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

01.09.2018 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.22. Информационная безопасность

1. Шифр 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: естественнонаучных и общеобразовательных дисциплин

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

7. Рекомендована: научно-методическим советом Филиала (протокол № 1 от 31.08.2018 г.)

8. Семестр: 8

9.**Цели и задачи учебной дисциплины:**

Целью 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 СЗИ 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» входит в блок Б1 «Дисциплины (модули)» и является дисциплиной вариативной части образовательной программы. Для изучения дисциплины требуется освоение курса «Информатика». Дисциплина является предшествующей для курсов « Методика обучения информатике», «Информационные системы».

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 выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-3	способность решать задачи воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности	**знает:** – задачи воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности на соответствующих ступенях общего образования; **умеет:** применять теоретические знания для решения практических задач воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности (*в том числе, знание основных понятий теории информационной безопасности и направлений разработки и применения средств защиты информации*); **владеет:** – навыками постановки цели, формулировки задач и прогнозирования духовно-нравственного развития и воспитания личности обучающегося (воспитанника) (*в том числе, способами осуществления выбора различных мер и средств обеспечения информационной безопасности в учебном процессе с учетом реального оснащения образовательного учреждения*);
ПК-6	готовность к взаимодействию с участниками образовательного процесса	**знает:** – основы и закономерности взаимодействия участников образовательного процесса; **умеет:** – осуществлять взаимодействие с участниками образовательного процесса для решения профессиональных задач;

		владеет: – навыками и технологиями эффективного взаимодействия с участниками образовательного процесса (*в том числе, с учётом обеспечения информационной безопасности на различных уровнях*)

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

Форма промежуточной аттестации зачет с оценкой.

13. Виды учебной работы

Очная форма обучения

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		8 сем.
Контактная работа, в том числе:	48	38
лекции	16	14
практические занятия	16	12
лабораторные работы	16	12
Самостоятельная работа	24	34
Форма промежуточной аттестации *(зачет с оценкой – 0 час.)*	0	0
Итого:	72	72

Заочная форма обучения

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		8 сем.
Контактная работа, в том числе:	12	12
лекции	4	4
практические занятия	4	4
лабораторные работы	4	4
Самостоятельная работа	56	56
Форма промежуточной аттестации *(зачет с оценкой – 4 час.)*	4	4
Итого:	72	72

13.1. Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
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	Общее представление о структуре защищенной информационной системы. Особенности современных

	защиты	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	Методика построения защищенных информационных систем	Использование защищенных компьютерных систем. Общие принципы построения защищенных систем. Иерархический метод разработки защищенных систем. Структурный принцип. Принцип модульного программирования. Исследование корректности реализации и верификации автоматизированных систем. Спецификация требований предъявляемых к системе. Основные этапы разработки защищенной системы: определение политики безопасности, проектирование модели ИС, разработка кода ИС, обеспечение гарантий соответствия реализации заданной политике безопасности.
1.5	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.
1.6	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.
1.7	Технические средства контроля доступа к компонентам информационных систем	Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.
1.8	Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.	Основные варианты организации защиты ЭП Расчет мощности UPS Устройства бесперебойного электропитания Управление UPS.
1.9	Методы и средства уничтожения информации	Особенности хранения компьютерной информации на физических носителях.
2. Практические занятия		
2.5	Организационно-правовые меры и средства защиты информации	Концепция информационной безопасности. Информационная безопасность образовательной организации.
2.6	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.
2.7	Технические средства контроля доступа к компонентам информационных систем	Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.

2.8	Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.	Требования к защите электропитания различных компонентов КС. Выбор политики защиты электропитания КС Выборочная защита. Частичная защита. Полная защита
2.9	Методы и средства уничтожения информации	Способы уничтожения информации без разрушения носителя: программные и физические. Способы уничтожения информации с разрушением носителя: механические, термические, химические радиационные.
2.10	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.
3. Лабораторные работы		
3.10	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.

13.2. Темы (разделы) дисциплины и виды занятий

Очная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1.	Угрозы информационной безопасности	1			4	5
2.	Информационные системы и их компоненты как объекты защиты	1			4	5
3.	Направления разработки и применения средств защиты информации	2			4	6
4.	Методика построения защищенных информационных систем	2			4	6
5.	Организационно-правовые меры и средства защиты информации	2	2		4	8
6.	Технические и программные средства защиты информации	2	2		2	6
7.	Технические средства контроля доступа к компонентам информационных систем	2	2		2	6
8.	Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.	1	2		2	5
9.	Методы и средства уничтожения информации	1	2		2	5
10.	Криптографические методы		2	12	6	20

	защиты информации					
11.	Зачет с оценкой					0
	Итого:	14	12	12	34	72

Заочная форма обучения

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1.	Угрозы информационной безопасности	1			4	5
2.	Информационные системы и их компоненты как объекты защиты	1			4	5
3.	Направления разработки и применения средств защиты информации	1			4	5
4.	Методика построения защищенных информационных систем	1			4	5
5.	Организационно-правовые меры и средства защиты информации		1		4	5
6.	Технические и программные средства защиты информации		1		4	5
7.	Технические средства контроля доступа к компонентам информационных систем		1		4	5
8.	Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем.		1		4	5
9.	Методы и средства уничтожения информации				4	4
10.	Криптографические методы защиты информации			4	20	24
11.	Зачет с оценкой					4
	Итого:	4	4	4	56	72

14. Методические указания для обучающихся по освоению дисциплины

Приступая к изучению учебной дисциплины, целесообразно ознакомиться с учебной программой дисциплины, электронный вариант которой размещён на сайте БФ ВГУ.

Это позволит обучающимся получить четкое представление о:

−перечне и содержании компетенций, на формирование которых направлена дисциплина;

−основных целях и задачах дисциплины;

−планируемых результатах, представленных в виде знаний, умений и навыков, которые должны быть сформированы в процессе изучения дисциплины;

−количестве часов, предусмотренных учебным планом на изучение дисциплины, форму промежуточной аттестации;

−количестве часов, отведенных на контактную и на самостоятельную работу;

−формах контактной и самостоятельной работы;

−структуре дисциплины, основных разделах и темах;

−системе оценивания учебных достижений;

−учебно-методическом и информационном обеспечении дисциплины.

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

Основными формами контактной работы по дисциплине являются лекции, практические занятия и лабораторные работы, посещение которых обязательно для всех студентов (кроме студентов, обучающихся по индивидуальному плану).
В ходе подготовки к лабораторным работам необходимо изучить в соответствии с вопросами для повторения 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 зачет с оценкой. Рекомендуется использовать конспекты лекций и источники, перечисленные в списке литературы в рабочей программе дисциплины, а также ресурсы электронно-библиотечных систем.
Для достижения планируемых результатов обучения используются интерактивные лекции, групповые дискуссии, 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 (23.06.2018).
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 (23.06.2018).

в) информационные электронно-образовательные ресурсы:

№ 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 (23.06.2018).
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 (23.06.2018).

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 (23.06.2018)
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 (23.06.2018).

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение, информационно-справочные системы и профессиональные базы данных

–ОС Microsoft Windows 7;

–Lazarus.

При реализации дисциплины применяется смешанное обучение с использованием онлайн-консультаций; электронной почты, сайта кафедры естественнонаучных и общеобразовательных дисциплин: http://pmii.ru/pumk/uchebnyie-materialyi.

Информационная система «Единое окно доступа к образовательным ресурсам» http://window.edu.ru/;

–Электронно-библиотечная система «Университетская библиотека online» – http://biblioclub.ru/.

18. Материально-техническое обеспечение дисциплины:

Компьютеры, объединенные в сеть с выходом в Интернет и обеспечением доступа в электронную информационно-образовательную среду ВГУ и БФ, проектор, принтер, интерактивный экран, аудио гарнитура.

19. Фонд оценочных средств:

19.1. Перечень компетенций с указанием этапов формирования и планируемых результатов обучения

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-3 способность решать задачи воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности	Знать: – задачи воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности на соответствующих ступенях общего образования.	Угрозы информационной безопасности Направления разработки и применения средств защиты информации Технические и программные средства защиты информации	Доклад
	Уметь: – применять теоретические знания для решения практических задач воспитания и духовно-нравственного развития обучающихся в учебной и внеучебной деятельности (*в том числе, знание основных понятий теории информационной безопасности и направлений разработки и применения средств защиты информации*).	Технические и программные средства защиты информации Технические средства контроля доступа к компонентам информационных систем Криптографические методы защиты информации	Тест
	Владеет (имеет навыки): – навыками постановки цели, формулировки задач и прогнозирования духовно-нравственного развития и воспитания личности обучающегося (воспитанника) (*в том числе, способами осуществления выбора различных мер и средств обеспечения информационной безопасности в учебном процессе с*	Организационно-правовые меры и средства защиты информации Технические и программные средства защиты информации Средства обеспечения бесперебойного и безопасного электропитания	Тест

	учетом реального оснащения образовательного учреждения).	компьютерных систем.	
ПК-6 готовность к взаимодействию с участниками образовательного процесса	Знать: – основы и закономерности взаимодействия участников образовательного процесса.	Информационные системы и их компоненты как объекты защиты Организационно-правовые меры и средства защиты информации Технические и программные средства защиты информации Технические средства контроля доступа к компонентам информационных систем	Доклад
	Уметь: – осуществлять взаимодействие с участниками образовательного процесса для решения профессиональных задач.	Организационно-правовые меры и средства защиты информации Технические и программные средства защиты информации Технические средства контроля доступа к компонентам информационных систем Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем. Методы и средства уничтожения информации Криптографические методы защиты информации	Тест
	Владеет (имеет навыки): – навыками и технологиями эффективного взаимодействия с участниками образовательного процесса (*в том числе, с учётом обеспечения информационной безопасности на различных уровнях*).	Методика построения защищенных информационных систем Технические и программные средства защиты информации Технические средства контроля доступа к компонентам информационных систем Средства обеспечения бесперебойного и безопасного электропитания компьютерных систем. Методы и средства уничтожения информации Криптографические методы защиты информации	Методические указания к лабораторным работам

Промежуточная аттестация – зачёт с оценкой	Вопросы к зачету с оценкой

19.2 Описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на зачете с оценкой используются следующие показатели (ЗУНы из 19.1):
1) знание учебного материала и владение понятийным аппаратом дисциплины;
2) умение связывать теорию с практикой;
3) умение применять теоретические знания для решения практических задач в области информатизации образовательного процесса.
Для оценивания результатов обучения на зачете с оценкой используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся в полной мере владеет понятийным аппаратом дисциплины «Информационная безопасность», способен иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения типовых задач и практических заданий более высокого уровня сложности в области информационной безопасности.	*Повышенный уровень*	*Отлично*
Обучающийся владеет понятийным аппаратом дисциплины «Информационная безопасность», способен иллюстрировать ответ примерами, фактами, применять теоретические знания при решении типовых задач, допускает незначительные ошибки при решении практических заданий более высокого уровня сложности в области информационной безопасности.	*Базовый уровень*	*Хорошо*
Обучающийся владеет частично теоретическими основами дисциплины «Информационная безопасность», фрагментарно способен иллюстрировать ответ примерами, фактами, в ряде случаев затрудняется применять теоретические знания при решении типовых задач, не всегда способен решить практические задания более высокого уровня сложности в области информационной безопасности.	*Пороговый уровень*	*Удовлетвори-тельно*
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки при решении типовых расчётных задач либо не имеет представления о способе их решения.	–	*Неудовлетвори-тельно*

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

19.3.1 Перечень вопросов к зачету с оценкой:

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.

19.3.2 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.

19.3.3 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.

19.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущий контроль успеваемости проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущий контроль успеваемости проводится в формах*: фронтальных опросов, докладов, защиты лабораторных работ.* Критерии оценивания приведены выше.

Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Контрольно-измерительные материалы промежуточной аттестации включают в себя теоретические вопросы, позволяющие оценить уровень полученных знаний и практическое задание, позволяющее оценить степень сформированности умений и навыков.

При оценивании используются количественные шкалы оценок. Критерии оценивания приведены выше.