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.

Безопасность и защита информации
(Наименование дисциплины)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Закреплена за кафедрой	информатики, информационных систем и технологий
Направление подготовки	09.04.03 Прикладная информатика
Направленность (профиль)	Программно-технические средства информатизации
Квалификация	Магистр
Форма обучения	очная, заочная
Общая трудоемкость	5 з.е.

Брянская область
2021

Программу составил(и):

к.т.н., доцент Никулин В.В.____________

Рецензент(ы):

к.э.н., доцент Лысенкова С.Н.____________

Рабочая программа дисциплины «Безопасность и защита информации» разработана в соответствии с ФГОС ВО – магистратура по направлению подготовки 09.04.03 Прикладная информатика, утверждённого приказом Министерства образования и науки РФ от 19 сентября 2017 г., № 916.

составлена на основании учебных планов 2021 года поступления:

направление подготовки 09.04.03 Прикладная информатика направленность (профиль) Программно-технические средства информатизации

утвержденных 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 - изучение вопросов, связанных с технологиями защиты информации с использованием программно-аппаратных средств, обеспечивающих предотвращение несанкционированных информационных воздействий на автоматизированные системы и компьютерные сети, формирование основополагающих знаний в области защиты информации и обеспечения информационной безопасности защищаемому объекту.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Блок ОПОП ВО: Б1.В.04

2.1 Требования к предварительной подготовке обучающегося:
Для успешного освоения дисциплины необходимы знания, умения и навыки, полученные в результате изучения дисциплин: «Операционные системы», «Вычислительные системы, сети и телекоммуникации», «Информационная безопасность».
2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
Знания, полученные при изучении дисциплины, необходимы при прохождении производственной практики (по получению профессиональных умений и опыта профессиональной деятельности), Производственной практики (преддипломной).

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.

В результате изучения дисциплины обучающийся должен усвоить трудовые функции в соответствии с профессиональным стандартом «Специалист по информационным системам» (утвержден приказом Министерства труда и социальной защиты РФ от России от 18 ноября 2014 года № 895н).

Обобщенная трудовая функция – Управление работами по сопровождению и проектами создания (модификации) ИС, автоматизирующих задачи организационного управления и бизнес-процессы (код – С/6).

Трудовая функция –Организационное и технологическое обеспечение интеграции ИС с существующими ИС у заказчика (код D/21.7)

Трудовые действия: Обеспечение соответствия процесса интеграции ИС у заказчика принятым в организации или проекте стандартам и технологиям

Освоение дисциплины направлено на формирование следующих компетенций:

Компетенция (код и наименование)	**Индикаторы достижения компетенций** (код и наименование)	**Результаты обучения**
Тип задач профессиональной деятельности: проектный		
ПКС-2. Способен управлять информационными ресурсами и	ПКС-2.1 Осуществляет организационное и технологическое обеспечение интеграции ИС с	**Знать:** *Интерфейсы обмена данными, устройство и функционирование современных ИС,*

информационными системами	существующими ИС у заказчика	*современные стандарты информационного взаимодействия систем, современный отечественный и зарубежный опыт в профессиональной деятельности* **Уметь**: *распределять работы и выделять ресурсы, контролировать выполнение поручений* **Владеть**: *навыками обеспечения соответствия процесса интеграции ИС у заказчика принятым в организации или проекте стандартам и технологиям*
	ПКС-2.2. Реализует организационное и технологическое обеспечение оптимизации работы ИС	**Знать:** *интерфейсы обмена данными, устройство и функционирование современных ИС, современные стандарты информационного взаимодействия систем, современный отечественный и зарубежный опыт в профессиональной деятельности* **Уметь:** *распределять работы и выделять ресурсы, контролировать выполнение поручений* **Владеть:** *навыками обеспечения соответствия процесса интеграции ИС у заказчика принятым в организации или проекте стандартам и технологиям*

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		Итого	
							УП	РПД					УП	РПД
Лекции							20	20					20	20
Лабораторные							20	20					20	20
Консультация перед экзаменом							1	1					1	1
Прием экзамена							0,25	0,25					0,25	0,25
Контактная работа обучающихся с преподавателем							41,25	41,25					41,25	41,25
Сам. работа							113	113					113	113
Контроль							25,75	25,75					25,75	25,75
Итого							180	180					180	180

Распределение часов дисциплины по курсам (заочная форма)

Вид занятий	1		2		3		4		5		6		Итого	
			УП	РПД									УП	РПД
Лекции			6	6									6	6
Лабораторные			6	6									6	6
Консультация перед экзаменом			1	1									1	1
Прием экзамена			0,25	0,25									0,25	0,25
Контактная работа обучающихся с преподавателем			13,25	13,25									13,25	13,25
Сам. работа			160	160									160	160
Контроль			6,75	6,75									6,75	6,75
Итого			180	180									180	180

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ) (очная форма)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часов	Индикаторы достижения компетенций
	Раздел 1. Защита программ и данных			
1.1	Особенности защиты программ и данных /Лек/	4	6	ПКС-2.1 ПКС-2.2
1.2	Анализ источников, каналов распространения и каналов утечки информации. /Лаб/	4	2	ПКС-2.1 ПКС-2.2
1.3	Резервирование и восстановление данных: методы и схемы резервного копирования; запоминающие устройства для хранения резервных копий; план резервного копирования; примеры средств резервного копирования /Ср/	4	21	ПКС-2.1 ПКС-2.2
	Угрозы безопасности и типичные атаки на операционную систему. Проведение анализа информации на предмет целостности /Лаб/		2	
	Раздел 2. Защита в операционных системах			
1.4	Защита в операционных системах различных производителей/Лек/	4	6	ПКС-2.1 ПКС-2.2
1.5	Оценка уязвимости информации /Лаб/	4	4	ПКС-2.1 ПКС-2.2
1.6	Средства обеспечения безопасности в ОС семейства Windows. Основы безопасности в ОС семейства UNIX /Ср/	4	24	ПКС-2.1 ПКС-2.2
	Раздел 3. Защита в компьютерных сетях			
1.7	Защита в локальных и глобальных компьютерных сетях /Лек/	4	4	ПКС-2.1 ПКС-2.2
1.8	Требования к безопасности информационных систем. /Лаб/	4	2	ПКС-2.1 ПКС-2.2
1.9	Введение в сетевую безопасность: преимущества использования сети Интернет и каналы утечки, связанные с ним; базовые принципы сетевого взаимодействия; модель взаимодействия открытых систем OSI; стек протоколов TCP/IP; механизмы реализации сетевых атак; обзор механизмов защиты компьютерных сетей /Ср/	4	24	ПКС-2.1 ПКС-2.2
1.10	Требования к безопасности информационных систем в России./Лаб/		4	
	Раздел 4. Защита в СУБД			
1.11	Защита данных от несанкционированного копирования в СУБД /Лек/	4	4	ПКС-2.1 ПКС-2.2
1.12	Определение требований к защите информации /Лаб/	4	2	ПКС-2.1 ПКС-2.2
1.13	Обеспечение безопасности данных в распределенных базах данных: кластерная организация сервера баз данных, защита коммуникаций между сервером и клиентами /Ср/	4	22	ПКС-2.1 ПКС-2.2

1.14	Общие сведения о стандартизации в области защиты информации. Понятие стандартизации. Роль стандартов в области защиты информации. Оценочные стандарты и технические спецификации/Ср/	4	22	ПКС-2.1 ПКС-2.2
1.15	Анализ терминов и определений информационной безопасности/Лаб/		2	
1.16	Анализ терминов и определений информационной безопасности /Лаб/		2	
	Контроль /К/		25,75	ПКС-2.1 ПКС-2.2
	Консультация перед экзаменом/К/		1	ПКС-2.1 ПКС-2.2
	Контактная работа при приеме экзамена/К/		0,25	ПКС-2.1 ПКС-2.2

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (заочная форма)

Код занятия	Наименование разделов и тем /вид занятия/	Курс	Часов	Индикаторы достижения компетенций
	Раздел 1. Защита программ и данных			
1.1	Особенности защиты программ и данных /Лек/	2	1	ПКС-2.1 ПКС-2.2
1.2	Анализ источников, каналов распространения и каналов утечки информации. /Лаб/	2	1	ПКС-2.1 ПКС-2.2
1.3	Резервирование и восстановление данных: методы и схемы резервного копирования; запоминающие устройства для хранения резервных копий; план резервного копирования; примеры средств резервного копирования /Ср/	2	30	ПКС-2.1 ПКС-2.2
	Раздел 2. Защита в операционных системах			
1.4	Защита в операционных системах различных производителей/Лек/	2	1	ПКС-2.1 ПКС-2.2
1.5	Оценка уязвимости информации /Лаб/	2	1	ПКС-2.1 ПКС-2.2
1.6	Средства обеспечения безопасности в ОС семейства Windows. Основы безопасности в ОС семейства UNIX /Ср/	2	30	ПКС-2.1 ПКС-2.2
	Раздел 3. Защита в компьютерных сетях			
1.7	Защита в локальных и глобальных компьютерных сетях /Лек/	2	2	ПКС-2.1 ПКС-2.2
1.8	Требования к безопасности информационных систем. /Лаб/	2	2	ПКС-2.1 ПКС-2.2
1.9	Введение в сетевую безопасность: преимущества использования сети Интернет и каналы утечки, связанные с ним; базовые принципы сетевого взаимодействия; модель взаимодействия открытых систем OSI; стек протоколов TCP/IP; механизмы реализации сетевых атак; обзор механизмов защиты компьютерных сетей /Ср/	2	15	ПКС-2.1 ПКС-2.2
1.10	Требования к безопасности информационных систем в России /Ср/		15	
	Раздел 4. Защита в СУБД			
1.11	Защита данных от несанкционированного копирования в СУБД /Лек/	2	2	ПКС-2.1 ПКС-2.2
1.12	Определение требований к защите информации /Лаб/	2	2	ПКС-2.1 ПКС-2.2
1.13	Обеспечение безопасности данных в распределенных базах данных: кластерная организация сервера баз данных, защита коммуникаций между сервером и клиентами /Ср/	2	30	ПКС-2.1 ПКС-2.2
1.14	Общие сведения о стандартизации в области защиты информации. Понятие стандартизации. Роль стандартов в области защиты информации. Оценочные стандарты и технические спецификации/Ср/	2	30	ПКС-2.1 ПКС-2.2
1.15	Анализ терминов и определений информационной безопасности/Ср/		10	
	Контроль /К/		6,75	ПКС-2.1 ПКС-2.2

	Консультация перед экзаменом/К/		1	ПКС-2.1 ПКС-2.2
	Контактная работа при приеме экзамена/К/		0,25	ПКС-2.1 ПКС-2.2

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 c. — 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 c.— 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. Профессиональная справочная система «Техэксперт»
3. Официальный интернет-портал базы данных правовой информации http://pravo.gov.ru/
4. Портал Федеральных государственных образовательных стандартов высшего образования http://fgosvo.ru/
5. Портал "Информационно-коммуникационные технологии в образовании" http://www.ict.edu.ru/
6. Web of Science Core Collection политематическая реферативно-библиографическая и наукометрическая (библиометрическая) база данных http://www.webofscience.com
7. Полнотекстовый архив «Национальный Электронно-Информационный Консорциум» (НЭИКОН) https://neicon.ru/
8. Базы данных издательства Springer https://link.springer.com/

6.3. Перечень программного обеспечения

1. Операционная система Microsoft Windows 10 Professional Russian
2. Виртуальная машина в Windows 10 Hyper-V
3. Операционная система Linux
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
Безопасность и защита информации

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

Направление подготовки: 09.03.03 Прикладная информатика

Профиль Программно-технические средства информатизации

Дисциплина: Безопасность и защита информации

Форма промежуточной аттестации: экзамен

2. ПЕРЕЧЕНЬ ФОРМИРУЕМЫХ КОМПЕТЕНЦИЙ И ЭТАПЫ ИХ ФОРМИРОВАНИЯ

2.1. Компетенции, закреплённые за дисциплиной ОПОП ВО.

Изучение дисциплины «Безопасность и защита информации» направлено на формирование следующих компетенций:

профессиональных компетенций (ПКС):

ПКС-2. Способен управлять информационными ресурсами и информационными системами

ПКС-2.1 Осуществляет организационное и технологическое обеспечение интеграции ИС с существующими ИС у заказчика

ПКС-2.2. Реализует организационное и технологическое обеспечение оптимизации работы ИС

2.2. Процесс формирования компетенций по дисциплине «Безопасность и защита информации»

№ раздела	Наименование раздела	З. 1	З. 2	У. 1	У. 2	Н. 1	Н.2
Раздел 1.	Защита программ и данных	+	+	+	+	+	+
Раздел 2.	Защита в операционных системах	+	+	+	+	+	+
Раздел 3.	Защита в компьютерных сетях	+	+	+	+	+	+
Раздел 4.	Защита в СУБД	+	+	+	+	+	+

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

2.3. Структура компетенций по дисциплине «Безопасность и защита информации»

<table>
<tr><td colspan="6">ПКС-2 Способен управлять информационными ресурсами и информационными системами
ПКС-2.1 Осуществляет организационное и технологическое обеспечение интеграции ИС с существующими ИС у заказчика</td></tr>
<tr><td colspan="2">Знать (З.3)</td><td colspan="2">Уметь (У .3)</td><td colspan="2">Владеть (Н.3)</td></tr>
<tr><td>Интерфейсы обмена данными, устройство и функционирование современных ИС, современные стандарты информационного взаимодействия систем, современный отечественный и зарубежный опыт в профессиональной деятельности</td><td>Лекции разделов № 1-4</td><td>распределять работы и выделять ресурсы, контролировать выполнение поручений</td><td>Лаб. раб разделов №1-4, СР разделов №1-4</td><td>навыками обеспечения соответствия процесса интеграции ИС у заказчика принятым в организации или проекте стандартам и технологиям</td><td>Лаб. раб разделов №1-4, СР разделов №1-4</td></tr>
<tr><td colspan="6">ПКС-2 Способен управлять информационными ресурсами и информационными системами
ПКС-2.2 Реализует организационное и технологическое обеспечение оптимизации работы ИС</td></tr>
<tr><td colspan="2">Знать (З.2)</td><td colspan="2">Уметь (У.2)</td><td colspan="2">Владеть (Н.2)</td></tr>
<tr><td>интерфейсы обмена данными, устройство и функционирование современных ИС, современные стандарты информационного взаимодействия систем, современный отечественный и зарубежный опыт в профессиональной деятельности</td><td>Лекции разделов № 1,2,3,4</td><td>распределять работы и выделять ресурсы, контролировать выполнение поручений</td><td>Лаб. раб разделов №1-4, СР разделов №1-4</td><td>навыками обеспечения соответствия процесса интеграции ИС у заказчика принятым в организации или проекте стандартам и технологиям</td><td>Лаб. раб разделов №1-4, СР разделов №1-4</td></tr>
</table>

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 компетенции	Оценочное средство (№ вопроса)
1	Раздел 1. Защита программ и данных	Защищаемая информация и основные способы несанкционированного доступа (НСД) в автоматизированной системе: виды информации, подлежащей защите; классификация угроз безопасности; модель нарушителя; основные методы и средства защиты информации. Роль и место программно-аппаратных средств информационной безопасности в КСЗИ: классификация средств защиты информации (СЗИ); основные функции средств защиты информации от НСД	ПКС-2 ПКС-2. ПКС-2.2	Вопрос на экзамене 1-20

2	Раздел 2. Защита в операционных системах	Общие сведения об операционных системах: назначение и функции операционной системы, особенности архитектуры операционных систем; классификация операционных систем, тенденции развития операционных систем; файловые системы. Средства обеспечения безопасности в ОС семейства Windows. Основы безопасности в ОС семейства UNIX	ПКС-2 ПКС-2. ПКС-2.2	Вопрос на экзамене 21-35
3	Раздел 3. Защита в компьютерных сетях	Введение в сетевую безопасность: преимущества использования сети Интернет и каналы утечки, связанные с ним; базовые принципы сетевого взаимодействия; модель взаимодействия открытых систем OSI; стек протоколов TCP/IP; механизмы реализации сетевых атак; обзор механизмов защиты компьютерных сетей. Межсетевые экраны: понятие периметра сети; определение и функции межсетевого экранирования; фильтрация трафика; трансляция адресов; классификация межсетевых экранов; инспекторы состояния; примеры межсетевых экранов	ПКС-2 ПКС-2. ПКС-2.2	Вопрос на экзамене 36-41
4	Раздел 4. Защита в СУБД	Введение в безопасность СУБД: объекты защиты, уязвимости СУБД, особенности защиты информации в базах данных, критерии защищенности СУБД; Средства обеспечения безопасности данных в базе: идентификация и аутентификация пользователей, управление доступом, регистрация событий безопасности, особенности шифрования данных. Обеспечение целостности базы данных: ограничения и ссылочная целостность, правила, использование хранимых процедур и триггеров, резервное копирование и восстановление, контрольные точки. Обеспечение безопасности данных в распределенных базах данных: защита коммуникаций между сервером и клиентами, тиражирование данных и синхронизация	ПКС-2 ПКС-2. ПКС-2.2	Вопрос на экзамене 42-50

Перечень вопросов к экзамену по дисциплине <u>Безопасность и защита информации</u>

1. Основные понятия и определения курса Безопасность и защита информации
2. Защищаемая информация и основные способы несанкционированного доступа (НСД) в автоматизированной системе
3. Основные составляющие информационной безопасности
4. Важность и сложность проблемы информационной безопасности
5. Сценарии реализации угроз информационной безопасности
6. Обход средств защиты от разглашения конфиденциальной информации
7. Кража конфиденциальной информации
8. Нарушение авторских прав на информацию
9. Нецелевое использование ресурсов
10. Актуальность задач компьютерной безопасности
11. Понятие «угрозы». Основные угрозы безопасности систем обработки информации
12. Необходимость применения объектно-ориентированного подхода к информационной безопасности
13. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем

14. Оценочные стандарты и технические спецификации. «Оранжевая книга» как оценочный стандарт
15. Информационная безопасность распределенных систем. Рекомендации X.800
16. Сетевые механизмы безопасности
17. Администрирование средств безопасности
18. Стандарт ISO/IEC 15408 «Общие критерии оценки безопасности информационных технологий»
19. Наиболее опасные угрозы информационной безопасности
20. классификация угроз безопасности;
21. Роль и место программно-аппаратных средств информационной безопасности в КСЗИ
22. классификация средств защиты информации (СЗИ);
23. основные функции средств защиты информации от НСД
24. назначение и функции операционной системы,
25. особенности архитектуры операционных систем;
26. Средства обеспечения безопасности в ОС семейства Windows.
27. Основы безопасности в ОС семейства UNIX
28. Введение в сетевую безопасность
29. преимущества использования сети Интернет и каналы утечки, связанные с ним;
30. базовые принципы сетевого взаимодействия;
31. модель взаимодействия открытых систем OSI;
32. стек протоколов TCP/IP;
33. механизмы реализации сетевых атак;
34. обзор механизмов защиты компьютерных сетей.
35. Межсетевые экраны: понятие периметра сети;
36. определение и функции межсетевого экранирования;
37. фильтрация трафика; трансляция адресов;
38. классификация межсетевых экранов; примеры межсетевых экранов
39. Введение в безопасность СУБД: объекты защиты, уязвимости СУБД, особенности защиты информации в базах данных,
40. критерии защищенности СУБД;
41. Средства обеспечения безопасности данных в базе:
42. идентификация и аутентификация пользователей, управление доступом, регистрация событий безопасности, представления, триггеры, особенности шифрования данных, транзакции.
43. Обеспечение целостности базы данных: ограничения и ссылочная целостность, правила, использование хранимых процедур и триггеров, резервное копирование и восстановление, контрольные точки.
44. Обеспечение безопасности данных в распределенных базах данных
45. кластерная организация сервера баз данных,
46. защита коммуникаций между сервером и клиентами,
47. проблемы параллелизма, сериализация транзакций,
48. блокировки, тиражирование данных и синхронизация
49. Межсетевые экраны: понятие периметра сети
50. определение и функции межсетевого экранирования

5.2. Темы письменных работ

1. Доктрина информационной безопасности РФ.
2. Информационное обеспечение государственной политики РФ.
3. Развитие современных информационных технологий.
4. Угрозы информационной безопасности РФ.
5. Информационно-психологическое оружие.

6. Информационо-психологическая война.
7. Защита информационных ресурсов от несанкционированного доступа.
8. Информационный терроризм.
9. Международное сотрудничество РФ в области защиты информации.
10. Государственная тайна.
11. Служебная тайна.
12. Коммерческая тайна.
13. Персональные данные.
14. Личная тайна.
15. Основные понятия административного уровня информационной безопасности
16. Политика безопасности
17. Программа безопасности
18. Синхронизация программы безопасности с жизненным циклом систем
19. Понятие об управлении рисками
20. Основные классы мер процедурного уровня
21. Физическая защита
22. Реагирование на нарушения режима безопасности
23. Основные понятия программно-технического уровня
24. информационной безопасности
25. Особенности современных информационных систем,
26. существенные при обеспечении информационной безопасности
27. Архитектура системы безопасности
28. Понятие криптографии
29. Системы идентификации и аутентификации пользователей
30. Системы шифрования дисковых данных
31. Системы шифрования данных
32. Системы аутентификации электронных данных
33. Средства управления ключевой информацией
34. Асимметричные криптосистемы
35. Криптосистема шифрования данных RSA
36. Процедуры шифрования и расшифрования в криптосистеме
37. RSA
38. Пример использования алгоритма RSA
39. Аутентификация данных и электронная цифровая подпись
40. Алгоритм цифровой подписи RSA
41. Понятие о симметричной криптосистеме
42. Система шифрования Цезаря
43. Система Цезаря с ключевым словом
44. Шифры сложной замены
45. Стандарт шифрования данных DES
46. Вредоносные программы и компьютерные вирусы
47. Способы распространения вредоносных программ
48. Последствия заражений вредоносной программой
49. Классификация вредоносных программ
50. Основы борьбы с вредоносными программами

Критерии оценки компетенций.

Промежуточная аттестация обучающихся по дисциплине «Безопасность и защита информации» 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 4 семестре в форме экзамена по очной форме обучения, на 2 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	- Студент свободно справляется с лабораторными работами, 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	- Студент свободно справляется с лабораторными работами, 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	- Студент справляется с лабораторными работами, 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	- Студент справляется с лабораторными работами, 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	- Студент справляется с лабораторными работами, 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	- Студент справляется с лабораторными работами, 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.
«удовлетворительно»	9	- Студент с трудом справляется с лабораторными работами, теоретический материал при этом может грамотно изложить, не допуская существенных неточностей в ответе на вопросы.
	8	- Студент с большим трудом справляется с лабораторными работами, теоретический материал при этом может грамотно изложить, не допуская существенных неточностей в ответе на вопросы.
	7	- Студент с большим трудом справляется с лабораторными работами, теоретический материал при этом излагается с существенными неточностями.
«неудовлетворительно»	0	- Студент не знает, как делать лабораторные работы, 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 (темы, вопросы)	Контролируемые компетенции	Оценочное средство)
1	Раздел 1. Защита программ и данных	Защищаемая информация и основные способы несанкционированного доступа (НСД) в автоматизированной системе виды информации, подлежащей защите; классификация угроз безопасности; модель нарушителя; основные методы и средства защиты информации	ПКС-2. ПКС-2.1 ПКС-2.2	Опросы Отчеты по лабораторным работам Отчеты по результатам выполнения самостоятельной работы Тесты
2	Раздел 2. Защита в операционных системах	Общие сведения об операционных системах назначение и функции операционной системы, особенности архитектуры операционных систем; классификация операционных систем, тенденции развития операционных систем; Средства обеспечения безопасности в ОС семейства Windows. Основы безопасности в ОС семейства UNIX	ПКС-2. ПКС-2.1 ПКС-2.2	Опросы Отчеты по лабораторным работам Отчеты по результатам выполнения самостоятельной работы Тесты
3	Раздел 3. Защита в компьютерных сетях	Введение в сетевую безопасность преимущества использования сети Интернет и каналы утечки, связанные с ним; базовые принципы сетевого взаимодействия; модель взаимодействия открытых систем OSI; стек протоколов TCP/IP; механизмы реализации сетевых атак; обзор механизмов защиты компьютерных сетей. Межсетевые экраны: понятие периметра сети; классификация межсетевых экранов; примеры межсетевых экранов	ПКС-2. ПКС-2.1 ПКС-2.2	Опросы Отчеты по лабораторным работам Отчеты по результатам выполнения самостоятельной работы Тесты
4	Раздел 4. Защита в СУБД	Введение в безопасность СУБД: объекты защиты, уязвимости СУБД, критерии защищенности СУБД; Средства обеспечения безопасности данных в базе: идентификация и аутентификация пользователей, Обеспечение безопасности данных в распределенных базах данных кластерная организация сервера баз данных, защита коммуникаций между сервером и клиентами, проблемы параллелизма, сериализация транзакций, блокировки, тиражирование данных и синхронизация	ПКС-2. ПКС-2.1 ПКС-2.2	Опросы Отчеты по лабораторным работам Отчеты по результатам выполнения самостоятельной работы Тесты

Примерные тестовые задания для промежуточной аттестации и текущего контроля знаний

Вопрос:1Сопоставьте названия программ и изображений

Укажите соответствие для всех 6 вариантов ответа:

1) 

2) 

3) 

4)

5)

6)

__ **Antivir**
__ **DrWeb**
__ **Nod 32**
__ **Antivirus Kaspersky**
__ **Avast**
__ **Antivirus Panda**

Вопрос:2 RAID-массив это
Выберите один из 5 вариантов ответа:
1) **Набор жестких дисков, подключенных особым образом**
2) **Антивирусная программа**
3) **Вид хакерской утилиты**
4) **База защищенных данных**
5) **Брандмауэр**

Вопрос: 3 Выразите свое согласие или несогласие
Укажите истинность или ложность вариантов ответа:
__ **Почтовый червь активируется в тот момент, когда к вам поступает электронная почта**
__ **Если компьютер не подключен к сети Интернет, в него не проникнут вирусы**
__ **Файловые вирусы заражают файлы с расширениями *.doc, *.ppt, *.xls**
__ **Чтобы защитить компьютер недостаточно только установить антивирусную программу**
__ **На Web-страницах могут находится сетевые черви**

Вопрос:4 Отметьте составные части современного антивируса
Выберите несколько из 5 вариантов ответа:
1) **Модем**
2) **Принтер**
3) **Сканер**
4) **Межсетевой экран**
5) **Монитор**

Вопрос: 5 Вредоносные программы - это
Выберите один из 5 вариантов ответа:
1) **шпионские программы**
2) **программы, наносящие вред данным и программам, находящимся на компьютере**
3) **антивирусные программы**
4) **программы, наносящие вред пользователю, работающему на зараженном компьютере**
5) **троянские утилиты и сетевые черви**

Вопрос:6 К вредоносным программам относятся:
Выберите несколько из 5 вариантов ответа:
1) **Потенциально опасные программы**
2) **Вирусы, черви, трояны**
3) **Шпионские и рекламмные программы**
4) **Вирусы, программы-шутки, антивирусное программное обеспечение**
5) **Межсетевой экран, брандмауэр**

Вопрос:7 Сетевые черви это
Выберите один из 5 вариантов ответа:
1) **Вредоносные программы, устанавливающие скрытно от пользователя другие вредоносные программы и утилиты**
2) **Вирусы, которые проникнув на компьютер, блокируют работу сети**
3) **Вирусы, которые внедряются в документы под видом макросов**
4) **Хакерские утилиты управляющие удаленным доступом компьютера**
5) **Вредоносные программы, которые проникают на компьютер, используя сервисы компьютерных сетей**

Вопрос:8 К биометрической системе защиты относятся:
Выберите несколько из 5 вариантов ответа:
1) **Защита паролем**
2) **Физическая защита данных**
3) **Антивирусная защита**
4) **Идентификация по радужной оболочке глаз**
5) **Идентификация по отпечаткам пальцев**

Вопрос:9 Вредоносная программа, которая подменяет собой загрузку некоторых программ при загрузке системы называется...
Выберите один из 5 вариантов ответа:
1) **Загрузочный вирус**
2) **Макровирус**
3) **Троян**
4) **Сетевой червь**
5) **Файловый вирус**

Вопрос:10 Программа, осуществляющая несанкционированные действия по сбору, и передаче информации злоумышленнику, а также ее разрушение или злонамеренную модификацию.
Запишите ответ:
____

Вопрос:11 Руткит - это...
Выберите один из 5 вариантов ответа:
1) **вредоносная программа, выполняющая несанкционированные действия по передаче управления компьютером удаленному пользователю**
2) **разновидность межсетевого экрана**
3) **программа использующая для распространения Рунет (Российскую часть Интернета)**
4) **вредоносная программа, маскирующаяся под макрокоманду**
5) **программа для скрытого взятия под контроль взломанной системы**

Вопрос:12 Компьютерные вирусы это

Выберите несколько из 5 вариантов ответа:
1) **Вредоносные программы, наносящие вред данным.**
2) **Программы, уничтожающие данные на жестком диске**
3) **Программы, которые могут размножаться и скрыто внедрять свои копии в файлы, загрузочные сектора дисков, документы.**
4) **Программы, заражающие загрузочный сектор дисков и препядствующие загрузке компьютера**
5) **Это скрипты, помещенные на зараженных интернет-страничках**

Вопрос:13 Вирус внедряется в исполняемые файлы и при их запуске активируется. Это...
Выберите один из 5 вариантов ответа:
1) **Загрузочный вирус**
2) **Макровирус**
3) **Файловый вирус**
4) **Сетевой червь**
5) **Троян**

Вопрос:14 Укажите порядок действий при наличии признаков заражения компьютера
Укажите порядок следования всех 3 вариантов ответа:
__ Сохранить результаты работы на внешнем носителе
__ Запустить антивирусную программу
__ Отключиться от глобальной или локальной сети

Вопрос:15 Вирус поражающий документы называется
Выберите один из 5 вариантов ответа:
1) **Троян**
2) **Файловый вирус**
3) **Макровирус**
4) **Загрузочный вирус**
5) **Сетевой червь**

***Вопрос:16*. Основные угрозы доступности информации:**
непреднамеренные ошибки пользователей
злонамеренное изменение данных
хакерская атака
отказ программного и аппаратного обеспечения
разрушение или повреждение помещений
перехват данных

17. Суть компрометации информации
внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

18. Информационная безопасность автоматизированной системы – это состояние

автоматизированной системы, при котором она, …
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды
с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
способна противостоять только информационным угрозам, как внешним так и внутренним
способна противостоять только внешним информационным угрозам

19. Методы повышения достоверности входных данных
Замена процесса ввода значения процессом выбора значения из предлагаемого множества
Отказ от использования данных
Проведение комплекса регламентных работ
Использование вместо ввода значения его считывание с машиночитаемого носителя
Введение избыточности в документ первоисточник
Многократный ввод данных и сличение введенных значений

20. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)
МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения
МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

21. Сервисы безопасности:
идентификация и аутентификация
шифрование
инверсия паролей
контроль целостности
регулирование конфликтов
экранирование
обеспечение безопасного восстановления
кэширование записей

22. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
несанкционированного управления удаленным компьютером
внедрения агрессивного программного кода в рамках активных объектов Web-страниц
перехвата или подмены данных на путях транспортировки
вмешательства в личную жизнь
поставки неприемлемого содержания

23. Причины возникновения ошибки в данных
Погрешность измерений
Ошибка при записи результатов измерений в промежуточный документ
Неверная интерпретация данных
Ошибки при переносе данных с промежуточного документа в компьютер
Использование недопустимых методов анализа данных

Неустранимые причины природного характера
Преднамеренное искажение данных
Ошибки при идентификации объекта или субъекта хозяйственной деятельности

24. К формам защиты информации не относится…
аналитическая
правовая
организационно-техническая
страховая

25. Наиболее эффективное средство для защиты от сетевых атак
использование сетевых экранов или «firewall»
использование антивирусных программ
посещение только «надёжных» Интернет-узлов
использование только сертифицированных программ-броузеров при доступе к сети Интернет

26. Информация, составляющая государственную тайну не может иметь гриф…
«для служебного пользования»
«секретно»
«совершенно секретно»
«особой важности»

27. Разделы современной криптографии:
Симметричные криптосистемы
Криптосистемы с открытым ключом
Криптосистемы с дублированием защиты
Системы электронной подписи
Управление паролями
Управление передачей данных
Управление ключами

28. Документ, определивший важнейшие сервисы безопасности и предложивший метод классификации информационных систем по требованиям безопасности
рекомендации X.800
Оранжевая книга
Закону «Об информации, информационных технологиях и о защите информации»

29. Утечка информации – это …
несанкционированный процесс переноса информации от источника к злоумышленнику
процесс раскрытия секретной информации
процесс уничтожения информации
непреднамеренная утрата носителя информации

30. Основные угрозы конфиденциальности информации:
маскарад
карнавал
переадресовка
перехват данных
блокирование
злоупотребления полномочиями

31. Элементы знака охраны авторского права:
буквы С в окружности или круглых скобках
буквы Р в окружности или круглых скобках
наименования (имени) правообладателя
наименование охраняемого объекта
года первого выпуска программы

32. Защита информации обеспечивается применением антивирусных средств
да
нет
не всегда

33. Вид угрозы действия, направленного на несанкционированное использование информационных ресурсов, не оказывающего при этом влияния на её функционирование – … угроза
активная
пассивная

34. Преднамеренная угроза безопасности информации
кража
наводнение
повреждение кабеля, по которому идет передача, в связи с погодными условиями
ошибка разработчика

35. Концепция системы защиты от информационного оружия не должна включать…
средства нанесения контратаки с помощью информационного оружия
механизмы защиты пользователей от различных типов и уровней угроз для национальной информационной инфраструктуры
признаки, сигнализирующие о возможном нападении
процедуры оценки уровня и особенностей атаки против национальной инфраструктуры в целом и отдельных пользователей

36. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …
обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации
реализацию права на доступ к информации»
соблюдение норм международного права в сфере информационной безопасности
выявление нарушителей и привлечение их к ответственности
соблюдение конфиденциальности информации ограниченного доступа
разработку методов и усовершенствование средств информационной безопасности

37. Заплата или патч (от англ. patch - латать, ставить заплаты) -
Выберите один ответ:
a. это программный алгоритм, используемый для модификации используемой программы
b. это программный комплекс, используемый для модификации используемой программы

- [x] c. это программный код, используемый для модификации используемой программы
- [ ] d. это программный шифр, используемый для модификации используемой программы

38. Все вредоносные программы в соответствии со способами распространения и вредоносной нагрузкой можно разделить на основные типы:
Выберите один ответ:

- [ ] a. другие программы
- [ ] b. трояны
- [x] c. Все перечисленное
- [ ] d. компьютерные вирусы
- [ ] e. Черви

39. Вирусы можно разделить на классы по следующим основным признакам:
Выберите один или несколько ответов:

- [x] a. операционная система (ОС)
- [x] b. особенности алгоритма работы
- [x] c. деструктивные возможности
- [ ] d. языкам программирования
- [x] e. среда обитания

40. По среде обитания вирусы можно разделить на:
Выберите один или несколько ответов:

- [x] a. сетевые
- [x] b. загрузочные
- [x] c. макро
- [ ] d. системные
- [x] e. файловые

41. Какие главные цели преследует реакция на нарушения режима безопасности:
Выберите один или несколько ответов:

- [ ] a. нарушение внешних организаций
- [x] b. выявление нарушителя;
- [x] c. локализация инцидента и уменьшение наносимого вреда;
- [x] d. предупреждение повторных нарушений;

42. Направления физической защиты:
Выберите один или несколько ответов:

- [x] a. защита мобильных систем.
- [ ] b. защита автомобильных систем
- [x] c. противопожарные меры;

- [x] d. физическое управление доступом;
- [x] e. защита поддерживающей инфраструктуры;
- [x] f. защита от перехвата данных;

43. В жизненном цикле информационного сервиса можно выделить следующие этапы:

Выберите один или несколько ответов:

- [x] a. Инициация
- [x] b. Установка
- [ ] c. продажа
- [x] d. Закупка
- [x] e. Эксплуатация
- [x] f. Выведение из эксплуатации

44. Направления физической защиты:

Выберите один или несколько ответов:

- [ ] a. защита автомобильных систем
- [x] b. защита от перехвата данных;
- [x] c. противопожарные меры;
- [x] d. защита мобильных систем.
- [x] e. защита поддерживающей инфраструктуры;
- [x] f. физическое управление доступом;

45. Какие элементы включает в себя информационная инфраструктура:

Выберите один или несколько ответов:

- [ ] a. информационные сервисы внутренних организаций
- [x] b. документацию
- [x] c. программы и данные
- [x] d. информационные сервисы внешних организаций
- [x] e. компьютеры

46. Какие основные виды требований безопасности содержит «Оранжевая книга»:

Выберите один или несколько ответов:

- [ ] a. не требующие доверия
- [ ] b. нефункциональные
- [x] c. требования доверия
- [x] d. Функциональные

47. Конфиденциальность информации – это

Выберите один ответ:

- ○ a. обязательное для выполнения лицом требование не передавать информацию третьим лицам без согласия ее обладателя;

b. добровольное для выполнения лицом требование не передавать информацию третьим лицам без согласия ее обладателя;

c. обязательное для выполнения лицом требование не передавать информацию третьим лицам без согласия ее обладателя;

48. Стандарты и спецификации бывают разных видов:

Выберите один или несколько ответов:

a. технических условий

b. госстандартов

c. оценочных стандартов;

d. технических спецификаций

49. Обладатель информации – это

Выберите один ответ:

a. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

b. лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

c. устройство самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

50. Информационные технологии – это

Выберите один ответ:

a. процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

b. совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

c. технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники

Критерии оценки тестовых заданий

Пример оценки тестовых заданий может определяться по формуле:

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

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