

Федеральное государственное бюджетное образовательное учреждение высшего образования  
«Алтайский государственный технический университет им. И.И. Ползунова»

**СОГЛАСОВАНО**

Декан ФИТ

А.С. Авдеев

## **Рабочая программа дисциплины**

Код и наименование дисциплины: **Б1.О.21 «Информационная безопасность»**

Код и наименование направления подготовки (специальности): **09.03.03**

**Прикладная информатика**

Направленность (профиль, специализация): **Прикладная информатика в экономике**

Статус дисциплины: **обязательная часть**

Форма обучения: **очная**

<b>Статус</b>	<b>Должность</b>	<b>И.О. Фамилия</b>
Разработал	доцент	М.С. Жуковский
Согласовал	Зав. кафедрой «ИСЭ»	А.С. Авдеев
	руководитель направленности (профиля) программы	А.С. Авдеев

г. Барнаул

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Содержание компетенции	Индикатор	Содержание индикатора
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	ОПК-3.1	Использует основы информационной и библиографической культуры при работе с профессиональной информацией
		ОПК-3.2	Применяет информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности
		ОПК-3.3	Учитывает основные требования информационной безопасности при решении стандартных задач профессиональной деятельности
ОПК-4	Способен участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью	ОПК-4.1	Применяет стандарты, нормы, правила, техническую документацию в профессиональной деятельности
		ОПК-4.2	Участствует в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью

## 2. Место дисциплины в структуре образовательной программы

Дисциплины (практики), предшествующие изучению дисциплины, результаты освоения которых необходимы для освоения данной дисциплины.	Архитектура ЭВМ, Вычислительные системы, сети и телекоммуникации
Дисциплины (практики), для которых результаты освоения данной дисциплины будут необходимы, как входные знания, умения и владения для их изучения.	

## 3. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающегося с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающегося

Общий объем дисциплины в з.е. /час: 3 / 108

Форма промежуточной аттестации: Зачет

Форма обучения	Виды занятий, их трудоемкость (час.)				Объем контактной работы обучающегося с преподавателем (час)
	Лекции	Лабораторные работы	Практические занятия	Самостоятельная работа	
очная	16	16	0	76	43

**4. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

**Форма обучения: очная**

**Семестр: 4**

**Лекционные занятия (48ч.)**

**1. Универсальные понятия информационной безопасности {лекция с разбором конкретных ситуаций} (2ч.)[2,5]** Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- доступность;
- целостность;
- конфиденциальность.

**1. Универсальные понятия информационной безопасности {лекция с разбором конкретных ситуаций} (2ч.)[2,5]** Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- доступность;
- целостность;
- конфиденциальность.

**1. Универсальные понятия информационной безопасности {лекция с разбором конкретных ситуаций} (2ч.)[2,5]** Цель мероприятий в области информационной безопасности – защитить интересы субъектов информационных отношений. Интересы эти многообразны, но все они концентрируются вокруг трех основных аспектов:

- доступность;
- целостность;
- конфиденциальность.

**2. Идентификация и аутентификация как базовые конструкции информационной безопасности {анализ казусов} (2ч.)[3,5]** Что такое идентификация, аутентификация, авторизация, какая между ними взаимосвязь и в чем разница? Проблемы безопасности при авторизации.

**2. Идентификация и аутентификация как базовые конструкции информационной безопасности {анализ казусов} (2ч.)[3,5]** Что такое идентификация, аутентификация, авторизация, какая между ними взаимосвязь и в чем разница? Проблемы безопасности при авторизации.

**2. Идентификация и аутентификация как базовые конструкции информационной безопасности {анализ казусов} (2ч.)[3,5]** Что такое идентификация, аутентификация, авторизация, какая между ними взаимосвязь и в чем разница? Проблемы безопасности при авторизации.

**3. Правовые основы информационной безопасности {анализ казусов} (2ч.)[2,6]** Как юридически корректно защищать информационную безопасность в компании

**3. Правовые основы информационной безопасности {анализ казусов} (2ч.)[2,6]** Как юридически корректно защищать информационную безопасность в компании

**3. Правовые основы информационной безопасности {анализ казусов} (2ч.)[2,6]** Как юридически корректно защищать информационную безопасность в компании

**4. Базовые системы сокрытия информации. Методы шифрования и дешифрования. {мини-лекция} (2ч.)[3,5]** Обзор общих методов шифрования. Стеганография. Биометрия.

**4. Базовые системы сокрытия информации. Методы шифрования и дешифрования. {мини-лекция} (2ч.)[3,5]** Обзор общих методов шифрования. Стеганография. Биометрия.

**4. Базовые системы сокрытия информации. Методы шифрования и дешифрования. {мини-лекция} (2ч.)[3,5]** Обзор общих методов шифрования. Стеганография. Биометрия.

**5. Современная криптография. {лекция с разбором конкретных ситуаций} (2ч.)[3,5]** Различие между симметричными и асимметричными системами. Системы RSA, ElGamal, Diffie–Hellman. Математика в основе асимметричных систем

**5. Современная криптография. {лекция с разбором конкретных ситуаций} (2ч.)[3,5]** Различие между симметричными и асимметричными системами. Системы RSA, ElGamal, Diffie–Hellman. Математика в основе асимметричных систем

**5. Современная криптография. {лекция с разбором конкретных ситуаций} (2ч.)[3,5]** Различие между симметричными и асимметричными системами. Системы RSA, ElGamal, Diffie–Hellman. Математика в основе асимметричных систем

**6. Векторы атак на информационную систему. {имитация} (4ч.)[1,2,5]** Вирусы, виды, особенности. Антивирусное ПО. Социальная инженерия. Атаки Man-in the-Middle. Перехват сообщений.

**6. Векторы атак на информационную систему. {имитация} (4ч.)[1,2,5]** Вирусы, виды, особенности. Антивирусное ПО. Социальная инженерия. Атаки Man-in the-Middle. Перехват сообщений.

**6. Векторы атак на информационную систему. {имитация} (4ч.)[1,2,5]** Вирусы, виды, особенности. Антивирусное ПО. Социальная инженерия. Атаки Man-in the-Middle. Перехват сообщений.

**7. Построение политики информационной безопасности. Разбор конкретных**

примеров. {дерево решений} (2ч.)[2,3,5,6]

7. Построение политики информационной безопасности. Разбор конкретных примеров. {дерево решений} (2ч.)[2,3,5,6]

7. Построение политики информационной безопасности. Разбор конкретных примеров. {дерево решений} (2ч.)[2,3,5,6]

#### Лабораторные работы (48ч.)

1. Анонимность в сети {использование общественных ресурсов} (4ч.)[1,2,6]  
Насколько велик объем информации о человеке в свободном доступе?

1. Анонимность в сети {использование общественных ресурсов} (4ч.)[1,2,6]  
Насколько велик объем информации о человеке в свободном доступе?

1. Анонимность в сети {использование общественных ресурсов} (4ч.)[1,2,6]  
Насколько велик объем информации о человеке в свободном доступе?

2. Криптостойкость паролей. {метод кейсов} (2ч.)[1,6]

2. Криптостойкость паролей. {метод кейсов} (2ч.)[1,6]

2. Криптостойкость паролей. {метод кейсов} (2ч.)[1,6]

3. Двухключевые методы шифрования на практике {имитация} (2ч.)[1]

3. Двухключевые методы шифрования на практике {имитация} (2ч.)[1]

3. Двухключевые методы шифрования на практике {имитация} (2ч.)[1]

4. Хакеры и как им противостоять {образовательная игра} (4ч.)[1]

4. Хакеры и как им противостоять {образовательная игра} (4ч.)[1]

4. Хакеры и как им противостоять {образовательная игра} (4ч.)[1]

5. Проверка "проблемности" компании - контрагента {анализ казусов} (2ч.)[1] Что можно выяснить о компании юридически корректными действиями

5. Проверка "проблемности" компании - контрагента {анализ казусов} (2ч.)[1] Что можно выяснить о компании юридически корректными действиями

5. Проверка "проблемности" компании - контрагента {анализ казусов} (2ч.)[1] Что можно выяснить о компании юридически корректными действиями

6. Разработка политики безопасности компании {дискуссия} (2ч.)[2,3,5]

6. Разработка политики безопасности компании {дискуссия} (2ч.)[2,3,5]

6. Разработка политики безопасности компании {дискуссия} (2ч.)[2,3,5]

#### Самостоятельная работа (228ч.)

1. Разбор юридических ситуаций по теме информационной безопасности {ПОПС (позиция, обоснование, пример, следствие) - формула} (15ч.)[5,6]

1. Разбор юридических ситуаций по теме информационной безопасности {ПОПС (позиция, обоснование, пример, следствие) - формула} (15ч.)[5,6]

1. Разбор юридических ситуаций по теме информационной безопасности {ПОПС (позиция, обоснование, пример, следствие) - формула} (15ч.)[5,6]

2. Нестандартные методы шифрования. {метод кейсов} (12ч.)[2]

2. Нестандартные методы шифрования. {метод кейсов} (12ч.)[2]

2. Нестандартные методы шифрования. {метод кейсов} (12ч.)[2]

**3. Разбор политик безопасности {метод кейсов} (24ч.)[5]**

**3. Разбор политик безопасности {метод кейсов} (24ч.)[5]**

**3. Разбор политик безопасности {метод кейсов} (24ч.)[5]**

**4. Сообщение о существенном событии в области ИБ {метод кейсов} (25ч.)[5]**

Подготовка материала для тезисного изложения важных событий за последний семестр

**4. Сообщение о существенном событии в области ИБ {метод кейсов} (25ч.)[5]**

Подготовка материала для тезисного изложения важных событий за последний семестр

**4. Сообщение о существенном событии в области ИБ {метод кейсов} (25ч.)[5]**

Подготовка материала для тезисного изложения важных событий за последний семестр

## **5. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине**

Для каждого обучающегося обеспечен индивидуальный неограниченный доступ к электронно-библиотечным системам: Лань, Университетская библиотека он-лайн, электронной библиотеке АлтГТУ и к электронной информационно-образовательной среде:

1. Жуковский М. С. Методические указания к выполнению лабораторных работ по дисциплине "Информационная безопасность" / М. С. Жуковский ; Алт. гос. техн. ун-т им. И. И. Ползунова. – Барнаул : Изд-во АлтГТУ, 2019. – 34с. Прямая ссылка: [http://elib.altstu.ru/eum/download/ise/Zhukovskiy\\_InfBezLR\\_mu.pdf](http://elib.altstu.ru/eum/download/ise/Zhukovskiy_InfBezLR_mu.pdf)

## **6. Перечень учебной литературы**

### **6.1. Основная литература**

2. Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/86938.html> (дата обращения: 07.12.2020). — Режим доступа: для авторизир. пользователей

3. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере : учебное пособие / А. Е. Фаронов. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 154 с. — ISBN 978-5-4497-0338-5. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: <https://www.iprbookshop.ru/89453.html> (дата обращения: 19.04.2023). — Режим доступа: для авторизир. пользователей

### **6.2. Дополнительная литература**

4. Артемов, А. В. Информационная безопасность : курс лекций / А. В.

Артемов. — Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. — 256 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: <http://www.iprbookshop.ru/33430.html> (дата обращения: 23.12.2020). — Режим доступа: для авторизир. пользователей

## **7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины**

5. <https://www.securitylab.ru/>
5. <https://habr.com/ru/hub/infosecurity/>
6. <https://digital.gov.ru/ru/activity/directions/874/>

## **8. Фонд оценочных материалов для проведения текущего контроля успеваемости и промежуточной аттестации**

Содержание промежуточной аттестации раскрывается в комплекте контролирующих материалов, предназначенных для проверки соответствия уровня подготовки по дисциплине требованиям ФГОС, которые хранятся на кафедре-разработчике РПД в печатном виде и в ЭИОС.

Фонд оценочных материалов (ФОМ) по дисциплине представлен в приложении А.

## **9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем**

Для успешного освоения дисциплины используются ресурсы электронной информационно-образовательной среды, образовательные интернет-порталы, глобальная компьютерная сеть Интернет. В процессе изучения дисциплины происходит интерактивное взаимодействие обучающегося с преподавателем через личный кабинет студента.

<b>№пп</b>	<b>Используемое программное обеспечение</b>
1	LibreOffice
2	Windows
3	Антивирус Kaspersky

<b>№пп</b>	<b>Используемые профессиональные базы данных и информационные справочные системы</b>
1	Бесплатная электронная библиотека онлайн "Единое окно к образовательным ресурсам" для студентов и преподавателей; каталог ссылок на образовательные интернет-ресурсы ( <a href="http://Window.edu.ru">http://Window.edu.ru</a> )
2	Национальная электронная библиотека (НЭБ) — свободный доступ читателей к фондам российских библиотек. Содержит коллекции оцифрованных документов (как открытого доступа, так и ограниченных авторским правом), а также каталог изданий, хранящихся в библиотеках России. ( <a href="http://нэб.рф/">http://нэб.рф/</a> )



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

Наименование специальных помещений и помещений для самостоятельной работы
учебные аудитории для проведения учебных занятий
помещения для самостоятельной работы

Материально-техническое обеспечение и организация образовательного процесса по дисциплине для инвалидов и лиц с ограниченными возможностями здоровья осуществляется в соответствии с «Положением об обучении инвалидов и лиц с ограниченными возможностями здоровья».