

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
24.05.2021

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.09.01 Информационная безопасность цифровой экономики

1. Код и наименование направления подготовки/специальности:

38.03.01 Экономика

2. Профиль подготовки/специализация:

Модели и методы анализа цифровой экономики

3. Квалификация (степень) выпускника: бакалавр

4. Форма обучения: очная

5. Кафедра, отвечающая за реализацию дисциплины:

информационных технологий и математических методов в экономике

6. Составитель программы:

Коротких В.В., канд. экон. наук

7. Рекомендована: НМС экономического факультета ВГУ протокол №4 от 15.04.21 г.

8. Учебный год: 2024-2025

Семестр(ы): 8

9. Цели и задачи учебной дисциплины:

Цель освоения учебной дисциплины:

- получение теоретических знаний и практических навыков в области защиты информации в цифровой экономике;
- развитие информационной культуры и подготовки, необходимых для понимания принципов построения систем защиты информации;
- демонстрация возможностей применения основных категорий мер защиты информации с оценкой их сильных и слабых сторон.

Задачи учебной дисциплины:

- ознакомление с основными понятиями информационной безопасности в цифровой экономике;
- формирование навыков выбора методов и средств защиты информации, соответствующих требованиям защиты информации в конкретных информационных системах;
- формирование навыков оценки соответствия существующих решений в области защиты информации конкретным требованиям;
- формирование навыков разработки предложений по совершенствованию системы обеспечения информационной безопасности в цифровой экономике.

10. Место учебной дисциплины в структуре ООП: часть, формируемая участниками образовательных отношений 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	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-2	Способен применять информационные технологии для проведения бизнес-анализа, подготовки информационно-аналитических материалов и прогнозирования экономических показателей	ПК-2.2	Оформляет промежуточные и итоговые результаты в виде аналитических документов	знать: основные понятия, конструкции и факты в сфере обеспечения информационной безопасности в цифровой экономике; уметь: применять на практике основные термины, связанные с защитой информации; описывать круг задач, решаемых в рамках обеспечения безопасности информации; владеть (иметь навык(и)): понятийным аппаратом, установленным в нормативных актах, относящихся к информации и информационным технологиями.
ПК-2	Способен применять информационные технологии для проведения бизнес-анализа, подготовки информационно-аналитических материалов и прогнозирования экономических показателей	ПК-2.4	Анализирует деятельность организаций в условиях цифровой экономики	знать: последовательность процедур контроля доступа субъектов; уметь: разрабатывать рекомендации по выбору методов и организации системы аутентификации пользователей, а также по выбору модели разграничения доступа для конкретной информационной системы; владеть: методами оценки надежности конкретного современного шифра на основе используемых преобразований и его параметров.

12. Объем дисциплины в зачетных единицах/час: 3/108.

Форма промежуточной аттестации: зачет.

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость			
		Всего	По семестрам		
			7 семестр	8 семестр	...
Аудиторные занятия		36		36	
в том числе:	лекции	18		18	
	практические				
	лабораторные	18		18	
Самостоятельная работа		72		72	
в том числе: курсовая работа (проект)					
Форма промежуточной аттестации: зачет с оценкой, экзамен					
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	Основы информационной безопасности. Основные понятия и определения	Понятие информации. Доступ к информации. Информационные системы.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.2	Меры обеспечения защиты информации	Организация защиты информации. Организационные меры защиты информации. Законодательные меры защиты информации. Административные меры защиты информации. Организационно-технические меры защиты информации.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.3	Организационные меры защиты информации	Законодательные меры защиты информации. Административные меры защиты информации: сущность и направления. Управление рисками. Политика безопасности организации. Управление персоналом. Планирование действий в чрезвычайных ситуациях.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.4	Методы контроля и разграничения доступа	Основные понятия контроля доступа субъектов. Аутентификация субъектов доступа. Аутентификация на основе знания. Аутентификация на основе владения. Аутентификация на основе признаков или действий.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.5	Обзор криптографических методов защиты информации	Понятие шифра. Шифр простой замены и его анализ. Шифры перестановки и их анализ. Варианты усложнения шифра простой замены. Шифр многоалфавитной замены и его анализ.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.6	Криптографические методы защиты информации	Требования к современным криптографическим системам. Шифры на основе сети Фейстеля. Шифры на основе SP-сети. Асимметричные системы	Информационная безопасность

		шифрования.	цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.7	Стеганографическая защита информации	Исторический обзор стеганографии. Основные понятия стеганографии. Основные угрозы безопасности стеганографических систем. Типы нарушителей безопасности стеганографических систем. Типы атак на стеганографические системы.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.8	Техническая защита информации	Основные понятия технической защиты информации. Технические каналы утечки информации. Акустический канал утечки информации. Оптический канал утечки информации. Радиоэлектронный канал утечки информации.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
1.9	Программно-технические меры защиты информации	Сервисы безопасности. Антивирусная защита. Типы вредоносных программ. Принципы обнаружения вредоносных программ. Выбор антивирусных средств. Межсетевое экранирование.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2. Лабораторные занятия			
2.1	Основы информационной безопасности. Основные понятия и определения	Обработка информации. Защита информации. Информационная безопасность	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2.2	Меры обеспечения защиты информации	Программно-технические средства защиты информации. Криптографические методы защиты информации. Стеганографические методы защиты информации. Методы и средства технической защиты информации	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2.3	Организационные меры защиты информации	Организационно-технические меры защиты информации: физическая защита объекта информатизации, защита поддерживающей инфраструктуры	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2.4	Методы контроля и разграничения доступа	Разграничение доступа. Дискреционная модель разграничения доступа. Мандатная модель разграничения доступа. Ролевая модель разграничения доступа.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2.5	Обзор криптографических методов защиты информации	Требования к шифрам. Шифровальные машины и подходы к их анализу. Идеальный шифр и классы стойкости шифров	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)

2.6	Криптографические методы защиты информации	Схемы электронной цифровой подписи. Хэш-функции. Криптографические протоколы. Перспективы криптографии.	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2.7	Стеганографическая защита информации	Компьютерная и цифровая стеганография. Сфера применения методов стеганографической защиты информации	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2.8	Техническая защита информации	Принципы осуществления технической разведки. Принципы защиты от технической разведки	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)
2.9	Программно-технические меры защиты информации	Системы предотвращения утечки информации. Протоколирование и аудит	Информационная безопасность цифровой экономики (https://edu.vsu.ru/course/view.php?id=4281)

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (количество часов)				Всего
		Лекции	Практические	Лабораторные	Самостоятельная работа	
1	Основы информационной безопасности. Основные понятия и определения	2	0	2	8	12
2	Меры обеспечения защиты информации	2	0	2	8	12
3	Организационные меры защиты информации	2	0	2	8	12
4	Методы контроля и разграничения доступа	2	0	2	8	12
5	Обзор криптографических методов защиты информации	2	0	2	8	12
6	Криптографические методы защиты информации	2	0	2	8	12
7	Стеганографическая защита информации	2	0	2	8	12
8	Техническая защита информации	2	0	2	8	12
9	Программно-технические меры защиты информации	2	0	2	8	12
	Итого:	18	0	18	72	108

14. Методические указания для обучающихся по освоению дисциплины:

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

В процессе лекций обучающимся рекомендуется вести конспект, что позволит впоследствии вспомнить изученный учебный материал, дополнить содержание при самостоятельной работе с литературой, подготовиться к текущей и промежуточной аттестации.

Следует также обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений.

Любая лекция должна иметь логическое завершение, роль которого выполняет заключение. Выводы формулируются кратко и лаконично, их целесообразно записывать. В конце лекции обучающиеся имеют возможность задать вопросы преподавателю по теме лекции.

В ходе подготовки к лабораторным занятиям обучающемуся рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях.

Прежде чем приступить к выполнению лабораторных заданий, обучающемуся необходимо ознакомиться с соответствующими разделами программы дисциплины по учебной литературе, рекомендованной программой курса; получить от преподавателя информацию о порядке выполнения лабораторных заданий, критериях оценки результатов работы; получить от преподавателя конкретное задание и информацию о сроках выполнения, о требованиях к оформлению и форме представления результатов.

При выполнении лабораторных заданий необходимо привести развёрнутые пояснения хода решения и проанализировать полученные результаты. При необходимости обучающиеся имеют возможность задать вопросы преподавателю по трудностям, возникшим при решении задач.

Самостоятельная работа обучающихся направлена на самостоятельное изучение отдельных тем и вопросов учебной дисциплины. Самостоятельная работа является обязательной для каждого обучающегося. При самостоятельной работе обучающийся взаимодействует с рекомендованными материалами при минимальном участии преподавателя.

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

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

а) основная литература:

№ п/п	Источник
1	Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник : [16+] / Б. И. Филиппов, О. Г. Шерстнева. – Москва ; Берлин : Директ-Медиа, 2019. – 241 с. – URL: https://biblioclub.ru/index.php?page=book&id=499170
2	Основы информационной безопасности : учебник / В. Ю. Рогозин, И. Б. Галушкин, В. Новиков, С. Б. Вепрев ; Академия Следственного комитета Российской Федерации. – Москва : Юнити-Дана : Закон и право, 2018. – 287 с. – URL: https://biblioclub.ru/index.php?page=book&id=562348

б) дополнительная литература:

№ п/п	Источник
3	Шилов, А. К. Управление информационной безопасностью : учебное пособие : [16+] / А. К. Шилов ; Южный федеральный университет, Институт компьютерных технологий и информационной безопасности. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 121 с. – URL: https://biblioclub.ru/index.php?page=book&id=500065
4	Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В. Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. – URL: https://biblioclub.ru/index.php?page=book&id=571485
5	Информационная безопасность в цифровом обществе : учебное пособие : [16+] / А. С. Исмагилова, И. В. Салов, И. А. Шагапов, А. А. Корнилова ; Башкирский государственный университет. – Уфа : Башкирский государственный университет, 2019. – 128 с. – URL: https://biblioclub.ru/index.php?page=book&id=611084
6	Гулятьева, Т. А. Основы информационной безопасности : учебное пособие : [16+] / Т. А. Гулятьева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. – URL: https://biblioclub.ru/index.php?page=book&id=574729

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

№ п/п	Ресурс
7	http://edu.vsu.ru/
8	http://www.lib.vsu.ru
9	http://biblioclub.ru
10	http://www.e-library.ru
11	http://www.ibooks.ru

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие : [16+] / А. В. Моргунов ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2019. – 83 с. – URL: https://biblioclub.ru/index.php?page=book&id=576726
2	Бекетнова, Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем : учебное пособие : [16+] / Ю. М. Бекетнова, Г. О. Крылов, С. Л. Ларионова. – Москва : Прометей, 2018. – 173 с. – URL: https://biblioclub.ru/index.php?page=book&id=494850

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

Дисциплина реализуется с элементами электронного обучения и дистанционных образовательных технологий в рамках электронного курса (ЭК) Информационная безопасность цифровой экономики, размещенного на портале «Электронный университет ВГУ» (<https://edu.vsu.ru/course/view.php?id=4281>). ЭК включает учебные материалы для самостоятельной работы обучающихся, а также обеспечивает возможность проведения контактных часов/аудиторных занятий в режиме онлайн.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория: специализированная мебель, ноутбук, проектор, экран для проектора; помещение для самостоятельной работы: специализированная мебель, компьютеры с возможностью подключения к сети "Интернет"; программное обеспечение OS Ubuntu, Okular, Mozilla Firefox, LibreOffice, WPS Office, Microsoft Office, RStudio, Gretl, Консультант+.

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	Основы информационной безопасности. Основные понятия и определения Техническая защита информации Программно-технические меры защиты информации Организационные меры защиты информации	ПК-2	ПК-2.2	Тестовые задания
2	Меры обеспечения защиты информации Методы контроля и разграничения доступа Обзор криптографических методов защиты информации	ПК-2	ПК-2.4	Тестовые задания

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
	Криптографические методы защиты информации Стеганографическая защита информации			
Промежуточная аттестация форма контроля – зачет				Перечень вопросов Практическое задание

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: тестовые задания.

Перечень тестовых заданий

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
 - разработка аппаратных средств обеспечения правовых данных
 - разработка и конкретизация правовых нормативных актов обеспечения безопасности
 - разработка и установка во всех компьютерных правовых сетях журналов учета действий
2. Основными рисками информационной безопасности являются:
 - техническое вмешательство, выведение из строя оборудования сети
 - потеря, искажение, утечка информации
 - искажение, уменьшение объема, перекодировка информации
3. Конфиденциальностью называется:
 - описание процедур
 - защита от несанкционированного доступа к информации
 - защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
4. В каком документе отражено понятие автоматизированной системы
 - Федеральный закон № 149-ФЗ
 - ГОСТ Р 34.003-90
 - ГОСТ 51275-2006
5. Согласно 149-ФЗ «Об информации, информационных технологиях и о защите информации», информация определяется как:
 - вся совокупность сведений об окружающем нас мире, о всевозможных протекающих в нем процессах, которые могут быть восприняты живыми организмами, электронными машинами и другими информационными системами.
 - совокупность сведений, подлежащих хранению, передаче, обработке и использованию в человеческой деятельности.
 - все то, чем могут быть дополнены наши знания и предположения.
 - сведения независимо от формы их представления
6. Криптографические методы ЗИ могут быть не эффективны для:
 - Внутренних нарушителей, имеющих физический доступ к носителям информации
 - Нарушителя, использующего средства несанкционированного получения информации, обрабатываемой техническими средствами в открытом виде
 - Внешнего нарушителя, вступающего в сговор с легальными пользователями
7. Укажите уровни защиты информации:
 - Административный
 - Законодательный

- Индустриальный
 - Промышленный
8. Криптографические методы ЗИ эффективны для:
- Нарушителей, способных осуществить сетевую атаку на ИС и получить доступ к конкретным информационным объектам
 - Нарушителей, обладающих значительными вычислительными ресурсами
 - Угроз утечки речевой и видовой информации по техническим каналам
 - Нарушителя, использующего халатность или ошибки легальных пользователей
9. Защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры понимается под ...
- Информационной безопасностью
 - Целостностью информации
 - Конфиденциальностью информации
 - Доступностью и гибкостью информации
10. К организационным мерам защиты информации НЕ относится:
- Законодательные меры ЗИ
 - Криптографические методы ЗИ
 - Административные меры ЗИ
11. 149-ФЗ «Об информации, информационных технологиях и о защите информации» регулирует отношения, возникающие при:
- Обеспечении распространения информации
 - Осуществлении права на поиск, получение, передачу и распространение информации
 - Обеспечении уничтожения информации
 - Обеспечении защиты информации
12. Что не относится к свойствам информационной безопасности:
- целостность
 - закрытость
 - конфиденциальность
 - доступность
13. К программно-техническим средствам защиты информации НЕ относится:
- Организационно-технические меры ЗИ
 - Стеганографические методы ЗИ
 - Методы и средства технической ЗИ

Критерии оценки контрольных работ

Для оценивания результатов обучения на зачете используется шкала – зачтено, не зачтено
Соотношение показателей, критериев и шкалы оценивания результатов обучения.

Критерии оценивания компетенций	Шкала оценок
<i>Обучающийся дал верные ответы не менее чем на 70% вопросов.</i>	<i>Зачтено</i>
<i>Обучающийся дал верные ответы менее чем на 70% вопросов.</i>	<i>Не зачтено</i>

20.2. Промежуточная аттестация

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 зачета.

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 проведения 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.

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств: перечень вопросов, практические задания.

Перечень вопросов к зачету

1. Понятие информации.
2. Доступ к информации.
3. Информационные системы.
4. Обработка информации.
5. Защита информации.
6. Информационная безопасность.
7. Организация защиты информации.
8. Организационные меры защиты информации.
9. Административные меры защиты информации.
10. Организационно-технические меры защиты информации.
11. Программно-технические средства защиты информации.
12. Криптографические методы защиты информации.
13. Стеганографические методы защиты информации.
14. Методы и средства технической защиты информации
15. Законодательные меры защиты информации.
16. Административные меры защиты информации: сущность и направления, управление рисками, политика безопасности организации, управление персоналом.
17. Планирование действий в чрезвычайных ситуациях.
18. Организационно-технические меры защиты информации: физическая защита объекта информатизации, защита поддерживающей инфраструктуры
19. Основные понятия контроля доступа субъектов.
20. Аутентификация субъектов доступа.
21. Аутентификация на основе знания.
22. Аутентификация на основе владения.
23. Аутентификация на основе признаков или действий.
24. Разграничение доступа.
25. Дискреционная модель разграничения доступа.
26. Мандатная модель разграничения доступа.
27. Ролевая модель разграничения доступа.
28. Понятие шифра.
29. Шифр простой замены и его анализ.
30. Шифры перестановки и их анализ.
31. Варианты усложнения шифра простой замены.
32. Шифр многоалфавитной замены и его анализ.
33. Требования к шифрам.
34. Шифровальные машины и подходы к их анализу.
35. Идеальный шифр и классы стойкости шифров
36. Требования к современным криптографическим системам.
37. Шифры на основе сети Фейстеля.
38. Шифры на основе SP-сети.
39. Асимметричные системы шифрования.
40. Схемы электронной цифровой подписи.
41. Хэш-функции.
42. Криптографические протоколы.
43. Перспективы криптографии.
44. Исторический обзор стеганографии.

45. Основные понятия стеганографии.
46. Основные угрозы безопасности стеганографических систем.
47. Типы нарушителей безопасности стеганографических систем.
48. Типы атак на стеганографические системы.
49. Компьютерная и цифровая стеганография.
50. Сфера применения методов стеганографической защиты информации
51. Основные понятия технической защиты информации.
52. Технические каналы утечки информации.
53. Акустический канал утечки информации.
54. Оптический канал утечки информации.
55. Радиоэлектронный канал утечки информации.
56. Принципы осуществления технической разведки.
57. Принципы защиты от технической разведки
58. Сервисы безопасности.
59. Антивирусная защита.
60. Типы вредоносных программ.
61. Принципы обнаружения вредоносных программ.
62. Выбор антивирусных средств.
63. Межсетевое экранирование.
64. Системы предотвращения утечки информации.
65. Протоколирование и аудит.

Перечень практических заданий

1. Используя шифр Виженера, зашифруйте сообщение "Несмотря на широкую распространённость, категория информации остаётся одной из самых дискуссионных в науке." В качестве ключа используйте слово "кино".
2. Используя шифр Виженера, зашифруйте сообщение "Несмотря на широкую распространённость, понятие информации остаётся одним из самых дискуссионных в науке." В качестве ключа используйте слово "защита".
3. Используя алфавит "l" "e" "k" "f" "v" "j" "p" "d" "t" "s" "c" "r" "h" "u" "x" "n" "y" "z" "a" "g" "q" "o" "i" "m" "w" "b", зашифруйте сообщение "Unus pro omnibus, omnes pro uno!" шифром Виженера. Ключ: "ave".
4. Используя алфавит "x" "r" "y" "k" "s" "d" "m" "f" "i" "a" "c" "q" "n" "e" "g" "l" "p" "t" "w" "j" "v" "o" "u" "h" "z" "b", зашифруйте сообщение "Unus pro omnibus, omnes pro uno!" шифром Виженера. Ключ: "ave".

Пример контрольно-измерительного материала

УТВЕРЖДАЮ
Заведующий кафедрой информационных технологий
и математических методов в экономике основ управления
Щепина И.Н.
__._.20__г.

Направление подготовки 38.03.01 Экономика
Дисциплина Б1.В.ДВ.09.01 Информационная безопасность цифровой экономики
Курс 4
Форма обучения Очная
Вид аттестации Промежуточная
Вид контроля Зачет

Контрольно-измерительный материал № 1

1. Стеганографические методы защиты информации.
2. Шифры на основе сети Фейстеля.
3. Используя алфавит "x" "r" "y" "k" "s" "d" "m" "f" "i" "a" "c" "q" "n" "e" "g" "l" "p" "t" "w" "j" "v" "o" "u" "h" "z" "b", зашифруйте сообщение "Unus pro omnibus, omnes pro uno!" шифром Виженера. Ключ: "ave".

Преподаватель _____ В. В. Коротких

Описание технологии проведения

Обучающемуся выдаётся КИМ, содержащий два теоретических вопроса и практическое задание. Обучающийся вначале излагает свой ответ на бланках документов для проведения аттестации, затем устно раскрывает теоретические вопросы и поясняет ход выполнения практического задания.

Для оценивания результатов обучения на экзамене используется 2-балльная шкала: «зачтено», «не зачтено». Соотношение показателей, критериев и шкалы оценивания результатов обучения:

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
<i>Обучающийся владеет теоретическими основами дисциплины и научной терминологией, грамотно излагает материал и способен иллюстрировать ответ примерами, фактами, данными научных исследований, применять теоретические знания для решения практических задач, но допускает отдельные несущественные ошибки.</i>	<i>Базовый уровень</i>	<i>Зачтено</i>
<i>Обучающийся не владеет теоретическими основами дисциплины и научной терминологией, демонстрирует отрывочные знания, не способен иллюстрировать ответ примерами, допускает множественные существенные ошибки в ответе.</i>	–	<i>Не зачтено</i>