windows 7 Professional Russian
2. Операционная система Microsoft Windows 10 Professional Russian
3. Виртуальная машина для Windows 10 Hyper-V
4. Офисное программное обеспечение Microsoft Office 2010 Standart
5. Офисное программное обеспечение Microsoft Office 2013 Standart
6. Офисное программное обеспечение Microsoft Office 2016 Standart
7. Офисное программное обеспечение OpenOffice
8. Офисное программное обеспечение LibreOffice
9. Программа для просмотра PDF Foxit Reader
10. Интернет-браузеры

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебная аудитория для проведения учебных занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – 3-404 ***Основное оборудование и технические средства обучения:*** *Специализированная мебель на 30 посадочных мест, доска настенная, рабочее место преподавателя.* *28 компьютеров с выходом в локальную сеть и Интернет, электронным учебно-методическим материалам, библиотечному электронному каталогу, ЭБС, к электронной информационно-образовательной среде, киоск информационный сенсорный, мультимедийный проектор, экран.* ***Учебно-наглядные пособия:*** *Информационно-тематический стенд* ***Лицензионное программное обеспечение:*** *ОС Windows 10 (Контракт №52 01.08.2019 с Экстрим Комп). Срок действия лицензии – бессрочно.* ***Лицензионное программное обеспечение отечественного производства:*** *Microsoft Office ProPlus 2019(Гос. контракт №8 от 16.04.2021 с ООО «+Альянс»). Срок действия лицензии – бессрочно.* *Консультант Плюс (справочно-правовая система) (Гос. контракт №41 от 30.03.2018 с ООО Альянс. Срок действия лицензии – бессрочно.* ***Свободно распространяемое программное обеспечение:*** *LibreOffice (свободно распространяемое ПО).* *Яндекс.Браузер (свободно распространяемое ПО).*
Учебная аудитория для проведения учебных занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – 3-306 ***Основное оборудование и технические средства обучения:*** *Специализированная мебель на 24 посадочных мест, доска настенная, рабочее место преподавателя.* *13 компьютеров с выходом в локальную сеть и Интернет, электронным учебно-методическим материалам, библиотечному электронному каталогу, ЭБС, к электронной информационно-образовательной среде, мультимедийный проектор.* ***Учебно-наглядные пособия:*** *Информационно-тематический стенд* ***Лицензионное программное обеспечение:*** *ОС Windows 10 (Контракт №112 от 30.07.2015). Срок действия лицензии – бессрочно.* *Microsoft Office ProPlus 2019(Гос. контракт №8 от 16.04.2021 с ООО «+Альянс»). Срок действия лицензии – бессрочно.* *ArcGIS 10.2 (Договор 28/1/3 от 28.10.2013 с ООО ЭСРИ СНГ). Срок действия лицензии – бессрочно.* *Microsoft Visual Studio 2010 ((Гос. контракт №8 от 16.04.2021 с ООО «+Альянс»). Срок действия лицензии – бессрочно.* ***Лицензионное программное обеспечение отечественного производства:***

CREDO III (Договор 485/12 от 05.09.2012 с ООО Кредо-Диалог). Срок действия лицензии – бессрочно. *КОМПАС-3D (Сублицензионный договор №МЦ-19-00205 от 07.05.2019 с АСКОН-ЦР). Срок действия лицензии – бессрочно.* *Наш Сад 10 (Контракт №CCG_БР-542 от 04.10.2017 с ООО Сити-Комп Групп). Срок действия лицензии – бессрочно.* *Консультант Плюс (справочно-правовая система) (Гос. контракт №41 от 30.03.2018 с ООО Альянс). Срок действия лицензии – бессрочно.* ***Свободно распространяемое программное обеспечение:*** *LibreOffice (свободно распространяемое ПО).* *GIMP (свободно распространяемое ПО).* *MetaTrader 4 (свободно распространяемое ПО).* *QGIS (свободно распространяемое ПО).* *Ramus Educational (свободно распространяемое ПО).* *StarUML (свободно распространяемое ПО).* *Bizagi Modeler (свободно распространяемое ПО).* *Figma (свободно распространяемое ПО).* *Яндекс.Браузер (свободно распространяемое ПО).*
Помещения для хранения и профилактического обслуживания учебного оборудования - 3-315, 3-303. *Оснащены специализированной мебелью (столы, стулья, шкафы с инструментами для ремонта и профилактического обслуживания учебного оборудования)*
Помещения для самостоятельной работы: *Читальный зал научной библиотеки.* ***Основное оборудование и технические средства обучения:*** *Специализированная мебель на 100 посадочных мест, доска настенная, кафедра, рабочее место преподавателя.* *15 компьютеров с выходом в локальную сеть и Интернет, электронным учебно-методическим материалам, библиотечному электронному каталогу, ресурсам ЭБС, к электронной информационно-образовательной среде.* ***Лицензионное программное обеспечение:*** *ОС Windows 10 (Договор 15948 от 14.11.2012). Срок действия лицензии – бессрочно.* ***Лицензионное программное обеспечение отечественного производства:*** *Консультант Плюс (справочно-правовая система) (Гос. контракт №41 от 30.03.2018 с ООО Альянс). Срок действия лицензии – бессрочно.* ***Свободно распространяемое программное обеспечение:*** *LibreOffice (свободно распространяемое ПО).* *Яндекс.Браузер (свободно распространяемое ПО).*

8. ОБЕСПЕЧЕНИЕ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

- для слепых и слабовидящих:

  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

  - письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

  - обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

  - для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

  - письменные задания оформляются увеличенным шрифтом;

  - экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

  - лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

  - письменные задания выполняются на компьютере в письменной форме;

  - экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

  - лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением;

- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

- электронно-оптическое устройство доступа к информации для лиц с ОВЗ предназначено для чтения и просмотра изображений людьми с ослабленным зрением.
- специализированный программно-технический комплекс для слабовидящих. (аудитория 1-203)

- для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;
- индивидуальные системы усиления звука

«ELEGANT-R» приемник 1-сторонней связи в диапазоне 863-865 МГц
«ELEGANT-T» передатчик
«Easy speak» - индукционная петля в пластиковой оплетке для беспроводного подключения устройства к слуховому аппарату слабослышащего
Микрофон петличный (863-865 МГц), Hengda
Микрофон с оголовьем (863-865 МГц)

- групповые системы усиления звука
-Портативная установка беспроводной передачи информации .

- для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемыми эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

Информационная безопасность

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: 09.03.03 Прикладная информатика

Профиль Программно-технические средства информатизации

Дисциплина: **Информационная безопасность**

Форма промежуточной аттестации: экзамен

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ

2.1. Компетенции, закреплённые за дисциплиной ОПОП ВО.

Изучение дисциплины «Информационная безопасность» направлено на формирование следующих компетенций:

Общепрофессиональных компетенций (ОПК):

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2.2. Процесс формирования компетенций по дисциплине «Информационная безопасность»

№ Раздела	Наименование раздела	З.1	У.1	Н.1
1	Раздел 1. Основные положения теории информационной безопасности.	+	+	+
2	Раздел 2. Криптографическая защита информации. Криптография и криптоалгоритмы	+	+	+
3	Раздел 3. Законы и стандарты в области Информационной безопасности	+	+	+
4	Раздел 4. Несанкционированный доступ (НСД) к информации и методы защиты от НСД	+	+	+

Сокращение:
З. - знание; У. - умение; Н. - навыки.

2.3. Структура компетенций по дисциплине Информационная безопасность

ОПК-3: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности **ОПК 3-2**: *Учитывает основные требования информационной безопасности при решении задач профессиональной деятельности*					
Знать (З.1)		Уметь (У .1)		Владеть (Н.1)	
стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Лекции раздела № 1-4	*использовать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*	Лаб. раб., раздела № 1-4, СР раздела № 1-4	*навыками использования стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности*	Лаб. раб., раздела № 1-4, СР раздела № 1-4

3. ПОКАЗАТЕЛИ, КРИТЕРИИ ОЦЕНКИ КОМПЕТЕНЦИЙ И ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ

3.1. Оценочные средства для проведения промежуточной аттестации дисциплины

Карта оценочных средств промежуточной аттестации дисциплины, проводимой в форме экзамена

№ п/п	Раздел дисциплины	Контролируемые дидактические единицы (темы, вопросы)	Контролируемые индикаторы достижения компетенций	Оценочное средство (№ вопроса)
1	Раздел 1. Основные положения теории информационной безопасности	Основные понятия и определения курса Информационная безопасность Проблемы информационной безопасности сетей Безопасность компьютерных сетей Политики безопасности. Основные понятия политики безопасности	ОПК-3-2	Вопрос на экзамене 1-11
2	Раздел 2. Криптографическая защита информации. Криптография и криптоалгоритмы	Принципы криптографической защиты информации. Использование цифровых сертификатов.Криптографические алгоритмы шифрования	ОПК-3-2	Вопрос на экзамене 12-24

3	Раздел 3. Законы и стандарты в области Информационной безопасности	Законодательный уровень обеспечения Информационной безопасности Стандарты и спецификации в области информационной безопасности	ОПК-3-2	Вопрос на экзамене 25-37
4	Раздел 4. Несанкционированный доступ (НСД) к информации и методы защиты от НСД	Несанкционированный доступ (нсд) к информации. Комплекс программно - технических средств и организационных мер по защите информации от НСД. Протоколы формирования защищенных каналов Защита информации на сетевом уровне — протокол IPSEC. Стратегия безопасности и характеристика глобальных политик Windows 2012/7/8/10. Настройка параметров безопасности ОС Windows	ОПК-3-2	Вопрос на экзамене 38-50

Перечень вопросов к экзамену
по дисциплинек экзамену дисциплине «Информационная безопасность»

1. Основные понятия и определения информационной безопасности.
2. Протоколы IPSec и Kerberos v5.
3. Модель сетевой безопасности
4. Групповая политика в ICF
5. Построение систем защиты от угроз нарушения конфиденциальности информации
6. Шифрующая файловая система EFS и ее работа
7. Методы защиты внешнего периметра
8. Корпоративная безопасность и управляемый доступ к сети
9. Введение в сетевой информационный обмен. Использование сети Интернет
10. Основные понятия модели безопасности Windows XP/7
11. Модель ISO/OSI и стек протоколов TCP/IP
12. Особенности реализации средств протокола IPSec
13. Анализ угроз сетевой безопасности и проблемы безопасности IP-сетей
14. Протокол управления криптоключами IKE
15. Угрозы и уязвимости проводных корпоративных сетей
16. Алгоритмы аутентификации и шифрования в IPSec
17. Угрозы и уязвимости беспроводных сетей
18. Защита передаваемых данных с помощью протоколов AH и ESP
19. Способы обеспечения информационной безопасности
20. Архитектура средств безопасности IPSec
21. Защита беспроводных сетей
22. Пути решения проблем защиты информации в сетях
23. Основные понятия политики безопасности
24. Протоколы формирования защищенных каналов на сеансовом уровне
25. Структура политики безопасности организации
26. Протоколы формирования защищенных каналов на канальном уровне
27. Процедуры безопасности
28. Вредоносные программы
29. Основные понятия криптографической защиты информации
30. Комплекс программно - технических средств и организационных мер по защите информации от НСД
31. Симметричные криптосистемы шифрования
32. Классификация нарушителей
33. Асимметричные криптосистемы шифрования
34. Несанкционированный доступ (НСД) Основные термины и определения
35. Комбинированная криптосистема шифрования
36. Отечественный стандарт ЭЦП и хэширования
37. Электронная цифровая подпись и функция хэширования

38. Асимметричные криптоалгоритмы
39. Управление криптоключами
40. Симметричные и блочные алгоритмы шифрования
41. Роль стандартов в информационной безопасности
42. Классификация криптографических алгоритмов
43. Международные стандарты информационной безопасности
44. Руководящие документы Гостехкомиссии России
45. Стандарты для беспроводных сетей
46. Гармонизированные критерии Европейских стран
47. Стандарты информационной безопасности в Интернете
48. Стандарт ISO/IEC 15408 "Критерии оценки безопасности ИТ". Основные понятия
49. Отечественные стандарты безопасности информационных технологий
50. Администрирование средств безопасности

Критерии оценки компетенций.

Промежуточная аттестация обучающихся по дисциплине «Информационная безопасность» проводится в соответствии с Уставом Университета, Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся по программам ВО. Промежуточная аттестация по дисциплине проводится в соответствии с рабочим учебным планом в 5 семестре в форме экзамена по очной форме обучения, на 4 курсе по заочной форме обучения.

Обучающиеся допускается к экзамену по дисциплине в случае выполнения им учебного плана по дисциплине: выполнения всех заданий и мероприятий, предусмотренных рабочей программой дисциплины.

Оценка знаний обучаемых на экзамене носит комплексный характер, является балльной и определяется его:

- ответом на экзамене;
- результатами тестирования знаний основных понятий;
- активной работой на лабораторных занятиях.

Знания, умения, навыки обучающегося на экзамене оцениваются оценками: «*отлично*», «*хорошо», «удовлетворительно», «неудовлетворительно».*

Оценивание обучающегося на экзамене

Оценка	**Баллы**	**Требования к знаниям**
«отлично»	*15*	- обучающийся свободно справляется с решением практических задач, причем не затрудняется с решением при видоизменении заданий, правильно обосновывает принятое решение, глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает на экзамене, умеет тесно увязывать теорию с практикой.
	14	- обучающийся свободно справляется с решением практических задач, причем не затрудняется с решением при видоизменении заданий, правильно обосновывает принятое решение, твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы.
	13	- обучающийся справляется с решением практических задач, причем не затрудняется с решением при видоизменении заданий, при этом при обосновании принятого решения могут встречаться незначительные неточности, твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы.
«хорошо»	*12*	- обучающийся справляется с решением практических задач, однако видоизменение заданий могут вызвать некоторое затруднение, правильно обосновывает принятое решение, твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы.

	11	- обучающийся справляется с решением практических задач, однако видоизменение заданий могут вызвать некоторое затруднение, при этом при обосновании принятого решения могут встречаться незначительные неточности, твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы.
	10	- обучающийся справляется с решением практических задач, однако видоизменение заданий могут вызвать некоторое затруднение, при этом при обосновании принятого решения могут встречаться незначительные неточности, в основном знает материал, при этом могут встречаться незначительные неточности в ответе на вопросы.
«удовлетвори тельно»	*9*	- обучающийся с трудом справляется с решением практических задач, теоретический материал при этом может грамотно изложить, не допуская существенных неточностей в ответе на вопросы.
	8	- обучающийся с большим трудом справляется с решением практических задач, теоретический материал при этом может грамотно изложить, не допуская существенных неточностей в ответе на вопросы.
	7	- обучающийся с большим трудом справляется с решением практических задач, теоретический материал при этом излагается с существенными неточностями.
«неудовлетвор ительно»	*0*	- обучающийся не знает, как решать практические задачи, несмотря на некоторое знание теоретического материала.

3.2. Оценочные средства для проведения текущего контроля знаний по дисциплине

Карта оценочных средств текущего контроля знаний по дисциплине

№ п/п	Раздел дисциплины	Контролируемые дидактические единицы	Контролируемые компетенции (или их части)	Оценочные средства
1	Раздел 1. Основные положения теории информационной безопасности	Основные понятия и определения курса Информационная безопасность Проблемы информационной безопасности сетей Безопасность компьютерных сетей Политики безопасности. Основные понятия политики безопасности	ОПК-3-2	Опросы Компьютерные тесты Отчеты по лабораторным работам Отчеты по результатам самостоятельной работы
2	Раздел 2. Криптографическая защита информации. Криптография и криптоалгоритмы	Принципы криптографической защиты информации. Использование цифровых сертификатов. Криптографические алгоритмы шифрования	ОПК-3-2	Опросы Компьютерные тесты Отчеты по лабораторным работам Отчеты по результатам самостоятельной работы
3	Раздел 3. Законы и стандарты в области Информационной безопасности	Законодательный уровень обеспечения Информационной безопасности Стандарты и спецификации в области информационной безопасности	ОПК-3-2	Опросы Компьютерные тесты Отчеты по лабораторным работам Отчеты по результатам самостоятельной работы
	Раздел 4. Несанкционированный доступ (НСД) к информации и методы защиты от НСД	Несанкционированный доступ (нсд) к информации. Комплекс программно - технических средств и организационных мер по защите информации от НСД. Протоколы формирования защищенных каналов Защита информации на сетевом уровне	ОПК-3-2	Опросы Компьютерные тесты Отчеты по лабораторным работам Отчеты по результатам

		— протокол IPSEC. Стратегия безопасности и характеристика глобальных политик Windows 2012/7/8/10. Настройка параметров безопасности ОС Windows		самостоятельной работы

Примерные тестовые задания для промежуточной аттестации и текущего контроля знаний

1. **Контроль целостности передаваемых по сетям данных осуществляется посредством**

a) электронной цифровой подписи
b) аутентификации данных
c) аудита событий
d) межсетевого экранирования

2. **Преобразовательный процесс, в ходе которого исходный текст (или открытый текст) заменяется изменённым текстом, называется**

a) шифрование
b) дешифрование
c) преобразование
d) искажение

3. **Процесс, в ходе которого шифрованный текст преобразуется в исходный, называется**

a) шифрование
b) дешифрование
c) преобразование
d) искажение

4. **Характеристика шифра, определяющая его стойкость к шифрованию без знания ключа, называется**

a) криптостойкостью
b) пароль
c) аудентификатор
d) шифратор

5. **Асимметричное шифрование для шифрования и расшифровки использует**

a) один открытый ключ и один закрытый ключ
b) один открытый ключ
c) один закрытый ключ
d) один и тот же ключ
e) два открытых ключа
f) два закрытых ключа

6. **Относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом, называется**

a) закрытый ключ шифрования
b) электронная цифровая подпись
c) вирусная маска
d) открытый ключ шифрования

7. **Криптосистема включает**

a) алгоритм шифрования

b) набор ключей, используемых для шифрования
c) систему управления ключами
d) антивирусное ПО
e) межсетевой экран

8. Идентификация и аутентификации применяются для
a) регистрации событий безопасности
b) выявления попыток несанкционированного доступа
c) обеспечения целостности данных
d) для ограничения доступа случайных и незаконных субъектов информационной системы к её объектам

9. Управление доступом, представляющее собой разграничение доступа между поименованными субъектами и поименованными объектами, называется
a) дискретное
b) мандатное
c) принудительное
d) статистическое

10. Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации
a) межсетевой экран
b) иммунизатор
c) антивирусная программа
d) CRC-сканер

11. Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации
a) firewall
b) иммунизатор
c) утилита скрытого администрирования
d) CRC-сканер

12. Программная или программно-аппаратная система, которая выполняет контроль информационных потоков, поступающих в информационную систему и/или выходящих из нее, и обеспечивает защиту информационной системы посредством фильтрации информации
a) брандмауэр
b) иммунизатор
c) антивирусная программа
d) CRC-сканер

13. Виртуальные частные сети включают следующие сервисы безопасности:
a) экранирование
b) шифрование
c) туннелирование
d) аудит
e) регистрацию и контроль доступа

14. Межсетевой протокол, отвечающий за адресацию в сети Интернет -
a) IP
b) ICMP
c) RARP
d) UDP

e) TCP

15. **Межсетевой протокол управления сообщениями**
    a) ICMP
    b) IP
    c) ARP
    d) RARP
    e) UDP
    f) TCP

16. **Протокол разрешения адресов, выполняющий преобразование аппаратных сетевых адресов в логические -**
    a) RARP
    b) IP
    c) ICMP
    d) UDP
    e) TCP

17. **Протокол пользовательских дейтаграмм …**
    a) UDP
    b) IP
    c) ICMP
    d) ARP
    e) RARP

18. **Информация, необходимая для беспрепятственного шифрования и дешифрования текстов, называется**
    a) ключ
    b) аудентификатор
    c) шифратор
    d) пароль

19. **Характеристика шифра, определяющая его стойкость к шифрованию без знания ключа, называется …**
    a) ·криптостойкостью ·
    b) пароль ·
    c) аудентификатор
    d) шифратор
    e) пароль

20. **Асимметричное шифрование для шифрования и расшифровки использует**
    a) один открытый ключ и один закрытый ключ
    b) один открытый ключ ·
    c) один закрытый ключ ·
    d) один и тот же ключ ·
    e) два открытых ключа
    f) ·два закрытых ключа

21. **Асимметричное шифрование для шифрования использует … ключ.**
    a) Открытый
    b) Закрытый
    c) Два открытых ключа
    d) Два закрытых ключа

22. **Асимметричное шифрование для расшифровки использует … ключ.**

a) Закрытый
b) Открытый
c) Закрытый
d) Два открытых ключа
e) Два закрытых ключа

23. При симметричном шифровании для шифрования и расшифровки используются … .

a) два ключа разной длины · два разных по значению ключа ·
b) один и тот же ключ
c) два открытых ключа ·два закрытых ключа
d) один открытый ключ и один закрытый ключ

24. Относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом, называется …

a) ·закрытый ключ шифрования ·
b) электронная цифровая подпись
c) ·вирусная маска
d) ·открытый ключ шифрования

25. Протокол SSL выполняет функции по

a) созданию защищенного канала
b) управления логической связью
c) взаимную аутентификацию
d) обеспечение конфиденциальности
e) целостности и аутентичности передаваемых данных

26. Протокол SSL выполняет установление

a) SSL-сессии
b) наличия прав доступа к ресурсам компьютера или сети
c) защищенного взаимодействия
d) аутентификации сторон

27. Какие режимы аутентификации поддерживает протокол SSL 3.0:

a) взаимную аутентификацию сторон;
b) одностороннюю аутентификацию сервера без аутентификации клиента;
c) полную анонимность
d) полную целостность

28. Протокол SOCKS организует процедуру взаимодействия клиент-серверных приложений на

a) транспортном уровне модели OSI через сервер-посредник, или proxy-сервер
b) сеансовом уровне модели OSI через сервер-посредник, или proxy-сервер
c) канальном уровне модели OSI через сервер-посредник, или proxy-сервер
d) сетевом уровне модели OSI через сервер-посредник, или proxy-сервер

29. Согласно спецификации протокола SOCKS различают

a) SOCKS-сервер
b) SOCKS- посредник
c) SOCKS-клиент
d) SOCKS- proxy

30. Канальный (Data Link) уровень стандарта 802.11 состоит из

a) управления физической связью PLC (Physical Link Control)
b) управления логической связью LLC (Logical Link Control)

c) управления доступом к носителю MAC (Media Access Control)
d) управления разрешением к носителю MPC (Media Permission Control)

31. При построении и настройке беспроводной сети необходимо уделять внимание
a) Физической защите
b) Правильной настройке
c) Физической аутентификации
d) Защите пользовательских устройств
e) Традиционным мерам
f) Мониторингу сети
g) VPN-агентам

32. Модель безопасности WinXP основана на
a) Аутентификации
b) Целостности
c) Авторизации
d) Доступности

33. При аутентификации проверяются
a) идентификационные данные компьютера
b) идентификационные данные пользователя
c) идентификационные данные сервера
d) идентификационные данные домена

34. При авторизации проверяются
a) наличие прав доступа к ресурсам домена и сервера
b) наличие прав доступа к файловой системе и сети
c) наличие прав доступа к ресурсам компьютера или сети
d) наличие прав доступа к ресурсам клиента или сети

35. Функции управления криптографическими ключами
a) генерация ·
b) хранение ·
c) распределение
d) изучение
e) уничтожение

36. Главное свойство компьютерных вирусов заключается в возможности
a) ·их самопроизвольного внедрения в различные объекты операционной системы
b) ·нарушения информационной безопасности ·
c) заражения окружающих
d) уничтожения данных и компьютера

37. Вирусы, которые заражают файлы - документы и электронные таблицы офисных приложений, называются … вирусы
a) файловые
b) сетевые
c) макро-
d) загрузочные

38. Самошифрование и полиморфичность используются для …
a) саморазмножения вируса ·
b) максимального усложнения процедуры обнаружения вируса
c) расшифровки тел вируса
d) для скрытия действий антивирусной программы

39. Одним из наиболее эффективных способов борьбы с вирусами является … ·
a) использование антивирусного программного обеспечения
b) ·использования операционной системы UNIX ·
c) ограничение доступа пользователей к ЭВМ
d) шифрование данных

40. Антивирусная программа, основанная на подсчёте контрольных сумм для присутствующих на диске файлов/системных секторов называется …
a) иммунизатор ·

b) блокировщик ·
c) сканер
d) CRC-сканер

41. Антивирусная программа, перехватывающая «вирусоопасные» ситуации и сообщающая об этом пользователю, называется …

a) иммунизатор ·
b) блокировщик
c) сканер
d) CRC-сканер

42. Компьютерным вирусом является …

a) полиморфик-генератор ·
b) утилита скрытого администрирования ·
c) макро-вирус
d) логическая бомба

43. Полиморфик-генератор осуществляет … ·

a) поиск новых вирусов ·
b) удаление антивирусной программы ·
c) шифрование тела вируса
d) размножение вируса

44. Труднообнаруживаемые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода называются …

a) полиморфик-вирусы
b) стелс-вирусы ·
c) макро-вирусы
d) конструкторы вирусов

45. Анализ накопленной информации, проводимый оперативно, в реальном времени или периодически называется …

a) аудит
b) идентификация ·
c) аутентификации
d) шифрование

46. Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется

a) активным
b) оперативным ·
c) неотложным
d) автоматическим

47. Укажите типы межсетевых экранов: …

a) межсетевые экраны с фильтрацией пакетов ·
b) шлюзы сеансового уровня ·
c) шлюзы прикладного уровня ·
d) межсетевые экраны экспертного уровня
e) шлюзы физического уровня
f) межсетевые экраны канального уровня

48. Виртуальные частные сети включают следующие сервисы безопасности: … ·

a) экранирование ·
b) шифрование ·
c) туннелирование
d) аудит ·регистрацию и контроль доступа
e) электронную цифровую подпись.

49. К сервисам безопасности относят:

a) Идентификация/аутентификация
b) Протоколирование/аудит
c) Шифрование
d) Аудит

50. Потенциальные угрозы, определяющие задачи защиты информации в компьютерных сетях:

a) Прослушивание каналов
b) Умышленное уничтожение или искажение информации;
c) Выход из строя операционной системы;
d) Внедрение сетевых вирусов.

Критерии оценки тестовых заданий
Пример оценки тестовых заданий может определяться по формуле:

$$оц.тестир. = \frac{\textit{Число правильных ответов}}{\textit{Всего вопросов в тесте}} * 4$$

Где *Оц.тестир.*- оценка за тестирование. Оценка за тест используется как составная общей оценки за курс, как указано в примере п.3.1.