**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ**

Департамент научно-технологической политики и образования
Федеральное государственное бюджетное образовательное учреждение высшего образования
**«КРАСНОЯРСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ»**
Институт экономики и управления АПК

---

Кафедра информационных технологий и математического обеспечения информационных систем

СОГЛАСОВАНО:
Директор института З.Е. Шапорова
«23» марта 2021 г.

УТВЕРЖДАЮ:
Ректор Н.И. Пыжикова
«26» марта 2021 г.



# РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
## Защита информации

ФГОС ВО

Специальность: 38.05.01 Экономическая безопасность
(шифр – название)

Специализация: Экономико-правовое обеспечение экономической безопасности

Курс I

Семестр II

Форма обучения очная

Квалификация выпускника экономист

Красноярск, 2021

Составители: Титовская Н.В., к.т.н., доцент

24 02 2021 г.

Программа разработана в соответствии с ФГОС ВО специальности 38.05.01 «Экономическая безопасность», утвержденному от 16.01.2017 № 20

Программа обсуждена на заседании кафедры информационных технологий и математического обеспечения информационных систем
протокол № 6 « 24» 02 2021 г.

Зав. кафедрой Титовская Н.В., к.т.н., доцент
(ФИО, ученая степень, ученое звание)

« 24» 02 2021 г.

**Лист согласования рабочей программы**

Программа принята методической комиссией института ЭиУАПК
протокол № 7 « 23 » 03 2021 г.

Председатель методической комиссии ИЭиУ АПК Рожкова А.В.
(ФИО, ученая степень, ученое звание)

« 23» 03 2021г.

Заведующий выпускающей кафедры по специальности подготовки
Филимонова Н.Г., д.э.н., профессор
(ФИО, ученая степень, ученое звание)

« 23» 03 2021г.

# Оглавление

# Аннотация

Дисциплина Б1.В.ДВ.03.01 «Защита информации» относится к дисциплинам по выбору вариативной части Блока 1 Дисциплины (модули) студентов по специальности 38.05.01 «Экономическая безопасность» специализация экономико-правовое обеспечение экономической безопасности. Дисциплина реализуется в институте экономики и управления АПК кафедрой информационных систем и математического обеспечения информационных систем.

Дисциплина нацелена на формирование профессиональных компетенций ПК-28, ПК-45.

Содержание дисциплины охватывает круг вопросов, связанных с законодательными, административными, организационными, программно-техническими мерами информационной безопасности, с действующими стандартами в этой области.

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные и практические работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме выполнения и защиты лабораторных работ и промежуточный контроль в форме зачета во 2 семестре.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единиц, 108 часов. Программой дисциплины предусмотрены лекционные (18 часов), лабораторные занятия (18 часа), практических работ (18 часов), СРС (54 часа).

# 1. Требования к дисциплине

## 1.1. Внешние и внутренние требования

Дисциплина Б1.В.ДВ.03.01 «Защита информации» относится к дисциплинам по выбору вариативной части Блока 1 Дисциплины (модули).

Реализация в дисциплине «Защита информации» требований ФГОС ВО, ОПОП ВО и Учебного плана по специальности 38.05.01 «Экономическая безопасность» должна формировать следующие компетенции:

ПК- 28 способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач

ПК- 45 способностью анализировать эмпирическую и научную информацию, отечественный и зарубежный опыт по проблемам обеспечения экономической безопасности.

## 1.2. Место дисциплины в учебном процессе

Предшествующими курсами, на которых непосредственно базируется дисциплина «Защита информации» являются «Информационные системы в экономике», «Информатика».

Содержание дисциплины охватывает круг вопросов, связанных с законодательными, административными, организационными, программно-техническими мерами информационной безопасности, с действующими стандартами в этой области.

Контроль знаний студентов проводится в форме текущей и промежуточной аттестации.

# 2. Цели и задачи дисциплины. Компетенции, формируемые в результате освоения.

**Целью** дисциплины «Защита информации» является заложить терминологический фундамент, научить правильно проводить анализ угроз информационной безопасности, выполнять основные этапы решения задач информационной безопасности, рассмотреть основные методологические принципы теории информационной безопасности, изучить методы и средства обеспечения информационной безопасности, методы нарушения конфиденциальности, целостности и доступности информации.

**Задачи** дисциплины: ознакомление студентов с терминологией информационной безопасности, развитие мышления студентов, изучение методов и средств обеспечения информационной безопасности, обучение определению причин, видов, каналов утечки и искажения информации.

В результате изучения дисциплины студент должен:

***Знать:***

– правовые основы защиты компьютерной информации, математические основы криптографии, организационные, технические и программные методы защиты информации в современных компьютерных системах и сетях, стандарты, модели и методы шифрования, методы идентификации пользователей, методы защиты программ от вирусов, основы

инфраструктуры систем, построенных с с использованием публичных и секретных ключей;

***Уметь:***

– применять известные методы и средства поддержки информационной безопасности в компьютерных системах, проводить сравнительный анализ, выбирать методы и средства, оценивать уровень защиты информационных ресурсов в прикладных системах;

***Владеть:***

– методологией и навыками решения научных и практических задач в области информационной безопасности.

В результате изучения дисциплины «Защита информации» формируются следующие *профессиональные* компетенции выпускника:

ПК- 28 способностью осуществлять сбор, анализ, систематизацию, оценку и интерпретацию данных, необходимых для решения профессиональных задач

ПК- 45 способностью анализировать эмпирическую и научную информацию, отечественный и зарубежный опыт по проблемам обеспечения экономической безопасности.

## 3. Организационно-методические данные дисциплины

Таблица 1

**Распределение трудоемкости дисциплины по видам работ по семестрам**

| Вид учебной работы | Трудоемкость | | |
|---|---|---|---|
| | зач. ед. | час. | по семестрам № 2 |
| **Общая трудоемкость** дисциплины по учебному плану | **3** | **108** | **108** |
| **Контактная работа** | **3** | **54** | **54** |
| в том числе: | | | |
| Лекции (Л) | 0,5 | 18 | 18 |
| Практические занятия (ПЗ) | 0,5 | 18 | 18 |
| Семинары (С) | | | |
| Лабораторные работы (ЛР) | 0,5 | 18 | 18 |
| **Самостоятельная работа** (СРС) | **3** | **54** | **54** |
| в том числе: | | | |
| курсовая работа (проект) | | | |
| самостоятельное изучение тем и разделов | | | 30 |
| контрольные работы | | | |
| реферат | | | |
| самоподготовка к контролю знаний (зачет) | | | 9 |
| подготовка к практическим занятиям | | | 15 |
| др. виды | | | |
| **Вид контроля:** | | | зачет |

## 4. Структура и содержание дисциплины

### 4.1. Структура дисциплины

Таблица 2

**Тематический план**

| № | Раздел дисциплины | Всего часов | В том числе | | | Формы контроля |
|---|---|---|---|---|---|---|
| | | | лекции | Лабораторные, практические занятия | СРС | |
| 1 | Модуль 1. Общие принципы обеспечения защиты информации | 62 | 8 | 24 | 30 | **зачет** |
| 2 | Модуль 2. Криптография и шифрование. | 30 | 8 | 8 | 14 | **зачет** |
| 3 | Модуль 3. Компьютерные вирусы | 16 | 2 | 4 | 10 | **зачет** |
| | Итого | 108 | 18 | 36 | 54 | **зачет** |

### 4.2. Трудоёмкость модулей и модульных единиц дисциплины

Таблица 3

**Трудоемкость модулей и модульных единиц дисциплины**

| Наименование модулей и модульных единиц дисциплины | Всего часов на модуль | Контактная работа | | Внеаудиторная работа (СРС) |
|---|---|---|---|---|
| | | Л | ЛПЗ | |
| **Модуль 1. Общие принципы обеспечения защиты информации** | **62** | **8** | **24** | **30** |
| **Модульная единица 1.1** Общие принципы обеспечения защиты информации | 14 | 2 | 2 | 10 |
| **Модульная единица 1.2** Меры защиты информации при возникновении угроз | 20 | 2 | 8 | 10 |
| **Модульная единица 1.3** Методы ограничения доступа к информационным системам | 28 | 4 | 14 | 10 |
| **Модуль 2. Криптография и шифрование** | **30** | **8** | **8** | **14** |
| **Модульная единица 2.1.** Криптография и шифрование | 30 | 8 | 8 | 14 |
| **Модуль 3. Компьютерные ви-** | 16 | 2 | 4 | 10 |

| Наименование модулей и модульных единиц дисциплины | Всего часов на модуль | Контактная работа | | Внеаудиторная работа (СРС) |
|---|---|---|---|---|
| | | Л | ЛПЗ | |
| **русы** | | | | |
| **Модульная единица 3.1**. Компьютерные вирусы | 16 | 2 | 4 | 10 |
| **ИТОГО** | **108** | **18** | **36** | **54** |

### 4.3. Содержание модулей дисциплины

**Модуль 1. Общие принципы обеспечения защиты информации**

**Модульная единица 1.1 Общие принципы обеспечения защиты информации.** Роль информации в современном мире. Проблема информационной безопасности общества. Составляющие ИБ. Международные стандарты информационного обмена. Задачи защиты информации. Уровни формирования режима ИБ. Задачи, решаемые на каждом уровне. Нормативно-правовые основы ИБ.

**Модульная единица 1.2** Меры защиты информации при возникновении угроз Уровни информационной защиты. Меры обеспечения ИБ на законодательном уровне. Меры обеспечения ИБ на административном уровне. Меры обеспечения ИБ на процедурном уровне. Программно-технический уровень. Методы реализации программно-технического уровня ЗИ ИС. Основные механизмы защиты компьютерных систем.

**Модульная единица 1.3** Методы ограничения доступа к информационным системам

Идентификация и аутентификация. Методы разграничения доступа. Регистрация и аудит.

**Модуль 2. Криптография и шифрование**

**Модульная единица 2.1. Криптография и шифрование.** Понятие криптографии, криптограммы, стойкости криптосистемы. Структура криптосистемы. Классификация систем шифрования данных. Симметричные и асимметричные методы шифрования. Механизм электронной цифровой подписи.

**Модуль 3. Способы защиты от компьютерных вирусов**

**Модульная единица 3.1. Способы защиты от компьютерных вирусов.** Способы защиты от компьютерных вирусов. Вирусы как угроза ИБ. «Вирусоподобные» программы. Антивирусные программы. Профилактика компьютерных вирусов. Использование защищенных систем. Обнаружение неизвестных вирусов.

Таблица 4

**Содержание лекционного курса**

| № п/п | № модуля и модульной единицы дисциплины | № и тема лекции | Вид контрольного мероприятия | Кол-во часов |
|---|---|---|---|---|
| **1.** | **Модуль 1. Общие принципы обеспечения защиты информации** | | | **8** |
| | **Модульная единица 1.1** Общие принципы обеспечения защиты информации | Лекция № 1. Основные положения теории информационной безопасности информационных систем | **зачет** | 2 |
| | **Модульная единица 1.2** Меры защиты информации при возникновении угроз | Лекция № 2. Общие принципы обеспечения защиты информации | **зачет** | 2 |
| | **Модульная единица 1.3** Методы ограничения доступа к информационным системам | Лекция № 3. Идентификация и аутентификация. | **зачет** | 2 |
| | | Лекция № 4. Методы разграничения доступа. Регистрация и аудит. | **зачет** | 2 |
| **2.** | **Модуль 2. Криптография и шифрование** | | **зачет** | **8** |
| | **Модульная единица 2.1. Криптография и шифрование** | Лекция № 5. Понятие криптографии, криптограммы, стойкости криптосистемы. Структура криптосистемы. | **зачет** | 2 |
| | | Лекция № 6. Классификация систем шифрования данных. | **зачет** | 2 |

| № п/п | № модуля и модульной единицы дисциплины | № и тема лекции | Вид контрольного мероприятия | Кол-во часов |
|---|---|---|---|---|
| | | Лекция № 7. Симметричные и асимметричные методы шифрования. | **зачет** | 2 |
| | | Лекция № 8. Механизм электронной цифровой подписи. | **зачет** | 2 |
| 3. | **Модуль 3.** Компьютерные вирусы | | **зачет** | **2** |
| | **Модульная единица 3.1.** Компьютерные вирусы | Лекция № 9. Способы защиты от компьютерных вирусов. | **зачет** | 2 |
| | **Итого** | | **зачет** | **18** |

### 4.4. Лабораторные и практические занятия

Таблица 5

**Содержание занятий и контрольных мероприятий**

| № п/п | № модуля и модульной единицы дисциплины | № и тема практического/лабораторного занятия | Вид контрольного мероприятия | Кол-во часов |
|---|---|---|---|---|
| **1.** | **Модуль 1. Общие принципы обеспечения защиты информации** | | **зачет** | **24** |
| | **Модульная единица 1.1** Общие принципы обеспечения защиты информации | Занятие № 1. Основные положения теории информационной безопасности информационных систем. | Защита лабораторного занятия | 2 |
| | **Модульная единица 2.1** Меры защиты информации при возникновении угроз | Занятие № 4. Общие принципы обеспечения защиты информации. | Защита лабораторного занятия | 2 |
| | | Занятие № 5. Понятие угрозы. | Защита лабораторного занятия | 2 |

| № п/п | № модуля и модульной единицы дисциплины | № и тема практического/лабораторного занятия | Вид контрольного мероприятия | Кол-во часов |
|---|---|---|---|---|
| | | Занятие № 6. Классификация угроз ИБ. | Защита лабораторного занятия | 2 |
| | | Занятие № 7. Стандарты информационной безопасности | Защита лабораторного занятия | 2 |
| | **Модульная единица 1.3** Методы ограничения доступа к информационным системам | Занятие № 8. Идентификация и аутентификация. | Защита лабораторного занятия | 6 |
| | | Занятие № 9. Методы разграничения доступа. | Защита лабораторного занятия | 4 |
| | | Занятие № 10. Регистрация и аудит. | Защита лабораторного занятия | 4 |
| **2.** | **Модуль 2. Криптография и шифрование** | | **зачет** | **8** |
| | **Модульная единица 2.1. Криптография и шифрование** | Занятие № 11. Понятие криптографии, криптограммы, стойкости криптосистемы. Структура криптосистемы. | Защита лабораторного занятия | 2 |
| | | Занятие № 12. Классификация систем шифрования данных. | Защита лабораторного занятия | 2 |
| | | Занятие № 13. Симметричные и асимметричные методы шифрования. | Защита лабораторного занятия | 2 |
| | | Занятие № 14. Механизм электронной цифровой подписи. | Защита лабораторного занятия | 2 |
| 3. | **Модуль . Компьютерные вирусы** | | **зачет** | **4** |
| | **Модульная единица 3.1.** Компьютерные вирусы | Занятие № 15. Классификация вирусов. | Защита лабораторного занятия | 2 |

| № п/п | № модуля и модульной единицы дисциплины | № и тема практического/лабораторного занятия | Вид контрольного мероприятия | Кол-во часов |
|---|---|---|---|---|
| | | Занятие № 16. Способы защиты от компьютерных вирусов. | Защита лабораторного занятия | 2 |
| | **Итого** | | **зачет** | **36** |

## 4.5. Самостоятельное изучение разделов дисциплины и виды самоподготовки к текущему контролю знаний

### *4.5.1. Перечень вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний*

Таблица 6

**Перечень вопросов для самостоятельного изучения и видов самоподготовки к текущему контролю знаний**

| №п/п | № модуля и модульной единицы | Перечень рассматриваемых вопросов для самостоятельного изучения | Кол-во часов |
|---|---|---|---|
| **1.** | **Самостоятельное изучение вопросов разделов, тем:** | | |
| 1.1 | **Модуль 1. Общие принципы обеспечения защиты информации** | | **10** |
| | **1.2.** Меры защиты информации при возникновении угроз | 1. Типовые удаленные атаки и их характеристика. Анализ способов нарушений ИБ. | 10 |
| 1.2. | **Модуль 2. Криптография и шифрование** | | **20** |
| | Модульная единица 2.1 Криптография и шифрование | 1. Алгоритмы симметричного шифрования. | 10 |
| | | 2. Стандарт криптографической защиты 21 века(AES). Структура шифра | 10 |
| **2.** | Самоподготовка к контролю знаний (зачет) | | **9** |
| **3.** | Подготовка к практическим занятиям | | **15** |
| | **Итого** | | **54** |

### 4.5.2. Курсовые проекты (работы)/ контрольные работы/ расчетно-графические работы/ учебно-исследовательские работы

Учебной программной не предусмотрено

## 5. Взаимосвязь видов учебных занятий

Таблица 8

**Взаимосвязь компетенций с учебным материалом и контролем знаний студентов**

| Компетенции | Лекции | ЛПЗ | СРС | Вид контроля |
|---|---|---|---|---|
| ПК-28 | Л 1-8 | ЛПЗ 1-16 | М 1,2,3 | Защита лабораторного занятия, зачет |
| ПК-45 | Л 1-8 | ЛПЗ 1-16 | М 1,2,3 | Защита лабораторного занятия, зачет |

## 6. Учебно-методическое и информационное обеспечение дисциплины

### 6.1. Основная литература

1. В. В. Трофимов [и др.] Информатика. Т1, Т. 2. -Москва : Юрайт, 2016;
2. Казарин, О В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов ЭБС Юрайт, 2019;
3. П. Жук и др.Защита информации М.: Инфра-М,2013;
4. С. К. Варлатая, М. В. Шаханова Защита и обработка конфиденциальных документов Москва : Проспект,2015;

### 6.2. Дополнительная литература

5. М. В. Шаханова Современные технологии информационной безопасности Москва : Проспект, 2015 .
6. Щеглов, А. Ю. Защита информации: основы теории : учебник для бакалавриата и магистратуры. ЭБС Юрайт, 2019;
7. Запечников, С. В. Криптографические методы защиты информации : учебник для академического бакалавриата. ЭБС Юрайт, 2019.

### 6.3. Методические указания, рекомендации и другие материалы к занятиям

На лабораторных занятиях (в соответствии с изучаемом разделом) выполняются упражнения, которые проводятся под руководством преподавателя. Упражнения могут выполняться индивидуально либо группами.

### 6.4. Программное обеспечение

Операционная система Windows (академическая лицензия № 44937729 от 15.12.2008).

Офисный пакет приложений MicrosoftOffice (академическая лицензия № 44937729 от 15.12.2008).

Программа для создания и просмотра электронных публикаций в формате PDFAcrobatProfessional (образовательная лицензия № CE0806966 от 27.06.2008).

Антивирусное программное обеспечение KasperskyEndpointSecurity (лицензия № 1800-191210-144044-563-2513 от 10.12.2019).

Система дистанционного образования «Moodle 3.5.6a» (бесплатно распространяемое ПО)

**6.5. Информационно-телекоммуникационные ресурсы сети ИНТЕРНЕТ**

*Электронные библиотечные системы:*

1. Электронная библиотечная система «Лань» e.lanbook.com (договор № 22-2-19 от 08.07.19)
2. Электронная библиотечная система «Юрайт» https://urait.ru/ (договор № 2/5-20)
3. Национальная электронная библиотека (Договор №101 / НЭБ / 2276 от 06.06.17)

*Электронные библиотеки*

4. Научная электронная библиотека eLIBRARY.RU elibrary.ru
5. Научная библиотека Красноярского ГАУ www.kgau.ru/new/biblioteka Ирбис 64) (web версия) договор сотрудничества от 2019 г.).

*Информационные справочные системы*

6. Информационно-правовая система система «КонсультантПлюс» http://www.consultant.ru (договор сотрудничества №20175200206 от 01.06.16).
7. Информационно-правовой портал «Гарант»: http://www.garant.ru

*Научные базы данных и профессиональные сайты*

*8.* Русскоязычный сайт международного издательства Elsevier www.elsevierscience.ru (Списки журналов Scopus, Списки журналов ScienceDirect )

*9. Научные базы данных и профессиональные сайты*

«Мегаэнциклопедия Кирилла и Мефодия», - Раздел «Техника / Компьютеры и Интернет» – Режим доступа: https://megabook.ru/

*10 Информационно - поисковые системы:*

- Google – Режим доступа: http://www.google.com
- Yandex – Режим доступа: http://www.yandex.ru
- Rambler – Режим доступа: http://www.rambler.ru

Таблица

**КАРТА ОБЕСПЕЧЕННОСТИ ЛИТЕРАТУРОЙ**

Кафедра ИТМОИС
Специальность 38.05.01 Экономическая безопасность
Дисциплина Защита информации
Количество студентов 25 чел очная форма обучения
Общая трудоемкость дисциплины : лекции __ час.; лабораторные работы ___час.; СРС __ час.; зачет

| Вид занятий | Наименование | Авторы | Издательство | Год издания | Вид издания | | Место хранения | | Необходимое количество экз. | Количество экз. в вузе |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Печ. | Электр. | Библ. | Каф. | | |
| 1 | 2 | 3 | 4 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Л, ЛЗ, СРС | Информатика : в 2 томах : учебник для академического бакалавриата : Т. 1. - 2016. - 552, [1] с. | В. В. Трофимов | Москва : Юрайт | 2016 | + | | + | | | 50 |
| Л, ЛЗ, СРС | Информатика : в 2 томах : учебник для академического бакалавриата : Т. 2. - 2016. - 406с. | В. В. Трофимов | Москва : Юрайт | 2016 | + | | + | | | 50 |
| Л, ЛЗ, СРС | Защита информации | А.П. Жук | М. : Риор : ИНФРА-М | 2013 | + | | | | | 25 |
| | Защита и обработка конфиденциальных документов | С. К. Варлатая, М. В. Шаханова | Москва : Проспект | 2015 | + | | + | | | 1 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Защита информационных процессов в компьютерных сетях | С. К. Варлатая, М. В. Шаханова | Москва : Проспект | 2015 | + | | + | | | 1 |
| | Современные технологии информационной безопасности | М. В. Шаханова | Москва : Проспект | 2015 | + | | + | | | 1 |
| Л, ЛЗ, СРС | Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов | О В. Казарин | М.:Юрайт | 2019 | | + | + | | | http://www.biblio-online.ru/bcode/437163 |
| Л, ЛЗ, СРС | Защита информации: основы теории: учебник для бакалавриата и магистратуры | А. Ю Щеглов | М.: Юрайт | 2019 | | + | + | | | http://www.biblio-online.ru/bcode/433715 |
| Л, ЛЗ, СРС | Криптографические методы защиты информации : учебник для академического бакалавриата | С. В. Запечников | М.:Юрайт | 2019 | | + | + | | | http://www.biblio-online.ru/bcode/433133 |

Зав. библиотекой_____Зорина Р.А.

Председатель МК_____Белова Л.А.
института

Зав. кафедрой_____Титовская Н.В.

## 7. Критерии оценки знаний, умений, навыков и заявленных компетенций

### 7.1. Текущая аттестация

***Текущая аттестация*** студентов производится в дискретные временные интервалы преподавателем, ведущим лекционные и практические занятия по дисциплине в следующих формах:

- посещение лекций 0,5 баллов
- выполнение лабораторного задания 1 балл
- опрос/проверочная работа 1 балла.

Оценка знаний студентов

| Количество модулей | Максимальная сумма баллов | Оценка | | |
|---|---|---|---|---|
| | | удовлетворительно | хорошо | отлично |
| 3 | 100 | 60-72 | 73-86 | 87-100 |

### 7.2 Рейтинг – план дисциплины «Защита информации»

| | Модули | Часы | Баллы |
|---|---|---|---|
| 1 | Модуль 1 | 62 | 33 |
| 2 | Модуль 2 | 30 | 17,5 |
| 3 | Модуль 3 | 16 | 9,5 |
| | **зачет** | | 40 |
| | **Итого** | **78** | **100** |

Рейтинг план

| Модуль | Максимально возможный балл по видам работ | | | **зачет** | ИТОГО: |
|---|---|---|---|---|---|
| | Текущая работа | | | | |
| | Лекции | Выполнение ПЗ | Опрос | | |
| М1 | 4 | 24 | 5 | | 33 |
| М2 | 4 | 8 | 5,5 | | 17,5 |
| М3 | 0,5 | 4 | 5 | | 9,5 |
| **зачет** | | | | 40 | 40 |
| ИТОГ: | 8,5 | 36 | 15,5 | 40 | 100 |

Студент, не набравший 60 баллов (минимальное количество) приходит на пересдачу в соответствии с графиком ликвидации задолженностей http://www.kgau.ru/new/news/news/2017/grafik_lz.pdf.

### 7.3. Промежуточный контроль

***Промежуточный контроль*** по результатам 2 семестра по дисциплине проходит в форме зачета.

Для допуска к промежуточному контролю по итогам текущей аттестации студент должен набрать необходимое количество баллов– **40-60** баллов.

Критерии оценивания:

Студент, давший правильные ответы 85-100%, получает максимальное количество баллов-40 б.

Студент, давший правильные ответы в пределах 70-84%, получает 15 баллов.

Студент, давший правильные ответы в пределах 60-69%, получает10 баллов

Итоговая оценка выводится суммированием баллов, полученных на текущей аттестации и зачете.

60 – 73 – минимальное количество баллов – оценка «удовлетворительно».

74 – 86 – среднее количество баллов – оценка «хорошо».

87 – 100 – максимальное количество баллов – оценка «отлично».

Студенту, не набравшему 60 баллов (минимальное количество), дается две недели для набора необходимых баллов.

Минимальные требования для ликвидации текущих задолженностей: обязательное выполнение всех лабораторных работ и компьютерное тестирование, по темам пропущенных занятий, с использованием электронного обучающего курса по дисциплине «Экономическая информатика» (на платформе LMS Moodle)/, Режим доступа: https://e.kgau.ru/

**Вопросы для зачета:**

1. Понятие информационной безопасности. Вопросы информационной безопасности в системе обеспечения национальной безопасности.
2. Основные составляющие и аспекты информационной безопасности.
3. Классификация угроз информационной безопасности: для личности, для общества, для государства.
4. Понятие информационной войны. Особенности информационной войны. Понятие информационного превосходства.
5. Концепция «информационной войны» по оценкам российских спецслужб.
6. Понятие информационного оружия. Что отличает информационное оружие от обычных средств поражения?
7. Сфера применения информационного оружия.
8. Особенности информационного оружия. Организация защиты.
9. Основные задачи в сфере обеспечения информационной безопасности.
10. Отечественные стандарты в области информационной безопасности
11. Зарубежные стандарты в области информационной безопасности

12. Понятие защиты информации. Какая система считается безопасной? Какая система считается надёжной?

13. Основные критерии оценки надежности: политика безопасности и гарантированность.

14. Понятие государственной тайны, профессиональной тайны.

15. Понятие коммерческой, елужебной тайны, банковской тайны.

16. Основные конституционные гарантии по охране и защите прав и свобод в информационной сфере.

17. Понятие надежности информации в автоматизированных системах обработки данных. Что понимается под системной защитой информации.

18. Уязвимость информации в автоматизированных системах обработки данных.

19. Элементы и объекты защиты в автоматизированных системах обработки данных.

20. Методы защиты информации от преднамеренного доступа.

21. Защита информации от исследования и копирования.

22. Опознавание с использованием простого пароля. Метод обратимого шифрования.

23. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.

24. Использование динамически изменяющегося пароля. Метод «запрос-ответ»

25. Использование динамически изменяющегося пароля. Функциональные методы

26. Криптографические методы защиты информации в автоматизированных системах. Основные направления использования криптографических методов. Симметричные криптосистемы. Системы с открытым ключом.

27. Электронная (цифровая) подпись. Цели применения.

28. Понятие криптостойкости шифра. Требования к криптографическим системам защиты информации.

29. Классификация методов криптографического закрытия.

30. Особенности защиты информации в персональных ЭВМ. Основные цели защиты информации.

31. Угрозы информации в персональных ЭВМ.

32. Обеспечение целостности информации в ПК. Физическая зашита ПК и носителей информации.

33. Защита ПК от несанкционированного доступа.

34. Способы опознавания (аутентификации) пользователей и используемых компонентов обработки информации. Дать краткую характеристику.

35. Классификация закладок. Причины защиты ПК от закладок. Аппаратные закладки.

36. Программные закладки. Классификация критериев вредоносного воздействия закладок.

37. Общие характеристики закладок.

38. Методы и средства защиты от закладок.

39. Компьютерный вирус. Какая программа считается зараженной.
40. По каким признакам классифицируются вирусы?
41. Способы заражения программ. Стандартные методы заражения.
42. Как работает вирус?
43. Методы защиты от вирусов.
44. Антивирусные программы. Программы-детекторы. Программы-доктора.
45. Антивирусы-полифаги. Эвристические анализаторы.
46. Программы-ревизоры. Программы-фильтры.
47. Цели, функции и задачи защиты информации в сетях ЭВМ. Угрозы безопасности для сетей передачи данных.
48. В чём заключаются задачи защиты в сетях передачи данных?
49. Проблемы защиты информации в вычислительных сетях.
50. Понятие сервисов безопасности: идентификация / аутентификация, разграничение доступа.
51. Понятие сервисов безопасности: шифрование, контроль целостности, контроль защищённости, обнаружение отказов и оперативное восстановление.
52. Архитектура механизмов защиты информации в сетях ЭВМ.

## 8. Материально-техническое обеспечение дисциплины

Материально-техническое обеспечение включает аудиторный фонд Университета:

| Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, | Адрес (местоположение) помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом |
|---|---|
| Ауд. 1-19 компьютерный класс – учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации: рабочие места преподавателя и студентов, укомплектованные специализированной мебелью, аудиторная доска, общая локальная компьютерная сеть Internet, 14 компьютеров на базе процессора Core 2 Duo в комплектации с монитором Samsung и др. внешними периферийными устройствами. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий. Комплект мультимедийного оборудования: ноутбук Acer Aspire 5, переносной экран на треноге Medium Professional, | 660130, Красноярский край, г. Красноярск ул. Е. Стасовой 44И |
| Помещения для самостоятельной работы<br>Ауд.3-13: рабочие места студентов, укомплектованные специализированной мебелью, общая локальная компьютерная сеть Internet, 11 компьютеров на базе процессора IntelCeleron в комплектации с мониторами Samsung, LG, Aser, Viewsonic и др. внешними периферийными устройствами<br>Ауд. 1-06. (научная библиотека КрасГАУ) 16 посадочных мест: рабочие места студентов, укомплектованные специализированной мебелью, Гигабитный интернет, 8 компьютеров на базе процессора IntelCorei3 в комплектации с монитором | 660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44и |

| | |
|---|---|
| Samsung и др. внешними периферийными устройствами, мультимедийный проектор Panasonic, экран, МФУ LaserJetM1212.<br>Ауд. 2-06 (научная библиотека КрасГАУ): 51 посадочное место: рабочие места студентов, укомплектованные специализированной мебелью, Гигабитный интернет, Wi-fi, 2 компьютера на базе процессора IntelCorei3 в комплектации с монитором Samsung и др. внешними периферийными устройствами, мультимедийный проектор AcerX 1260P, экран, телевизор Samsung | 660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44г<br><br>660130, Красноярский край, г. Красноярск, ул. Елены Стасовой, 44г |

## 9. Методические рекомендации для обучающихся по освоению дисциплины

Цель обучения достигается сочетанием применения классических и инновационных педагогических технологий.

При проведении лекционных занятий применяются такие формы обучения как лекция-визуализация, сопровождая изложение теоретического материала презентациями.

В соответствии со спецификой ВУЗа в процессе преподавания дисциплины в каждом разделе выделяются наиболее важные темы, которые рассматриваются на конкретных примерах.

Основной упор в методике проведения практических занятий сделан на отработке и закреплении учебного материала в процессе выполнения заданий с применением ПЭВМ в компьютерном классе. Особое внимание при этом уделено применению элементов проблемного и контекстного обучения, опережающей самостоятельной работе студентов.

Текущий контроль усвоения знаний осуществляется путем выполнения, подготовки и сдачи отчетов по итогам выполнения лабораторных работ, опросов, проверки выполнения различных учебных задач и тестов на практических занятиях.

На изучение дисциплины отводятся один семестр. Итоговая отчетность по дисциплине – зачет.

## 10. Образовательные технологии

Таблица 10

| Название раздела дисциплины или отдельных тем | Вид занятия | Используемые образовательные технологии | Часы |
|---|---|---|---|
| Модуль 1<br>Модуль 2 | Л ЛЗ ПЗ | Информационно-коммуникационная технология | 32<br>16 |
| Модуль 3 | Л ЛЗ ПЗ | Проблемное обучение | 6 |
| Интерактивные технологии (15 т.е.) | ЛЗ ПЗ | Круглый стол, дискуссии | 12 |
| | | Итого | 54 |

**РЕЦЕНЗИЯ**

**на рабочую программу по дисциплине «Защита информации»**

для подготовки по специальности

38.05.01 «Экономическая безопасность»

специализация экономико- правовое обеспечение экономической безопасности

Дисциплина «Защита информации» относится к вариативному блоку дисциплин по выбору. Дисциплина реализуется в институте Экономики и управления АПК кафедрой Информационных технологий и математического обеспечения информационных систем.

Содержание дисциплины охватывает круг вопросов, связанных с связанных с законодательными, административными, организационными, программно-техническими мерами информационной безопасности, с действующими стандартами в этой области..

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные и практические работы, самостоятельная работа студента.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости в форме опроса, выполнения заданий лабораторных работ и промежуточная аттестация в форме зачета.

Общая трудоемкость освоения дисциплины составляет 3 зачетные единицы, 108 часов.

В целом рабочая программа соответствует требованиям ФГОС ВО. Содержательная часть модульных единиц каждого модуля сформирована конкретно и четко, подробно указаны темы занятий и виды контрольных мероприятий. Предложенное программное обеспечение включает актуальные и востребованные современные программы по тематике дисциплины.

На основании вышеизложенного, считаю возможным рекомендовать рабочую программу по дисциплине «Защита информации» к использованию в учебном процессе института Экономики и управления АПК по специальности «Экономическая безопасность» специализация экономико-правовое обеспечение экономической безопасности.

Директор НОЦ ИКИВТ
Сибирского государственного университета
науки и технологий им. М.Ф. Решетнёва
доктор физико-математических наук, профессор
Кузнецов А.А.

«24» 02 2017г.