

Министерство науки и высшего образования Российской Федерации

ЧИТИНСКИЙ ИНСТИТУТ (ФИЛИАЛ)  
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО  
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»



УТВЕРЖДАЮ  
Первый заместитель директора  
Н.В. Раевский

26 февраля 2025 г.

М.П.

**Рабочая программа дисциплины**  
**Б1.У.10 Информационная безопасность**

Направление подготовки: *38.03.05 Бизнес-информатика*

Направленность (профиль): *Цифровая экономика*

Квалификация выпускника: *бакалавр*

Форма обучения: *очная*

	очная ФО
Курс	2
Семестр	2.1
Лекции (час)	28
Практические (сем., лаб.) занятия (час)	28
Самостоятельная работа, включая подготовку к экзаменам и зачетам (час)	88
Курсовая работа (час)	-
Всего часов	144
Зачет (семестр)	-
Экзамен (семестр)	2.1

Рабочая программа обсуждена и утверждена на заседании кафедры информационных технологий и высшей математики

24 февраля 2025 г. протокол № 6

Зав. кафедрой  
*Л.И. Трухина*  
24 февраля 2025 г.

(подпись)

Рабочая программа согласована:  
Зав. кафедрой информационных технологий и высшей математики

*Л.И. Трухина*  
26 февраля 2025 г.

(подпись)

Чита, 2025

Программа составлена в соответствии с ФГОС ВО по направлению *38.03.05 Бизнес-информатика*

Автор (ы)

К.Т.Н., декан

Е.А. Михайлова

## 1. Цели изучения дисциплины

Целью курса является изучение проблематики информационной безопасности, общей структуры мер законодательного, административного, процедурного и программно-технического характера по обеспечению информационной безопасности, стандартов и спецификаций в области информационной безопасности, а также формирование у студентов теоретических знаний и практических навыков выбора и использования технических и программных средств защиты информации.

## 2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

### Компетенции обучающегося, формируемые в результате освоения дисциплины

<i>Код компетенции по ФГОС ВО</i>	<i>Компетенция</i>
<b>ПК-2</b>	Способен выявлять потребности, оценивать, контролировать, оптимизировать процесс управления информационной безопасностью

### Структура компетенции

<i>Компетенция</i>	<i>Формируемые ЗУНы</i>
ПК-2 Способен выявлять потребности, оценивать, контролировать, оптимизировать процесс управления информационной безопасностью	3. сущность и актуальность проблемы информационной безопасности; концептуальные подходы к обеспечению информационной безопасности; угрозы информации, средства и методы обеспечения информационной безопасности У. ориентироваться в проблемах ИБ, методах и средствах защиты информации Н. теоретическими знаниями о принципах построения безопасных ИС

## 3. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Б1.У.10 «Информационная безопасность» входит в Блок «Б1 дисциплины (модули)»

Весь теоретический материал, перечисленный в программе, излагается на лекциях. Главной задачей практических занятий является формирование и развитие умений и навыков, необходимых для практического применения дисциплины.

При построении курса реализуется принцип преемственности обучения - он опирается на знания, умения и навыки студентов, приобретенные ими на первом, втором и третьем курсах в рамках изучения высшей математики, дискретной математики, теории вероятностей, математической статистики, основ алгоритмизации и языков программирования, баз данных, вычислительных машин, систем и сетей.

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

Общая трудоемкость дисциплины составляет 4 зач. ед., 144 часов.

	Количество
--	------------

Вид учебной работы	часов (очная ФО)
Контактная (аудиторная) работа	
Лекции	28
Практические (сем., лаб.) занятия	28
Самостоятельная работа, включая подготовку к экзаменам и зачетам	88
Всего часов	144

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

### **5.1. Содержание разделов дисциплины**

№ п/п	Раздел и тема дисциплины	Семестр	Лекции	Семинар Лаборат.Пра ктич.	Самостоят. раб.	В интеракти вной форме	Формы текущего контроля успеваемости и
<b>1</b>	<b>Основные составляющие информационной безопасности</b>		<b>4</b>	<b>8</b>	<b>22</b>		<b>Уо, К</b>
1.1	Основные понятия информационной безопасности	2.1	4	8	22		Уо, К
<b>2</b>	<b>Криптографические способы защиты информации</b>		<b>6</b>	<b>12</b>	<b>22</b>		<b>Уо, К</b>
2.1	Криптографические способы защиты информации	2.1	6	12	22		Уо, Л
<b>3</b>	<b>Антивирусная защита</b>		<b>6</b>	<b>4</b>	<b>22</b>		<b>Уо, К</b>
3.1	Антивирусная защита	2.1	6	4	22		Уо, К
<b>4</b>	<b>Сетевая безопасность</b>		<b>12</b>	<b>4</b>	<b>22</b>		<b>Уо, К</b>
4.1	Сетевая безопасность	2.1	12	4	22		Уо, К
	<b>ИТОГО</b>		<b>28</b>	<b>28</b>	<b>88</b>		

**\*Формы текущего контроля успеваемости (оценочные средства):**

**Уо** -устный опрос, собеседование

**КО** -коллоквиум, конференция

**Л** -лабораторная работа

**ДИ** -деловая игра

**СЗ** -ситуационные задания

**К** -контрольные работы

**Т** -тестирование

**РЗ** -решение задач  
**РГ** -расчетно-графическая работа  
**ЭС** -эссе  
**Р** -реферат  
**УИ** -учебное исследование  
**П** -прочие  
**Э** -экзамен  
**З** -зачет  
**КР** -курсовая работа  
**О** -отчет  
**Г** -государственный итоговый экзамен  
**ВКР** -выпускная квалификационная работа  
**По** -письменный опрос

## 5.2. Лекционные занятия, их содержание

№ п/п	Наименование разделов и тем	Содержание
1.	Основные понятия информационной безопасности	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Методы и средства организационно-правовой защиты информации
2.	Основные понятия информационной безопасности	Методы и средства инженерно-технической защиты. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности
3.	Криптографические способы защиты информации	Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка. Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований
4.	Криптографические способы защиты информации	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы
5.	Криптографические способы защиты информации	Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA

6.	Антивирусная защита	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ
7.	Антивирусная защита	Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса
8.	Антивирусная защита	Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы
9.	Сетевая безопасность	Защита информации в локальных сетях. Основы построения локальной компьютерной сети
10.	Сетевая безопасность	Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов
11.	Сетевая безопасность	Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и безопасность сети
12.	Сетевая безопасность	Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS.
13.	Сетевая безопасность	Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана
14.	Сетевая безопасность	Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS

### 5.3. Семинарские, практические, лабораторные занятия, их содержание

№ раздела и темы	Содержание и формы проведения
Раздел 1. Тема 1.	Базовые понятия теории информации
Раздел 1. Тема 1.	Основные понятия информационной безопасности. Классификация угроз
Раздел 1. Тема 1.	Целостность и конфиденциальность. Классификация средств защиты информации
Раздел 1. Тема 1.	Методы и средства инженерно-технической защиты
Раздел 2. Тема 1.	Простые криптосистемы. Шифрование методом замены (подстановки): Одноалфавитная подстановка

Раздел Тема 1.	2.	Простые криптосистемы. Шифрование методом замены (подстановки): Многоалфавитная многоконтурная подстановка
Раздел Тема 1.	2.	Перестановка, усложненная по таблице. Перестановка, усложненная по маршрутам
Раздел Тема 1.	2.	Стандарт шифрования данных RSA
Раздел Тема 1.	2.	Основные приемы криптоанализа при симметричных ключах
Раздел Тема 1.	3.	Защита информации в локальных сетях. Основы построения локальной компьютерной сети. Уровни антивирусной защиты сети
Раздел Тема 1.	4.	Конфигурация межсетевого экрана. Построение набора правил межсетевого экрана для различных типов архитектуры

**6. Фонд оценочных средств для проведения промежуточной аттестации по дисциплине (полный текст приведен в приложении к рабочей программе)**

**6.1. Текущий контроль**

№ п/ п	Этапы формирования компетенций (Тема из рабочей программы дисциплины)	Перечень формируемых компетенций по ФГОС ВО	ЗУНы (З.1...З.п, У.1...У.п, Н.1...Н.п)	Контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы (Наименование оценочного средства)	Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания (по 100-балльной шкале)
1	Основные понятия информационной безопасности			Уо, К	25
2	Криптографические способы защиты информации			Уо, Л	25
3	Антивирусная защита			Уо, К	25
4	Сетевая безопасность			Уо, К	25
5	Итого по текущей аттестации	ПК-2			100
6	Промежуточная аттестация	ПК-2			100

**6.2. Промежуточный контроль (зачет, экзамен)**

Промежуточный контроль проводится в виде Экзамена.

#### ВОПРОСЫ ДЛЯ ПРОВЕРКИ ЗНАНИЙ:

Компетенция: ПК-2 Способен выявлять потребности, оценивать, контролировать, оптимизировать процесс управления информационной безопасностью

Знание: Знать способы и методы выявления потребности, оценки, контроля процесса управления информационной безопасностью

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности.
3. Законодательный уровень информационной безопасности. Российское законодательство в области информационной безопасности
4. Объектно-ориентированный подход к информационной безопасности: основные понятия, достоинства применения.
5. Основные определения и критерии классификации угроз.
6. Угрозы доступности. Основные угрозы целостности. Угрозы конфиденциальности.
7. Административный уровень информационной безопасности. Политика безопасности информационных систем.
8. Процедурный уровень информационной безопасности: классы мер и принципы их реализации.
9. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.
10. Понятие сервиса информационной безопасности. Идентификация и аутентификация.
11. Понятие сервиса информационной безопасности. Управление доступом.
12. Понятие сервиса информационной безопасности. протоколирование и аудит.
13. Понятие сервиса информационной безопасности. управление и анализ защищенности.
14. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.
15. Понятие сервиса информационной безопасности. экранирование и туннелирование.
16. Понятие сервиса информационной безопасности. криптография: шифрование.
17. Понятие сервиса информационной безопасности. криптография: контроль целостности.
18. Криптология: базовые понятия и терминология.
19. Криптографические примитивы и их свойства.
20. Модели основных криптоаналитических атак.
21. Антивирусная защита. История развития вирусов и их классификация. Методы защиты от вредоносных программ.

#### ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ УМЕНИЙ:

Компетенция: ПК-2 Способен выявлять потребности, оценивать, контролировать, оптимизировать процесс управления информационной безопасностью

Умение: Уметь выявлять потребности, оценивать, контролировать, оптимизировать процесс управления информационной безопасностью

Задача № 1. Определите к какому типу по ограничению доступа относится информация, представленная в вашем варианте задания и объясните какие нормативно-правовые документы устанавливают этот статус.



## ТИПОВЫЕ ЗАДАНИЯ ДЛЯ ПРОВЕРКИ НАВЫКОВ:

Компетенция: ПК-2 Способен выявлять потребности, оценивать, контролировать, оптимизировать процесс управления информационной безопасностью

Навык: Владеть навыками выявления потребности, оценки, контроля процесса информационной безопасности

Задание № 1. Проанализировать объект защиты согласно вашему варианту и классифицировать возможные угрозы по источнику и предложить меры и средства нейтрализации наиболее актуальных.

### ОБРАЗЕЦ БИЛЕТА

Министерство науки и высшего образования  
Российской Федерации  
Читинский институт (филиал)  
Федерального государственного бюджетного  
образовательного учреждения  
высшего образования  
«БАЙКАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ  
УНИВЕРСИТЕТ»  
(ЧИ ФГБОУ ВО «БГУ»)

Направление - 38.03.05 Бизнес-  
информатика  
Профиль - Цифровая экономика  
Кафедра информационных  
технологий и высшей математики  
Дисциплина - Информационная  
безопасность

### БИЛЕТ № 1

1. Тест (30 баллов).

2. Определите к какому типу по ограничению доступа относится информация, представленная в вашем варианте задания и объясните какие нормативно-правовые документы устанавливают этот статус. (35 баллов).

3. Проанализировать объект защиты согласно вашему варианту и классифицировать возможные угрозы по источнику и предложить меры и средства нейтрализации наиболее актуальных. (35 баллов).

Составитель \_\_\_\_\_ Е.А. Михайлова  
Заведующий кафедрой \_\_\_\_\_ Л.И. Трухина

### 7. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

#### а) основная литература:

1. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации / Ю.Н. Загинайлов. - М. ; Берлин : Директ-Медиа, 2015. <http://biblioclub.ru/index.php?page=book&id=276557> (10.01.2017)
2. Артемов, А.В. Информационная безопасность : курс лекций / А.В. Артемов ; Межрегиональная академия безопасности и выживания. - Орел : МАБИБ, 2014. <http://biblioclub.ru/index.php?page=book&id=428605> (10.01.2017).
3. Прохорова, О.В. Информационная безопасность и защита информации. - Самара : Самарский государственный архитектурно-строительный университет, 2014. [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=438331> (11.01.2017).
4. Информационная безопасность и защита информации : сборник студенческих работ / отв. ред. А.Ю. Колябин. - М. : Студенческая наука, 2012. <http://biblioclub.ru/index.php?page=book&id=227774> (10.01.2017).
5. Заика, А. Компьютерная безопасность / А. Заика. - М. : Рипол Классик, 2013. <http://biblioclub.ru/index.php?page=book&id=227317> (10.01.2017).

#### **б) дополнительная литература:**

1. Фаронов, А.Е. Основы информационной безопасности при работе на компьютере / А.Е. Фаронов. - М. : Интернет-Университет Информационных Технологий, 2011. <http://biblioclub.ru/index.php?page=book&id=227317> (10.01.2017).
2. Башлы, П.Н. Информационная безопасность : учебно-практическое пособие. - М. : Евразийский открытый институт, 2011. [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=90539> (11.01.2017).
3. Спицын, В.Г. Информационная безопасность вычислительной техники. - Томск : Эль Контент, 2011. [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=208694> (11.01.2017).
4. Сычев, Ю.Н. Основы информационной безопасности : учебно-практическое пособие / Ю.Н. Сычев. - М. : Евразийский открытый институт, 2010. [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=90790> (11.01.2017).

#### **в) интернет-ресурсы:**

1. Лаборатория Касперского [электронный ресурс]: <http://www.kaspersky.ru>
2. Информационная безопасность. Защита информации [электронный ресурс]: <http://all-ib.ru>
3. Information Security / Информационная безопасность. Журнал [электронный ресурс]: <http://www.itsec.ru/main.php>
4. Консультант плюс [электронный ресурс]: <http://www.consultant.ru/online/>

### **8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля), включая профессиональные базы данных и информационно-справочные системы**

Для освоения дисциплины обучающемуся необходимы следующие ресурсы информационно-телекоммуникационной сети «Интернет»:

Сайт ЧИ ФГБОУ ВО «БГУ», адрес доступа: <http://bgu-chita.ru/>, доступ круглосуточный неограниченный;

Цифровой образовательный ресурс IPR SMART – объединяет новейшие информационные технологии и учебную лицензионную литературу, предназначенный для разных направлений подготовки и специальностей. Контент отвечает требованиям стандартов высшего, среднего профессионального и дополнительного образования. Ресурсом обеспечивается круглосуточный полнотекстовый доступ к учебникам, журналам, статьям и другой литературе для всех зарегистрированных пользователей. Адрес доступа: [http://www.iprbookshop.ru](http://www.iprbookshop.ru;);

eLIBRARY.RU – крупнейшая в России электронная библиотека научных публикаций, обладающая богатыми возможностями поиска и анализа научной информации. eLIBRARY.RU является разработчиком российского индекса научного цитирования (РИНЦ). Пользование НЭБ eLibrary общедоступно и бесплатно для всех пользователей. Адрес доступа: [https://www.elibrary.ru](https://www.elibrary.ru;);

Электронный каталог библиотеки дает возможность поиска литературы, имеющейся в фонде библиотеки, обеспечивает полнотекстовый доступ к учебным пособиям, монографиям, статьям преподавателей и обучающихся, учебно-методическим комплексам и выпускным квалификационным работам. Адрес доступа: [http://lib.bgu-chita.ru](http://lib.bgu-chita.ru;);

Электронный ресурс цифровой образовательной среды СПО «PROФобразование». Адрес доступа: [https://profspo.ru](https://profspo.ru;);

Федеральная служба государственной статистики (Росстат). Адрес доступа: <https://rosstat.gov.ru/>;

### **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Изучать дисциплину рекомендуется в соответствии с той последовательностью, которая обозначена в ее содержании. Для успешного освоения курса обучающиеся должны иметь первоначальные знания в области Математики и Информатики и программирования.

На лекциях преподаватель озвучивает тему, знакомит с перечнем литературы по теме, обосновывает место и роль этой темы в данной дисциплине, раскрывает ее практическое значение. В ходе лекций студенту необходимо вести конспект, фиксируя основные понятия и проблемные вопросы.

Лабораторные занятия по своему содержанию связаны с тематикой лекционных занятий. Начинать подготовку к занятию целесообразно с конспекта лекций. Задание на лабораторное занятие сообщается обучающимся до его проведения. На семинаре преподаватель организует обсуждение этой темы, выступая в качестве организатора, консультанта и эксперта учебно-познавательной деятельности обучающегося.

Изучение дисциплины (модуля) включает самостоятельную работу обучающегося.

Основными видами самостоятельной работы студентов с участием преподавателей являются:

- текущие консультации;
- коллоквиум как форма контроля освоения теоретического содержания дисциплин: (в часы консультаций, предусмотренные учебным планом);
- прием и защита лабораторных работ (во время проведения занятий).

Основными видами самостоятельной работы студентов без участия преподавателей являются:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- самостоятельное изучение отдельных тем или вопросов по учебникам или учебным пособиям;
- написание рефератов, докладов;
- подготовка к лабораторным работам;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и др.

#### **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения**

В процессе изучения дисциплины используются как традиционные, так и инновационные технологии, активные и интерактивные методы и формы обучения: лекция, лекция-презентация, лабораторное занятие, самостоятельная работа, консультация, активные и интерактивные методы: разбор конкретных ситуаций, решение ситуационных задач, реферативная работа.

Подход разбора конкретных ситуаций используется во время лекций и анализа результатов выполнения лабораторных работ. Каждая конкретная задача при своем моделировании (исследовании) имеет множество подходов, а это требует разбора и оценки целой совокупности конкретных ситуаций.

#### **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю):**

В учебном процессе используются аудитории для проведения учебных занятий, предусмотренных программой бакалавриата, оснащенные оборудованием и техническими средствами обучения:

учебные аудитории, оснащенные специализированной мебелью, магнитно-маркерной доской, трибуной для выступлений, техническими средствами обучения;

учебные аудитории для групповых и индивидуальных консультаций, оснащенные специализированной мебелью, магнитно-маркерной доской, техническими средствами обучения – ноутбук, проектор;

помещения для самостоятельной работы, оснащенные специализированной мебелью, доской, техническими средствами обучения – мультимедийное оборудование: проектор, компьютерная техника с возможностью подключения к сети Интернет и обеспечением доступа в ЭИОС.

**2025 год набора**