МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой
естественнонаучных и
общеобразовательных дисциплин

С.Е. Зюзин
27.06.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.О.05.10 Информационная безопасность

1. Код и наименование направления подготовки:

44.03.05 Педагогическое образование (с двумя профилями подготовки)

2. Профили подготовки:

Математика. Информатика и информационные технологии в образовании

3. Квалификация выпускника: бакалавр

4. Форма обучения: очная/заочная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра естественнонаучных и общеобразовательных дисциплин

6. Составитель программы: Хвостов М.Н., кандидат физико-математических наук

7. Рекомендована: научно-методическим советом Филиала от 25.04.2023 протокол № 7

8. Учебный год: ОФО – 2026-2027 **Семестр:** 9

ЗФО – 2027-2028 **Семестр:** 11

9.Цель и задачи учебной дисциплины:

Целью освоения учебной дисциплины является: становление профессиональной компетенции педагога через формирование целостного представления о роли информационных технологий в современной образовательной среде и педагогической деятельности на основе овладения комплексными методами и современными средствами защиты компьютерных систем и их компонентов от различных угроз безопасности.

Задачи учебной дисциплины:

- дать теоретические основы знаний в области принципов и физических основ, используемых для защиты информации, алгоритмов их работы и методик применения;
- выработка у студентов умений формулировать и обосновывать технические требования к средствам защиты информации, осуществлять обоснованный выбор комплекса средств защиты информации для конкретных компьютерных систем и использовать их в практической деятельности;
- формирование у студентов представлений об особенностях, тенденциях, проблемах и перспективах развития средств защиты информации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации.

10. Место учебной дисциплины в структуре образовательной программы:

Дисциплина «Информационная безопасность» относится к дисциплинам обязательной части блока Б1 и включена в Предметно-содержательный модуль. Для освоения дисциплины «Информационная безопасность» необходимы знания, умения, навыки, сформированные в ходе изучения дисциплин: «Информатика» «Программирование». Изучение данной дисциплины является необходимой основой для написания ВКР.

Условия реализации дисциплины для лиц с ОВЗ определяются особенностями восприятия учебной информации и с учетом индивидуальных психофизических особенностей.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ОПК-9	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-9.1	Осуществляет поиск, сбор, хранение, обработку, представление информации при решении задач профессиональной деятельности	Знать: - инструментарий средств защиты информации для безопасного сбора, хранения, обработки, представления, передачи информации в сфере профессиональной деятельности Уметь: - использовать основные методы, приемы и хранения, обработки, представления, передачи информации для решения задач профессиональной деятельности
		ОПК-9.2	Подбирает и использует информационные технологии при решении задач профессиональной	

			деятельности	
ПК-3	Способен осваивать и использовать базовые научно-теоретические знания и практические умения по предмету в профессиональной деятельности	ПК-3.1	Демонстрирует знание основ общетеоретических и профильных дисциплин в объеме, необходимом для решения педагогических, методических и организационно-управленческих задач	Знать: - основы общетеоретических и профильных дисциплин в объеме, необходимом для решения педагогических, методических и организационно-управленческих задач; связь теоретических основ и технологических приёмов учебной дисциплины с содержанием предметной области «Математика и информатика» Уметь: - использовать знание основ учебных дисциплин предметной области «Математика и информатика» для перевода информации с естественного языка на язык предметной области «Математика и информатика» и обратно; применять теоретические знания в описании процессов и явлений в различных областях знания; использовать преимущества технологических приемов учебных дисциплин предметной области «Математика и информатика» при решении задач школьного курса Владеть: - конструктивными умениями как одним из главных аспектов профессиональной культуры будущего педагога; материалом учебных дисциплин предметной области «Математика и информатика» на уровне, позволяющем формулировать и решать задачи, возникающие в ходе учебной деятельности по преподаваемым предметам, а также в практической деятельности, требующие углубленных профессиональных знаний; навыками формализации теоретических и прикладных практических задач
		ПК-3.2	Применяет навыки комплексного анализа и систематизации базовых научно-теоретических знаний предметной области «Математика и информатика» для решения профессиональных задач (в соответствии с профилем и уровнем обучения)	

12. Объем дисциплины в зачетных единицах/часах — 2/72.

Форма промежуточной аттестации: *зачет с оценкой*.

13. Трудоемкость по видам учебной работы

ОФО

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			семестр №9
Контактная работа		40	40
в том числе:	лекции	14	22
	практические	26	32
Самостоятельная работа		32	32
Итого:		72	72

ЗФО

Вид учебной работы	Трудоемкость	
	Всего	По семестрам

			семестр №11
Контактная работа		12	12
в том числе:	лекции	6	22
	практические	6	32
Самостоятельная работа		56	56
Промежуточная аттестация – зачет с оценкой		4	4
Итого:		72	72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
1. Лекции			
1.1	Угрозы информационной безопасности	Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. Анализ угроз информационной безопасности. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). Свойства информации: конфиденциальность, доступность, целостность. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации.	–
1.2	Информационные системы и их компоненты как объекты защиты	Общее представление о структуре защищенной информационной системы. Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы. Понятие информационного сервиса безопасности. Виды сервисов безопасности.	–
1.3	Направления разработки и применения средств защиты информации	Системные принципы информационной безопасности. Выработка политики безопасности. Направления применения методов и средств защиты информации	–
1.4	Организационно-правовые меры и средства защиты информации	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства. Особенности сертификации и стандартизации криптографических услуг. Законодательная база информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны.	
1.5	Технические и программные средства защиты информации	Идентификация и аутентификация. Парольные схемы аутентификации. Симметричные схемы аутентификации субъекта. Несимметричные схемы аутентификации (с открытым ключом). Аутентификация с третьей доверенной стороной (схема Kerberos). Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.	

		Обеспечение защиты корпоративной информационной среды от атак на информационные сервисы. Защита Интернет-подключений, функции и назначение межсетевых экранов. Понятие демилитаризованной зоны. Виртуальные частные сети (VPN), их назначение и использование в корпоративных информационных системах. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Основные варианты организации защиты ЭП Расчет мощности UPS Устройства бесперебойного электропитания Управление UPS. Особенности хранения компьютерной информации на физических носителях.	
1.6	Криптографические методы защиты информации	Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. Изучение устройства и принципа работы шифровальной машины Энигма. Стандарт симметричного шифрования AES Rijndael. Генерация простых чисел, используемых в асимметричных системах шифрования. Электронная цифровая подпись. Шифрование методом скользящей перестановки. Корректирующие коды. Методы сжатия.	
2. Практические занятия			
2.1	Организационно-правовые меры и средства защиты информации	Концепция информационной безопасности. Информационная безопасность образовательной организации.	–
2.2	Технические и программные средства защиты информации	Защита данных и сервисов от воздействия вредоносных программ. Вирусы, троянские программы. Антивирусное программное обеспечение. Защита системы электронной почты. Спам, борьба со спамом. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом. Требования к защите электропитания различных компонентов КС. Выбор политики защиты электропитания КС Выборочная защита. Частичная защита. Полная защита Способы уничтожения информации без разрушения носителя: программные и физические. Способы уничтожения информации с разрушением носителя: механические, термические, химические радиационные.	–
2.3	Криптографические методы защиты информации	Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации. Исследование различных методов защиты текстовой информации и их стойкости на основе подбора ключей. Генерация простых чисел, используемых в асимметричных системах шифрования. Электронная цифровая подпись. Шифрование методом скользящей перестановки.	–

13.2. Темы (разделы) дисциплины и виды занятий

ОФО

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего
1	Угрозы информационной безопасности	2	0	0	2	4
2	Информационные системы и	2	0	0	6	8

	их компоненты как объекты защиты					
3	Направления разработки и применения средств защиты информации	2	0	0	6	8
4	Организационно-правовые меры и средства защиты информации	2	4	0	6	12
5	Технические и программные средства защиты информации	4	10	0	6	20
6	Криптографические методы защиты информации	2	12	0	6	20
	Итого:	14	26	0	32	72

ЗФО

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические занятия	Лабораторные работы	Самостоятельная работа	Всего
1	Угрозы информационной безопасности	1	0	0	9	10
2	Информационные системы и их компоненты как объекты защиты	1	0	0	9	10
3	Направления разработки и применения средств защиты информации	1	0	0	9	10
4	Организационно-правовые меры и средства защиты информации	1	2	0	9	12
5	Технические и программные средства защиты информации	1	2	0	11	14
6	Криптографические методы защиты информации	1	2	0	9	12
	Зачет с оценкой					4
	Итого:	6	6	0	56	72

14. Методические указания для обучающихся по освоению дисциплины

Приступая к изучению учебной дисциплины, прежде всего обучающиеся должны ознакомиться с учебной программой дисциплины. Вводная лекция содержит информацию об основных разделах рабочей программы дисциплины; электронный вариант рабочей программы размещён на сайте БФ ВГУ.

Знание основных положений, отраженных в рабочей программе дисциплины, поможет обучающимся ориентироваться в изучаемом курсе, осознавать место и роль изучаемой дисциплины, строить свою работу в соответствии с требованиями, заложенными в программе.

Основными формами контактной работы по дисциплине являются лекции и практические занятия, посещение которых обязательно для всех студентов (кроме студентов, обучающихся по индивидуальному плану).

В ходе лекционных занятий следует не только слушать излагаемый материал и кратко его конспектировать, но очень важно участвовать в анализе примеров, предлагаемых преподавателем, в рассмотрении и решении проблемных вопросов, выносимых на обсуждение. Необходимо критически осмысливать предлагаемый материал, задавать вопросы как уточняющего характера, помогающие уяснить отдельные излагаемые положения, так и вопросы продуктивного типа, направленные на расширение и

углубление сведений по изучаемой теме, на выявление недостаточно освещенных вопросов, слабых мест в аргументации и т.п.
Подготовка к практическим занятиям ведется на основе планов практических занятий, которые размещены на сайте филиала. В ходе подготовки к практическим занятиям необходимо изучить в соответствии с вопросами для повторения конспекты лекций, основную литературу, ознакомиться с дополнительной литературой. Кроме того, следует повторить материал лекций, ответить на контрольные вопросы, изучить образцы решения задач, выполнить упражнения (если такие предусмотрены).
При подготовке к промежуточной аттестации необходимо повторить пройденный материал в соответствии с учебной программой, примерным перечнем вопросов, выносящихся на экзамен. Рекомендуется использовать конспекты лекций и источники, перечисленные в списке литературы в рабочей программе дисциплины, а также ресурсы электронно-библиотечных систем. Необходимо обратить особое внимание на темы учебных занятий, пропущенных по разным причинам. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.
Для достижения планируемых результатов обучения используются интерактивные лекции, анализ имитационных моделей.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учебное пособие для студентов вузов.- 3-е изд., стер.- М.: Академия, 2007

б) дополнительная литература:

№ п/п	Источник
2	Башлы П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. - М.: Евразийский открытый институт, 2011. - 375 с. - ISBN 978-5-374-00301-7 ; [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=90539 (04.04.2022).
3	Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов. - М.; Берлин : Директ-Медиа, 2015. - 253 с.: ил. - Библиогр. в кн. - ISBN 978-5-4475-3946-7; [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=276557 (04.04.2022).

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет):

№ п/п	Источник
4	Артемов А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем.; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605 (04.04.2022).
5	Гатчин Ю.А., Сухостат В.В. Теория информационной безопасности и методология защиты информации. - СПб.: СПбГУ ИТМО, 2010. - 98 с. [Электронный ресурс]. – URL: http://window.edu.ru/resource/984/71984 (04.04.2022).

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная Академия безопасности и выживания. - Орел : МАБИВ, 2014. - 257 с. : табл., схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=428605 (04.04.2022)
2	Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331 (04.04.2022).

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины используются вводная лекция, обзорные лекции по разделу «Численное интегрирование»; лабораторные работы.

18. Материально-техническое обеспечение дисциплины:
Программное обеспечение:
- Win10, OfficeProPlus 2010
- браузеры: Yandex, Google, Opera, Mozilla Firefox, Explorer
- STDU Viewer version 1.6.2.0
- 7-Zip

Мультимедийное оборудование (проектор, ноутбук или стационарный компьютер, экран), компьютерный класс (компьютеры, объединенные в сеть с выходом в Интернет и обеспечением доступа в электронную информационно-образовательную среду ВГУ и БФ).

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Угрозы информационной безопасности	ОПК-9 ПК-3	ОПК-9.1 ОПК-9.2 ПК-3.1 ПК-3.2	Тест Доклад
2	Информационные системы и их компоненты как объекты защиты	ОПК-9 ПК-3	ОПК-9.1 ОПК-9.2 ПК-3.1 ПК-3.2	Тест Доклад
3	Направления разработки и применения средств защиты информации	ОПК-9 ПК-3	ОПК-9.1 ОПК-9.2 ПК-3.1 ПК-3.2	Тест Доклад
4	Организационно-правовые меры и средства защиты информации	ОПК-9 ПК-3	ОПК-9.1 ОПК-9.2 ПК-3.1 ПК-3.2	Тест Доклад
5	Технические и программные средства защиты информации	ОПК-9 ПК-3	ОПК-9.1 ОПК-9.2 ПК-3.1 ПК-3.2	Тест Доклад Контрольная работа
6	Криптографические методы защиты информации	ОПК-9 ПК-3	ОПК-9.1 ОПК-9.2 ПК-3.1 ПК-3.2	Тест Доклад
Промежуточная аттестация форма контроля – зачет с оценкой				Перечень вопросов к зачету с оценкой

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Тематика практических занятий

Правовые акты, регулирующие законодательство в области защиты информации.
Настройка безопасности операционной системы.
Настройка безопасности приложений.
Настройка безопасности браузеров.
Антивирусное программное обеспечение.
Шифрование методом замены.
Шифрование методом перестановки.
Поточное шифрование.
Алгоритм RSA.
Электронная цифровая подпись.

Перечень докладов

1. Компьютерные вирусы.
2. Классификация компьютерных вирусов по среде обитания.
3. Классификация компьютерных вирусов по заражаемой операционной системе.
4. Классификация компьютерных вирусов по деструктивным возможностям.
5. Классификация компьютерных вирусов по особенностям алгоритма работы.
6. Вредоносные программы.
7. Троянские программы.
8. Mail Senders.
9. Back Door.
10. Log Writers.
11. Trojan-Dropper.
12. RootKit.
13. Снифферы.
14. Dos, DDos-атаки.
15. Фатальные сетевые атаки.
16. Взломщики удаленных компьютеров.
17. Flooder.
18. Конструкторы вирусов и троянских программ.
19. FileCryptor, PolyCryptor.
20. Полиморфные генераторы.
21. Антивирусные программы.
22. Сканеры.
23. Ревизоры.
24. Блокировщики.
25. Иммунизаторы.

Критерии оценки:

- оценка **«зачтено»** выставляется студенту, если студент раскрывает тему доклада, хорошо ориентируется в рассматриваемом вопросе;
- оценка **«не зачтено»** выставляется студенту, если студент не раскрывает тему доклада, плохо ориентируется в рассматриваемом вопросе.

Тестовые задания

1. Информационная безопасность характеризует защищённость:

А) Пользователя и информационной системы
Б) Информации и поддерживающей её инфраструктуры
В) Источника информации
Г) Носителя информации

2. Что из перечисленного является составляющей информационной безопасности?

А) Нарушение целостности информации
Б) Проверка прав доступа к информации
В) Доступность информации
Г) Выявление нарушителей

3. Получение требуемой информации информационной услуги пользователем за определённое время, это:
А) Целостность информации
Б) Конфиденциальность информации
В) Доступность информации
Г) Защищенность информации
4. Конфиденциальность информации гарантирует:
А) Доступность информации кругу лиц, для кого она предназначена
Б) Защищённость информации от потери
В) Защищённость информации от фальсификации
Г) Доступность информации только автору
5. Сколько уровней формирования режима информационной безопасности?
А) Три
Б) Четыре
В) Два
Г) Пять
6.Год издания закона Российской Федерации «О государственной тайне»:
А) 2000 год
Б) 1993 год
В) 1995 год
Г) 1996 год
7. Номер статьи Уголовного кодекса предусматривающей наказание за разглашение государственной тайны?
А) 138
Б) 283
В) 273
Г) 237
8. Неправомерный доступ к компьютерной информации наказывается лишением свободы
А) До пяти лет
Б) До трех лет
В) До года
Г) До двух лет
9. Основной источник внутренних отказов?
А) Невозможность пользователя работать с системой в силу отсутствия соответствующей подготовки
Б) Нежелание пользователя работать с информационной системой
В) Отступление от установленных правил эксплуатации
Г) Нарушение работы систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования
10. Уровни не относящиеся к уровням формирования режима информационной безопасности?
А) Законодательно-правовой
Б) Информационный
В) Административный (организационный)
Г) Программно-технический
11. На сколько классов подразделяют угрозы информационной безопасности?
А) 4
Б) 3
В) 2
Г) 5
12. Что является самым эффективным при борьбе с непреднамеренными случайными ошибками?
А) Резервирование аппаратуры
Б) Определение степени ответственности за ошибки
В) Максимальная автоматизация и строгий контроль
Г) Контроль действий пользователя
13. Средства защиты информации какого из уровней формирования режима информационной безопасности связаны непосредственно с защищаемой информацией
А) Законодательно-правовой

Б) Информационный
В) Административный (организационный)
Г) Программно-технический
14. Основополагающим документом по информационной безопасности в РФ является:
А) Конституция РФ
Б) Уголовный кодекс
В) Закон о средствах массовой информации
Г) Закон об информационной безопасности
15. Целостность информации гарантирует:
А) Существование информации в исходном виде
Б) Принадлежность информации автору
В) Доступ информации определенному кругу пользователей
Г) Защищенность информации от несанкционированного доступа
16. Сколько категорий государственных информационных ресурсов определяет закон «Об информации, информатизации и защите информации»?
А) Три
Б) Четыре
В) Два
Г) Пять
17. Неправомерный доступ к компьютерной информации наказывается штрафом:
А) От 5 до 20 минимальных размеров оплаты труда
Б) От 200 до 500 минимальных размеров оплаты труда
В) От 150 до 200 минимальных размеров оплаты труда
Г) До 300 минимальных размеров оплаты труда
18. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети наказывается ограничением свободы на срок:
А) До года
Б) До двух лет
В) До пяти лет
Г) До трех месяцев
19. Защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации – это:
А) Компьютерная безопасность
Б) Информационная безопасность
В) Защита информации
Г) Защита государственной тайны
20. Что из перечисленного является задачей информационной безопасности?
А) Устранение неисправностей аппаратных средств
Б) Устранение последствий стихийных бедствий
В) Защита технических и программных средств информатизации от ошибочных действий персонала
Г) Восстановление линий связи
21. Выберите правильную иерархию пространства требований в «Общих критериях»:
А) Класс – семейство – компонент – элемент
Б) Элемент – класс – семейство – компонент
В) Компонент – семейство – класс – элемент
Г) Семейство – компонент – класс – элемент
22. Сколько классов СВТ по уровню защищенности от НСД к информации определено в руководящем документе Гостехкомиссии «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»?
А) Три
Б) Семь
В) Пять
Г) Четыре
23. Комплекс предупредительных мер по обеспечению информационной безопасности организации – это:
А) Информационная политика

Б) Политика безопасности
В) Информационная безопасность
Г) Защита информации
24. Аутентичность связана:
А) С доказательством авторства документа
Б) С проверкой прав доступа
В) С изменением авторства документа
Г) С контролем целостности данных
25. Что не рассматривается в политике безопасности?
А) Требуемый уровень защиты данных
Б) Роли субъектов информационных отношений
В) Анализ рисков
Г) Защищенность механизмов безопасности
26. Исполняемый или интерпретируемый программный код, обладающий свойством несанкционированного распространения и самовоспроизведения в автоматизированных системах или коммуникационных сетях с целью изменить или уничтожить программное обеспечение и /или данные, хранящиеся в автоматизированных системах – это:
А) Троянская программа
Б) Компьютерный вирус
В) Программный вирус
Г) Вирус
27. Какие вирусы заражают файлы-документы и электронные таблицы офисных приложений?
А) Файловый вирус
Б) Сетевой вирус
В) Макро-вирус
Г) Загрузочный вирус
28. Основная особенность компьютерных вирусов заключается:
А) В возможности их самопроизвольного внедрения в различные объекты операционной системы
Б) В возможности нарушения информационной безопасности
В) В возможности заражения окружающих
Г) В их постоянном существовании
29. Первый сетевой вирус появился:
А) В начале 60-х гг.
Б) В начале 80-х гг.
В) В начале 70-х гг.
Г) В середине 60-х гг.
30. По особенностям алгоритма работы вируса бывают
А) Резидентные и стелс-вирусы
Б) Полиморфик-генераторы и загрузочные вирусы
В) Макро-вирусы и логические бомбы
Г) Утилиты скрытого администрирования
31. «Маски» вирусов используются:
А) Для поиска известных вирусов
Б) Для создания известных вирусов
В) Для уничтожения известных вирусов
Г) Для размножения вирусов
32. Какой вирус самостоятельно выходил в сеть через модем и сохранял свою копию на удаленной машине?
А) Elk Kloner
Б) Pervading Animal
В) Creeper
Г) Brain
33. Евгений Касперский переориентировался на создание антивирусных программ после обнаружения на своем компьютере вируса:
А) Chameleon
Б) Cascade
В) Eddie
Г) Virdem

34. Первый вирус, противодействовавший антивирусному программному обеспечению:
А) Eddie
Б) DiskKiller
В) Dir_II
Г) Virdem
35. Первый макровирус, поражавший документы MSWord:
А) GreenStripe
Б) Wazzu
В) Concept
Г) DiskKiller
36. Первый полиморфный вирус:
А) DiskKiller
Б) Chameleon
В) MtE
Г) Brain
37. Вирус 1987 года, заражающий только системные файлы Command.com, и уничтожающий всю информацию на текущем диске, - это:
А) Suriv
Б) Jerusalem
В) Lehigh
Г) MtE
38. $189 – такую сумму предлагалось прислать тем пользователям, чей компьютер был заражен вирусом…
А) Aids Information Diskette
Б) Cascade
В) Eddie
Г) MtE
39. Первый сетевой вирус-червь, использующий протокол передачи данных FTP (1997 г.)
А) Homer
Б) ShareFar
В) BackOrifice
Г) Червь Морриса
40. Достаточно труднообнаружимые вирусы, не имеющие сигнатур, то есть не содержащие ни одного постоянного участка кода – это:
А) Полиморфик-вирусы
Б) Стелс-вирусы
В) Макро-вирусы
Г) Конструкторы вирусов
41. Угроза перехвата данных может привести:
А) К нарушению доступности данных
Б) К нарушению доступности и целостности данных
В) К нарушению целостности данных
Г) К нарушению конфиденциальности данных
42. Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным – это:
А) Аутентификация
Б) Идентификация
В) Аутентичность
Г) Конфиденциальность
43. Черви, использующие для распространения системы мгновенного обмена сообщениями:
А) IM-черви
Б) P2P-черви
В) Почтовые черви
Г) IRC-черви
44. Что из перечисленного не является идентификатором при аутентификации?
А) Пароль
Б) Особенности поведения пользователя
В) Персональный идентификатор

Г) Секретный ключ
45. Постоянные пароли относятся к:
А) Статической аутентификации
Б) Временной аутентификации
В) Устойчивой аутентификации
Г) Постоянной аутентификации
46. Относительно небольшое количество дополнительной аутентифицирующей информации, передаваемой вместе с подписываемым текстом – это:
А) Закрытый ключ шифрования
Б) Вирусная маска
В) Электронная цифровая подпись
Г) Открытый ключ шифрования
47. Какое управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах, и официального разрешения субъекта к информации соответствующего уровня конфиденциальности?
А) Мандатное управление доступом
Б) Принудительное управление доступом
В) Дискретное управление доступом
Г) Статистическое управление доступом
48. Резидентные программы, перехватывающие вирусоопасные ситуации и сообщающие об этом пользователю, это:
А) Иммунизаторы
Б) Блокировщики
В) Сканеры
Г) CRC-сканеры
49. Технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов, это:
А) Эвристический анализ
Б) Поведенческий анализ
В) Анализ контрольных сумм
Г) Поиск вирусов по запросу пользователя
50. Какое управление доступом основано на сопоставлении меток конфиденциальности информации, содержащейся в объектах, и официального разрешения субъекта к информации соответствующего уровня конфиденциальности?
А) Мандатное управление доступом
Б) Принудительное управление доступом
В) Дискретное управление доступом
Г) Статистическое управление доступом

Критерии оценки:
- оценка **«отлично»** выставляется студенту, если правильно выполнено более 90% заданий;
- оценка **«хорошо»** выставляется студенту, если правильно выполнено более 70% заданий;
- оценка **«удовлетворительно»** выставляется студенту, если правильно выполнено более 50% заданий;
- оценка **«неудовлетворительно»** выставляется студенту, если правильно выполнено менее 50% заданий.

Контрольная работа
1. Подготовьте инструкцию пользователя по установке программы-антивируса. Кратко опишите возможности программы.
2. Подготовьте инструкцию пользователя по настройке программы антивируса.
3. Подготовьте инструкцию пользователя по использованию программы антивируса.

Описание технологии проведения контрольной работы

Контрольная работа выполняется в электронном виде по вариантам после изучения соответствующего теоретического материала.
Критерии оценки

Оценка **«отлично»** выставляется, если все задания выполнены аккуратно и в полном объеме, студент в полной мере владеет теоретическим материалом.
Оценка **«хорошо»** выставляется, если задания выполнены в полном объеме, но имеются погрешности в оформлении, студент владеет теоретическим материалом и допускает неточности.
Оценка **«удовлетворительно»** выставляется, если задания выполнено не менее 2 заданий или имеются серьезные погрешности в оформлении, студент в основном владеет теоретическим материалом.
Оценка **«неудовлетворительно»** выставляется, если задания выполнено менее 2 заданий или работа не оформлена надлежащим образом, студент не владеет теоретическим материалом.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Собеседование по вопросам к экзамену.

1. Понятие «Информационная безопасность». Основные компоненты информационной безопасности. Важность и комплексность проблемы информационной безопасности.
2. Понятие информационной угрозы. Классификация видов угроз информационной безопасности по различным признакам Примеры реализации угроз информационной безопасности.
3. Защита информации. Основные принципы обеспечения информационной безопасности в автоматизированных системах. Причины, виды и каналы утечки информации
4. Особенности современных информационных систем, факторы, влияющие на безопасность информационной системы. Виды сервисов безопасности.
5. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
6. Организационно-правовые меры и средства защиты информации
7. Технические и программные средства защиты информации
8. Понятие «вредоносное программное обеспечение». Основная классификация вредоносного программного обеспечения согласно лаборатории Касперского.
9. Понятие компьютерный вирус. Основные механизмы развития и распространения.
10. Антивирусное обеспечение. Основные компоненты антивирусной программы.
11. Технические средства контроля доступа к компонентам информационных систем
12. Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.
13. Методы и средства уничтожения информации
14. Краткая история криптографии.
15. Основные понятия криптографии.
16. Симметричные криптосистемы. Перестановки. Метод Цезаря.
17. Симметричные криптосистемы. Перестановки. Метод Ришелье.
18. Метод моноалфавитной подстановки. Шифр Цезаря с использованием слова впереди алфавита.
19. Метод полиалфавитной подстановки. Шифр Вигнера.
20. Механические криптосистемы.
21. Асимметричные криптосистемы (с публичным ключом). Основные понятия. Необратимые функции.
22. Реализация асимметричной криптосистемы на основе задачи рюкзака. Секретная информация для криптосистем с публичным ключом.
23. Принципы построения криптосистемы с публичным ключом.
24. Электронная подпись. Общие понятия.
25. Электронные платежные системы. Основные свойства. Безопасность электронных платежей.

Для оценивания результатов обучения на экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».
Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности	Шкала оценок

	компетенций	
Обучающийся в полной мере владеет теоретическими основами дисциплины, способен иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач в области численных методов и исследования операций, способен сформулировать и доказать собственную точку зрения, демонстрирует готовность полное освоение показателей формируемых компетенций;	*Повышенный уровень*	*Отлично*
Обучающийся владеет понятийным аппаратом теоретическими основами дисциплины, имеет представление об основных подходах к излагаемому материалу, в основном демонстрирует готовность применять теоретические знания в практической деятельности и освоение большинства показателей формируемых компетенций;	*Базовый уровень*	*Хорошо*
Обучающийся частично владеет теоретическими основами дисциплины, фрагментарно способен применять теоретические знания в практической деятельности и демонстрирует освоение некоторых показателей формируемых компетенций;	*Пороговый уровень*	*Удовлетворительно*
Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки, не ориентируется в теоретическом материале, не демонстрирует готовность применять теоретические знания в практической деятельности и освоение показателей формируемых компетенций.	–	*Неудовлетворительно*