Министерство науки и высшего образования Российской Федерации

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Врио ректора
«Курганский государственный университет»
_____ / Н.В.Дубив /
«30» сентября 2019 г.

Рабочая программа учебной дисциплины

# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

образовательной программы высшего образования –
программы бакалавриата

**38.03.01 Экономика**

Направленность: Бухгалтерский учет, анализ и аудит
Финансы и кредит

Форма обучения: очная, очно-заочная, заочная

Курган 2019

Рабочая программа дисциплины «Информационная безопасность» составлена в соответствии с учебным планом по программе бакалавриата «Экономика» («Бухгалтерский учет, анализ и аудит», «Финансы и кредит»), утвержденными:
- для очной формы обучения «29» августа 2019 года
- для очно-заочной формы обучения «29» августа 2019 года
- для заочной «29» августа 2019 года

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 28 сентября 2019 года, протокол № 2.

Рабочую программу составил:
ст. преподаватель А.В. Человечкова

Согласовано:

Заведующий кафедрой «БИАС»
канд. пед. наук, доцент Е.Н. Полякова

Заведующий кафедрой «Учет и внешнеэкономическая деятельность»
к.э.н., доцент Н.Н. Зотова

Заведующий кафедрой «Финансы и экономическая безопасность»
к.э.н., доцент Н.Я. Чепелюк

Специалист по учебно-методической работе Учебно-методического отдела Г.В. Казанкова

Начальник управления образовательной деятельности С.Н. Синицын

## 1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

### Очная форма обучения

| Вид учебной работы | На всю дисциплину | Семестр |
|---|---|---|
| | | 3 |
| **Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:** | **40** | **40** |
| Лекции | 16 | 16 |
| Лабораторные работы | - | - |
| Практические занятия | 24 | 24 |
| Аудиторные занятия в интерактивной форме, часов | - | - |
| **Самостоятельная работа, всего часов в том числе:** | **68** | **68** |
| Подготовка к зачету | 18 | 18 |
| Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю) | 50 | 50 |
| **Вид промежуточной аттестации** | **зачет** | **зачет** |
| **Общая трудоемкость дисциплины и трудоемкость по семестрам, часов** | **108** | **108** |

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

### Очно-заочная форма обучения

| Вид учебной работы | На всю дисциплину | Семестр |
|---|---|---|
| | | 3 |
| **Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:** | **18** | **18** |
| Лекции | 8 | 8 |
| Лабораторные работы | - | - |
| Практические занятия | 10 | 10 |
| Аудиторные занятия в интерактивной форме, часов | - | - |
| **Самостоятельная работа, всего часов в том числе:** | **90** | **90** |
| Подготовка к зачету | 18 | 18 |
| Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю) | 72 | 72 |
| **Вид промежуточной аттестации** | **зачет** | **зачет** |
| **Общая трудоемкость дисциплины и трудоемкость по семестрам, часов** | **108** | **108** |

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

**Заочная форма обучения**

| Вид учебной работы | На всю дисциплину | Семестр |
|---|---|---|
| | | 4 |
| **Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:** | **8** | **8** |
| Лекции | 2 | 2 |
| Лабораторные работы | - | - |
| Практические занятия | 6 | 6 |
| Аудиторные занятия в интерактивной форме, часов | - | - |
| **Самостоятельная работа, всего часов в том числе:** | **100** | **100** |
| Подготовка к зачету | 18 | 18 |
| Другие виды самостоятельной работы (подготовка к практическим занятиям и рубежному контролю) | 64 | 64 |
| Контрольная работа | 18 | 18 |
| **Вид промежуточной аттестации** | **зачет** | **зачет** |
| **Общая трудоемкость дисциплины и трудоемкость по семестрам, часов** | **108** | **108** |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Информационная безопасность» относится к дисциплинам по выбору вариативной части Блока 1.

Изучение дисциплины базируется на результатах школьной дисциплины «Информатика», дисциплины «Экономическая информатика».

Изучение дисциплины должно способствовать обеспечению выпускников комплексом знаний, навыков и умений, которые позволят участвовать ему в развитии и поддержке стратегии развития предприятий и организаций, а практические навыки, полученные из курса «Информационная безопасность», будут использованы студентами при изучении других дисциплин профессионального цикла, а также при разработке курсовых и дипломных работ.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Основной целью курса является ознакомление студентов с современным состоянием проблемы хранения, обработки, поиска, передачи, преобразования, закрытия и восстановления конфиденциальной информации в организациях и на предприятиях различных направлений деятельности и различных форм собственности, рассмотрение на современном уровне вопросов разработки средств и систем сбора и защиты информации.

Задачами дисциплины являются: ознакомление с терминологией информационной безопасности; дать основы обеспечения информационной безопасности личности, общества, государства; методологии создания систем защиты информации; методов и средств ведения информационных войн; оценки защищенности и обеспечения информационной безопасности автоматизированных систем.

Компетенции, формируемые в результате освоения дисциплины:

– способностью работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (ОК-5);

– способность использовать основы правовых знаний в различных сферах деятельности (ОК-6);

– способностью использовать для решения коммуникативных задач современные технические средства и информационные технологии (ПК-10).

В результате изучения дисциплины обучающийся должен:

*знать:*

– место и роль информационной безопасности в системе национальной безопасности РФ, основы государственной информационной политики, стратегию развития информационного общества в России (для ОК-6);

– основные законы, нормативно-правовые акты, руководящие документы, регулирующие отношения в сфере информационной безопасности (для ОК-6);

*уметь:*

– работать в коллективе, толерантно воспринимая социальные, этнические, конфессиональные и культурные различия (для ОК-5);

– анализировать базовые документы, регулирующие аспекты информационной безопасности (для ПК-10);

*владеть:*

– профессиональной терминологией в области информационной безопасности (для ПК-10);

– навыками безопасного использования технических средств в профессиональной деятельности (для ПК-10);

– методами формирования требований по защите информации (для ПК-10).

# 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

## 4.1. Учебно-тематический план.

## Очная форма обучения

| Рубеж | Номер раздела, темы | Наименование раздела, темы | Количество часов контактной работы с преподавателем | |
|---|---|---|---|---|
| | | | Лекции | Практичес. занятия |
| Рубеж 1 | 1 | ***Основы безопасности автоматизированных систем.*** | ***4*** | ***6*** |
| | | Актуальность проблемы обеспечения безопасности автоматизированных систем (АС). Основные понятия в области безопасности автоматизированных систем. | 1 | |
| | | Угрозы безопасности автоматизированных систем. | 1 | |
| | | Меры и основные принципы обеспечения безопасности. Основные механизмы обеспечения информационной безопасности. | 1 | |
| | | Правовые основы обеспечения автоматизированных систем. Государственная система защиты информации. | 1 | |
| | 2 | ***Обеспечение безопасности автоматизированных систем*** | ***6*** | ***12*** |
| | | Организационная структура системы обеспечения безопасности АС | 1 | |
| | | Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях | 2 | |
| | | Регламентация работ по обеспечению безопасности автоматизированных систем | 1 | |
| | | Категорирование и документирование защищенных ресурсов | 1 | |
| | | Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем АС. | 1 | |

| | | | | |
|---|---|---|---|---|
| Рубеж 2 | 3 | ***Средства защиты информации от несанкционированного доступа*** | ***6*** | ***6*** |
| | | Назначение и возможности средств защиты информации от несанкционированного доступа | 2 | |
| | | Аппаратно-программные средства защиты информации от несанкционированного доступа. | 2 | |
| | | Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. | 2 | |
| | | **Всего** | **16** | **24** |

## Очно-заочная форма обучения

| **Рубеж** | **Номер раздела, темы** | **Наименование раздела, темы** | Количество часов контактной работы с преподавателем | |
|---|---|---|---|---|
| | | | Лекции | Практичес. занятия |
| | 1 | Основы безопасности автоматизированных систем. | 2 | 2 |
| Рубеж 1 | 2 | Обеспечение безопасности автоматизированных систем | 4 | 4 |
| Рубеж 2 | 3 | Средства защиты информации от несанкционированного доступа | 2 | 4 |
| | | **Всего** | **8** | **10** |

## Заочная форма обучения

| **Номер раздела, темы** | **Наименование раздела, темы** | Количество часов контактной работы с преподавателем | |
|---|---|---|---|
| | | Лекции | Практичес. занятия |
| 1 | Основы безопасности автоматизированных систем. | 1 | 2 |
| 2 | Обеспечение безопасности автоматизированных систем | - | 2 |
| 3 | Средства защиты информации от несанкционированного доступа | 1 | 2 |
| | **Всего** | **2** | **6** |

## 4.2. Содержание лекционных занятий

***1. Основы безопасности автоматизированных систем.***

Актуальность проблемы обеспечения безопасности автоматизированных систем (АС). Место и роль автоматизированных систем в управлении бизнес-процессами. Обострение проблемы обеспечения безопасности автоматизированных систем (АС) на современном этапе. Защита АС как процесс управления рисками. Методы оценки целесообразности затрат на обеспечение безопасности. Особенности современных АС как объектов защиты.

Основные понятия в области автоматизированных систем. Определение безопасности АС. Информация и информационные ресурсы. Субъекты информационных систем, их безопасность. Цель защиты автоматизированной системы и циркулирующей в ней информации.

Угрозы безопасности автоматизированных систем. Уязвимость основных структурно-функциональных элементов, распределенных АС. Угрозы безопасности информации, АС и субъектов информационных отношений.

Классификация угроз безопасности.

Классификация каналов проникновения в АС и утечки информации. Неформальная модель нарушителя.

Меры и основные принципы обеспечения безопасности АС. Виды мер противодействия угрозам безопасности. Принципы построения системы обеспечения безопасности информации в АС.

Правовые основы обеспечения безопасности АС. Защищаемая информация. Лицензирование. Сертификация средств защиты информации и аттестация объектов информатизации. Специальные требования и рекомендации по технической защите конфиденциальной информации. Юридическая значимость электронных документов с электронной подписью. Ответственность за нарушения в сфере защиты информации.

Государственная система защиты информации. Главные направления работ по защите информации. Структура государственной системы защиты информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. Финансирование мероприятий по защите информации.

***2. Обеспечение безопасности автоматизированных систем.***

Организационная структура системы обеспечения безопасности АС. Технология управления безопасностью информации и ресурсов в АС. Институт ответственных за обеспечение информационной безопасности. Регламентация действий пользователей и обслуживающего персонала АС. Политика безопасности организации. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты. Распределение функций по обеспечению безопасности АС. Организационно-распорядительные документы по обеспечению безопасности АС.

Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях. Проблема человеческого фактора. Общие правила обеспечения безопасности. Обязанности

ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения требований обеспечения безопасности. Порядок работы с носителями ключевой информации.

Регламентация работ по обеспечению безопасности автоматизированных систем. Регламентация правил парольной и антивирусной защиты. Регламентация порядка допуска к работе и изменения полномочий пользователей АС. Регламентация порядка изменения конфигурации аппаратно-программных средств АС. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач.

Категорирование и документирование защищенных ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов.

Концепция информационной безопасности. Планы защиты и обеспечения непрерывной работы и восстановления подсистем АС. Концепция информационной безопасности организации. План защиты информации. План обеспечения непрерывной работы и восстановления подсистем АС.

***3. Средства защиты информации от несанкционированного доступа.***

Назначение и возможности средств защиты информации от несанкционированного доступа. Основные механизмы защиты АС. Защита периметра компьютерных сетей и управление механизмами защиты. Страхование информационных рисков.

Аппаратно-программные средства защиты информации от несанкционированного доступа. Рекомендации по выбору средств защиты информации от несанкционированного доступа. Обзор существующих на рынке средств защиты информации от несанкционированного доступа. Средства аппаратной поддержки. Способы аутентификации.

Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. Стратегия безопасности Microsoft. Защита от вмешательства в процессе нормального функционирования АС. Разграничение доступа зарегистрированных пользователей к ресурсам АС. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

## 4.3 Практические занятия
## Очная форма обучения

| Номер раздела | Наименование раздела, темы | Наименование тем практических занятий | Норматив времени, час. |
|---|---|---|---|
| 1 | Основы безопасности автоматизированных систем | *Практическое занятие №1.* Угрозы безопасности автоматизированных систем. | 2 |
| | | *Практическое занятие №2.* Меры и основные принципы обеспечения безопасности. Основные механизмы обеспечения информационной безопасности. | 2 |
| | | *Практическое занятие №3.* Правовые основы обеспечения автоматизированных систем. | 1 |
| ***1-ый рубежный контроль*** | | ***Тестирование*** | 1 |
| 2 | Обеспечение безопасности автоматизированных систем | *Практическое занятие №4.* Организационная структура системы обеспечения безопасности АС. | 2 |
| | | *Практическое занятие №5.* Политика безопасности организации. | 2 |
| | | *Практическое занятие №6.* Общие правила обеспечения безопасности. | 2 |
| | | *Практическое занятие №7.* Допуск сотрудников к работе с АС и доступ к её ресурсам. | 2 |
| | | *Практическая работа №8.* Определение требований к защите конкретной информации, её носителей и процессов обработки. | 2 |
| | | *Практическое занятие №9.* Лицензирование и сертификация в области защиты информации. | 2 |
| 3 | Средства защиты информации от несанкционированного доступа | *Практическое занятие №10.* Назначение и возможности средств защиты информации от несанкционированного доступа. | 2 |
| | | *Практическое занятие №11.* Аппаратно-программные средства защиты информации от несанкционированного доступа. | 2 |
| | | *Практическое занятие №12.* Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. | 1 |
| ***2-ый рубежный контроль*** | | ***Тестирование*** | ***1*** |
| | ***Итого*** | | **24** |

## Очная-заочная форма обучения

| Номер раздела | Наименование раздела, темы | Наименование тем практических занятий | Норматив времени, час. |
|---|---|---|---|
| 1 | Основы безопасности автоматизированных систем | *Практическое занятие №1.* Угрозы безопасности автоматизированных систем. | 1 |
| | | *Практическое занятие №2.* Меры и основные принципы обеспечения безопасности. Основные механизмы обеспечения информационной безопаснсоти. | 1 |
| 2 | Обеспечение безопасности автоматизированных систем | *Практическое занятие №3.* Обеспечение необходимого уровня доступности, целостности и конфиденциальности компонентов АС. | 2 |
| | | *Практическое занятие №4.* Определение требований к защите конкретной информации, её носителей и процессов обработки. | 1 |
| ***1-ый рубежный контроль*** | | ***Тестирование*** | ***1*** |
| 3 | Средства защиты информации от несанкционированного доступа | *Практическое занятие №5.* Разграничение прав пользователей в операционных системах Windows 2000/XP. | 2 |
| | | *Практическое занятие №6.* Способы аутентификации. Защита информации с помощью пароля. | 1 |
| ***2-ый рубежный контроль*** | | ***Тестирование*** | ***1*** |
| | ***Итого*** | | **10** |

## Заочная форма обучения

| Номер раздела | Наименование раздела, темы | Наименование тем практических занятий | Норматив времени, час. |
|---|---|---|---|
| 1 | Основы безопасности автоматизированных систем | *Практическое занятие №1.* Угрозы безопасности автоматизированных систем. | 2 |
| 2 | Обеспечение безопасности автоматизированных систем | *Практическая работа №2.* Определение требований к защите конкретной информации, её носителей и процессов обработки. | 2 |
| 3 | Средства защиты информации от несанкционированного доступа | *Практическое занятие №3.* Аппаратно-программные средства защиты информации от несанкционированного доступа. | 2 |
| | ***Итого*** | | **6** |

### 4.4 Контрольная работа для заочной формы обучения

В процессе выполнения контрольной работы у студентов формируются навыки ведения самостоятельной работы. Контрольные задания способствуют более углубленному изучению основ дисциплины и повышению теоретической и профессиональной подготовки студентов. Написание контрольной работу способствует лучшему усвоению материала.

Студент выбирает одну из предложенных преподавателем тем, самостоятельно готовит презентацию работы и выносит ее на обсуждение на занятии.

Результат выполнения контрольной работы оформляется в виде пояснительной записки, объемом 15-20 страниц, которая содержит:

- титульный лист;
- содержание;
- введение;
- основную часть отчета;
- заключение;
- список использованных источников;
- приложения.

При оформлении контрольной работы студент должен руководствоваться методическими указаниями к оформлению текстовой документации для студентов. По результатам проверки представленной студентом контрольной работы преподаватель принимает решение о допуске ее к защите или возвращает студенту на доработку в соответствии с отмеченными замечаниями.

### Тематика контрольных работ

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Правовая база обеспечения информационной безопасности личности (общества, государства).
3. Виды защищаемой информации.
4. Интересы личности (общества, государства) в информационной сфере.
5. Угрозы информационной безопасности Российской Федерации.
6. Внешние (внутренние) источники угроз информационной безопасности государства.
7. Проблемы региональной информационной безопасности.
8. Информационное оружие, его классификация и возможности.
9. Методы нарушения конфиденциальности (целостности, доступности) информации.
10. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности.
11. Компьютерная система как объект информационной безопасности.
12. Обеспечение информационной безопасности компьютерных систем.
13. Понятие национальной безопасности. Виды безопасности.

14. Дайте определение терминам «несанкционированный» и «неавторизованный «доступ к информации».

15. Чем отличаются понятия «защита информации» и «информационная безопасность»?

16. Что такое неавторизованный доступ к информации?

17. Какие существуют правовые аспекты защиты информации?

18. Что такое сетевая атака? Назовите средства защиты от сетевых атак.

19. Определите особенности защиты компьютерной информации от несанкционированного доступа.

20. Как обеспечить безопасность информации в локальной сети?

21. Назовите способы защиты электронной почты от вирусов.

22. Определите методы и средства защиты информации в глобальных сетях.

23. Внешние источники угроз.

24. Внутренние источники угроз.

25. Направления обеспечения информационной безопасности государства.

26. Субъекты информационного противоборства. Цели информационного противоборства.

27. Методы нарушения конфиденциальности, целостности и доступности информации.

28. Причины, виды, каналы утечки и искажения информации.

## 5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей практической работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения практических работ является самостоятельная подготовка к ним накануне путем повторения материалов лекций. Рекомендуется подготовить вопросы по неясным моментам и обсудить их с преподавателем в начале работы.

Преподавателем запланировано применение на практических занятиях технологий развивающейся кооперации, коллективного взаимодействия, разбора конкретных ситуаций.

Для текущего контроля успеваемости по очной, очно-заочной форме обучения преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так

и на практических работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к практическим работам, к рубежным контролям (для очной, очно-заочной формы обучения), подготовку к зачету и выполнение контрольной работы (для заочной формы обучения)

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

**Рекомендуемый режим самостоятельной работы**

| **Наименование вида самостоятельной работы** | **Рекомендуемая трудоемкость, акад. час.** | | |
|---|---|---|---|
| | **Очная форма** | **Очно-заочная форма** | **Заочная форма** |
| **Самостоятельное изучение тем дисциплины** | **22** | **58** | **58** |
| Актуальность проблемы обеспечения безопасности автоматизированных систем (АС). | 1 | - | 2 |
| Основные понятия в области безопасности автоматизированных систем. | | - | 4 |
| Угрозы безопасности автоматизированных систем. | 1 | 5 | 3 |
| Меры и основные принципы обеспечения безопасности. | 1 | 6 | 5 |
| Основные механизмы обеспечения информационной безопасности. | | | 3 |
| Правовые основы обеспечения автоматизированных систем. | 1 | 6 | 3 |
| Государственная система защиты информации. | | | 3 |
| Организационная структура системы обеспечения безопасности АС | 3 | 4 | 3 |
| Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях | 3 | 5 | 4 |
| Регламентация работ по обеспечению безопасности автоматизированных систем | 3 | 4 | 3 |
| Категорирование и документирование защищенных ресурсов. | 3 | 5 | 4 |
| Концепция информационной безопасности. | 3 | 5 | 3 |
| Планы защиты и обеспечения непрерывной работы и восстановления подсистем АС. | | | 4 |
| Средства защиты информации от несанкционированного доступа | - | - | 3 |

| Наименование вида самостоятельной работы | Рекомендуемая трудоемкость, акад. час. | | |
|---|---|---|---|
| | Очная форма | Очно-заочная форма | Заочная форма |
| **Самостоятельное изучение тем дисциплины** | **22** | **58** | **58** |
| Назначение и возможности средств защиты информации от несанкционированного доступа | 1 | 5 | 3 |
| Аппаратно-программные средства защиты информации от несанкционированного доступа. | 1 | 8 | 4 |
| Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. | 1 | 5 | 4 |
| **Подготовка к практическим работам** (по 2 часа на занятия) | 24 | 10 | 6 |
| **Подготовка к рубежным контролям** (по 2 часа на каждый рубеж) | 4 | 4 | - |
| **Выполнение контрольной работы** | - | - | 18 |
| **Подготовка к зачету** | 18 | 18 | 18 |
| **Всего** | **68** | **90** | **100** |

## 6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

### 6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ (для очной, очно-заочной формы обучения).
2. Отчеты студентов по практическим занятиям.
3. Банк тестовых заданий к рубежным контролям № 1, № 2 (для очной, очно-заочной формы обучения).
4. Вопросы к зачету.
5. Контрольная работа (для заочной формы обучения).

### 6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

**Очная форма обучения**

| № | Наименование | Содержание | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)* | Распределение баллов | | | | | |
| | | Вид учебной работы: | Посещение лекций | Выполнение практической работы | Рубежный контроль №1 | Рубежный контроль №2 | Зачет |
| | | Балльная оценка: | 1б х 8 = 8б | 3б х 12 = 36б | 13 | 13 | 30 |
| 2 | Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета | 60 и менее баллов – не зачтено;<br>61 и более – зачтено; | | | | | |
| 3 | Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов | Для допуска к промежуточной аттестации (зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все практические работы.<br>Для получения зачета» «автоматически» студенту необходимо набрать 61 балл.<br>По согласованию с преподавателем студенту, могут быть добавлены дополнительные (бонусные) баллы за активность на практических работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры. | | | | | |

| | | |
|---|---|---|
| 4 | Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра | В случае, если к промежуточной аттестации (зачету), набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических работ.<br>Формы дополнительных заданий (назначаются преподавателем):<br>- выполнение пропущенной практической работы (при невозможности дополнительного проведения практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 3 баллов.<br>Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем. |

## Очно-заочная форма обучения

| № | Наименование | Содержание | | | | | |
|---|---|---|---|---|---|---|---|
| | | Распределение баллов | | | | | |
| 1 | Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы *(доводятся до сведения студентов на первом учебном занятии)* | Вид учебной работы: | Посещение лекций | Выполнение практической работы | Рубежный контроль №1 | Рубежный контроль №2 | Зачет |
| | | Балльная оценка: | $2_б \times 4 = 8_б$ | $8_б \times 5 = 40_б$ | 11 | 11 | 30 |
| 2 | Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета | 60 и менее баллов – не зачтено;<br>61 и более – зачтено; | | | | | |
| 3 | Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета (экзаменационной оценки) по дисциплине, возможность получения бонусных баллов | Для допуска к промежуточной аттестации (зачету) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все практические работы.<br>Для получения зачета» «автоматически» студенту необходимо набрать 61 балл.<br>По согласованию с преподавателем студенту, могут быть добавлены дополнительные (бонусные) баллы за активность на практических работах, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических работ, за участие в значимых учебных и внеучебных мероприятиях кафедры. | | | | | |

| | | |
|---|---|---|
| 4 | Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра | В случае, если к промежуточной аттестации (зачету), набрана сумма менее 50 баллов, студенту необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. При этом необходимо проработать материал всех пропущенных практических работ.<br>Формы дополнительных заданий (назначаются преподавателем):<br>- выполнение пропущенной практической работы (при невозможности дополнительного проведения практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 3 баллов.<br>Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем. |

### 6.3. Процедура оценивания результатов освоения дисциплины

Рубежные контроли проводятся в форме письменного тестирования.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии. Варианты тестовых заданий состоят для рубежных контролей из 11 вопросов для очной формы обучения и из 12 вопросов для очно-заочной формы обучения. На каждое тестирование при рубежном контроле студенту отводится 1 академический час.

Баллы студенту выставляются в зависимости от числа правильно выбранных ответов. Итоговая оценка по тесту формируется путем суммирования набранных баллов и отнесения их к общему количеству вопросов в задании. Помножив полученное значение на 100%, можно привести итоговую оценку к традиционной следующим образом:

«неудовлетворительно» – менее 50%

«удовлетворительно» – 50% - 70%

«хорошо» – 70% - 90%

«отлично» – 90% - 100%.

Преподаватель оценивает в баллах результаты тестирования каждого студента по количеству правильных ответов и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме ответа на 2 вопроса, выбранных преподавателем. Вопросы к зачету доводятся до студентов на последней лекции в семестре. Каждый вопрос оценивается в 15 баллов. На подготовку ответа студенту отводится 1 астрономический час.

Результаты текущего контроля успеваемости и зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный

отдел института в день зачета, а также выставляются в зачетную книжку студента.

### 6.4. Процедура оценивания результатов освоения дисциплины (заочная форма обучения)

Тематика контрольных работ доводится до студентов на установочной лекции. Студенты самостоятельно выполняют контрольную работу и предоставляют ее на проверку в начале сессии. По результатам проверки представленной студентом контрольной работы преподаватель принимает решение о допуске ее к защите или возвращает студенту на доработку в соответствии с отмеченными замечаниями.

Зачет проводится в форме ответа на вопросы. Вопросы к зачету доводятся до студентов на лекции. На подготовку ответа студенту отводится 1 астрономический час.

Результаты проверки контрольной работы и приема зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку студента.

### 6.5. Примеры оценочных средств для рубежных контролей и зачета

***1-ый рубежный контроль***

***1. Активный перехват информации это – перехват, который:***

1) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

2) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

3) неправомерно использует технологические отходы информационного процесса;

4) осуществляется путем использования оптической техники;

5) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

***2. Как называется способ несанкционированного доступа к информации, который заключается в несанкционированном доступе в компьютер или компьютерную сеть без права на то?***

1) «За дураком»;

2) «Брешь»;

3) «Компьютерный абордаж»;

4) «За хвост»;

5) «Неспешный выбор».

***3. Защита информации – это:***

1) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

2) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

3) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

4) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

5) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на нее.

***2-ой рубежный контроль***

***1. Защита информации от разглашения – это деятельность по предотвращению:***

1) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

2) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

3) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

4) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

5) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

***2. Носитель информации – это:***

1) физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов;

2) субъект, осуществляющий пользование информацией и реализующий полномочия распоряжения в пределах прав, установленных законом и/или собственником информации;

3) субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением;

4) субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией в соответствии с законодательными актами;

5) участник правоотношений в информационных процессах.

***3. Троянские программы, скрытно осуществляющие анонимный доступ к различным Интернет-ресурсам, обычно используются для рассылки спама:***

1) Trojan-PSW; 2) Trojan-Spy; 3) Trojan-Proxy;

4) Trojan-Downloader; 5) Trojan-Dropper.

## ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Актуальность проблемы обеспечения безопасности автоматизированных систем (АС). Место и роль автоматизированных систем в управлении бизнес-процессами.
2. Защита АС как процесс управления рисками. Особенности современных АС как объектов защиты.
3. Угрозы безопасности автоматизированных систем.
4. Уязвимость основных структурно-функциональных элементов, распределенных АС.
5. Угрозы безопасности информации, АС и субъектов информационных отношений.
6. Классификация угроз безопасности.
7. Классификация каналов проникновения в АС и утечки информации.
8. Неформальная модель нарушителя.
9. Меры и основные принципы обеспечения безопасности АС.
10. Виды мер противодействия угрозам безопасности.
11. Принципы построения системы обеспечения безопасности информации в АС.
12. Правовые основы обеспечения безопасности АС.
13. Защищаемая информация. Лицензирование. Сертификация средств защиты информации и аттестация объектов информатизации.
14. Специальные требования и рекомендации по технической защите конфиденциальной информации.
15. Юридическая значимость электронных документов с электронной подписью. Ответственность за нарушения в сфере защиты информации.
16. Государственная система защиты информации.
17. Организация защиты информации в системах и средствах информатизации и связи.
18. Организационная структура системы обеспечения безопасности АС.
19. Технология управления безопасностью информации и ресурсов в АС.
20. Регламентация действий пользователей и обслуживающего персонала АС.
21. Политика безопасности организации.
22. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты.
23. Распределение функций по обеспечению безопасности АС.
24. Организационно-распорядительные документы по обеспечению безопасности АС.
25. Обязанности пользователей и ответственных за обеспечение информационной безопасности в подразделениях.
26. Обязанности ответственного за обеспечение безопасности информации в подразделении.
27. Ответственность за нарушения требований обеспечения безопасности.
28. Порядок работы с носителями ключевой информации.

29. Регламентация работ по обеспечению безопасности автоматизированных систем.

30. Регламентация правил парольной и антивирусной защиты.

31. Регламентация порядка допуска к работе и изменения полномочий пользователей АС.

32. Регламентация порядка изменения конфигурации аппаратно-программных средств АС.

33. План защиты информации.

34. Назначение и возможности средств защиты информации от несанкционированного доступа.

35. Основные механизмы защиты АС.

36. Защита периметра компьютерных сетей и управление механизмами защиты. Страхование информационных рисков.

37. Аппаратно-программные средства защиты информации от несанкционированного доступа.

38. Средства аппаратной поддержки.

39. Способы аутентификации.

40. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа. Разграничение доступа зарегистрированных пользователей к ресурсам АС.

41. Оперативное оповещение о зарегистрированных попытках несанкционированного доступа.

42. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

### 6.6. Фонд оценочных средств

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

## 7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

### 7.1. Основная учебная литература

1. Галатенко В.А. Основы информационной безопасности: Курс лекций. - М.: Интернет- Университет Информационных технологий, 2006. – 208 с. (13 экз.)

2. Куприянов А.И. Основы защиты информации. [Электронный ресурс] Издательский центр «Академия», 2009. – 256 с. – Доступ из ЭБС «znanium.com».

3. Мельников В.П. Информационная безопасность и защита информации. Издательский центр «Академия», 2008. – 336 с. (11 экз.)

4. Расторгуев С.П. Основы информационной безопасности. Издательский центр «Академия» 2009. (10 экз.)

### 7.2 Дополнительная учебная литература:

1. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности. [Электронный ресурс] М.: Горячая линия-Телеком, 2006. – Доступ из ЭБС «znanium.com»

### 7.3 Методическая литература

1. Москвин В.В., Полякова Е.Н. Методические указания к выполнению практических работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». Часть 1. РИЦ Курганского государственного университета. 2017.- 52 с.

2. Москвин В.В., Полякова Е.Н. Методические указания к выполнению практических работ по дисциплине «Основы информационной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». Часть 2. РИЦ Курганского государственного университета. 2017.- 41 с.

3. Новоструев, А.В., Солодовников, В.М., Терентьева, А.А. Тезаурус в сфере информационной безопасности [Текст]/ А.В. Новоструев, В.М. Солодвников, А.А. Терентьева: Учебное пособие. – Курган: Изд-во Курганского гос. Ун-та, 2014. – 471 с.

### 7.4 Нормативно-правовое обеспечение дисциплины:

1. Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента РФ 5 декабря 2016 г. №646).

2. Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1.

3. Закон РФ «О коммерческой тайне» от 29 июля 2004 г. № 98-ФЗ.

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ.

5. Федеральный закон «О персональных данных» от 27 июля 2006 г. № 152-ФЗ.

6. Федеральный закон «Об электронной подписи» от 6 апреля 2011 г. № 63-ФЗ.

7. Положение по аттестации объектов информатизации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 27.10.1994).

8. Положение о сертификации средств защиты информации по требованиям безопасности информации (утв. Государственной технической комиссией при Президенте РФ 25.11.1995, приказ №199).

9. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (утв. Государственной технической комиссией при Президенте РФ 30.08.2002, приказом №282).

10. ISO/IEC 27001 - 2005 (2013). Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.

## 8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1) официальный сайт Президента РФ: http://kremlin.ru;
2) официальный сайт Правительства РФ: http://government.ru;
3) официальный сайт Государственной Думы: http://www.duma.gov.ru;
4) официальный сайт Совета Безопасности РФ: http://www.scrf.gov.ru;
5) официальный сайт Федеральной службы по техническому и экспортному контролю РФ: http://fstec.ru;
6) официальный сайт ФСБ России: http://www.fsb.ru и т.д.
7) «Консультант-плюс»: http://www.consultant.ru;
8) «Гарант»: http://www.garant.ru;
9) «Кодекс»: http://www.kodeks.ru
10) [Электронный ресурс] Internet Security Glossary, Version 2 - http:/ /www.ietf.org/rfc/rfc4949.txt;
11) [Электронный ресурс] Behavior of and Requirements for Internet Firewalls -htt:/ /www.ietf.org/rfc/rfc2979.txt

## 9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

Информационно-справочная система «КонсультантПлюс».

При чтении лекций используются слайдовые презентации.

Минимальные требования к операционной системе и программному обеспечению компьютера, используемого при показе слайдовых презентаций: Windows XP, Libre Office.

## 10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Переносной проектор BENQ PB6110 с экраном, локальная сеть компьютеров на базе Intel Core i3-2120 - 16 шт. с выходом в Internet, коммутатор 2-го уровня D-LINK DGS-101D/E1A.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
**«Информационная безопасность»**

образовательной программы высшего образования –
программы бакалавриата

**38.03.01 – Экономика**

Направленность: Бухгалтерский учет, анализ и аудит
Финансы и кредит

*Трудоемкость дисциплины:* 3 з.е. (108 академических часа)
*Семестр:* 3 (очная форма обучения), 3 (очно-заочная форма обучения), 4 (заочная форма обучения)
*Форма промежуточной аттестации:* зачет
*Содержание дисциплины. Основные разделы*
Основы безопасности автоматизированных систем. Актуальность проблемы обеспечения безопасности автоматизированных систем (АС). Основные понятия в области автоматизированных систем. Угрозы безопасности автоматизированных систем. Классификация угроз безопасности. Меры и основные принципы обеспечения безопасности АС. Правовые основы обеспечения безопасности АС. Государственная система защиты информации. Организационная структура системы обеспечения безопасности АС. Мероприятия по созданию и обеспечению функционирования комплексной системы защиты. Средства защиты информации от несанкционированного доступа. Аппаратно-программные средства защиты информации от несанкционированного доступа. Применение штатных и дополнительных средств защиты информации от несанкционированного доступа.