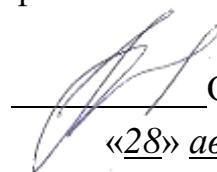


Федеральное государственное образовательное бюджетное  
учреждение высшего образования  
**«Финансовый университет при Правительстве Российской  
Федерации»**  
**(Финансовый университет)**  
**Липецкий филиал Финуниверситета**

УТВЕРЖДАЮ  
Заместитель директора  
по учебно-методической работе  
Липецкого филиала Финуниверситета

 О.Н. Левчegov  
«28» августа 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**«ОП.12 КИБЕРБЕЗОПАСНОСТЬ В СФЕРЕ ФИНАНСОВ»**

по специальности 10.02.04 Обеспечение информационной безопасности  
телекоммуникационных систем

Липецк - 2024

Рабочая программа дисциплины «Кибербезопасность в сфере финансов» разработана на основе федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.04 «Обеспечение информационной безопасности телекоммуникационных систем».

Разработчики:

Якушов Ю.А. старший преподаватель кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Рабочая программа дисциплины рассмотрена и рекомендована к утверждению на заседании кафедры Учет и информационные технологии в бизнесе Липецкого филиала Финуниверситета.

Протокол от 27.08.2024 г. №1

Заведующий кафедрой

Учет и информационные технологии в бизнесе \_\_\_\_\_ Н.С. Морозова

## СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ	13

# 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

## 1.1. Место дисциплины в структуре основной образовательной программы

Дисциплина «Кибербезопасность в сфере финансов» является вариативной частью общепрофессионального учебного цикла основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Дисциплина «Кибербезопасность в сфере финансов» обеспечивает формирование общих компетенций по всем видам деятельности ФГОС специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем. Особое значение дисциплина имеет при формировании и развитии общих компетенций:

Код ОК	Содержание общих компетенций
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.
ОК 09	Пользоваться профессиональной документацией на государственном и иностранном языках.

Рабочая программа дисциплины «Кибербезопасность в сфере финансов» может быть использована в дополнительном профессиональном образовании (в программах повышения квалификации и переподготовки) и профессиональной подготовке по профилю основной профессиональной образовательной программы среднего профессионального образования.

Рабочая программа составлена для очной формы обучения, в том числе с применением элементов дистанционных образовательных технологий и электронного обучения.

При обучении инвалидов и лиц с ограниченными возможностями здоровья дистанционные образовательные технологии и электронное обучение предусматривают возможность приема-передачи информации в доступных для них формах.

## 1.2. Цель и планируемые результаты освоения дисциплины

В рамках программы дисциплины обучающимися осваиваются умения и знания:

Код ОК	Умения	Знания
ОК 01	Умеет обосновать и сформулировать	Знает основы обеспечения
ОК 02	предложения, связанные с совершенствованием	информационной безопасности в
ОК 03	бизнес-процессов по обеспечению	финансовой сфере.
ОК 04	информационной безопасности.	Знает основные положения
ОК 05	Умеет использовать информационные	национальных и международных
ОК 06	технологии в бизнес-процессах.	стандартов и руководств в области
ОК 07	Организует аппаратно-информационное	управления информационными
ОК 09	обеспечение и обеспечение информационной	технологиями и информационной

## 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 2.1. Объем дисциплины и виды учебной работы

Вид учебной работы	Объем в часах
Объем образовательной программы учебной дисциплины	108
Объем работы обучающихся во взаимодействии с преподавателем	72
в том числе:	
теоретические занятия	50
практические занятия и лабораторные работы	22
самостоятельная работа	36
Промежуточная аттестация в форме дифференцированного зачета	

## 2.2. Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем часов	Коды компетенций
1	2	3	4
Введение	<b>Содержание учебного материала</b>		
	Введение в дисциплину. Цели, задачи, структура дисциплины. Организационные и методические основы. Рейтинговая система оценки знаний.	2	ОК 03
<b>Раздел 1. Финансовые технологии в цифровой экономике</b>		<b>34</b>	
Тема 1.1. Особенности информационных взаимодействий в финансовом секторе	<b>Содержание учебного материала</b>		
	Платежные системы. Платежная система Банка России. Электронные средства платежа.	1	ОК 01 - ОК 07 ОК 09
	Эквайринг. Национальная система платежных карт (НПС). Система быстрых платежей (СБП).	1	
	Применение систем искусственного интеллекта в управлении организацией.	2	
	<b>Практические занятия</b>		
	Выполнение онлайн тестов на платформе MOODLE	2	
	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE.	4	
Тема 1.2. Современные финансовые технологии. Цифровая трансформация финансовых услуг	<b>Содержание учебного материала</b>		ОК 01 - ОК 07 ОК 09
	Экономические приложения компьютерных сетей.	1	
	Инструментальные средства автоматизации бухгалтерского учета.	1	
	Комплексная автоматизация управления предприятиями.	1	
	Электронная подпись.	1	
	<b>Практические занятия</b>		
	Выполнение онлайн практических занятий по составлению таблицы «Инструментальные средства автоматизации бухгалтерского учета»	2	
	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
Тема 1.3. Влияние цифровых технологий	<b>Содержание учебного материала</b>		ОК 01 - ОК 07

на развитие банковской сферы	Информационные технологии в банковском секторе	1	ОК 09
	Формирование архитектуры банковских информационных систем (БИС)	1	
	Технология операционного дня для банка.	1	
	Расчетные, депозитные, ссудные операции и формирование отчетных форм в автоматизированной банковской системе.	1	
	Цифровая трансформация банковских технологий.	1	
	Практика применения информационных технологий во внешнеэкономической деятельности Российской Федерации.	1	
	<b>Практические занятия</b>		
	Онлайн тесты на платформе MOODLE	2	
	Семинарское занятие на тему «Применение информационных технологий во внешнеэкономической деятельности Российской Федерации»	2	
	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
<b>Раздел 2. Финансовая кибербезопасность: общие положения</b>		<b>36</b>	ОК 01 - ОК 07 ОК 09
Тема 2.1. Концепция (стратегия) национальной информационной безопасности Российской Федерации. Законодательство в сфере финансовой кибербезопасности	<b>Содержание учебного материала</b>		
	Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».	1	
	«Стандарт Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» СТО БР ИББС-1.0-2014»	1	
	Положение Банка России от 25.07.2022 N 802-П (ред. от 25.07.2022) «О требованиях к защите информации в платежной системе Банка России»	1	
	Положение Банка России от 16.12.2003 N 242-П (ред. от 04.10.2017) «Об организации внутреннего контроля в кредитных организациях и банковских группах»	1	
	<b>Практические занятия</b>		
	Работа с нормативно-правовыми актами в области финансовой кибербезопасности, действующими на территории РФ.	2	

	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
<b>Тема 2.2. Современные угрозы в цифровом секторе</b>	<b>Содержание учебного материала</b>		ОК 01 - ОК 07 ОК 09
	Вредоносное программное обеспечение. Переполнение буфера. Компьютерные вирусы. Черви. Троянский конь (троян). Бот-нет. Спам. Мобильные приложения.	2	
	Новые виды угроз. Атаки Meltdown и Spectre.	2	
	Компьютерные вирусы, искажающие информацию в базе данных.	1	
	Основные угрозы безопасности банковских информационных систем.	1	
	<b>Практические занятия</b>		
	Практическая работа «Основные виды киберугроз и методы обеспечения информационной безопасности»	2	
	Онлайн тесты на платформе MOODLE.	2	
	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
<b>Тема 2.3. Финансовая кибербезопасность в РФ: угрозы и противодействие им</b>	<b>Содержание учебного материала</b>		ОК 01 - ОК 07 ОК 09
	Оценка четкости образов при распознавании лиц в системах безопасности финансово-кредитных организаций.	1	
	Организация противодействия операциям без согласия клиентов в условиях дистанционного банковского обслуживания.	1	
	Обеспечение комплексной безопасности объектов кредитно-финансовой сферы.	1	
	Обнаружение вторжений и реагирование на атаки в информационно-технологическом пространстве финансово-кредитных организаций.	1	
	Защита информации, речевая информация, речевой сигнал, речеподобный сигнал, образный анализ-синтез.	1	
	Графическое моделирование процессов формирования требований к системе защиты информации в финансовых организациях.	1	

	<b>Практические занятия</b>		
	Практическое занятие: Проектирование информационной безопасности на предприятии – профилактические и оперативные меры противодействия киберугрозам.	2	
	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
<b>Раздел 3. Киберпреступность и способы её предотвращения в финансовой сфере</b>		<b>34</b>	OK 01 - OK 07 OK 09
<b>Тема 3.1. Преступления в сфере информационных технологий</b>	<b>Содержание учебного материала</b>		
	Преступления в сфере компьютерной информации.	2	
	Мошенничество с использованием банковских карт.	2	
	Мошенничество и другие преступления в сфере оборота электронных расчетов и платежей.	2	
	<b>Практические занятия</b>		
	Онлайн тестирование на платформе MOODLE	2	
	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
<b>Тема 3.2. Хакеры и проблемы обеспечения финансовой безопасности</b>	<b>Содержание учебного материала</b>		OK 01 - OK 07 OK 09
	Хакеры и иные девианты цифрового мира.	2	
	Организованная преступность цифрового мира.	2	
	Кибертерроризм и киберэкстримизм.	2	
	<b>Практические занятия</b>		
	Онлайн тестирование на платформе MOODLE	2	
	<b>Самостоятельная работа</b>		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
<b>Тема 3.3. Международное сотрудничество в сфере финансовой кибербезопасности</b>	<b>Содержание учебного материала</b>		OK 01 - OK 07 OK 09
	Организационно-правовые проблемы международной информационной безопасности.	2	
	Международные правовые акты в области обеспечения информационной безопасности.	1	
	Зарубежный опыт правового обеспечения информационной безопасности.	1	
	<b>Практические занятия</b>		

	Онлайн тестирование на платформе MOODLE	2	
	Самостоятельная работа		
	Самостоятельное изучение лекций и ресурсов, размещенных в курсе на платформе MOODLE	4	
Промежуточная аттестация в форме дифференцированного зачета		2	
Всего		108	
из них:			
Теоретические занятия		48	
Практические занятия		22	
Самостоятельная работа		36	
Промежуточная аттестация		2	

### **3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ**

#### **3.1. Материально-техническое обеспечение**

1. Учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации  
(Кабинет социально-экономических дисциплин)

Специализированная мебель:

Лекционные парты + скамья – 24 шт.

Стулья – 2 шт.

Стол письменный – 2 шт.

Учебная доска – 1 шт.

Экран настенный – 1 шт.

Технические средства обучения:

Компьютер преподавателя – 1 шт.

Мультимедиа проектор – 1 шт.

Аудиоколонки – 1шт.

#### **2. Компьютерный класс**

Специализированная мебель:

Экран настенный – 1 шт.

Компьютерные столы – 22 шт.

Стол письменный – 12 шт.

Кресло компьютерное – 22 шт.

Стулья – 24 шт.

Шкаф для документов – 1 шт.

Технические средства обучения:

Персональные компьютеры (моноблоки) – 24 шт.

Мультимедиа проектор – 1шт.

Аудиоколонки – 1шт.

3. Учебная аудитория для проведения занятий всех видов, предусмотренных образовательной программой, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации  
(Методический кабинет)

Специализированная мебель:

Компьютерные столы – 20 шт.

Стол письменный – 13 шт.

Кресло компьютерное – 20 шт.

Стулья – 26 шт.

Шкаф для учебно-методических материалов – 6 шт.

Технические средства обучения:

Персональные компьютеры – 18 шт.

Мультимедиа проектор – 1 шт.

Экран настенный – 1 шт.

Аудиоколонки – 1шт.

4. Помещения для самостоятельной работы: Библиотека и читальный зал с выходом в сеть Интернет

Специализированная мебель:

Стол кафедра – 3 шт.

Каталожный ящик – 1 шт.

Шкаф для читательских формуляров – 3 шт.

Витрина для книг – 3 шт.

Стол ученический – 24 шт.

Кресло компьютерное – 2 шт.

Стул - 48 шт.

Стол эргономичный с тумбой – 1 шт.

Шкаф для документов – 3 шт.

Технические средства обучения:

Персональные компьютеры– 18 шт.

## **3.2. Информационное обеспечение реализации программы**

Для реализации программы библиотечный фонд организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

### **3.2.1. Электронные издания (электронные ресурсы):**

1. Воронцова С.В. Обеспечение информационной безопасности в банковской сфере (Законность и правопорядок) : монография / Воронцова С.В. — Москва : КноРус, 2021. — 159 с. — ISBN 978-5-406-08497-7. — URL: <https://book.ru/book/940132> (дата обращения: 09.08.2024). — Текст : электронный.
2. Козьминых С. Информационная безопасность финансово-кредитных организаций в условиях цифровой трансформации экономики : монография / Козьминых С., И. — Москва : КноРус, 2021. — 281 с. — ISBN 978-5-406-08948-4. — URL: <https://book.ru/book/941548> (дата обращения: 09.08.2024). — Текст : электронный.
3. Ивасенко А. Информационные технологии в экономике и управлении : учебное пособие / Ивасенко А., Г., Гридасов А., Ю., Павленко В. А. — Москва : КноРус, 2023. — 154 с. — ISBN 978-5-406-11150-5. — URL: <https://book.ru/book/948685> (дата обращения: 09.08.2024). — Текст : электронный.
4. Рустамова И. Информационные технологии во внешнеэкономической деятельности : учебное пособие / Рустамова И., Т., Курочкин В., А., Рустамов Н. Н. — Москва : Русайнс, 2021. — 87 с. — ISBN 978-5-4365-6600-9. — URL: <https://book.ru/book/939376> (дата обращения: 09.08.2024). — Текст : электронный.
5. Щербак, А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2023. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://ezpro.fa.ru:2058/bcode/519614> (дата обращения: 09.08.2024).
6. Казакова В. Уголовное право Российской Федерации. Общая и Особенная части : учебник / Казакова В., А., Кораблева С., Ю. — Москва : Юстиция, 2023. — 262 с. — ISBN 978-5-406-10426-2. — URL: <https://book.ru/book/945194> (дата обращения: 09.08.2024). — Текст : электронный.
7. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2023. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. —

Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://ezpro.fa.ru:2058/bcode/511239> (дата обращения: 10.08.2024).

8. Овчинский, В. С. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. — Москва : Норма : ИНФРА-М, 2023. — 352 с. - ISBN 978-5-91768-896-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1917647> (дата обращения: 10.08.2024). — Режим доступа: по подписке.

В соответствии со ст. 43 Конституции Российской Федерации, 273-ФЗ «Об образовании в Российской Федерации» от 29.12.2012, приказом Минобрнауки России от 09.11.2015 N 1309 «Об утверждении Порядка обеспечения условий доступности для инвалидов объектов и предоставляемых услуг в сфере образования, а также оказания им при этом необходимой помощи», ГОСТ Р 57723-2017 «Информационно-коммуникационные технологии в образовании. Системы электронно-библиотечные. Общие положения», ГОСТ Р 52872-2019 «Интернет-ресурсы и другая информация, представленная в электронно-цифровой форме. Приложения для стационарных и мобильных устройств, иные пользовательские интерфейсы. Требования доступности для людей с инвалидностью и других лиц с ограничениями жизнедеятельности», все предлагаемые электронные ресурсы максимально комфортны для чтения слабовидящими людьми. Масштабирование текста достигает 300 процентов. При изменении масштаба сохраняется возможность видеть всю страницу текста, не обрезая его.

#### 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения практических занятий и лабораторных работ, тестирования, а также выполнения обучающимися индивидуальных заданий.

<i>Результаты обучения</i>	<i>Критерии оценки</i>	<i>Методы оценки</i>
<b>Знания</b>		
Знание основ обеспечения информационной безопасности в финансовой сфере. Знание основных положений национальных и международных стандартов и руководств в области управления информационными технологиями и информационной безопасностью.	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 06 ОК 07 ОК 09	Оценивание сформированности знаний обучающихся происходит посредством: – Проведения практических работ – Выполнения тестовых заданий – Участия в семинарских занятиях.
<b>Умения</b>		
Умение обосновать и сформулировать предложения, связанные с совершенствованием бизнес-процессов по обеспечению информационной безопасности. Умение использовать информационные технологии в бизнес-процессах. Организация аппаратно-информационное обеспечения и обеспечения информационной безопасности в сфере финансового консультирования. Использование информационных технологий в процессе корпоративного кредитования.	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 06 ОК 07 ОК 09	Оценивание сформированности умений обучающихся происходит посредством: – Проведения практических работ – Выполнения тестовых заданий Участия в семинарских занятиях.