УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УНИВЕРСИТЕТ УПРАВЛЕНИЯ «ТИСБИ»

Кафедра информационных технологий

Утверждаю
Зав. кафедрой
О.В.Федорова

Протокол заседания
кафедры № 10
от 06.04.2026

Рабочая программа дисциплины

Наименование дисциплины	Информационная безопасность и этика
Направлению подготовки	09.03.04 «Программная инженерия»
Профиль подготовки	Информационные технологии
Год набора	2026

Составитель:
ст. преподаватель
Ахтямов Р.Р.

Казань

Содержание

1. Цели и задачи учебной дисциплины	3
2. Место дисциплины в структуре ОПОП	3
3. Требования к результатам освоения дисциплины	4
4. Структура и содержание дисциплины	4
4.1 Модульно-тематический план и пояснительная записка с указанием этапов формирования компетенций	5
4.2 Содержание дисциплины по темам (разделам)	8
4.3 Планы практических и семинарских занятий	8
4. 4 Планы практической подготовки/лабораторных занятий	8
5. Учебно-методическое обеспечение самостоятельной работы студентов	10
6. Учебно-методическое и информационное обеспечение дисциплины	12
7. Материально-техническое обеспечение дисциплины	13
8. Оценка компетенций по изучаемой дисциплине	13
Приложение 1. Методические указания для обучающихся по освоению дисциплины	13
Приложение 2. Фонд оценочных средств для проведения текущей и промежуточной аттестации по дисциплине	16

1. Цели и задачи учебной дисциплины

Данная дисциплина относится к обязательной части (Блок 1) учебного плана подготовки бакалавра по направлению 09.03.04 «Программная инженерия».

Цель дисциплины - изучение организационных, технических и правовых методов и средств защиты компьютерной информации, криптосистем, законодательства и стандартов в области проектирования автоматизированных систем обработки информации и управления (АСОИУ).

Задачи дисциплины:

Знать требования информационной безопасности для решения стандартных задач профессиональной деятельности.

Уметь выявлять угрозы информационной безопасности

Владеть основными методами предотвращения угроз информационной безопасности

2. Место дисциплины в структуре ОПОП

Данная дисциплина относится к обязательной части (Блок 1) учебного плана подготовки бакалавра по направлению 09.03.04 «Программная инженерия». До начала изучения дисциплины «Информационная безопасность и этика» у студента должны быть сформированы компоненты компетенций, полученных в результате изучения дисциплин основы операционных систем. Дисциплина находится во взаимосвязи с дисциплинами согласно схеме:

Обеспечивающие учебные дисциплины

↓ ОСНОВЫ ОПЕРАЦИОННЫХ СИСТЕМ

Информационная безопасность и этика

↓ Производственная практика (преддипломная практика)

3. Требования к результатам освоения дисциплины

Дисциплина «Информационная безопасность и этика» участвует в формировании следующих компетенций в соответствии с ФГОС ВО по направлению «Программная инженерия»:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

Индикаторы	**Результаты обучения по дисциплине**
Компетенция ОПК-3	
ОПК-3.1. Решает стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	**ОПК-3.1. З.2.** Знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. **ОПК-3.1. У.2.** Умеет выявлять угрозы информационной безопасности
ОПК-3.2. Применяет навыки подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	**ОПК-3.2. В.2.** Владеет основными методами предотвращения угроз информационной безопасности

4. Структура и содержание дисциплины.

4.1. Модульно-тематический план и пояснительная записка с указанием этапов формирования компетенций

Общая трудоемкость дисциплины составляет 4 зачетные единицы (144 академических часа)

	Модульная разбивка курса				
	Направление Прикладная информатика Дисциплина: информационная безопасность				
Наименование модулей	Количество ауд. Часов		Самостоятельная работа очное	Всего часов	Индикаторы компетенции
	Лекции Очное	Практика Очное			
Модуль 1					

Тема 1. Основы информационной безопасности.	2	2	4	8	ОПК-3.1
Тема 2. Категории атак.	2	2	10	14	
Тема 3. Службы информационной безопасности.	2	2	10	14	ОПК-3.1 ОПК-3.2
Тема 4. Шифрование.	2	2	10	14	
Модуль 2					
Тема 5. Процедурный уровень информационной безопасности.	2		6	8	ОПК-3.1 ОПК-3.2
Тема 6. Идентификация и аутентификация, управление доступом.	2	4	10	16	
Модуль 3					
Тема 7. Межсетевые экраны.	2		8	10	ОПК-3.1 ОПК-3.2
Тема 8. Управление риском.	2		8	10	
Тема 9. Обеспечение информационной безопасности.	2	4	10	16	
Тема 10. Обеспечение сетевой безопасности.	2	4	10	16	
Подготовка к зачету			18	18	
Всего	20	20	104	144	

Пояснительная записка
с этапами формирования компетенций

Данный курс разбит на три логически завершенных и взаимосвязанных между собой модуля, которые охватывают весь материал дисциплины, обеспечивают приобретение образовательных результатов в соответствии с федеральными государственными образовательными стандартами. Порядок освоения модулей выстраивает траекторию и этапы формирования заявленных компетенций (или их составляющих).

Каждый модуль состоит из нескольких тем, содержащих определенный раздел учебного материала, и представляет собой законченный блок информации. По каждой теме в соответствии с учебным планом читаются лекции и проводятся практические занятия. Предусмотрена индивидуальная самостоятельная работа, состоящая из подготовки к разделам, выделенным для самостоятельного изучения, подготовки к практическим занятиям по соответствующим темам с использованием лекционного материала, учебных пособий, учебно-методических комплексов, Internet-ресурсов, а также рекомендованной дополнительной литературы.
После прохождения первого модуля, включающего в себя четыре темы, будут получены следующие образовательные результаты:
Студент должен иметь понятия о основных понятиях о безопасности и основах атак и защиты от них.

Знать - основы защиты компьютерной информации; правовые основы защиты компьютерной информации, организационные, технические программные методы защиты информации , стандарты, модели и методы шифрования, правила работы с конфиденциальной информацией

Уметь - выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.

Владеть- навыками проектирования программ для криптографического шифрования

Уровень освоения полученных знаний и умений проверяется компьютерным тестированием и решением практических задач с

использованием программных средств в соответствии с темами изучаемого модуля.

После прохождения второго модуля, включающего в себя три темы, будут получены следующие образовательные результаты:
Студент должен иметь понятия о: о процедурном уровне информационной безопасности, основах идентификации и аутентификации и основах межсетевых экранов и защиты от рисков и основы защиты сетевой безопасности

Знать - организационные, технические программные методы защиты информации. модели и методы аутентификации пользователей

Уметь - обосновывать организационно-технические мероприятия по защите информации в ИС, выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в ИС.

Владеть- навыками проектирования политик безопасности

Уровень освоения полученных знаний и умений проверяется компьютерным тестированием и решением практических задач с использованием программных средств в соответствии с темами изучаемого модуля.

После прохождения третьего модуля, включающего в себя две темы, будут получены следующие образовательные результаты:
Студент должен иметь понятия о основных понятиях о обеспечении сетевой и информационной безопасности

Знать - Определение риска. Оценка стоимости. Разработка политики. Порядок разработки политик

Уметь выявлять угрозы информационной технической и физической безопасности

Владеть - методами реализации политики безопасности, административной безопасности, технической и физической безопасности.

Данное деление дисциплины на модули активизирует самостоятельную

работу студентов, повышает интенсивность и системность учебной работы, регулирует контроль учебной деятельности студентов в течении семестров, усиливает мотивацию студентов к изучению учебного материала.

Контроль знаний, умений и навыков является неотъемлемой частью процесса освоения учебного материала и включает в себя следующие формы:

- текущий контроль;
- промежуточный контроль.

4.2. Содержание дисциплины по темам (разделам)

Тема 1. Основы информационной безопасности.

Основные понятия информационной безопасности. ФЗ "Об информации, информационных технологиях и о защите информации. Определение безопасности как процесса. О защите государственной тайны.

Тема 2. Категории атак.

Определение атаки доступа. Как выполняются атаки доступа. Информация в электронном виде. Определение атаки модификации. Как выполняются атаки модификации. Определение атак на отказ в обслуживании. Как выполняются атаки на отказ в обслуживании. Определение атаки на отказ от обязательств.

Тема 3. Службы информационной безопасности.

Конфиденциальность. Идентифицируемость.

Тема 4. Шифрование.

Основные концепции шифрования. Шифрование с открытым ключом. Цифровые подписи. Управление ключами. Доверие в информационной системе. Разработка системы шифрования. Шифрование.

Тема 5. Процедурный уровень информационной безопасности.

Основные классы мер процедурного уровня. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ. Основные программно-технические меры

Основные понятия программно-технического уровня информационной безопасности.

Тема 6. Идентификация и аутентификация, управление доступом.

Идентификация и аутентификация. Управление доступом. Ролевое управление доступом.

Тема 7. Межсетевые экраны.

Определение типов межсетевых экранов. Межсетевые экраны прикладного уровня. Межсетевые экраны с пакетной фильтрацией.

Тема 8. Управление риском.

Определение риска. Уязвимость. Угроза. Выявление риска для организации. Исследование контрмер. Оценка риска. Методика оценки риска.

Тема 9. Обеспечение информационной безопасности.

Определение риска. Оценка стоимости. Разработка политики. Порядок разработки политик. Реализация политики безопасности. Проведение профессиональной переподготовки. Проведение аудита.

Тема 10. Обеспечение сетевой безопасности.

Административная безопасность. Планы выхода из критических ситуаций. Техническая безопасность. Физическая безопасность.

4.3. Планы семинарских и практических занятий

1. Изучить симметричные алгоритмы подстановки, перестановки, шифр Кардано
2. Подготовить сообщение и зашифровать его каждым из этих алгоритмов.
3. Изучить симметричные и ассиметричные протоколы взаимной проверки подлинности (с отметками времени и без).
4. Написать программу для проверки аутентификации
5. Разработать презентацию по основам информационной безопасности*

4.4.Планы практической подготовки/лабораторных занятий

Не предусмотрено учебным планом.

5.Учебно-методическое обеспечение самостоятельной работы студентов

В процессе самостоятельного изучения студент обязан проработать перечисленные ниже темы, для углубления теоретических знаний и практических навыков.

Темы для самостоятельного изучения

Тема 1. Критерии и оценки защищенности информационных систем . Руководящие документы Гостехкомиссии РФ. Классификация автоматизированных систем и требования по защите информации. Критерии оценки безопасности компьютерных систем Министерства оборона США.

Тема 2.Организационная защита. Служба информационной безопасности. Политика безопасности. Работа с персоналом. Физическая защита. Защита от несанкционированного доступа. Безопасность операционных систем.

Тема 3. Статистический анализ шифрованного текста. Многоалфавитные системы. Системы одноразового использования. Гаммирование. Алгоритм DES и стандарты шифрования данных. Системы с открытым ключом. Управление ключами. Проблемы и перспективы криптографических систем. Реализация криптографических методов.

Тема 4. Виды аутентификации. Защита паролей административными методами. Криптографические методы аутентификации. Протоколы взаимной проверки подлинности. Протоколы и модели цифровых сигнатур с посредником и без участия посредника.

Тема 5. Правовая защита. Защита конфиденциальной информации. Уголовный кодекс о защите информации.

6. Учебно-методическое и информационное обеспечение

Основная:

1. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — 2-е изд. — Саратов : Вузовское образование, 2024. — 214 c. — ISBN 978-5-4487-1026-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/142805.html — Режим доступа: для авторизир. Пользователей
2. Мельников, А. В. Основы информационной безопасности : учебное пособие / А. В. Мельников, С. В. Зарубин. — Москва : Российский государственный университет правосудия имени В.М. Лебедева, 2025. — 220 с. — ISBN 978-5-00209-188-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/152309.html — Режим доступа: для авторизир. пользователей

Дополнительная

1. Бондаренко И.С. Информационная безопасность [Электронный ресурс]: учебник/ Бондаренко И.С.— Электрон. текстовые данные.— М.: Издательский Дом МИСиС, 2023.— 254 с.— Режим доступа: https://ipr-smart.ru/137525.— IPR SMART, по паролю Лицензия: весь срок охраны авторского права
2. Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128406.html — Режим доступа: для авторизир. Пользователей Гарантированный срок размещения в IPR SMART до 22.03.2028 (автопролонгация)

Интернет-ресурсы и перечень ежегодно обновляемых современных профессиональных баз данных и информационных справочных систем:

1. http://www.iprbookshop.ru Цифровой образовательный ресурс IPR SMART
2. www.securitylab.ru
3. http://citforum.ru/

7. Материально-техническое обеспечение дисциплины

В процессе изучение данной дисциплины используется учебная аудитория, кабинет для самостоятельной работы студентов, читальный зал, видеопроекционное оборудование, компьютер, оснащенный типовым пакетом системного и офисного ПО, в соответствии с Реестром материально-технического обеспечения аудиторного фонда Университета управления «ТИСБИ».

Во время лекций: проектор, экран, компьютер с выходом в интернет
Во время практики: компьютерный класс

1.Типовой пакет системного и офисного ПО, Персональный компьютер с выходом в интернет в компьютерных классах Университета для каждого студента на практических занятиях.
Учебная аудитория в соответствии с расписанием, кабинет для самостоятельной работы студентов.

Пакет лицензионного системного и офисного ПО включает в себя:

- Операционная система Microsoft Windows 10 Pro.
- Microsoft Office 2013.

Программное обеспечение, входящее в типовой установочный пакет, получает обновление в автоматическом, установленном разработчиком (компанией Microsoft) порядке, посредством сети Интернет.

Подтверждающие документы: Microsoft Open License №40962726 от 16.08.2006г., №44971865 от 24.12.2008г., №46256422 от 11.12.2009г., №61280992 от 13.12.2012г.; Акт приема-передачи неисключительного ограниченного права на лицензионное ПО № ПРСЧ-12-04326 от 18.12.2013г., №558 от 18.12.2014г., №ПРСЧ-15-01353 от 10.11.2015г., №272 от 15.04.2016г., бухгалтерск

- Открытая среда разработки программного обеспечения - Lazarus.

8. Оценка компетенций по изучаемой дисциплине

Для оценки результатов обучения рекомендуется использовать модульно-рейтинговую систему оценивания знаний, умений и навыков студентов по окончанию изучения каждого Модуля в соответствии с Положением о модульно-рейтинговой системе организации образовательного процесса. Итоговая оценка (в баллах) складывается из баллов, набранных по каждому Модулю (семестровая оценка) и баллов, набранных, непосредственно на экзамене.
Расчет набранных баллов по дисциплине осуществляется в следующей последовательности:

$C = \frac{M_1 + M_2 + ...M_n}{n} \times 0{,}6$, где М – количество баллов по модулю; n – количество модулей

$З = К \times 0{,}4$, где К - количество баллов на экзамене (зачете);

$И = С + З + П$, где П – поощрительные баллы (от 1 до 5).

Уровень сформированности компетенций и их основные признаки оцениваются по следующим таблицам:

Оценка уровня сформированности компетенции ОПК-3
«Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности» в части дисциплины «Информационная безопасность и этика»

№ п/п	Уровни сформированности компетенции	Основные признаки уровня	Инструменты оценки сформированности уровня
1	**Пороговый уровень (как минимально допустимый)** (обязательный для всех студентов-выпускников вуза по завершении освоения ОПОП ВО) (от 60 до 70 баллов)	Частично знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. Частично умеет выявлять угрозы информационной безопасности Владеет основными методами предотвращения угроз информационной безопасности	Компьютерное тестирование, Решение практических задач Зачет
2	**Базовый уровень (относительно порогового уровня)** **(**От 71 до 85 баллов**)**	Знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. умеет выявлять угрозы информационной безопасности Владеет основными методами предотвращения угроз информационной безопасности	Компьютерное тестирование, Решение практических задач Зачет
3	**Повышенный уровень (относительно порогового уровня)** (От 86 до 100 баллов)	В основном знает требования информационной безопасности для решения стандартных задач профессиональной деятельности. В основном умеет выявлять угрозы информационной безопасности Владеет основными методами предотвращения угроз информационной безопасности	Компьютерное тестирование, Решение практических задач Зачет

Приложение 1

Методические указания для обучающихся по освоению дисциплины.

Самостоятельная работа является важным элементом освоения основной программы курса. В соответствии со спецификой предмета, самостоятельная работа включает в себя:

- подготовку к практическим занятиям по темам;
- самостоятельное изучение материала по заданным преподавателем темам;
- работу с литературой и учебно-методическими пособиями;

Самостоятельная подготовка к практическим занятиям выполняется студентом в свободное от занятий время и включает в себя:

- проработку лекционного материала по указанной теме;
- подготовку к семинарам по темам, предложенным преподавателем;
- предоставление результатов самостоятельной работы преподавателю.