

**«Финансовый университет при Правительстве Российской Федерации»
(Финуниверситет)**

Калужский филиал Финуниверситета

Кафедра «Бизнес-информатика и высшая математика»

«УТВЕРЖДАЮ»

**Директор Калужского филиала
Финуниверситета**



В.А. Матчинов **В.А. Матчинов**

«27» июня 2024 г.

А.А. Кучеров

**УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТЬЮ**

Рабочая программа дисциплины

для студентов, обучающихся по направлению подготовки
38.03.05 «Бизнес-информатика»
Образовательная программа
«Цифровая трансформация управления бизнесом»
Очная форма обучения

*Рекомендовано Ученым советом Калужского филиала Финуниверситета
(протокол № 16 от 27 июня 2024 г.)*

*Одобрено кафедрой «Бизнес-информатика и высшая математика»
Калужского филиала Финуниверситета
(протокол № 12 от 27 июня 2024 г.)*


КАЛУГА 2024

Рабочая программа предназначена для преподавания дисциплины «Управление информационной безопасностью» студентам, обучающимся по направлению подготовки 38.03.05 «Бизнес-информатика», образовательная программа «Цифровая трансформация управления бизнесом», по очной форме обучения.

В рабочей программе излагаются планируемые результаты освоения дисциплины, содержание дисциплины, тематика и содержание семинаров и практических занятий, технологии их проведения. Приводится перечень учебно-методического обеспечения для самостоятельной работы обучающихся, фонд оценочных средств для проведения промежуточной аттестации обучающихся, перечень основной и дополнительной литературы, а также ресурсов информационно-телекоммуникационной сети Интернет.

СОГЛАСОВАНО:

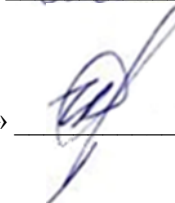
Заместитель директора
по учебно-методической работе
«27» июня 2024 г.

 /Орловцева О.М./

Начальник учебно-методического отдела
«27» июня 2024 г.

 /Толстикова В.С./

Заведующий кафедрой
«Бизнес-информатика и высшая математика»

 /Дробышева И.В./

«27» июня 2024 г.

Содержание

1. Наименование дисциплины⁴
2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения, соотнесённых с планируемыми результатами обучения по дисциплине⁴
3. Место дисциплины в структуре образовательной программы⁵
4. Объем дисциплины в зачётных единицах и в академических часах с выделением объёма аудиторной (лекции, семинары) и самостоятельной работы обучающихся⁵
5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объёмов (в академических часах) и видов учебных занятий⁵
 - 5.1. Содержание дисциплины⁵
 - 5.2. Учебно-тематический план⁶
 - 5.3. Содержание семинаров, практических занятий⁷
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине⁸
 - 6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы⁸
 - 6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю успеваемости⁸
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине⁹
 - 7.1 Перечень компетенций с указанием индикаторов их достижения в процессе освоения дисциплины⁹
 - 7.2 Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний⁹
8. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины¹⁰
9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины¹¹
10. Методические указания для обучающихся по освоению дисциплины¹¹
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем¹¹
 - 11.1 Комплект лицензионного программного обеспечения:¹¹
 - 11.2 Современные профессиональные базы данных и информационные справочные системы:¹¹
 - 11.3 Сертифицированные программные и аппаратные средства защиты информации: не предусмотрены.¹²
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине¹²

1. Наименование дисциплины

«Управление информационной безопасностью».

2. Перечень планируемых результатов освоения образовательной программы (перечень компетенций) с указанием индикаторов их достижения, соотносённых с планируемыми результатами обучения по дисциплине

В результате изучения дисциплины у студентов должны быть сформированы следующие компетенции:

Таблица 1

Код компетенции	Наименование компетенции	Индикаторы достижения компетенции	Результаты обучения (владения, умения и знания), соотносённые с компетенциями/индикаторами достижения компетенции
ПКН-12	Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Знать организацию систем хранения данных и инфраструктурных решений центров обработки данных Уметь проводить анализ рынка вычислительного оборудования
		2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных	Знать состав вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Уметь выбрать вычислительное оборудование, систему хранения данных и инфраструктурных решений центров обработки данных
УК-7	Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда	Знать проблемы, связанные с нарушениями техники безопасности на рабочем месте Уметь выявить проблемы, связанные с нарушениями техники безопасности на рабочем месте
		2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах	Уметь осуществить выполнение мероприятий по защите персонала и вычислительного оборудования

		3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества	Знать ситуации, связанные с безопасностью использования вычислительного оборудования Уметь организовать безопасность использования вычислительного оборудования
		4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания	Уметь действовать в экстремальных ситуациях

3. Место дисциплины в структуре образовательной программы

Дисциплина «Управление информационной безопасностью» относится к дисциплине общепрофессионального цикла, отражающего специфику ВУЗа по направлению подготовки 38.03.05 «Бизнес-информатика», ОП «Цифровая трансформация управления бизнесом».

4. Объем дисциплины в зачётных единицах и в академических часах с выделением объёма аудиторной (лекции, семинары) и самостоятельной работы обучающихся

Таблица 2

Вид учебной работы по дисциплине	Всего (в з/е и часах)	Семестр 2 (в часах)
Общая трудоемкость дисциплины	3 з/е, 108 ч.	108 ч.
Контактная работа – аудиторные занятия	50	50
Лекции	16	16
Семинары, практические занятия	34	34
Самостоятельная работа	58	58
Вид текущего контроля	Контрольная работа	Контрольная работа
Вид промежуточной аттестации	экзамен	экзамен

5. Содержание дисциплины, структурированное по темам (разделам) дисциплины с указанием их объёмов (в академических часах) и видов учебных занятий

5.1. Содержание дисциплины

Тема 1. Основные понятия информационной безопасности

Общие требования к информационной безопасности – аутентичность, доступность, конфиденциальность и целостность. Субъект, объект и право доступа. Виды угроз безопасности – подделка, прерывание, перехват и изменение. Виды вредоносных программ.

Тема 2. Криптографические системы

Формальное определение криптосистемы. Шифрование и дешифрование. Отличие от кодирования и декодирования. Симметричные и асимметричные криптографические системы. Открытый и закрытый ключ. Криптографическая стойкость. Криптоанализ. Имитозащита. Имитоподстановка. Электронная подпись.

Тема 3. Элементарные шифры

Шифры подстановки и шифры перестановки. Классические криптосистемы. Шифр Цезаря. Шифр пар (шифрование простой заменой). Шифр четырех квадратов. Матричный шифр. Шифр ADFGX. Шифр Виженера. Шифр Вермана. Шифрование с использованием аналитических преобразований. Шифрование кодовым словом. Шифрование гаммированием.

5.2. Учебно-тематический план

Таблица 3

№	Наименование тем (разделов) дисциплины	Трудоемкость в часах					Формы текущего контроля успеваемости
		Всего	Аудиторная работа			Самостоятельная работа	
			Общая	Лекции	Семинары, практические занятия		
Тема 1. Основные понятия информационной безопасности							
1	Общие требования к информационной безопасности	11	5	1	4	6	Выполнение и защита практических работ
2	Виды угроз безопасности. Виды вредоносных программ	12	6	2	4	6	Выполнение и защита практических работ
Тема 2. Криптографические системы							
3	Понятие криптографической системы. Симметричные и асимметричные криптографические системы	12	6	2	4	6	Выполнение и защита практических работ
4	Электронная подпись, назначение и реализация	12	6	2	4	6	Выполнение и защита практических работ
Тема 3. Элементарные шифры							

5	Шифр Цезаря. Шифр пар (шифрование простой заменой). Шифр четырех квадратов. Матричный шифр	19	9	3	6	10	Выполнение и защита практических работ
6	Шифр ADFGX. Шифр Виженера. Шифр Вермана	21	9	3	6	12	Выполнение и защита практических работ
7	Шифрование с использованием аналитических преобразований. Шифрование кодовым словом. Шифрование гаммированием	21	9	3	6	12	Выполнение и защита практических работ
В целом по дисциплине		108	50	16	34	58	Контрольная работа

5.3. Содержание семинаров, практических занятий

Таблица 4

Наименование тем (разделов) дисциплины	Перечень вопросов для обсуждения на семинарских, практических занятиях, рекомендуемые источники из разделов 8, 9	Формы проведения занятий
Тема 1. Основные понятия информационной безопасности	<ul style="list-style-type: none"> Изучение угроз безопасности вычислительных систем и способов борьбы с ними. <p>Основная литература: 1,2 Дополнительная литература: 6</p>	Компьютерный практикум
Тема 2. Криптографические системы	<ul style="list-style-type: none"> Изучение основных возможностей криптографических систем. Симметричные и асимметричные системы. Области применения криптографических систем. <p>Основная литература: 1,4 Дополнительная литература: 6</p>	Компьютерный практикум
Тема 3. Элементарные шифры	<ul style="list-style-type: none"> Создание и исследование программных моделей элементарных шифров на языке Python. Исследование их криптостойкости. <p>Основная литература: 1,4 Дополнительная литература: 11</p>	Компьютерный практикум

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Перечень вопросов, отводимых на самостоятельное освоение дисциплины, формы внеаудиторной самостоятельной работы

Таблица 5

Наименование тем (разделов) дисциплины	Перечень вопросов, отводимых на самостоятельное освоение	Формы внеаудиторной самостоятельной работы
Тема 1. Основные понятия информационной безопасности	<ul style="list-style-type: none"> Изучение алгоритмов шифрования AES. 2.8 и алгоритма блочного шифрования ГОСТ 28147-89. <p>Основная литература: 1,4 Дополнительная литература: 6</p>	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной и дополнительной литературы, интернет-источников. Подготовка к практическим работам
Тема 2. Криптографические системы	<ul style="list-style-type: none"> Изучение алгоритма шифрования DES. Создание и исследование программной модели алгоритма DES на языке Python. <p>Основная литература: 1,4 Дополнительная литература: 6</p>	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной и дополнительной литературы, интернет-источников. Подготовка к практическим работам
Тема 3. Элементарные шифры	<ul style="list-style-type: none"> Изучение алгоритма шифрования RSA. Создание и исследование программной модели алгоритма RSA на языке Python. <p>Основная литература: 1,4 Дополнительная литература: 6</p>	Изучение методических материалов по теме в электронном виде и рекомендуемых разделов основной и дополнительной литературы, интернет-источников. Подготовка к практическим работам

6.2. Перечень вопросов, заданий, тем для подготовки к текущему контролю успеваемости

Примерные темы для контрольной работы:

1. Основные требования к безопасности ИС.
2. Основные виды угроз безопасности.
3. Типы вредоносного ПО и способы борьбы с ними.
4. Антивирусные программы, их виды и возможности
5. Списки возможностей и списки контроля доступа в современных операционных системах.
6. Межсетевые экраны, их назначение, виды, возможности.
7. Основные криптографические методы защиты информации.
8. Электронная подпись.
9. Основные технические и программные средства защиты информации.

10. Основные законы, регулирующие порядок работы с конфиденциальной информацией.

Критерии балльной оценки по контрольной работе содержатся в соответствующих методических рекомендациях кафедры.

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием индикаторов их достижения в процессе освоения дисциплины

Перечень компетенций представлен в разделе 2, который характеризует перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.

7.2 Типовые контрольные задания или иные материалы, необходимые для оценки индикаторов достижения компетенций, умений и знаний

Таблица 6

Компетенция	Типовые задания
ПКН-12 Способность применять вычислительное оборудование, системы хранения данных и инфраструктурные решения центров обработки данных	1. Проводит анализ рынка вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Задание 1. Предложите вычислительное оборудование для решения поставленных задач Задание 2. Предложите систем хранения данных для управления знаниями заданного типа
	2. Консультирует по использованию вычислительного оборудования, систем хранения данных и инфраструктурных решений центров обработки данных Задание 1. Выберите модель представления знаний в организации заданного типа Задание 2. Предложите ПО для управления системой хранения данных заданного типа
УК-7 Способность создавать и поддерживать безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, владеть основными методами защиты от возможных последствий аварий, катастроф, стихийных бедствий и военных конфликтов	1. Выявляет и устраняет проблемы, связанные с нарушениями техники безопасности на рабочем месте, обеспечивая безопасные условия труда Задание 1. Найдите уязвимость в ПО организации заданного типа Задание 2. Предложите криптографический метод для устранения уязвимости ПО
	2. Осуществляет выполнение мероприятий по защите населения и территорий в чрезвычайных ситуациях и военных конфликтах Задание 1. Устраните найденную уязвимость в ПО
	3. Находит пути решения ситуаций, связанных с безопасностью жизнедеятельности людей для сохранения природной среды, обеспечения устойчивого развития общества Задание 1. Найдите решение по защите в ситуации

	множественных кибернетических атак на сайт предприятия
	4. Действует в экстремальных и чрезвычайных ситуациях, применяя на практике основные способы выживания

Критерии балльной оценки различных форм текущего контроля успеваемости содержатся в соответствующих методических рекомендациях кафедры.

Примерные вопросы к зачету:

1. Поясните различие понятий информация, данные и знания.
2. Раскройте основные виды угроз безопасности вычислительной системы.
3. Дайте определение криптографической системе.
4. Раскройте отличия симметричных и асимметричных криптографических систем.
5. Раскройте отличия открытого и закрытого ключей криптографической системы.
6. Дайте определение и раскройте назначение хэш-функции.
7. Раскройте назначение и способы формирования электронной подписи. Приведите известные вам алгоритмы шифрования, используемые для формирования цифровой подписи.
8. Опишите организацию шифра Цезаря и шифра простой замены.
9. Опишите организацию шифра 4-х квадратов.
10. Опишите организацию матричного шифра.
11. Опишите организацию алгоритма шифрования RSA.
12. Опишите организацию алгоритма шифрования DES.
13. Опишите организацию алгоритма шифрования AES.
14. Приведите известные вам асимметричные системы шифрования.
15. Приведите известные вам симметричные системы шифрования.

8. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины

Основная литература:

1. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – М.: Издательство Юрайт, 2023. – 277 с. – URL: <https://urait.ru/bcode/531084>
2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. – М.: Издательство Юрайт, 2023. – 107 с. – URL: <https://urait.ru/bcode/530927>
3. Щербак, А. В. Информационная безопасность: учебник для среднего профессионального образования / А. В. Щербак. – М.: Издательство Юрайт, 2023. – 259 с. – URL: <https://urait.ru/bcode/519614>
4. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность: учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. – М.: Издательство Юрайт, 2023. – 473 с. – URL: <https://urait.ru/bcode/511138>

5. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты: учебник для вузов / В. М. Фомичёв, Д. А. Мельников; под редакцией В. М. Фомичёва. – М.: Издательство Юрайт, 2023. – 209 с. – URL: <https://urait.ru/bcode/511700>

Дополнительная литература:

6. Васильева, И. Н. Криптографические методы защиты информации: учебник и практикум для вузов / И. Н. Васильева. – М.: Издательство Юрайт, 2023. – 349 с. – URL: <https://urait.ru/bcode/511890>
7. Иванов, Б. Н. Дискретная математика и теория графов: учебное пособие для вузов / Б. Н. Иванов. – М.: Издательство Юрайт, 2023. – 177 с. – URL: <https://urait.ru/bcode/520078>

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

1. Электронная библиотека Финансового университета <http://elib.fa.ru/>
2. Электронно-библиотечная система BOOK.RU <http://www.book.ru>
3. Электронно-библиотечная система «Университетская библиотека ОН-ЛАЙН» <http://biblioclub.ru/>
4. Электронно-библиотечная система издательства «ЮРАЙТ» <https://www.urait.ru/>
5. Электронно-библиотечная система издательства «Лань» <https://e.lanbook.com/>
6. Деловая онлайн-библиотека «AlpinaDigital» <http://lib.alpinadigital.ru>
7. Электронная библиотека Финансового университета <http://elib.fa.ru>

10. Методические указания для обучающихся по освоению дисциплины

Рекомендации по освоению дисциплины приведены в «Методических рекомендациях для студентов бакалавриата по освоению дисциплин образовательных программ высшего образования», утвержденных приказом № 1040 ректора Финуниверситета от 11 мая 2021 г.

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень необходимого программного обеспечения и информационных справочных систем

11.1 Комплект лицензионного программного обеспечения:

1. Операционная система – Windows 8 или выше, Linux.
2. Среды для разработки приложений на языке Python – Microsoft Visual Studio Code, PyCharm.

11.2 Современные профессиональные базы данных и информационные справочные системы:

№	Название рекомендуемых технических и компьютерных средств обучения	Наименование разделов и тем
1	Правовая база данных «КонсультантПлюс»	Все темы
2	Справочно-правовая система «Гарант»	Все темы
3	www.skrin.ru – Система комплексного раскрытия информации «СКРИН»	Все темы
4	http://www.iteam.ru/publications/strategy – Технологии корпоративного управления	Все темы
5	Информационная система СПАРК	Все темы
6	Информационная система Bloomberg	Все темы
7	Информационная система Thomson Reuters	Все темы
8	https://spravochnick.ru/informacionnye_tehnologii/ – Информационные технологии	Все темы

11.3 Сертифицированные программные и аппаратные средства защиты информации: не предусмотрены.

12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Помещения для проведения лекций, семинарских занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы.