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

УТВЕРЖДАЮ
Заведующий кафедрой экономической теории
и мировой экономики
_____ д.э.н., проф. Т.Н.Гоголева
18.05.2023 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.09 Информационная безопасность и защита информации

1. Код и наименование направления подготовки: 38.04.01 Экономика

2. Профиль подготовки: Экономика организаций и рынков

3. Квалификация выпускника: магистр

4. Форма обучения: заочная

5. Кафедра, отвечающая за реализацию дисциплины: кафедра экономической теории и мировой экономики

6. Составители программы: Маслова М.И., преподаватель кафедры экономической теории и мировой экономики

7. Рекомендована: Научно-методическим советом экономического факультета ВГУ от 20.04.2023 г., протокол №4

8. Учебный год: 2024/2025 **Триместр: 6**

9. Цели и задачи учебной дисциплины:

Целями освоения учебной дисциплины являются:

- анализ и использование различных источников информации с учетом требований информационной безопасности и защиты информации;

- овладение методами решения исследовательских задач с применением аппарата, используемого при проектировании и реализации систем защиты информации.

Задачи учебной дисциплины:

- ознакомить студентов с общими вопросами информационной безопасности, криптологии, стеганографии для осуществления хранения и архивирования документов и информации;

- приобрести навыки поиска информации с использованием открытых источников информации и специализированных баз данных с учетом требований информационной безопасности и защиты информации;

- получить навыки обработки полученных данных принимая во внимание требования информационной безопасности.

10. Место учебной дисциплины в структуре ООП: дисциплина «Информационная безопасность и защита информации» входит в вариативную часть блока Б1.

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	Индикаторы	Планируемые результаты обучения
ПК-2	Способен собрать и проанализировать данные для расчета экономических и социально-экономических показателей, характеризующих товарные, факторные и финансовые рынки, на которых осуществляется деятельность хозяйствующих субъектов	ПК-2.1	Осуществляет хранение и архивирование информации, документов	Знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

ПК-4	Способен использовать для решения аналитических и прикладных задач современные технические средства и информационные технологии	ПК-4.1	Проводит информационный поиск для решения исследовательских задач с использованием открытых источников информации и специализированных баз данных	Знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.
		ПК-4.4	Обрабатывает полученные данные с использованием современных методов анализа информации	Знать: средства и методы предотвращения и обнаружения вторжений; технические каналы утечки информации; возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; организацию защиты информации от утечки по техническим каналам на объектах информатизации; Уметь: пользоваться нормативными документами по противодействию технической разведке; оценивать качество готового программного обеспечения; Владеть: методами и средствами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты информации.

12. Объем дисциплины в зачетных единицах/час. — 3 ЗЕТ / 108 час.

Форма промежуточной аттестации зачет с оценкой

13. Трудоемкость по видам учебной работы:

Вид учебной работы		Трудоемкость	
		Всего	По триместрам
			6 триместр
Аудиторные занятия		14	14
в том числе:	лекции	6	6
	практические	8	8
Самостоятельная работа		90	90
Форма промежуточной аттестации		зачет с оценкой - 4	зачет с оценкой - 4
Итого:		108	108

13.1 Содержание дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК*
1. Лекции			
1.1	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в	Стандарты в области информационной безопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность.	-

	условиях функционирования в России глобальных сетей.		
1.2	Три вида возможных нарушений информационной системы. Защита.	Три вида возможных нарушений информационной безопасности. 3 составляющих ИБ - целостность, доступность, конфиденциальность. Защита информационной системы от угроз.	-
1.3	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	Схема построения информационной безопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения информационной безопасности государства. Военные подразделения в сфере информационной безопасности.	-
1.4	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы.	-
1.5	Методы криптографии	Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная цифровая подпись.	-
1.6	Основные технологии построения защищенных систем	Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.	-
1.7	Место информационной безопасности экономических систем в национальной безопасности страны	Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция информационной безопасности. Основные сведения и положения.	-
2. Практические занятия			
2.1	Виды противников или «нарушителей». Понятие о видах вирусов	Понятие нарушителя информационной безопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	-
2.2	Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны.	-
2.3	Основные положения теории информационной безопасности. Модели без-	Основные положения теории информационной безопасности. Анализ различных моделей безопасности, как для крупного объекта, так и для относительно небольшой компании. Модели безопасности для домаш-	-

	опасности и их применение	ней информационной системы. Применение методов информационной безопасности.	
2.4	Измерение результатов экономической деятельности. Валовой внутренний продукт и его исчисление. Другие макроэкономические показатели	Понятие таксономии нарушения безопасности. Причины нарушения информационной безопасности. Аудит событий в рамках информационной системы.	-
2.5	Анализ способов нарушений информационной безопасности	Анализ различных способов нарушений информационной безопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем.	-
2.6	Методы криптографии	Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная цифровая подпись.	-
2.7	Основные технологии построения защищенных систем	Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.	-

13.2 Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)			
		Лекции	Практические	Самостоятельная работа	Всего
1.	Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей.	1	1	12	12
2.	Три вида возможных нарушений информационной системы. Защита.	1	1	14	16
3.	Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.	1	1	14	16
4.	Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	1	1	12	14
5.	Методы криптографии	1	1	14	18
6.	Основные технологии построения защищенных систем	1	1	12	14
7.	Место информационной безопасности экономических систем в национальной безопасности страны	-	2	12	14
	Итого:	6	8	90	104

14. Методические указания для обучающихся по освоению дисциплины:

Основой успешного освоения дисциплины является работа с конспектами лекций, с основной рекомендуемой литературой по дисциплине, полное и своевременное выполнение практических заданий по всем разделам дисциплины, полученным в ходе практических занятий.

Тестирование в течение каждого семестра освоения дисциплины, а также задания текущей аттестации включают разобранные на практических занятиях практические задания с возможными надстройками, разобранными в рамках теоретических занятий.

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

а) основная литература:

№ п/п	Источник
1	Информационная безопасность и защита информации : учебное пособие для студ. вузов, обуч. по специальности 230201 "Информационные системы и технологии" / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова .— Москва : ACADEMIA, 2006 .— 330 с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с. 327-328.

б) дополнительная литература:

№ п/п	Источник
1	Информационная безопасность и защита информации : учебное пособие для студ. , обуч. по специальности "Информационные системы и технологии" днев. и заоч. форм обучения / Ю.М. Краковский .— М. ; Ростов н/Д : МарТ, 2008 .— 287 с. : ил .— (Учебный курс) .— Библиогр.: с.221 .— ISBN 978-5-241-00925-8.
2	Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330 .— ISBN 978-5-369-01761-6 .— ISBN 978-5-16-013849-7.

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

№ /п	Ресурс
8	ЭБС «Университетская библиотека online»
9	ЭБС «Лань»
10	Электронно-библиотечная система (ЭБС) ВГУhttps://lib.vsu.ru/?p=4&t=8b

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	

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

Реализация учебной дисциплины предполагает применение дистанционных образовательных технологий (работу на образовательном портале «Электронный университет ВГУ»).

18. Материально-техническое обеспечение дисциплины:

Учебные аудитории для проведения учебных занятий (лекционных, практических), оснащенных оборудованием и техническими средствами обучения: специализированная мебель, проектор, экран для проектора, компьютер с возможностью подключения к сети "Интернет", проводной микрофон, комплект активных громкоговорителей

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	Темы 1-7	ПК-2 Способен собрать и проанализировать данные для расчета экономических и социально-экономических показателей, характеризующих товарные, факторные и финансовые рынки, на которых осуществляется деятельность хозяйствующих субъектов	ПК-2.1 Собирает и анализирует данные для расчета экономических и социально-экономических показателей, характеризующих структуру и конъюнктуру рынка	Примерный перечень вопросов
		ПК-4 Способен планировать работу, выбирать методы решения исследовательских задач, проводить исследования в рамках реализации научного проекта адекватно поставленным целям с учетом широкого понимания профессиональной области обучения, в том числе на междисциплинарном уровне	ПК-4.1 Применяет информационно-коммуникационные технологии для поиска и обмена необходимой социально-экономической информацией для решения аналитических и прикладных задач	Примерный перечень вопросов
			ПК-4.4 Использует современное ПО для решения экономических задач оценки риска	
Промежуточная аттестация форма контроля – зачет с оценкой				Примерный 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: теоретические вопросамы для проведения собеседования (индивидуальный опрос, фронтальная беседа), материалы с практическими заданиями (кейсы), тесты.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета.

Критерии оценивания приведены ниже.

Формирование оценки текущего контроля успеваемости и промежуточной аттестации по итогам освоения дисциплины осуществляется с использованием балльно-рейтинговой оценки работы студента.

Критерии оценивания приведены ниже.

Примерный перечень вопросов для собеседования:

1. Что такое информационная безопасность?
2. Какие предпосылки и цели обеспечения информационной безопасности?
3. В чем заключаются национальные интересы РФ в информационной сфере?
4. Что включает в себя информационная борьба?
5. Какие пути решения проблем информационной безопасности РФ существуют?
6. Каковы общие принципы обеспечения защиты информации?
7. Какие имеются виды угроз информационной безопасности предприятия (организации)?

8. Какие источники наиболее распространенных угроз информационной безопасности существуют?
9. Какие виды сетевых атак имеются?
10.Какими способами снизить угрозу сниффинга пакетов?
11.Какие меры по устранению угрозы IP -спуфинга существуют?
12.Что включает борьба с атаками на уровне приложений?
13.Какие существуют проблемы обеспечения безопасности локальных вычислительных сетей?
14.В чем заключается распределенное хранение файлов?
15.Что включают в себя требования по обеспечению комплексной системы информационной безопасности?
16.Какие уровни информационной защиты существуют, их основные составляющие?
17.В чем заключаются задачи криптографии?
18.Зачем нужны ключи?
19.Какая схема шифрования называется многоалфавитной подстановкой?
20.Какие системы шифрования вы знаете?
21.Что включает в себя защита информации от несанкционированного доступа?
22.В чем заключаются достоинства и недостатки программно-аппаратных средств защиты информации?
23.Какие виды механизмов защиты могут быть реализованы для обеспечения идентификации и аутентификации пользователей?
24.Какие задачи выполняет подсистема управления доступом?
25.Какие требования предъявляются к подсистеме протоколирования аудита?
26.Какие виды механизмов защиты могут быть реализованы для обеспечения конфиденциальности данных и сообщений?
27.В чем заключается контроль участников взаимодействия?
28.Какие функции выполняет служба регистрации и наблюдения?
29.Что такое информационно-опасные сигналы, их основные параметры?
30.Какие требования необходимо выполнять при экранировании помещений, предназначенных для размещения вычислительной техники?
31.Какой процесс называется аутентификацией пользователя?
32.Какие схемы аутентификации вы знаете?
33.Что такое смарт-карты?
34.Какие требования предъявляются к современным криптографическим системам защиты информации?
35.Что такое симметричная криптосистема?
36.Какие виды симметричных криптосистем существуют?
37.Что такое асимметричная криптосистема?
38.Что понимается под односторонней функцией?
39.Как классифицируются криптографические алгоритмы по стойкости?
40.В чем заключается анализ надежности криптосистем?
41.Что такое дифференциальный криптоанализ?
42.В чем сущность криптоанализа со связанными ключами?
43.В чем сущность линейного криптоанализа?
44.Какие атаки изнутри вы знаете?
45.Какая программа называется логической бомбой?
46.Какими способами можно проверить систему безопасности?
47.Что является основными характеристиками технических средств защиты информации?
48.Какие требования предъявляются к автоматизированным системам третьей группы?
49.Какие требования предъявляются к автоматизированным системам защиты второй группы?

50.Какие требования предъявляются к автоматизированным системам защиты первой группы?
51.Какие классы защиты информации от несанкционированного доступа для средств вычислительной техники имеются? От чего зависит выбор класса защищенности?
52.Какие требования предъявляются к межсетевым экранам?
53.Какие имеются показатели защищенности межсетевых экранов?
54.Какие атаки системы снаружи вы знаете?
55.Какая программа называется вирусом?
56.Какая атака называется атакой отказа в обслуживании?
57.Какие виды вирусов вы знаете?
58.Какие вирусы называются паразитическими?
59.Как распространяются вирусы?
60.Какие методы обнаружения вирусов вы знаете?
61.Какая программа называется монитором обращения?
62.Что представляет собой домен?
63.Как осуществляется защита при помощи ACL -списков?
64.Какой список называется перечнем возможностей?
65.Какие способы защиты перечней возможностей вы знаете?
66.Из чего состоит высоконадежная вычислительная база (TCB)?
67.Какие модели многоуровневой защиты вы знаете?
68.В чем заключается организация работ по защите от несанкционированного доступа интегрированной информационной системы управления предприятием?
69.Какие характеристики положены в основу системы классификации информационных систем управления предприятием?
70.Какие задачи решает система компьютерной безопасности?
71.Какие пути защиты информации в локальной сети существуют?
72.Какие задачи решают технические средства противодействия экономическому шпионажу?
73.Какой порядок организации системы видеонаблюдения?
74.Что включает в себя защита информационных систем с помощью планирования?
75.Какие условия работы оцениваются при планировании?
76.Из каких этапов состоят работы по обеспечению информационной безопасности предприятия?
77.Что такое мобильные программы?
78.Что такое концепция потоков?
79.Что представляет собой метод «песочниц»?
80.Что такое интерпретация?
81.Что такое программы с подписями?
82.Что представляет собой безопасность в системе Java?
83.Назовите несколько примеров политик безопасности пакета JDK 1.2?
84.Какие международные документы регламентируют деятельность по обеспечению защиты информации?
85.Что понимают под политикой информационной безопасности?
86.Что включает в себя политика информационной безопасности РФ?
87.Какие нормативные документы РФ определяют концепцию защиты информации?

Соотношение критериев оценивания компетенций, уровня сформированной компетенций и шкалы оценивания результатов обучения для зачета с оценкой

Критерии оценивания компетенций	Уровень сформированной компетенций	Шкала оценок
Полный, исчерпывающий, аргументированный ответ на все вопросы и задания. Ответы должны отличаться логической последовательностью, четкостью в выражении мыслей и обоснованностью выводов, демонстрирующих знание источников основной и дополнительной литературы, понятийного аппарата и умения ими пользоваться при ответе.	*Повышенный уровень*	*Отлично*
Полный, исчерпывающий, аргументированный ответ на вопросы и задания. Ответы должны отличаться логичностью, четкостью, знанием понятийного аппарата и литературы при незначительных упущениях при ответах на вопросы и выполнении заданий.	*Базовый уровень*	*Хорошо*
Неполных и слабо аргументированный ответ, демонстрирующих общее представление и элементарное понимание существа поставленных вопросов и заданий, понятийного аппарата и обязательной литературы.	*Пороговый уровень*	*Удовлетворительно*
Обучающийся демонстрирует незнание и непонимание существа экзаменационных вопросов. При выставлении неудовлетворительной оценки преподаватель должен объяснить студенту недостатки его ответа.	–	*Неудовлетворительно*

Критерии оценки:

Оценка **«отлично»** выставляется при полных, исчерпывающих, аргументированных ответах. Ответы должны отличаться логической последовательностью, четкостью в выражении мыслей и обоснованностью выводов, демонстрирующих знание понятийного аппарата дисциплины, теоретических положений и умения пользоваться ими.

Оценка **«хорошо»** выставляется при полных, аргументированных ответах на вопросы. Ответы должны отличаться логичностью, четкостью, знанием понятийного аппарата и умения пользоваться им.

Оценка **«удовлетворительно»** выставляется при неполных и слабо аргументированных ответах, демонстрирующих общее представление и элементарное понимание существа поставленных вопросов.

Оценка **«неудовлетворительно»** выставляется при незнании и непонимании студентом существа поставленных вопросов.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: перечень вопросов для проведения промежуточной аттестации в форме зачета с оценкой.

Для оценивания результатов обучения на зачете используются следующие показатели:

- знание материала по вопросам и заданиям контрольно-измерительного материала;
- умение выделять существенные положения по поставленному в КИМе вопросу и представленному заданию;
- умение применять теоретические знания для анализа конкретных экономических ситуаций и решения прикладных заданий.

Зачет с оценкой проводится в форме собеседования по вопросам, изучаемым в течение семестра и обсуждении практической ситуации

Уровень сформированности компетенций на промежуточной аттестации в форме зачета с оценкой оценивается по шкале: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»