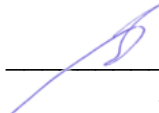


МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
БОРИСОГЛЕБСКИЙ ФИЛИАЛ
(БФ ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
естественнонаучных и
общеобразовательных дисциплин


С.Е. Зюзин
27.11.2019 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.Б.12 Информационная безопасность

1. Код и наименование направления подготовки:

38.03.10 Жилищное хозяйство и коммунальная инфраструктура

2. Профиль подготовки:

Управление жилищным фондом и многоквартирными домами

3. Квалификация выпускника: бакалавр

4. Форма обучения: заочная

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

6. Составитель программы: Хвостов Михаил Николаевич, кандидат физико-
математических наук

7. Рекомендована: научно-методическим советом Филиала (протокол № 3 от
25.11.2019 г.)

8. Учебный год: ЗФО 2022-2023 **Семестр:** 5

9. Цели и задачи учебной дисциплины:

Цель учебной дисциплины: формирование целостного представления о роли информационных технологий в современном обществе 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;
- выработать у студентов умения 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;
- сформировать у студентов представления об особенностях, тенденциях, проблемах и перспективах развития средств защиты информации.

10. Место учебной дисциплины в структуре образовательной программы:

Дисциплина «Информационная безопасность» входит в блок Б1 «Дисциплины (модули)» и относится к дисциплинам базовой части образовательной программы. Для освоения дисциплины «Информационная безопасность» необходимы знания, умения, навыки, сформированные в ходе изучения дисциплины «Информатика и информационные технологии».

Изучение дисциплины «Информационная безопасность» является необходимой основой для прохождения преддипломной практики и последующей профессиональной деятельности выпускника.

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	
ОК-12	способность понимать сущность и значение информации в развитии современного информационного общества, осознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны	знает (имеет представление): - об основных опасностях и угрозах, характерных для развитого информационного общества; - основные требования информационной безопасности, в том числе защиты государственной тайны; умеет: - использовать современные компьютерные технологии для обеспечения информационной безопасности, в том числе защиты государственной тайны в профессиональной деятельности; владеет: - основными способами ориентирования в современном информационном пространстве;
ОК-13	способность пользоваться основными методами, способами и средствами получения, хранения, переработки информации, владением навыками работы с компьютером как	знает: - основные способы и средства получения, хранения, переработки информации; умеет: - использовать современные компьютерные технологии (включая пакеты прикладных программ, локальные и глобальные компьютерные сети) как средство управления

средством управления информацией, способностью работать с информацией в глобальных компьютерных сетях	информацией; - использовать современные компьютерные технологии для организации научно-практической деятельности в профессиональной сфере; владеет: - навыками работы с информацией в глобальных компьютерных сетях.
---	---

12. Объем дисциплины в зачетных единицах/час. — 4 / 144 ч.

Формы промежуточной аттестации: экзамен, курсовая работа

13. Виды учебной работы

Вид учебной работы	Трудоемкость (часы)	
	Всего	По семестрам
		5 сем
Контактные часы, в том числе:	20	20
лекции	10	10
практические	10	10
Самостоятельная работа, в том числе:	115	115
курсовая работа	36	36
Форма промежуточной аттестации – экзамен, курсовая работа	9	9
Итого:	144	144

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 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. Системные принципы информационной безопасности. Выработка политики безопасности. Направления применения методов и средств защиты информации.
1.3	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.
1.4	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.
1.5	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.
2. Практические занятия		
2.3	Организационно-правовые меры и средства защиты информации	Концепция информационной безопасности. Информационная безопасность организации.
2.4	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.
2.5	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

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
5 семестр						
1	Угрозы информационной безопасности	2	0	0	15	17
2	Информационные системы и их компоненты как объекты защиты	2	0	0	16	18
3	Организационно-правовые меры и средства защиты	2	2	0	16	20

	информации					
4	Технические и программные средства защиты информации	2	4	0	16	22
5	Криптографические методы защиты информации	2	4	0	16	22
	Курсовая работа				36	36
	Экзамен					9
	Итого:	10	10	0	115	144

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.

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 и практические занятия.

Подготовка к практическим занятиям ведется на основе их планов. В ходе подготовки к практическим занятиям необходимо изучить основную литературу, ознакомиться с дополнительной литературой. Кроме того, следует изучить образцы выполнения задач и упражнений (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/экзамен. Рекомендуется использовать источники, перечисленные в списке литературы в рабочей программе дисциплины, а также ресурсы электронно-библиотечных систем.

По дисциплине предусмотрено выполнение курсовой работы. Примерные темы курсовых работ представлены в рабочей программе дисциплины. Методические указания к выполнению курсовой работы и требования к её оформлению содержатся в методических материалах к основной образовательной программе и размещаются на сайте Филиала в разделе Образование.

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

а) основная литература:

№ п/п	Источник
1	Башлы, П.Н. Информационная безопасность : учебно-практическое пособие / П.Н. Башлы, Е.К. Баранова, А.В. Бабаш. – Москва : Евразийский открытый институт, 2011. – 375 с. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=90539 (дата обращения: 24.10.2019). – ISBN 978-5-374-00301-7. – Текст : электронный.
2	Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. – Москва ; Берлин : Директ-Медиа, 2015. – 253 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=276557 (дата обращения: 24.10.2019). – Библиогр. в кн. – ISBN 978-5-4475-3946-7. – DOI 10.23681/276557. – Текст : электронный.

б) дополнительная литература:

№ п/п	Источник
-------	----------

3	Хорев П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пос. / П.Б. Хорев. – 3-е изд, стер. – М. : Академия, 2007. – 256 с.
---	---

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. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=428605 (дата обращения: 24.10.2019). – Текст : электронный.
5	Шилов, А.К. Управление информационной безопасностью: учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный университет», Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. – 121 с. : ил. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=500065 (дата обращения: 22.10.2019). – Библиогр.: с. 81-82. – ISBN 978-5-9275-2742-7. – Текст : электронный.
6	Электронно-библиотечная система «Университетская библиотека online» – http://biblioclub.ru/ .
7	ООО «Политехресурс» Электронная библиотека технического вуза (ЭБС «Консультант студента») – http://www.studentlibrary.ru/ .
8	Научная электронная библиотека – http://www.scholar.ru/ .

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. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=428605 (дата обращения: 24.10.2019). – Текст : электронный.
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. – Режим доступа: по подписке. – URL: http://biblioclub.ru/index.php?page=book&id=438331 (дата обращения: 24.10.2019). – Библиогр. в кн. – ISBN 978-5-9585-0603-3. – Текст : электронный.

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

Программное обеспечение:

- Win10 (или Win7), OfficeProPlus 2010
- браузеры: Yandex, Google, Opera, Mozilla Firefox, Explorer
- STDU Viewer version 1.6.2.0
- 7-Zip
- GIMP GNU Image Manipulation Program
- Paint.NET
- Tux Paint
- Adobe Flash Player

Информационно-справочные системы:

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

- Государственная информационная система ЖКХ (ГИС ЖКХ) <https://www.dom.gosuslugi.ru>
- Онлайн-версия КонсультантПлюс: Студент.

Профессиональные базы данных:

Федеральные сайты по вопросам ЖКХ

- Портал государственных услуг Российской Федерации (Госуслуги) www.gosuslugi.ru/category/property
- Ассоциация ТСЖ и ЖСК. Сайт Ассоциации некоммерческих организаций по содействию развития товариществ собственников жилья и жилищно-строительных кооперативов <http://tsg-rf.ru>

Региональные сайты по вопросам ЖКХ

- Департамент жилищно-коммунального хозяйства и энергетики Воронежской области <https://www.govrn.ru/organizacia/-/~id/844389>
- ЖКХ: управляющие компании и ТСЖ в Воронежской области <http://vsezhkh.ru/regions/voronezhskaya-oblast/>.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория для занятий лекционного и семинарского типов, групповых и индивидуальных консультаций, курсовых работ, текущего контроля и промежуточной аттестации.

Лаборатория информатики и информационно-коммуникационных технологий: компьютеры, объединенные в сеть с выходом в Интернет и обеспечением доступа в электронную информационно-образовательную среду ВГУ и БФ:

Интерактивная доска, проектор, колонки, принтер.

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)
ОК-12: способность понимать сущность и значение информации в развитии современного информационного общества, осознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе	знает (имеет представление): - об основных опасностях и угрозах, характерных для развитого информационного общества; - основные требования информационной безопасности, в том числе защиты государственной тайны;	Угрозы информационной безопасности. Информационные системы и их компоненты как объекты защиты. Организационно-правовые меры и средства защиты информации. Технические и программные средства защиты информации. Криптографические методы защиты информации.	Доклад
	умеет: - использовать современные компьютерные технологии для обеспечения информационной безопасности, в том числе защиты государственной тайны в профессиональной деятельности;		Тест, контрольная работа 1
	владеет: - основными способами ориентирования в современном информационном пространстве;		Тест

защиты государственной тайны			
ОК-13: способность пользоваться основными методами, способами и средствами получения, хранения, переработки информации, владением навыками работы с компьютером как средством управления информацией, способностью работать с информацией в глобальных компьютерных сетях	знает: - основные способы и средства получения, хранения, переработки информации;	Угрозы информационной безопасности. Информационные системы и их компоненты как объекты защиты. Организационно-правовые меры и средства защиты информации.	Доклад, контрольная работа
	умеет: - использовать современные компьютерные технологии (включая пакеты прикладных программ, локальные и глобальные компьютерные сети) как средство управления информацией; - использовать современные компьютерные технологии для организации научно-практической деятельности в профессиональной сфере;		Тест
	владеет: - навыками работы с информацией в глобальных компьютерных сетях.		Тест
Промежуточная аттестация – экзамен, курсовая работа			Вопросы к экзамену, тема курсовой работы

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 информационной безопасности.

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

Соотношение показателей, критериев и шкалы оценивания результатов обучения (экзамен и зачёт с оценкой).

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
<i>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.</i>	<i>Повышенный уровень</i>	<i>Отлично</i>
<i>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.</i>	<i>Базовый уровень</i>	<i>Хорошо</i>
<i>Обучающийся владеет частично теоретическими основами</i>	<i>Пороговый</i>	<i>Удовлетвори-</i>

<i>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.</i>	уровень	тельно
<i>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.</i>	–	Неудовлетворительно

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 Примерный перечень вопросов 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.

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) Защищённость 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:*
- A) Eddie
 - Б) DiskKiller
 - В) Dir_II
 - Г) Virdem
35. *Первый макровирус, поражавший документы MSWord:*
- A) GreenStripe
 - Б) Wazzu
 - В) Concept
 - Г) DiskKiller
36. *Первый полиморфный вирус:*
- A) 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:*
- A) Suriv
 - Б) Jerusalem
 - В) Lehigh
 - Г) MtE
38. *\$189 – такую сумму предлагалось прислать тем пользователям, чей компьютер был заражен вирусом...*
- A) Aids Information Diskette
 - Б) Cascade
 - В) Eddie
 - Г) MtE
39. *Первый сетевой вирус-червь, использующий протокол передачи данных FTP (1997 г.)*
- A) 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:*
- A) Полиморфик-вирусы
 - Б) Стелс-вирусы
 - В) Макро-вирусы
 - Г) Конструкторы вирусов
41. *Угроза перехвата данных может привести:*
- A) 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:*
- A) Аутентификация
 - Б) Идентификация
 - В) Аутентичность
 - Г) Конфиденциальность
43. *Черви, использующие для распространения системы мгновенного обмена сообщениями:*
- A) 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.

19.3.4 Задания для контрольных работ

Контрольная работа 1

Выполнить проверку ЭВМ и съемных носителей на наличие вирусов и вредоносных программ. Классифицировать найденные угрозы безопасности вычислительной системы. Рассмотреть актуальные угрозы безопасности информации. Составить план мероприятий по устранению причин возникновения угроз.

Контрольная работа 2

Задание 1. Зашифровать текст объемом не менее 1000 знаков одним из изученных способов.

Задание 2. Расшифровать предложенный текст.

Критерии оценки:

- 5 баллов выставляется студенту, если: показано умение применять полученные теоретические знания, глубокое и творческое овладение основной и дополнительной литературой; материал излагается аргументировано и логически стройно; показаны достаточно прочные практические навыки, умение теоретически обосновывать высказываемые положения, сделаны выводы;

- 4 балла выставляется студенту, если: показано умение применять полученные теоретические знания, овладение основной и дополнительной литературой; материал излагается аргументировано и логически стройно; показаны достаточно прочные практические навыки, умение теоретически обосновывать высказываемые положения сделаны выводы, но допущены незначительные ошибки или неточности;

- 3 балла выставляется студенту, если: мысли излагались недостаточно чётко и без должной логической последовательности; показаны недостаточные знания основной литературы и недостаточно прочные практические навыки; не сделаны выводы;

- 2 балла выставляется студенту, если мысли излагались недостаточно чётко и без должной логической последовательности; показаны недостаточные знания основной литературы, практические навыки не продемонстрированы, не сделаны выводы.

19.3.5 Примерные темы курсовых работ

1. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей.
2. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей.
3. Анализ методов и средств анализа защищенности беспроводных сетей.
4. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения.
5. Виброакустические средства современных систем обеспечения информационной безопасности.
6. Средства защиты от ПЭМИН, современное состояние, проблемы и решения.
7. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений.
8. Средства обеспечения информационной безопасности банков данных.
9. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса).
10. Анализ критических характеристик линий связи с точки зрения обеспечения защиты информации.
11. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота.
12. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа.
13. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации.
14. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела.
15. Инструментальные средства анализа рисков информационной безопасности.
16. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками.

17. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).
18. Разработка модели угроз безопасности информации коммерческой фирмы
19. Разработка модели угроз безопасности информации государственной организации.
20. Анализ рынка биометрических средств ввода пароля.

Критерии оценки:

Цель курсовой работы состоит в приобретении навыков самостоятельного решения практических проблем с научных позиций и письменного изложения полученных результатов. В процессе подготовки и написания курсовых работ, обучающиеся должны научиться проведению стандартного прикладного исследования в определённой области психологии.

По результатам защиты курсовой работы выставляется оценка: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется если:

- работа выполнена самостоятельно, носит творческий характер, возможно содержание элементов научной новизны;

- собран, обобщен и проанализирован достаточный объем литературных источников;

- при написании и защите работы студентом продемонстрирован высокий уровень развития общекультурных и профессиональных компетенций, теоретические знания и наличие практических навыков;

- работа хорошо оформлена и своевременно представлена на кафедру, полностью соответствует требованиям, предъявляемым к содержанию и оформлению курсовых работ;

- на защите освещены все вопросы исследования, ответы студента на вопросы профессионально грамотны, исчерпывающие, результаты исследования (если оно проводилось) подкреплены статистическими критериями;

Оценка «хорошо» ставится, если:

- тема работы раскрыта, однако выводы и рекомендации не всегда оригинальны и / или не имеют практической значимости, есть неточности при освещении отдельных вопросов темы;

- собран, обобщен и проанализирован необходимый объем психологической литературы, но не по всем аспектам исследуемой темы сделаны выводы и обоснованы практические рекомендации;

- при написании и защите работы студентом продемонстрирован средний уровень развития общекультурных и профессиональных компетенций, наличие теоретических знаний и достаточных практических навыков;

- работа своевременно представлена на кафедру, допускаются отдельные недостатки в ее оформлении;

- в процессе защиты работы были неполные ответы на вопросы.

Оценка «удовлетворительно» ставится, если:

- тема работы раскрыта частично, но в основном правильно, отдельные вопросы темы изложены поверхностно;

- в работе недостаточно полно была использована специальная литература, выводы и практические рекомендации не отражают в достаточной степени содержание работы;

- при написании и защите работы студентом продемонстрирован удовлетворительный уровень развития общекультурных и профессиональных компетенций, поверхностный уровень теоретических знаний и практических навыков;

- работа своевременно представлена на кафедру, однако не в полном объеме по содержанию и / или оформлению соответствует предъявляемым требованиям;

- в процессе защиты выпускник недостаточно полно изложил основные положения работы, испытывал затруднения при ответах на вопросы.

Оценка «неудовлетворительно» ставится, если:

– содержание работы не раскрывает тему, вопросы изложены бессистемно и поверхностно, нет анализа практического материала, основные положения и рекомендации не имеют обоснования;

– работа не оригинальна, основана на компиляции публикаций по теме;

– при написании и защите работы студентом продемонстрирован неудовлетворительный уровень развития общекультурных и профессиональных компетенций;

– работа несвоевременно представлена на кафедру, не в полном объеме по содержанию и оформлению соответствует предъявляемым требованиям или работа студентом не представлена;

– на защите студент дневного отделения показал поверхностные знания по исследуемой теме, отсутствие представлений об актуальных проблемах по теме работы, не всегда отвечал на вопросы.

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: *докладов, контрольных работ, тестирования*. 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.