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

В.В. Давнис
23.04.2020г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Б1.В.ДВ.08.01 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 16.04.20 г.

8. Учебный год: 2023-2024 **Семестр(ы): 8**

9.Цели и задачи учебной дисциплины:
Целью изучения дисциплины является знакомство обучающихся с основными понятиями защиты информации в цифровой экономике, основными принципами построения систем защиты информации, а также основными категориями мер защиты информации, их возможностями с точки зрения защиты информации, сильными и слабыми сторонами.
Задачи изучения дисциплины состоят в освоении обучающимися навыков выбора решений из различных категорий методов и средств защиты информаций, соответствующих требованиям защиты информации в конкретных информационных системах, оценки соответствия существующих решений таким требованиям, разработки предложений по совершенствованию системы обеспечения информационной безопасности в цифровой экономике.

10. Место учебной дисциплины в структуре ООП: вариативная часть, дисциплина по выбору.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников):

Компетенция		Планируемые результаты обучения
Код	Название	
ПК-8	способностью использовать для решения аналитических и исследовательских задач современные технические средства и информационные технологии	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. Виды учебной работы

Вид учебной работы	Трудоемкость (часы), всего
Аудиторные занятия	36
в том числе: лекции	18
практические	0
лабораторные	18
Самостоятельная работа	72
Форма промежуточной аттестации (зачет – 0 час. / экзамен – __час.)	0
Итого:	108

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины
1.	Основы информационной безопасности. Основные понятия и определения	Понятие информации. Доступ к информации. Информационные системы. Обработка информации. Защита информации. Информационная безопасность
2.	Меры обеспечения защиты информации	Организация защиты информации. Организационные меры защиты информации. Законодательные меры защиты информации. Административные меры защиты информации. Организа-

		ционно-технические меры защиты информации. Программно-технические средства защиты информации. Криптографические методы защиты информации. Стеганографические методы защиты информации. Методы и средства технической защиты информации
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. Организационно-технические меры защиты информации: физическая защита объекта информатизации, защита поддерживающей инфраструктуры
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. Разграничение доступа. Дискреционная модель разграничения доступа. Мандатная модель разграничения доступа. Ролевая модель разграничения доступа.
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. Требования к шифрам. Шифровальные машины и подходы к их анализу. Идеальный шифр и классы стойкости шифров
6.	Криптографические методы защиты информации	Требования к современным криптографическим системам. Шифры на основе сети Фейстеля. Шифры на основе SP-сети. Асимметричные системы шифрования. Схемы электронной цифровой подписи. Хэш-функции. Криптографические протоколы. Перспективы криптографии.
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. Компьютерная и цифровая стеганография. Сфера применения методов стеганографической защиты информации
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. Принципы осуществления технической разведки. Принципы защиты от технической разведки
9.	Программно-технические меры защиты информации	Сервисы безопасности. Антивирусная защита. Типы вредоносных программ. Принципы обнаружения вредоносных программ. Выбор антивирусных средств. Межсетевое экранирование. Системы предотвращения утечки информации. Протоколирование и аудит

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела) дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
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

(рекомендации обучающимся по освоению дисциплины: работа с конспектами лекций, презентационным материалом, выполнение практических заданий, тестов, заданий текущей аттестации и т.д.)

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

а) основная литература:

№ п/п	Источник
1.	Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2018. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/413854
2.	Внуков, А. А. Защита информации : учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 261 с. — (Высшее образование). — ISBN 978-5-534-01678-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/414082
3.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2018. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/422364
4.	Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2018. — 245 с. — (Бакалавр. Академический курс). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/422366
5.	Лось, А. Б. Криптографические методы защиты информации : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2018. — 473 с. — (Высшее образование). — ISBN 978-5-534-01530-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/413075
6.	Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2018. — 312 с. — (Специалист). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/414681

б) дополнительная литература:

№ п/п	Источник
7.	Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией А. А. Стрельцова. — Москва : Издательство Юрайт, 2018. — 325 с. — (Бакалавр и ма-

	гистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/413158
8.	Гашков, С. Б. Дискретная математика : учебник и практикум для академического бакалавриата / С. Б. Гашков, А. Б. Фролов. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2018. — 448 с. — (Высшее образование). — ISBN 978-5-534-04435-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/413380

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

№ п/п	Ресурс
9.	Электронный университет ВГУ. Электронный курс по дисциплине "Финансовая математика" –: https://edu.vsu.ru/course/view.php?id=4281
10.	Электронно-библиотечная система "Университетская библиотека online" – http://biblioclub.ru/
11.	Электронно-библиотечная система "Консультант студента" – http://www.studmedlib.ru
12.	Электронно-библиотечная система "Лань" – https://e.lanbook.com/
13.	Национальный цифровой ресурс "РУКОНТ" – http://rucont.ru
14.	ЗНБ ВГУ – https://lib.vsu.ru

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

17. Информационные технологии, используемые для реализации учебной дисциплины, включая программное обеспечение и информационно-справочные системы (при необходимости)

RStudio – среда разработки программного обеспечения с открытым исходным кодом для языка программирования R; СПС Консультант Плюс.

Программа курса реализуется с применением дистанционных образовательных технологий.

18. Материально-техническое обеспечение дисциплины:

Учебная аудитория (ауд. 307Б): специализированная мебель, ноутбук HP Probook 450 15.6", проектор Acer X1240, экран для проектора настенный Projecta Compact Electrol, WHDMI-приемник

Учебная аудитория (ауд. 3А): специализированная мебель, компьютеры 3QNTP-Shell NM-10-B260GBP-525 (11 шт.)

19. Фонд оценочных средств:

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

Код и содержание компетенции (или ее части)	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенции посредством формирования знаний, умений, навыков)	Этапы формирования компетенции (разделы (темы) дисциплины или модуля и их наименование)	ФОС* (средства оценивания)
ПК-8	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		Контрольная работа

	параметров.		
Промежуточная аттестация			КИМ

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

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

Критерии оценивания компетенций	Шкала оценок
*Полное соответствие ответа обучающегося всем перечисленным критериям. Продемонстрировано **знание** основных понятий, конструкций и фактов в сфере обеспечения информационной безопасности в цифровой экономике; последовательность процедур контроля доступа субъектов, **умение** применять на практике основные термины, связанные с защитой информации; описывать круг задач, решаемых в рамках обеспечения безопасности информации; разрабатывать рекомендации по выбору методов и организации системы аутентификации пользователей, а также по выбору модели разграничения доступа для конкретной информационной системы, **владение** понятийным аппаратом, установленным в нормативных актах, относящихся к информации и информационным технологиями, методами оценки надежности конкретного современного шифра на основе используемых преобразований и его параметров.*	*Зачтено*
Ответ на контрольно-измерительный материал не соответствует любым трем (четырем) из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки.	*Не зачтено*

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

19.3.1 Перечень вопросов к зачету:
Понятие информации.
Доступ к информации.
Информационные системы.
Обработка информации.
Защита информации.
Информационная безопасность.
Организация защиты информации.
Организационные меры защиты информации.
Административные меры защиты информации.
Организационно-технические меры защиты информации.
Программно-технические средства защиты информации.
Криптографические методы защиты информации.
Стеганографические методы защиты информации.
Методы и средства технической 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.
Организационно-технические меры защиты информации: физическая защита объекта информатизации, защита поддерживающей инфраструктуры
Основные понятия контроля доступа субъектов.
Аутентификация субъектов доступа.
Аутентификация на основе знания.
Аутентификация на основе владения.
Аутентификация на основе признаков или действий.
Разграничение доступа.
Дискреционная модель разграничения доступа.

Мандатная модель разграничения доступа.
Ролевая модель разграничения доступа.
Понятие шифра.
Шифр простой замены и его анализ.
Шифры перестановки и их анализ.
Варианты усложнения шифра простой замены.
Шифр многоалфавитной замены и его анализ.
Требования к шифрам.
Шифровальные машины и подходы к их анализу.
Идеальный шифр и классы стойкости шифров
Требования к современным криптографическим системам.
Шифры на основе сети Фейстеля.
Шифры на основе SP-сети.
Асимметричные системы шифрования.
Схемы электронной цифровой подписи.
Хэш-функции.
Криптографические протоколы.
Перспективы криптографии.
Исторический обзор стеганографии.
Основные понятия стеганографии.
Основные угрозы безопасности стеганографических систем.
Типы нарушителей безопасности стеганографических систем.
Типы атак на стеганографические системы.
Компьютерная и цифровая стеганография.
Сфера применения методов стеганографической защиты информации
Основные понятия технической защиты информации.
Технические каналы утечки информации.
Акустический канал утечки информации.
Оптический канал утечки информации.
Радиоэлектронный канал утечки информации.
Принципы осуществления технической разведки.
Принципы защиты от технической разведки
Сервисы безопасности.
Антивирусная защита.
Типы вредоносных программ.
Принципы обнаружения вредоносных программ.
Выбор антивирусных средств.
Межсетевое экранирование.
Системы предотвращения утечки информации.
Протоколирование и аудит

19.3.4 Перечень заданий для контрольных работ

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
Полное соответствие ответа обучающегося всем перечисленным критериям. Обучающийся дал верные ответы не менее чем на 60% вопросов.	*Зачтено*
Обучающийся дал верные ответы менее чем на 60% вопросов.	*Не зачтено*

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.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в форме контрольной работы. Промежуточная аттестация проводится в соответствии с Положением о промежуточной аттестации обучающихся по программам высшего образования.

Промежуточная аттестация по дисциплинам (модулям) 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/)). Промежуточная аттестация обучающихся осуществляется в форме экзамена /зачета с оценкой / зачета (выбрать, что соответствует «Вашей» дисциплине). 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. 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.

Контрольно-измерительные материалы промежуточной аттестации включают в себя практические задания, позволяющие оценить степень сформированности умений и навыков. При оценивании используются качественные шкалы оценок. Критерии оценивания приведены выше.

Комплект КИМ

УТВЕРЖДАЮ
Заведующий кафедрой ИТиММЭ
_____ проф. В.В. Давнис
__.__.20__

Направление подготовки / специальность: 38.03.01 Экономика
Дисциплина: Информационная безопасность цифровой экономики
Форма обучения: Очное
Вид контроля: Зачет
Вид аттестации: промежуточная

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

УТВЕРЖДАЮ
Заведующий кафедрой ИТиММЭ
_____ проф. В.В. Давнис
__.__.20__

Направление подготовки / специальность: 38.03.01 Экономика
Дисциплина: Информационная безопасность цифровой экономики
Форма обучения: Очное
Вид контроля: Зачет
Вид аттестации: промежуточная

Контрольно-измерительный материал № 2

1. Принципы защиты от технической разведки
2. Аутентификация субъектов доступа.
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".

Преподаватель _____ В.В. Коротких

УТВЕРЖДАЮ
Заведующий кафедрой ИТиММЭ
_____ проф. В.В. Давнис
__.__.20__

Направление подготовки / специальность: 38.03.01 Экономика
Дисциплина: Информационная безопасность цифровой экономики
Форма обучения: Очное
Вид контроля: Зачет
Вид аттестации: промежуточная

Контрольно-измерительный материал № 3

1. Шифры на основе SP-сети.
2. Системы предотвращения утечки информации.
3. Используя шифр Виженера, зашифруйте сообщение "Несмотря на широкую распространённость, понятие информации остаётся одним из самых дискуссионных в науке." В качестве ключа используйте слово "защита".

Преподаватель _____ В.В. Коротких

УТВЕРЖДАЮ
Заведующий кафедрой ИТиММЭ
_____ проф. В.В. Давнис
__.__.20__

\

Направление подготовки / специальность: 38.03.01 Экономика
Дисциплина: Информационная безопасность цифровой экономики
Форма обучения: Очное
Вид контроля: Зачет
Вид аттестации: промежуточная

Контрольно-измерительный материал № 4

1. Аутентификация на основе владения.
2. Шифр многоалфавитной замены и его анализ.
3. Используя шифр Виженера, зашифруйте сообщение "Несмотря на широкую распространённость, категория информации остаётся одной из самых дискуссионных в науке." В качестве ключа используйте слово "кино".

Преподаватель _____ В.В. Коротких