МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ
имени И.Т. ТРУБИЛИНА»

Институт цифровой экономики и инноваций
Цифровая кафедра



УТВЕРЖДЕНО
Директор
Семидоцкий В.А.
Протокол от 04.05.2026 № 24

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

Уровень высшего образования: бакалавриат

Направление подготовки: 38.03.01 Экономика

Направленность (профиль)подготовки: Цифровая экономика

Квалификация (степень) выпускника: Бакалавр

Форма обучения: очная

Год набора (приема на обучение): 2026

Срок получения образования: 4 года

Объем: в зачетных единицах: 2 з.е.
в академических часах: 72 ак.ч.

2026

Разработчики:
Старший преподаватель, кафедра компьютерных технологий и систем Параскевов А.В.

Рабочая программа дисциплины (модуля) составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 38.03.01 Экономика, утвержденного приказом Минобрнауки от 12.08.2020 № 954, с учетом трудовых функций профессиональных стандартов: "Бизнес-аналитик", утвержден приказом Минтруда России от 22.11.2023 № 821н; "Маркетолог", утвержден приказом Минтруда России от 08.11.2023 № 790н; "Экономист предприятия", утвержден приказом Минтруда России от 30.03.2021 № 161н.

Согласование и утверждение

№	Подразделение или коллегиальный орган	Ответственное лицо	ФИО	Виза	Дата, протокол (при наличии)
1	Институт цифровой экономики и инноваций	Председатель методической комиссии/совета	Семидоцкий В.А.	Согласовано	04.05.2026, № 10
2		Руководитель образовательной программы	Семидоцкий В.А.	Согласовано	04.05.2026, № 24

1. Цель и задачи освоения дисциплины (модуля)

Цель освоения дисциплины - формирование у обучаемых знаний в области теоретических основ информационной безопасности, приобретение ими умений и навыков практического обеспечения ее защиты, безопасного использования программных средств в вычислительных систем и сетей.

Задачи изучения дисциплины:

- изучение теоретических основ информационной безопасности;
- понимание необходимости и грамотного применения основ информационной безопасности ;
- отработки умений и навыков эффективного практического использования аспектов обеспечения информационной безопасности при осуществлении профессиональной деятельности.

2. Планируемые результаты обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

Компетенции, индикаторы и результаты обучения

ПК-П4 Способен применять методы обработки и анализа данных, необходимые для решения профессиональных задач, с использованием современных цифровых технологий и интеллектуальных информационно-аналитических систем

ПК-П4.1 Осуществляет выбор решений в области анализа данных, интеллектуальных систем и защиты информации

Знать:

ПК-П4.1/Зн1

ПК-П4.1/Зн2 Основные подходы, методы и принятия решений в области анализа данных, интеллектуальных систем и защиты информации

Уметь:

ПК-П4.1/Ум1 Выбирать решения в области анализа данных, интеллектуальных систем и защиты информации

Владеть:

ПК-П4.1/Нв1 Выбора основных решений в области анализа данных, интеллектуальных систем и защиты информации

ПК-П4.2 Работает с данными, владеет современными инструментами анализа данных, в том числе навыками программирования и алгоритмизации

Знать:

ПК-П4.2/Зн1

ПК-П4.2/Зн2

Уметь:

ПК-П4.2/Ум1 Работать с данными, современными инструментами анализа данных

Владеть:

ПК-П4.2/Нв1 Владеет современными инструментами анализа данных,

ПК-П4.3 Использует технологии машинного обучения в профессиональной деятельности

Знать:

ПК-П4.3/Зн1 Основ разработки и адаптации прикладного программного обеспечения для решения задач в сфере экономики и управления

Уметь:

ПК-П4.3/Ум1 Разрабатывать, внедрять и адаптировать различные виды прикладного программного обеспечения для решения задач экономики и управления

Владеть:

ПК-П4.3/Нв1 Навыками разработки алгоритмов решения прикладных задач в области экономики и управления

3. Место дисциплины в структуре ОП

Дисциплина (модуль) «Информационная безопасность» относится к формируемой участниками образовательных отношений части образовательной программы и изучается в семестре(ах): 6.

В процессе изучения дисциплины студент готовится к решению типов задач профессиональной деятельности, предусмотренных ФГОС ВО и образовательной программой.

4. Объем дисциплины (модуля) и виды учебной работы

Период обучения	Общая трудоемкость (часы)	Общая трудоемкость (ЗЕТ)	Контактная работа (часы, всего)	Внеаудиторная контактная работа (часы)	Зачет (часы)	Лекционные занятия (часы)	Практические занятия (часы)	Самостоятельная работа (часы)	Промежуточная аттестация (часы)
Шестой семестр	72	2	59	1		30	28	13	Зачет
Всего	72	2	59	1		30	28	13	

5. Содержание дисциплины (модуля)

5.1. Разделы, темы дисциплины и виды занятий

(часы промежуточной аттестации не указываются)

Наименование раздела, темы	Всего	Внеаудиторная контактная работа	Лекционные занятия	Практические занятия	Самостоятельная работа	Планируемые результаты обучения, соотнесенные с результатами освоения программы
Раздел 1. Понятие и порядок осуществления комплекса мер обеспечения информационной безопасности	**72**	**1**	**30**	**28**	**13**	ПК-П4.1 ПК-П4.2 ПК-П4.3
Тема 1.1. Объект и предмет информационной безопасности	5		2	2	1	
Тема 1.2. Защита информации от угроз	5		2	2	1	

Тема 1.3. Защита от несанкционированного доступа	10		4	4	2	
Тема 1.4. Компьютерные вирусы	9		4	4	1	
Тема 1.5. Криптографическая защита информации	6		2	2	2	
Тема 1.6. Защита информации в компьютерных сетях	5		2	2	1	
Тема 1.7. Компьютерные системы защиты информации	5		2	2	1	
Тема 1.8. Нормативно-правовые аспекты защиты персональных данных и соблюдение информационной гигиены	9		4	4	1	
Тема 1.9. ФСТЭК	5		2	2	1	
Тема 1.10. Обеспечение безопасности носителей информации	5		2	2	1	
Тема 1.11. Искусственный интеллект	8	1	4	2	1	
Итого	**72**	**1**	**30**	**28**	**13**	

5.2. Содержание разделов, тем дисциплин

Раздел 1. Понятие и порядок осуществления комплекса мер обеспечения информационной безопасности
(Внеаудиторная контактная работа - 1ч.; Лекционные занятия - 30ч.; Практические занятия - 28ч.; Самостоятельная работа - 13ч.)

Тема 1.1. Объект и предмет информационной безопасности
(Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 1ч.)
Определение объекта и предмета информационной безопасности

Тема 1.2. Защита информации от угроз
(Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 1ч.)
Способы и методы защиты информации от угроз

Тема 1.3. Защита от несанкционированного доступа
(Лекционные занятия - 4ч.; Практические занятия - 4ч.; Самостоятельная работа - 2ч.)
Способы защиты информации от несанкционированного доступа

Тема 1.4. Компьютерные вирусы
(Лекционные занятия - 4ч.; Практические занятия - 4ч.; Самостоятельная работа - 1ч.)
Понятие, виды, способы защиты

Тема 1.5. Криптографическая защита информации
(Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 2ч.)
Подходы к криптографической защите информации

Тема 1.6. Защита информации в компьютерных сетях
(Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 1ч.)
Способы и методы защиты информации в компьютерных сетях

Тема 1.7. Компьютерные системы защиты информации
(Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 1ч.)
Понятие, виды, методы защиты

Тема 1.8. Нормативно-правовые аспекты защиты персональных данных и соблюдение информационной гигиены
(Лекционные занятия - 4ч.; Практические занятия - 4ч.; Самостоятельная работа - 1ч.)
Обзор, понятие, санкции

Тема 1.9. ФСТЭК
(Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 1ч.)
Направление деятельности, контрольно-разрешительная деятельность

Тема 1.10. Обеспечение безопасности носителей информации
(Лекционные занятия - 2ч.; Практические занятия - 2ч.; Самостоятельная работа - 1ч.)
Подходы и меры, информационная гигиена

Тема 1.11. Искусственный интеллект
(Внеаудиторная контактная работа - 1ч.; Лекционные занятия - 4ч.; Практические занятия - 2ч.; Самостоятельная работа - 1ч.)
Искусственный интеллект как объект и субъект информационных угроз

6. Оценочные материалы текущего контроля

Раздел 1. Понятие и порядок осуществления комплекса мер обеспечения информационной безопасности

Форма контроля/оценочное средство: Кейс-задание

Вопросы/Задания:

1. Опиши категории персональных данных и уровни их защиты на коммерческом предприятии

Необходимо определить вид деятельности предприятия, провести его категоризацию и определить уровень хранимых персональных данных и мероприятия по их защите в соответствии с законодательством

7. Оценочные материалы промежуточной аттестации

Шестой семестр, Зачет
Контролируемые ИДК: ПК-П4.1 ПК-П4.2 ПК-П4.3
Вопросы/Задания:

1. Концепция информационной безопасности

2. Актуальность проблемы защиты информации

3. Основные нормативные, руководящие и справочные документы

4. Классификация методов защиты информации

5. Классификация средств защиты информации

6. Механизм защиты информации от несанкционированного доступа

7. Защита персональных данных

8. Требования по построению средств защиты информации

9. Криптографические системы защиты информации

10. Методы контроля доступа к ресурсам

11. Журналы доступа

12. Аудит безопасности информационных систем

13. Управление доступом

14. Алгоритмы шифрования

15. Разрушающие программные средства

16. Компьютерные вирусы

17. Электронная цифровая подпись

18. Криптографические преобразования

19. Целостность информации

20. Защита сетевых накопителей

21. Средства анализа программ

22. Защита программного кода от декомпиляции и трассировки

23. Управление доступом пользователей сетевого программного обеспечения

24. Антивирусные системы: понятие и разновидности

25. Группы учетных записей пользователей

26. Защита сетей от проникновения

27. Виды атак на сетевые ресурсы

28. Метод "песочницы"

29. Тестирование уровня защищенности программного обеспечения

30. Криптографическая защита информации

8. Материально-техническое и учебно-методическое обеспечение дисциплины

8.1. Перечень основной и дополнительной учебной литературы

Основная литература

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - 4 - Москва: Издательский Центр РИОР, 2025. - 336 с. - 978-5-16-013849-7. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.ru/cover/2178/2178344.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

2. Клименко, И.С. Информационная безопасность и защита информации: модели и методы управления: Монография / И.С. Клименко. - 1 - Москва: ООО "Научно-издательский центр ИНФРА-М", 2024. - 180 с. - 978-5-16-108124-2. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.com/cover/2052/2052391.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

3. Баланов, А.Н. Комплексная информационная безопасность: полный справочник специалиста: Практическое пособие / А.Н. Баланов. - Вологда: Инфра-Инженерия, 2024. - 156 с. - 978-5-9729-1771-6. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.ru/cover/2169/2169705.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

Дополнительная литература

1. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - 1 - Москва: ООО "Научно-издательский центр ИНФРА-М", 2021. - 118 с. - 978-5-16-108813-5. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.com/cover/1178/1178153.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

2. Партыка, Т. Л. Информационная безопасность: Учебное пособие / Т. Л. Партыка, И.И. Попов.; Российский экономический университет им. Г.В. Плеханова. - 5 - Москва: Издательство "ФОРУМ", 2021. - 432 с. - 978-5-16-013174-0. - Текст: электронный // Общество с ограниченной ответственностью «ЗНАНИУМ»: [сайт]. - URL: https://znanium.com/cover/1189/1189328.jpg (дата обращения: 08.09.2025). - Режим доступа: по подписке

3. Куликов,, С. С. Информационная безопасность локальных компьютерных сетей: практикум / С. С. Куликов,. - Информационная безопасность локальных компьютерных сетей - Воронеж: Воронежский государственный технический университет, ЭБС АСВ, 2021. - 57 с. - 978-5-7731-0969-3. - Текст: электронный // IPR SMART: [сайт]. - URL: https://www.iprbookshop.ru/118614.html (дата обращения: 08.10.2025). - Режим доступа: по подписке

8.2. Профессиональные базы данных и ресурсы «Интернет», к которым обеспечивается доступ обучающихся

Профессиональные базы данных

1. http://www.iprbookshop.ru/ - IPRbook

Ресурсы «Интернет»

1. https://edu.kubsau.ru/ - Образовательный портал КубГАУ

8.3. Программное обеспечение и информационно-справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Информационные технологии, используемые при осуществлении образовательного процесса по дисциплине позволяют:
– обеспечить взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействие посредством сети «Интернет»;
– фиксировать ход образовательного процесса, результатов промежуточной аттестации по дисциплине и результатов освоения образовательной программы;
– организовать процесс образования путем визуализации изучаемой информации посредством использования презентаций, учебных фильмов;
– контролировать результаты обучения на основе компьютерного тестирования.
Перечень лицензионного программного обеспечения:
1 Microsoft Windows - операционная система.
2 Microsoft Office (включает Word, Excel, Power Point) - пакет офисных приложений.
Перечень профессиональных баз данных и информационных справочных систем:
1 Гарант - правовая, https://www.garant.ru/
2 Консультант - правовая, https://www.consultant.ru/
3 Научная электронная библиотека eLibrary - универсальная, https://elibrary.ru/
Доступ к сети Интернет, доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения
(обновление производится по мере появления новых версий программы)
Не используется.

Перечень информационно-справочных систем
(обновление выполняется еженедельно)
Не используется.

8.4. Специальные помещения, лаборатории и лабораторное оборудование

Компьютерный класс
222гл
Интерактивная панель Samsung - 1 шт.
Компьютер персональный Aquarius i5/4Gb/500Gb/21,5" - 1 шт.

9. Методические указания по освоению дисциплины (модуля)

Учебная работа по направлению подготовки осуществляется в форме контактной работы с преподавателем, самостоятельной работы обучающегося, текущей и промежуточной аттестаций, иных формах, предлагаемых университетом. Учебный материал дисциплины структурирован и его изучение проводится в тематической последовательности. Содержание методических указаний должно соответствовать требования ФГОС и учебных программ по дисциплине. Самостоятельная работа студентов по дисциплине может быть выполнена с помощью материалов, расположенных на портале поддержки Moodle.

10. Методические рекомендации по освоению дисциплины (модуля)