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

УТВЕРЖДАЮ

Заведующий кафедрой
Информационных технологий
и математических методов в экономике

_____ И.Н. Щепина
18.04.2024

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.13 Основы информационной безопасности
Код и наименование дисциплины в соответствии с Учебным планом

1. Код и наименование направления подготовки / специальности:
51.03.06 Библиотечно-информационная деятельность

2. Профиль подготовки / специализация:
Библиотечно-информационное обеспечение социокультурной деятельности

3. Квалификация (степень) выпускника: *бакалавр*

4. Форма обучения: *очная*

5. Кафедра, отвечающая за реализацию дисциплины: кафедра
Информационных технологий и математических методов в экономике

6. Составители программы: *Шуршикова Галина Владимировна*
ФИО

К.т.н.	*доцент*
ученая степень	*ученое звание*

7. Рекомендована:
НМС экономического факультета ВГУ 21.03.2024 протокол № 3
(наименование рекомендующей структуры, дата, номер протокола)

8. Учебный год: *2025/2026* **Семестр(-ы): 4**

9. Цели и задачи учебной дисциплины: изучение основ информационной безопасности, особенностей функционирования и направлений совершенствования правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты информации в сферах охраны интеллектуальной собственности и сохранности их информационных ресурсов.

Задачи:

- овладение теоретическими, практическими и методическими вопросами обеспечения информационной безопасности;

- изучение системных комплексных методов защиты информации от различных видов объективных и субъективных угроз в процессе ее возникновения, обработки, использования и хранения.

10. Место учебной дисциплины в структуре ООП: дисциплина входит в обязательную часть блока дисциплин учебного плана. Для ее освоения необходимы знания, умения и компетенции, сформированные в результате изучения информационных технологий. Дисциплина связана с дисциплиной Стандарты библиотечно-информационной деятельности и профессиональная этика в части защиты персональных данных и конфиденциальной информации.

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	Коды	Индикатор(ы)	Планируемые результаты обучения
ОПК-3	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-3.1	Понимает возможности, предоставляемые современными информационно-коммуникационными технологиями для решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности; информационные процессы профессиональной деятельности; использует основы теории, нормативную базу, составляющие и пути формирования информационной и библиографической культуры	Знать: – основы и базовые требования информационной безопасности; – нормативные правовые акты в области защиты информации; Уметь: – работать с нормативными документами сферы защиты информации и информационной безопасности Владеть: – навыками разработки нормативных документов, регламентирующими защиту государственной и коммерческой тайны и иной служебной информации в организации;
		ОПК-3.2	Применяет информационно-коммуникационные технологии с учетом основных требований информационной безопасности; осуществляет самодиагностику уровня профессиональной информационной компетентности	Знать: – организационно-правовое обеспечение систем защиты информации Уметь: – применять технологии обеспечения информационной безопасности с целью предотвращения несанкционированного доступа, модификации или утраты информации, циркулирующей в информационных системах Владеть: – навыками работы с программными средствами обеспечения информационной безопасности в профессиональной деятельности
		ОПК-3.3	Использует методы повышения уровня информационной и библиографической культуры для решения задач профессиональной деятельности	Знать: – источники информации в сфере информационной безопасности Уметь: – анализировать опыт деятельности по обеспечению информационной безопасности Владеть: – навыками планирования мероприятий для повышения уровня информационной безопасности

12. Объем дисциплины в зачетных единицах/часах в соответствии с учебным планом — 3 / 108.

Форма промежуточной аттестации*(зачет/экзамен) - зачет*.

13. Трудоемкость по видам учебной работы

Вид учебной работы	Трудоемкость (часы)		
	Всего	По семестрам	
		№ сем. 4 сем.	Ч., в форме практической подготовки
Аудиторные занятия	*74*	74	0
в том числе: лекции	*14*	14	0
практические	60	60	0
лабораторные			
самостоятельная работа	*34*	34	0
форма промежуточной аттестации - зачет	*0*	0	
Итого:	*108*	108	0

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
	1. Лекции	
1.1	Информационная безопасность как составляющая общественной безопасности	Понятие безопасности. Доктрина информационной безопасности Российской Федерации. Безопасность в экономической сфере России. Международные договоры, доктрины в области информационной безопасности. Информационные права граждан.
1.2	Организационные основы защиты информации	Разработка и ведение перечня сведений, составляющих тайну. Состав сведений, которые не могут быть тайной. Назначение нормативно-методических материалов по регламентации системы защиты информации.
1.3	Инженерно-техническая защита информации	Физические средства защиты. Угрозы безопасности собственности фирмы и персоналу. Виды охраняемых объектов, категории защищаемых помещений. Виды, назначение, задачи и организационные формы охраны объектов, функции персонала охраны
1.4	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсе-

		тевые экраны как средство защиты от несанкционированного доступа.
2. Практические занятия		
3.1	Информационная безопасность как составляющая общественной безопасности	Информационные ресурсы в сфере информационной безопасности Определение угроз безопасности информации в информационных системах (по методике ФСТЭК России) Информационная безопасность как институт информационного права. Законодательство в области интеллектуальной собственности, информационных ресурсов, информационных продуктов и информационных услуг. Законодательство о безопасности и защите информации, его структура и содержание. Законодательство о защите государственной и коммерческой тайны, персональных данных, его структура и содержание. Основные задачи и уровни реализации информационной безопасности.
3.2	Организационные основы защиты информации	Методическое обеспечение защиты информации. Оценка возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя) Регламентация структуры и содержания комплексной системы защиты информации организации. Регламентация технологии защиты информации от потенциальных и реальных угроз. Регламентация технологии обработки, движения и хранения конфиденциальных документов на традиционных и технических носителях. Регламентация технологии работы персонала с документами, вычислительной и организационной техникой, средствами связи. Регламентация работы с персоналом. Регламентация системы охраны. Регламентация защиты информации в экстремальных ситуациях. Состав методических указаний, правил, памяток, схем и иных наглядных пособий.
3.3	Инженерно-техническая защита информации	Основные характеристики и сравнительный анализ программно-аппаратных комплексов обеспечения защиты информации. Классификация экстремальных (чрезвычайных) ситуаций. Аппаратные средства защиты.
3.4	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	Программно-технические методы обеспечения информационной безопасности. Парольная защита с помощью стандартных системных средств. Идентификация и аутентификация. Разграничение доступа. Протоколирование и аудит. Межсетевые экраны как средство защиты от несанкционированного доступа. Персональные и корпоративные межсетевые экраны. Критерии оценки защищённости систем информационной безопасно-

		сти. Основные виды компьютерных вирусов: загрузочные вирусы, вирусы в исполняемых компьютерных файлах, макро-вирусы, скрипт-вирусы, вирусы-мистификации. Профилактика вирусного заражения. Антивирусные программы. Сравнительный анализ антивирусных программ. Методика применения антивирусных программ. Криптографические средства защиты. Криптографическое преобразование данных. Симметричные и асимметричные методы шифрования. Общая технология шифрования. Технология шифрования речи.
3. Лабораторные работы – не предусмотрены		

13.2 Разделы дисциплины и виды занятий:

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)			
		Лекции	Практические занятия	Самостоятельная работа	Всего
1	Информационная безопасность как составляющая общественной безопасности	4	14	8	26
2	Организационные основы защиты информации	4	16	8	28
3	Инженерно-техническая защита информации	2	14	8	24
4	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	4	16	10	30
	Итого:	14	60	34	108

14. Методические указания для обучающихся по освоению дисциплины

В процессе изучения дисциплины используются такие виды учебной работы, как лекции, практические занятия, а также различные виды самостоятельной работы обучающихся.

Обучающимся рекомендуется вести конспект лекции, в котором должны быть ссылки на номера слайдов и демонстрационные примеры, основные определения и положения необходимо конспектировать, в конце лекции обучающиеся имеют возможность задать вопросы преподавателю по теме лекции. Презентации лекций и демонстрационный материал в виде файлов предоставляются обучающимся.

Для подготовки к практическому занятию обучающийся должен заранее ознакомиться с заданием и теоретическим материалом, после выполнения работы оформить отчет о проделанной работе. Все отчеты формируются в виде текстового файла и высылаются преподавателю для проверки.

При подготовке практическим занятиям работам особое внимание следует уделять особенностям использования изучаемых программных продуктов и грамотному оформлению полученных результатов.

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем и вопросов учебной дисциплины и является обязатель-

ной для каждого обучающегося, ее объем определяется учебным планом, обучающийся работает с рекомендованными материалами при минимальном участии преподавателя.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и ресурсами сети Internet, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Вопросы, которые вызывают у обучающихся затруднения при подготовке, должны быть заранее сформулированы и озвучены во время занятий в аудитории для дополнительного разъяснения преподавателем.

Виды самостоятельной работы: конспектирование учебной и научной литературы; проработка учебного материала (по конспектам лекций, учебной и научной литературе); работа в электронной библиотечной системе; работа с информационными справочными системами, выполнение домашних заданий; выполнение контрольных работ; подготовка к практическим занятиям; работа с вопросами для самопроверки.

15. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

№ п/п	Источник
1.	Ищейнов, В. Я. Информационная безопасность и защита информации : теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 10.03.2024). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
2.	Ерохин, В. В. Безопасность информационных систем : учебное пособие : [16+] / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко ; Брянский государственный университет им. акад. И. Г. Петровского. – 4-е изд., стер. – Москва : ФЛИНТА, 2022. – 184 с. : табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=562458 (дата обращения: 10.03.2024). – Библиогр. в кн. – ISBN 978-5-9765-1904-6. – Текст : электронный.
3.	Аверченков, В. И. Защита персональных данных в организации / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. – 4-е изд., стер. – Москва : ФЛИНТА, 2021. – 124 с. : табл., схем. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93260 (дата обращения: 10.03.2024). – Библиогр.: с. 107-109. – ISBN 978-5-9765-1273-3. – Текст : электронный.

б) дополнительная литература:

№ п/п	Источник
4.	**Петренко, В. И.** Защита персональных данных в информационных системах : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации ; Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет» .— Ставрополь : СКФУ, 2016 .— 201 с. : схем. — http://biblioclub.ru/ .— <URL:http://biblioclub.ru/index.php?page=book&id=459205>.
5.	Аудит информационной безопасности органов исполнительной власти : учебное пособие : [16+] / В. И. Аверченков, М. Ю. Рытов, А. В. Кувыклин, М. В. Рудановский. – 5-е изд., стер. – Москва : ФЛИНТА, 2021. – 100 с. : ил., схем.,

	табл. – (Организация и технология защиты информации). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=93259 (дата обращения: 10.03.2024). – Библиогр.: с. 83-84. – ISBN 978-5-9765-1277-1. – Текст : электронный.
6.	Журнал **Information Security. Информационная безопасность** -: http://www.itsec.ru/subscription.php#sthash.MLS78aeE.dpuf
7.	ГОСТ Р ИСО/МЭК 27002-2021 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности
8.	ГОСТ Р ИСО/МЭК 27001-2021 – Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1.	Зональная научная библиотека ВГУ https://www.lib.vsu.ru/
2.	Портал «Электронный университет ВГУ» – Moodle: URL: https://edu.vsu.ru/course/view.php?id=11717
3.	ЭБС Университетская библиотека online https://biblioclub.ru/
4.	Российская государственная библиотека. Единый электронный каталог http://www.rsl.ru/ru/s97/s977242/
5.	http://firewall.ru/law.htm - раздел сайта компании Infotecs. Сборник законодательных актов РФ, ведомственных нормативных документов.

16. Перечень учебно-методического обеспечения для самостоятельной работы *(учебно-методические рекомендации, пособия, задачники, методические указания по выполнению практических (контрольных) работ и др.)*

№ п/п	Источник
1.	http://www.gosecure.ru/ - сайт компании Gosecure Software Development.
2.	http://www.securit.ru/ - сайт компании SecurIT.
3.	http://www.abipage.ru/ - сайт компании «Агентство безопасности информации АБИ»

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

Программа дисциплины реализуется с применением элементов дистанционных образовательных технологий

Каждый обучающийся обеспечен индивидуальным неограниченным доступом к электронно-библиотечным системам (электронным библиотекам) и к электронной информационно-образовательной среде. Электронно-библиотечная система (электронная библиотека) и электронная информационно-образовательная среда обеспечивают возможность доступа обучающегося из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети «Интернет», как на территории ФГБОУ ВО «ВГУ», так и вне ее.

Информационно-справочные ресурсы

1. www.consultant.ru - официальный сайт ЗАО «Консультант Плюс».
2. www.garant.ru - официальный сайт ООО «НПП Гарант-Сервис».
3. www.kodeks.ru - официальный сайт информационно-правового консорциума «Кодекс».

18. Материально-техническое обеспечение дисциплины:
Используется Свободное программное обеспечение. Используются программные продукты, распространяемые по свободной лицензии или в режиме демодоступа. Учебный корпус факультета имеет: нужное количество лекционных аудиторий, оснащенных мультимедийным оборудованием, компьютерные классы, имеется необходимый комплект лицензионного программного обеспечения. Имеется в наличии в библиотечном фонде факультета достаточное количество учебников и учебно-методических пособий, перечисленных как в списке основной, так и в списке дополнительной литературы данной рабочей программы. Студенты имеют доступ к учебной литературе, представленной в ЭБС.

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.	Информационная безопасность как составляющая общественной безопасности	ОПК-3	ОПК-3.1 ОПК3-3	*Доклад*
2	Организационные основы защиты информации	ОПК-3	ОПК-3.1 ОПК-3.2	*Доклад* *Домашнее задание*
3	Инженерно-техническая защита информации	ОПК-3	ОПК3-2	*Доклад*
4	Программные средства защиты информации в компьютерах, локальных сетях и средствах связи	ОПК-3	ОПК3-2 ОПК-3.3	Доклад
Промежуточная аттестация форма контроля - зачет				*Перечень вопросов*

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: доклады и домашнее задание

Текущие аттестации проводятся в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета.

20.1.1 Перечень тем *докладов*

Описание технологии проведения

Цель - овладение навыками самостоятельной работы с нормативной документацией и навыками анализа задач обеспечения информационной безопасности. Доклад выполняется в виде текстового файла и сопровождается презентацией.

По разделу **Информационная безопасность как составляющая общественной безопасности**

1. Понятия национальной и информационной безопасности Российской Федерации в соответствии с «Доктриной информационной безопасности Российской Федерации» и «Концепцией национальной безопасности Российской Федерации».
2. Национальные интересы России в информационной сфере, сформулированные в «Концепции национальной безопасности Российской Федерации».
3. Задачи, обеспечивающие национальную безопасность РФ, в редакции «Концепции национальной безопасности Российской Федерации». Основные объекты безопасности, определенные в Федеральном законе «О безопасности» от 28 декабря 2010.
4. Внешние источники угроз информационной безопасности Российской Федерации, сформулированные в «Доктрине информационной безопасности Российской Федерации».
5. Внутренние источники угроз информационной безопасности Российской Федерации, сформулированные в «Доктрине информационной безопасности Российской Федерации».
6. Основные виды угроз информационной безопасности Российской Федерации, определенные в «Доктрине информационной безопасности Российской Федерации».
7. Основные права и свободы человека и гражданина в информационной сфере, гарантируемые Конституцией Российской Федерации.

По разделу Организационные основы защиты информации

1. Определение термина «государственная тайна». Классификация сведений, отнесенных к государственной тайне, определенным в законодательстве Российской Федерации.
2. Сведения конфиденциального характера, определенные в Указе Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера».
3. Сведения, не подлежащим отнесению к государственной тайне и засекречиванию.
4. Ограничения прав должностных лиц и граждан, допущенных к сведениям составляющим государственную тайну?
5. Стратегии защиты информации.
6. Политика информационной безопасности
7. Аудит информационной безопасности
8. Методическое обеспечение защиты информации.
1. Оценка возможностей нарушителя по реализации угроз безопасности информации (разработка модели нарушителя)
2. Регламентация технологии работы персонала с документами, вычислительной и организационной техникой, средствами связи.
3. Регламентация работы с персоналом.
4. Регламентация системы охраны.

По разделу Инженерно-техническая защита информации

1. Классификации средств защиты информации.
2. Мероприятия при создании механизмов защиты информации.
3. Первоочередные оборонительные мероприятия, которые необходимо провести для снижения уровня риска несанкционированного доступа.

4. Основные типы средств несанкционированного доступа.
5. Основные угрозы для сетей передачи данных.
6. Уязвимость информационной системы

По разделу Программные средства защиты информации в компьютерах, локальных сетях и средствах связи

1. Атака на информационную систему. Классификация атак.
2. Понятие криптографического протокола, примеры протоколов.
3. Назначение криптографических протоколов: обмена конфиденциальными сообщениями; формирования электронной подписи; распределения ключей.
4. Основные положения ФЗ-63 «Об электронной подписи»
5. Определение ЭП
6. Виды ЭП и примеры использования
7. Антивирусные средства защиты

Требования к выполнению заданий (шкалы и критерии оценивания):

Оценка обучающегося зависит от качества проведенного анализа, представленных рекомендаций и ответов на вопросы. Доклад в электронной форме. Оформление доклада должно соответствовать требованиям, предъявляемым к письменным работам. Титульный лист установленной формы. Шрифт Times New Roman, размер шрифта 14, абзацный отступ 1,5, межстрочный интервал 1,5. Размеры полей: левое 3 см, правое 1 см, верхнее и нижнее 2 см. Номер страницы проставляют внизу по центру. Там, где это необходимо, в качестве аналитического инструмента можно использовать графики, диаграммы и таблицы, которые должны быть оформлены в соответствии с требованиями ГОСТ.

Технологии проведения. Обучающийся готовит доклад с презентацией, выступает на занятии, отвечает на вопросы по теме доклада

Шкала оценивания – зачтено – не зачтено,

Критерии оценки:

Обучающиеся считаются освоившими пороговый уровень подготовки (оценка – зачтено), если ими раскрыта тема, даны грамотные и обоснованные ответы на дополнительные вопросы.

Оценка «не зачтено», если тема не раскрыта или обучающийся отказался от ответа.

2.1.2. Домашнее задание

Описание технологии проведения

Цель - овладение навыками самостоятельной работы. Обучающиеся готовят сообщения и презентацию, оформляют задание в виде текстового файла, выступают на занятии, отвечает на вопросы по теме

1. Разработка наглядных пособий по вопросам защиты информации
2. Разработка программы внутреннего аудита информационной безопасности.
3. Разработка и оформление перечня сведений, составляющих тайну
4. Разработка модели нарушителя

Требования к выполнению заданий (или шкалы и критерии оценивания)

Задание должно выполняться индивидуально. Оценка зависит от качества проведенного анализа, представленных результатов, рекомендаций и ответов на вопросы.

Шкала оценивания – зачтено – не зачтено,

Критерии оценки:

- оценка «зачтено» тема раскрыта в полном объеме и сделана презентация;
- оценка «не зачтено», если тема не раскрыта, задание не выполнено.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: собеседование по вопросам к зачету, проводится по КИМ, в составе КИМ 2 теоретических вопроса из списка

Перечень вопросов к зачету

1. Концепция и структура защиты информации.
2. Системный подход к защите информации
3. Система защиты информации. Основные требования и условия функционирования
4. Система защиты информации. Виды обеспечений.
5. Доктрина информационной безопасности РФ. Национальные интересы России в информационной сфере
6. Доктрина информационной безопасности РФ. Общие методы обеспечения информационной безопасности страны.
7. Компоненты модели информационной безопасности
8. Угрозы конфиденциальной информации. Классификация
9. Угрозы конфиденциальной информации. Разглашение
10. Угрозы конфиденциальной информации. Утечка
11. Угрозы конфиденциальной информации. Несанкционированный доступ.
12. Виды и характеристики угроз конфиденциальной информации
13. Типовые модели угроз безопасности персональных данных
14. Перечень персональных данных, подлежащих защите. Примеры формулировки целей обработки ПДн.
15. Методика определения актуальных угроз безопасности персональных данных (ПДн) при их обработке в информационных системах персональных данных (ИСПДн). Содержание и основные положения
16. Порядок определения актуальных угроз безопасности персональных данных в ИСПдн
17. Состав документационного обеспечения организации в области безопасности ПДн
18. Основные положения ФЗ РФ «О персональных данных» № 152-ФЗ
19. Виды классификаций ИСПДн. Порядок проведения классификации, содержание акта по результатам классификации ИСПДн
20. Действия, приводящие к неправомерному овладению конфиденциальной информацией
21. Условия, способствующие неправомерному овладению конфиденциальной информацией
22. Основные положения Доктрины информационной безопасности РФ
23. Характеристика угроз программно-математических воздействий. Основные виды вредоносных программ.
24. Классификация программных вирусов и сетевых червей
25. Основные направления защиты информации: правовая защита
26. Основные направления защиты информации: организационная защита
27. Основные направления защиты информации: инженерно-техническая защита
28. Способы защиты информации
29. Учет вопросов безопасности в должностных обязанностях и при найме персонала

30. Реагирование на инциденты нарушения информационной безопасности и сбои
31. Аутентификация, идентификация, авторизация: сущность, цель использования.
32. Аудит информационной безопасности: сущность, этапы и цели
33. Сбор исходных данных для проведения аудита
34. Методы расчёта рисков безопасности
35. Стандарты в области ИБ и защиты информации

20.2.1. В рамках промежуточной аттестации предусмотрен этап - Тестирование.

Примеры тестовых заданий. **Правильный ответ веделен**

Задания закрытого типа (примерные)

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- **Разработка и конкретизация правовых нормативных актов обеспечения безопасности**

2. Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
- **Перехват данных, хищение данных, изменение архитектуры системы**
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3. **Цели информационной безопасности – своевременное обнаружение, предупреждение:**

- **несанкционированного доступа, воздействия в сети**
- инсайдерства в организации
- чрезвычайных ситуаций

4. **Основные объекты информационной безопасности:**

- **Компьютерные сети, базы данных**
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

5. **Основными рисками информационной безопасности являются:**

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- **Потеря, искажение, утечка информации**

6. **К основным принципам обеспечения информационной безопасности относится:**

- **Экономической эффективности системы безопасности**
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

7. **Основными субъектами информационной безопасности являются:**
- руководители, менеджеры, администраторы компаний
- **органы права, государства, бизнеса**
- сетевые базы данных, файрволлы

8. **К основным функциям системы безопасности можно отнести все перечисленное:**
- **Установление регламента, аудит системы, выявление рисков**
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

9. Какие **угрозы** безопасности информации являются преднамеренными:
- а) ошибки персонала
- б) открытие электронного письма, содержащего вирус
- **в) не авторизованный доступ**

10. Какой **подход** к обеспечению безопасности имеет место:
- теоретический
- **комплексный**
- логический

11. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
- **Сотрудники**
- Хакеры
- Атакующие
- Контрагенты (лица, работающие по договору)

12. Под информационной безопасностью понимается:
- **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре**
- программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
- нет верного ответа

13. Защита информации:
- небольшая программа для выполнения определенной задачи
- **комплекс мероприятий, направленных на обеспечение информационной безопасности**
- процесс разработки структуры базы данных в соответствии с требованиями пользователей

14. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
- Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
- Когда риски не могут быть приняты во внимание по политическим соображениям
- Когда необходимые защитные меры слишком сложны

- **Когда стоимость контрмер превышает ценность актива и потенциальные потери**

15. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это
- аудит
- **аутентификация**
- авторизация
- идентификация

16. Соответствие средств безопасности решаемым задачам характеризует
- эффективность
- корректность
- **адекватность**
- унификация

17. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это
- уязвимость информации
- надежность информации
- защищенность информации
- **безопасность информации**

18. Надежность системы защиты информации определяется
- усредненным показателем
- **самым слабым звеном**
- количеством отраженных атак
- самым сильным звеном

19. Политика информационной безопасности — это
- профиль защиты
- итоговый документ анализа рисков
- стандарт безопасности
- совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации

20. Выделения пользователем и администраторам только тех прав доступа, которые им необходимы это
- принцип многоуровневой защиты
- **принцип минимизации привилегий**
- принцип простоты и управляемости ИС
- принцип максимизации привилегий

21. Троянские программы — это
- программы-вирусы, которые распространяются самостоятельно
- все программы, содержащие ошибки
- **часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба**
- текстовые файлы, распространяемые по сети

22.Основной целью системы брандмауэра является управление доступом
- к архивам
- внутри защищаемой сети
- к секретной информации
- **к защищаемой сети**

Задания открытого типа (примерные)

1. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это
Модель ответа. Аутентификация

2. Соответствие средств безопасности решаемым задачам характеризует
Модель ответа. Адекватность

3. Присвоение субъектам и объектам доступа уникальных «меток» и сравнение метки, предъявляемой пользователем системы, с утвержденным перечнем - это
Модель ответа. Идентификация

Задание открытого типа (повышенный уровень сложности)

8. Раскройте сущность понятия «Организационно-правовое обеспечение информационной безопасности».
Модель ответа.
Организационно-правовое обеспечение информационной безопасности представляет совокупность законов и других нормативно-правовых актов, а также организационных решений, которые регламентируют как общие вопросы обеспечения защиты информации, так и организацию, и функционирование защиты конкретных объектов и систем. Обеспечивает регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе, исключающей или существенно затрудняющей неправомерное овладение конфиденциальной информацией.

Описание технологии проведения

Продолжительность выполнения – 4**0 минут.**

Работа состоит из **заданий** на выбор одного или нескольких правильных ответов, задания на сопоставление или упорядочивание и т.д. и заданий – открытого типа - ответ необходимо ввести в соответствующем поле, в том числе, задание -эссе.

Задания работы предлагаются в произвольном порядке, с возможностью перемещаться по ним произвольным образом, но задание – эссе – последнее.

Требования к выполнению заданий, шкалы и критерии оценивания

Задания в виде тестов выполняются в ЭОС Moodle

Критерии оценивания

Задания закрытого типа, средний уровень сложности (одиночный выбор, множественный выбор, соответствие):

1 балл – указан верный ответ;

0 баллов – указан неверный ответ, в том числе частично.

Задание открытого типа, средний уровень сложности:

2 балла – указан верный ответ;

0 баллов – указан неверный ответ, в том числе частично.

Задание открытого типа (повышенный уровень сложности)

5 баллов – задание выполнено верно (получен правильный ответ, обоснован характер принятого решения);

2 балла – задание выполнено с незначительными ошибками, но приведен правильный ход рассуждений, или получен верный ответ, но отсутствует обоснование характера принятого решения, или задание выполнено не полностью, но получены промежуточные результаты, отражающие правильность хода выполнения задания;

0 баллов – задание не выполнено, или ответ содержательно не соотнесен с заданием, или задание выполнено неверно.

Тест считается пройденным, если набрано 75% верных ответов

Задания раздела 20.2.1 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных знаний по результатам освоения данной дисциплины

Технология проведения промежуточной аттестации

Промежуточная аттестация проводится в форме собеседования по вопросам билета (2 вопроса)

Требования к ответу на зачете, описание критериев и шкалы оценивания компетенций (результатов обучения) при промежуточной аттестации

Для оценивания результатов обучения на зачете используются следующие показатели:

- владение понятийным аппаратом и теоретическими основами дисциплины,
- способность иллюстрировать ответ примерами практического использования теоретического материала,
- способность связать вопросы теории с практическими заданиями,
- применять теоретические знания для решения практических задач,
- ориентация в функциональных возможностях изучаемых программных продуктах,
- грамотная, уверенная, связанная речь при устном ответе,
- способность быстро ориентироваться в материале, отвечая на дополнительные вопросы в рамках изучаемого объема.

Результат обучения оценивается: «зачтено», «не зачтено».

Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Продемонстрировано знание базовых требований информационной безопасности; нормативных правовых актов в области защиты информации; основных методов, способов и мероприятий по обеспечению информационной безопасности в профессиональной деятельности; умение использовать программное обеспечение для решения задач, владение понятийным аппаратом дисциплины.	Пороговый	Зачтено
Ответ на контрольно-измерительный материал не соответствует перечисленным показателям. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки в ответе на вопрос КИМ, затрудняется ответить на дополнительные вопросы.	–	Не зачтено

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.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах: устного опроса (фронтальная беседа и доклады); оценки результатов практических заданий. 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.
При оценивании используются шкала Зачтено-не зачтено. Критерии оценивания приведены выше.

Промежуточная аттестация с применением ДОТ

1. Промежуточная аттестация с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) проводится в рамках электронного курса, размещенного в ЭИОС (образовательный портал «Электронный университет ВГУ» (LMS Moodle, https://edu.vsu.ru/)).

2. Промежуточная аттестация обучающихся осуществляется в форме экзамена.

3. Обучающиеся, проходящие промежуточную аттестацию с применением ДОТ, должны располагать техническими средствами и программным обеспечением, позволяющим обеспечить процедуры аттестации. Обучающийся самостоятельно обеспечивает выполнение необходимых технических требований для про-

ведения промежуточной аттестации с применением дистанционных образовательных технологий.

4. Идентификация личности обучающегося при прохождении промежуточной аттестации обеспечивается посредством использования каждым обучающимся индивидуального логина и пароля при входе в личный кабинет, размещенный в ЭИОС ВГУ.