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:
Ректор КГУ

_____ / Н.В. Дубив/

«31» августа 2020 г.

Рабочая программа учебной дисциплины

# КОМПЛЕКСНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

образовательной программы высшего образования –

программы специалитета

10.05.03 Информационная безопасность автоматизированных систем

Направленность: (специализация №7) обеспечение информационной безопасности распределенных информационных систем

Форма обучения: очная

Курган 2020

Рабочая программа дисциплины «Комплексное обеспечение информационной безопасности автоматизированных систем» составлена в соответствии с учебным планом по программе специалитета «Информационная безопасность автоматизированных систем» (Обеспечение информационной безопасности распределенных информационных систем), утвержденным для очной формы обучения « 28 » августа 2020 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» 31 августа 2020 года, протокол № 1.

Рабочую программу составил:
канд. пед. наук, доцент Е.Н. Полякова

Согласовано:

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

Начальник Управления
образовательной деятельности С.Н. Синицын

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

## 1. ОБЪЕМ ДИСЦИПЛИНЫ

Всего: 4 зачетных единицы трудоемкости (144 академических часа)

**Очная форма обучения**

| Вид учебной работы | На всю дисциплину | Семестр |
|---|---|---|
| | | 8 |
| **Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:** | **48** | **48** |
| Лекции | 16 | 16 |
| Лабораторные работы | 16 | 16 |
| Практические занятия | 16 | 16 |
| Аудиторные занятия в интерактивной форме, часов | - | - |
| **Самостоятельная работа, всего часов в том числе:** | 96 | 96 |
| Подготовка к зачету | 18 | 18 |
| Другие виды самостоятельной работы (подготовка к практическим занятиям, лабораторным работам и рубежному контролю) | 60 | 60 |
| Контрольная работа | 18 | 18 |
| **Вид промежуточной аттестации** | **зачет с оценкой** | **зачет с оценкой** |
| **Общая трудоемкость дисциплины и трудоемкость по семестрам, часов** | **144** | **144** |

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» относится к дисциплинам вариативной части по выбору Блока 1.

Изучение дисциплины базируется на результатах обучения, сформированных при изучении следующих дисциплин:

- Основы информационной безопасности.
- Организационное и правовое обеспечение информационной безопасности.
- Техническая защита информации
- Программно-аппаратные средства защиты информации
- Безопасность сетей ЭВМ.
- Стандарты информационной безопасности.
- Основы управленческой деятельности.

Результаты обучения по дисциплине необходимы для выполнения разделов выпускной квалификационной работы.

## 3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Дисциплина «Комплексное обеспечение информационной безопасности автоматизированных систем» имеет целью раскрыть основы правового регулирования отношений в информационной сфере, понятие и виды компьютерных преступлений, а также соотношение программных, аппаратных и административных средств в комплексном обеспечении информационной безопасности автоматизированных систем обработки данных.

*Задачей дисциплины является* наиболее полно и объективно научить студентов согласованному применению разнородных средств при построении целостной системы защиты, перекрывающей все существующие каналы реализации угроз.

Компетенции, формируемые в результате освоения дисциплины:

– способность осуществлять поиск, изучение, обобщение и систематизацию научно-технической информации, нормативных и методических материалов в сфере профессиональной деятельности, в том числе на иностранном языке (ПК-1);

– способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);

– способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

– способность организовывать работу малых коллективов исполнителей, вырабатывать и реализовывать управленческие решения в сфере профессиональной деятельности (ПК-18);

– способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);

– способность разрабатывать проекты документов, регламентирующих работу по обеспечению информационной безопасности автоматизированных систем (ПК-21);

– способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации (ПК-22);

– способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа (ПК-23);

– способностью разрабатывать и исследовать модели информационно-технологических ресурсов, разрабатывать модели угроз и модели нарушителя информационной безопасности в распределенных информационных системах (ПСК-7.1);

– способность проводить анализ рисков информационной безопасности и разрабатывать, руководить разработкой политики безопасности в распределенных информационных системах (ПСК-7.2);

– способностью проводить аудит защищенности информационно-технологических ресурсов распределенных информационных систем (ПСК-7.3);

– способность координировать деятельность подразделений и специалистов по защите информации в организациях, в том числе на предприятии и в учреждении (ПСК-7.5).

В результате изучения дисциплины обучающийся должен

*знать:*

- основы безопасности вычислительных сетей (для ПК-6, ПК-20);

- основы правового регулирования взаимоотношений администрации и персонала в области защиты информации (для ПК-1, ПК-18,ПК-23);

- основные технические средства и методы защиты информации (для ПК-8, ПК-23, ПСК-7.5);

- основные программно-аппаратные средства обеспечения информационной безопасности (для ПК-6, ПК-21, ПК-22);

*уметь:*

- разрабатывать проекты нормативных материалов, регламентирующих работу по защите информации, а также положений, инструкций и других организационно-распорядительных документов (для ПК-1, ПК-6, ПК-21, ПСК-7.1, ПСК-7.2, ПСК-7.3, ПСК-7.5);

*иметь навыки:*

- работы с нормативно-правовыми актами (для ПК-1, ПК-8, ПК-20, ПК-23, ПСК-7.2);

- работы с основными средствами обеспечения информационной безопасности (для ПК-6, ПК-21).

## 4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 4.1. Учебно-тематический план. Очная форма обучения

| Рубеж | Номер темы | Наименование темы | Количество часов контактной работы с преподавателем | | |
|---|---|---|---|---|---|
| | | | Лекции | Практич. занятия | Лаборатор. работы |
| *Семестр 8* | | | | | |
| Рубеж 1 | 1 | Компоненты комплексной системы информационной безопасности | 2 | 4 | - |
| | 2 | Проектирование комплексной системы информационной безопасности | 2 | 4 | - |
| | 3 | Управление комплексной системой информационной безопасности. | 2 | - | - |
| Рубеж 2 | 4 | Методика построения административного управления КСИБ. | 2 | 4 | - |
| | 5 | Оценка качества комплексной системы информационной безопасности. | 2 | - | 14 |
| | 6 | Сопровождение комплексной системы информационной безопасности. | 4 | 4 | 2 |
| | 7 | Перспективы развития комплексного обеспечения информационной безопасности. | 2 | - | - |
| | | **Всего:** | **16** | **16** | **16** |

### 4.2. Содержание лекционных занятий

**Тема 1. Компоненты комплексной системы информационной безопасности.**

***Введение. Основные цели и задачи систем защиты информации. Цели защиты информации.*** Основные задачи систем защиты информации. Три класса задач, связанных с уменьшением степени распознавания объектов: скрытие информации, дезинформация противника и легендирование.

Задачи, связанные с защитой содержания информации. Введение избыточности элементов системы. Регулирование доступа к средствам обработки информации. Регулирование использования элементов системы и защищаемой информации. Маскировка информации. Регистрация сведений. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования. Управление системой защиты. Обеспечение требуемого уровня готовности обслуживающего персонала.

Защита информации от информационного воздействия - защита от информационного воздействия на технические средства, защита от информационного воздействия на общество, защита от информационного воздействия на психику человека.

***Методология формирования задач защиты информации. Три стратегии защиты: оборонительная, наступательная и упреждающая.*** Интеграция средств информационной безопасности в технологическую среду. Назначение инструментального базиса. Функции центров защиты информации.

**Тема 2. Проектирование комплексной системы информационной безопасности.**

***Основные этапы проектирования КСИБ, требования к ним.*** Принципы проектирования систем защиты информации. Принцип конечной цели. Принцип измерения. Принцип эквифинальности (завершенности). Принцип единства. Принцип связности. Принцип модульного построения. Принцип иерархии. Принцип функциональности. Принцип развития. Принцип разумного сочетания централизации и децентрализации. Принцип неопределенности.

Основные средства систем защиты информации. Пассивные и активные способы. Формальные и неформальные средства реализации задач защиты информации.

Стратегии применения средств защиты информации.

***Порядок и особенности проведения испытаний и внедрения в эксплуатацию КСИБ.*** Порядок и особенности проведения испытаний КСИБ. Контроль выполнения требований, предъявляемых к персоналу, допущенного к конфиденциальной информации. Контроль организации и обеспечения работы с конфиденциальной информацией. Контроль соответствия размещения, охраны, специального оборудования помещений требованиям информационной безопасности. Контроль порядка учёта, хранения, использования и уничтожения документов. Проверка организации и осуществления контроля за обеспечением информационной безопасности. Контроль выполнения основных специальных требований по размещению и монтажу оборудования информационных систем.

Порядок и особенности внедрения КСИБ в эксплуатацию.

**Тема 3. Управление комплексной системой информационной безопасности.**

***Мониторинг окружающей среды, выявление каналов несанкционированного доступа.*** Общие сведения поисковых мероприятий. Периодичность поисковых мероприятий. Уровни чисток. Перечень поисковых работ. Варианты комплектации поисковых подразделений.

***Методика построения административного управления КСИБ.*** Управление проектами. Сетевое планирование. Управление стоимостью. Управление проектными рисками. Планирование систем для бизнеса. Системное (тотальное) управление качеством. Международный стандарт ISO 9000. Методика BSP. Подход CPI.

**Тема 4. Методика построения административного управления КСИБ.**

***Оценка качества комплексной системы информационной безопасности.*** Общие сведения об оценке качества КСИБ. Методы оценки качества КСИБ. Понятия «объективная вероятность» и «субъективная вероятность». Сущность количественных и качественных показателей качества КСИБ. Метод экспертных оценок. Основные этапы организации работы экспертов. Факторы при разработке технологии экспертных оценок.

**Тема 5. Оценка качества комплексной системы информационной безопасности.**

***Оценка качества КСИБ методом экспертных структурных вопросников.*** Метод Дельфи. Общая характеристика метода. Основные недостатки метода Дельфи. Этапы экспертного оценивания. Метод QUEST. Метод SEER. Постановка

цели исследования. Выбор формы исследования, определение бюджета проекта. Подготовка информационных материалов. Подбор экспертов. Проведение экспертизы. Статистический анализ результатов. Морфологический анализ.

*Оценка качества КСИБ методом оценки уязвимости информации Хоффмана.* Общая характеристика метода. Виды угроз информации, которые можно выделить во внешней среде. Общая схема воздействия на информацию в организационно-экономической системе. Объективные предпосылки возникновения угроз информации. Субъективные предпосылки возникновения угроз информации. Классификация каналов несанкционированного доступа по степени взаимодействия злоумышленника с информационными подсистемами. Оценка уязвимостей по Дж. Хоффману.

***Оценка качества КСИБ методом оценки риска Фишера.*** Общая характеристика метода. Оценка рисков по двум факторам. Оценка рисков по трем факторам. Особенности и область применения оценки рисков по двум факторам. Особенности и область применения оценки рисков по трем факторам.

**Тема 6. Сопровождение комплексной системы информационной безопасности.**

***Эксплуатационная документация КСИБ.*** Комплект документов, поставляемых предприятием-изготовителем. Формуляр (технический паспорт, паспорт). Техническое описание. Инструкция по эксплуатации.

Документация, разрабатываемая на месте эксплуатации. Паспорт-формуляр. Положение по обеспечению информационной безопасности предприятия (организации). Другие документы. Категории для технических средств в соответствии с их техническим состоянием.

***Аттестация объектов по требованиям информационной безопасности.*** Порядок работ по подготовке и проведению аттестации объектов информатизации АС.

***Особенности эксплуатации КСИБ на объекте защиты.*** Основы, направления и этапы защиты информации. Правовые аспекты защиты информации. Общие сведения. Подсистема организационно-правовой защиты. Промышленный шпионаж и законодательство. Защита программного обеспечения авторским правом. Последовательность команд. Творческая активность. Стиль. Алгоритм. Отбор и сопряжение элементов. Оригинальность программ. Удачность.

Стандарты и рекомендации по защите информации. Недостатки существующих стандартов и рекомендаций. Требования к содержанию нормативно-методических документов по ЗИ. Разработка нормативно-методической основы ЗИ. План защиты информации.

***«Организационно-функциональные задачи службы безопасности».*** Организационно-штатная структура службы безопасности. Системы защиты информации. Понятие «ядро системы защиты информации». Структурная схема системы защиты информации. Понятия «стандартизация» и «типизация» СЗИ. Допустимые и целесообразные типы СЗИ различных категорий. Классификация типов информационных систем по В.А. Герасименко. Совокупность рубежей защиты информации. Функциональные задачи службы защиты информации.

**Тема 7. Перспективы развития комплексного обеспечения информационной безопасности.**

***Особенности проектирования на современном уровне и синтез КСИБ.*** Многокритериальный синтез. Целевая функция. Критериальный язык описания выбора. Постановка задач оптимизации и их классификации. Последовательность решения оптимизационных задач. Учет при синтезе различного вклада функциональных подсистем в эффективность целостной системы. Синтез систем на основе качественных классификационных признаков. Метод морфологического древовидного синтеза. Морфологический метод лабиринтного синтеза. Синтез многофункциональных систем с различным числом самостоятельных составляющих подсистем. Анализ морфологических множеств по различным комбинациям критериев. Морфологический синтез систем по критерию комбинационной новизны.

## 4.3 Практические занятия

| Номер темы | Наименование темы | Наименование тем практических занятий | Норматив времени, час. |
|---|---|---|---|
| 1 | Компоненты комплексной системы информационной безопасности. | Нормативно-правовая база комплексной системы информационной безопасности | 4 |
| 2 | Проектирование комплексной системы информационной безопасности. | Принципы ИБ реализуемые в АС | 3 |
| | ***1-ый рубежный контроль*** | ***Тестирование*** | *1* |
| 4 | Методика построения административного управления КСИБ. | Формирование правил и подразделений службы ИБ | 4 |
| 6 | Сопровождение комплексной системы информационной безопасности. | Комплексное обеспечение информационной безопасности АС | 3 |
| | ***2-ой рубежный контроль*** | ***Тестирование*** | *1* |
| | ***Итого*** | | **16** |

## 4.4. Лабораторные работы

| Номер темы | Наименование темы | Наименование лабораторных работ | Норматив времени, час. |
|---|---|---|---|
| 5 | Оценка качества комплексной системы информационной безопасности. | Оценивание рисков | 2 |
| | | Технология оценки угроз и уязвимостей | 4 |
| | | Оценка показателей качества функционирования комплексной системы защиты информации на предприятии | 4 |
| | | Определение показателей защищенности информации при несанкционированном доступе. | 4 |
| 6 | Сопровождение комплексной системы информационной безопасности. | Расследование инцидентов в области ИБ. Реагирование на инциденты. | 2 |
| | **Итого:** | | **16** |

### 4.5 Контрольная работа

Целью контрольной работы является применение теоретических знаний студентов при построении целостной системы защиты, перекрывающей все существующие каналы реализации угроз.

Примерный объем контрольной работы 10-15 листов формата А4.

#### ПРИМЕРНАЯ ТЕМАТИКА КОНТРОЛЬНЫХ РАБОТ

1. Комплексный подход к обеспечению информационной безопасности объекта.
2. Концепция обеспечения информационной безопасности.
3. Основные этапы нарушения информационной безопасности.
4. Характеристика, структура и алгоритм формирования облика нарушителя.
5. Алгоритм проведения анализа информационного риска на предприятии.
6. Обеспечение информационной безопасности в чрезвычайных обстоятельствах.
7. План обеспечения информационной безопасности предприятия.
8. Последовательность процедур безопасности.
9. Аутентификация, авторизация и администрирование действий пользователя.
10. Разработка подпрограммы входа в систему на основе многоразовых паролей.
11. Управление идентификацией и доступом.

## 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 лабораторной или 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 лабораторных и 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 лабораторной или практической работы.

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

Для текущего контроля успеваемости по очной 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 и лабораторных занятиях в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает самостоятельное изучение разделов дисциплины, подготовку к лабораторным и практическим занятиям, к рубежным контролям, выполнение контрольной работы и подготовку к зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

**Рекомендуемый режим самостоятельной работы**

| **Наименование вида самостоятельной работы** | Рекомендуемая трудоемкость, акад. час. |
|---|---|
| Самостоятельное изучение тем раздела | 29 |
| - Компоненты комплексной системы информационной безопасности | 4 |
| - Проектирование комплексной системы информационной безопасности | 4 |
| - Управление комплексной системой информационной безопасности | 4 |
| - Методика построения административного управления КСИБ. | 4 |
| - Оценка качества комплексной системы информационной безопасности | 4 |
| - Сопровождение комплексной системы информационной безопасности. | 6 |
| - Перспективы развития комплексного обеспечения информационной безопасности | 3 |
| Подготовка к практическим занятиям (по 3 часа на занятие) | 12 |
| Подготовка к лабораторным работам (по 3 часа на работу) | 15 |
| Подготовка к рубежным контролям (по 2 часа на каждый рубежный контроль) | 4 |
| Выполнение контрольной работы | 18 |
| Подготовка к зачету | 18 |
| **Всего:** | **96** |

## 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.
2. Отчеты студентов по лабораторным работам.
3. Отчеты студентов по практическим занятиям.
4. Банк тестовых заданий к рубежным контролям № 1, № 2.
5. Контрольная работа.
6. Вопросы к зачету

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

| № | Наименование | Содержание |
|---|---|---|

<table>
<tr><td rowspan="3">1</td><td rowspan="3">Распределение баллов за семестры по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="8">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита отчетов по лабораторным работам</td><td>Выполнение практической работы</td><td>Защита контрольной работы</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Зачет</td></tr>
<tr><td>Балльная оценка:</td><td>$1_б$ x 8 =$8_б$</td><td>$5_б$ x 5 = $25_б$</td><td>$4_б$ x 4 =$16_б$</td><td>9</td><td>6</td><td>6</td><td>30</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и зачета</td><td colspan="8">60 и менее баллов – неудовлетворительно; не зачтено;<br>61…73 – удовлетворительно; зачтено;<br>74… 90 – хорошо;<br>91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматического зачета по дисциплине, возможность получения бонусных баллов</td><td colspan="8">Для допуска к промежуточной аттестации (зачету с оценкой) студент должен набрать по итогам текущего и рубежного контроля не менее 50 баллов и должен выполнить все лабораторные, практические работы и контрольную работу.<br>Для получения экзаменационной оценки «автоматически» студенту необходимо набрать следующее минимальное количество баллов:<br>- 68 для получения «автоматически» зачета с оценкой.<br>По согласованию с преподавателем студенту, набравшим 68 баллов, могут быть добавлены дополнительные (бонусные) баллы за активность на практических занятиях, активное участие в научной и методической работе, оригинальность принятых решений в ходе выполнения практических и лабораторных работ, за участие в значимых учебных и внеучебных мероприятиях кафедры и выставляется оценка хорошо, отлично «автоматически».</td></tr>
<tr><td>4</td><td>Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра</td><td colspan="8">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 лабораторных и практических работ.<br>Формы дополнительных заданий (назначаются преподавателем):<br>- выполнение и защита пропущенной лабораторной или практической работы (при невозможности дополнительного проведения лабораторной или практической работы преподаватель устанавливает форму дополнительного задания по тематике пропущенной работы самостоятельно) – до 5 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.</td></tr>
</table>

### 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 1 и 2 рубежного контроля из 10 вопросов. На каждое тестирование при рубежном контроле студенту отводится 1 академических часа.

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.

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

Зачет состоит из 2 вопросов. 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. Примеры оценочных средств для рубежных контролей и зачета

***1-ый рубежный контроль***

*1. Комплексная система технической защиты информации включает*

1. Совокупность мер от побочных электромагнитных излучений
2. Совокупность организационных и инженерных мероприятий, а также программно-аппаратурных средств, которые обеспечивают защиту информации в АС
3. совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации
4. Практические правила управления информационной безопасностью
5. Механизмы контроля, необходимых для построения системы управления информационной безопасностью организации, определённых на основе лучших примеров мирового опыт

*2. Целостность имеет две базовые реализации:*

1. защита отдельных информационных полей
2. для сетей с установлением связи
3. достоверность происхождения (источника) данных
4. системы с установлением связи
5. достоверность объекта коммуникации
6. системы без установления связи
7. защита от контроля трафика

8. без установления связи, каждая из которых может применяться для избранных групп информационных полей

*3. Средства защиты должны обеспечить защиту по следующим пяти направлениям:*

1. Защита процессов, процедур и программ обработки информации;
2. Организационная защита
3. Защита персонала
4. Защита объектов информационных систем;
5. Защита каналов связи
6. Правовая защита
7. Управление системой защиты
8. Защита конфиденциальных данных
9. Шифрование
10. Подавление побочных электромагнитных излучений

***2-ой рубежный контроль***

*1. Заключительным этапом построения системы защиты является*

1. Анализ уязвимых мест
2. Планирование
3. Сопровождение

*2. Какие меры НЕ позволяют повысить надежность параллельной защиты?*

1. Выбор простого пароля
2. Ограничение числа неудачных попыток входа в систему
3. управление сроком действия паролей, их периодическая смена

*3. К активным угрозам относятся…*

1. …копирование информации
2. …попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания
3. …разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ и операционной системы.

## ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЗАЧЕТУ

1. Основные задачи систем защиты информации.
2. Скрытие информации, дезинформация противника и легендирование.
3. Регулирование доступа к средствам обработки информации.
4. Маскировка информации. Регистрация сведений.
5. Уничтожение информации. Обеспечение сигнализации. Обеспечение реагирования.
6. Управление системой защиты. Обеспечение требуемого уровня готовности обслуживающего персонала.
7. Интеграция средств информационной безопасности в технологическую среду.
8. Функции центров защиты информации.
9. Принципы проектирования систем защиты информации.
10. Принцип конечной цели. Принцип измерения.

11. Принцип эквифинальности (завершенности). Принцип единства.
12. Принцип связности. Принцип модульного построения.
13. Принцип иерархии. Принцип функциональности. Принцип развития.
14. Принцип разумного сочетания централизации и децентрализации. Принцип неопределенности.
15. Формальные и неформальные средства реализации задач защиты информации.
16. Стратегии применения средств защиты информации.
17. Порядок и особенности проведения испытаний КСИБ.
18. Проверка организации и осуществления контроля за обеспечением информационной безопасности.
19. Контроль выполнения основных специальных требований по размещению и монтажу оборудования информационных систем.
20. Порядок и особенности внедрения КСИБ в эксплуатацию.
21. Общие сведения поисковых мероприятий. Периодичность поисковых мероприятий. Уровни чисток.
22. Перечень поисковых работ. Варианты комплектации поисковых подразделений.
23. Управление проектами. Сетевое планирование.
24. Управление стоимостью. Управление проектными рисками.
25. Планирование систем для бизнеса. Системное (тотальное) управление качеством.
26. Международный стандарт ISO 9000. Методика BSP. Подход CPI.
27. Методы оценки качества КСИБ.
28. Понятия «объективная вероятность» и «субъективная вероятность».
29. Сущность количественных и качественных показателей качества КСИБ.
30. Метод Дельфи. Общая характеристика метода. Основные недостатки. Этапы экспертного оценивания.
31. Метод QUEST. Метод SEER.
32. Постановка цели исследования. Выбор формы исследования, определение бюджета проекта. Подготовка информационных материалов.
33. Подбор экспертов. Проведение экспертизы. Статистический анализ результатов.
34. Общая характеристика метода Хоффмана. Оценка уязвимостей по Дж. Хоффману.
35. Виды угроз информации, которые можно выделить во внешней среде.
36. Общая схема воздействия на информацию в организационно-экономической системе.
37. Объективные предпосылки возникновения угроз информации.
38. Субъективные предпосылки возникновения угроз информации. Классификация каналов несанкционированного доступа по степени взаимодействия злоумышленника с информационными подсистемами.
39. Общая характеристика метода оценок рисков Фишера.
40. Эксплуатационная документация КСИБ.
41. Порядок работ по подготовке и проведению аттестации объектов информатизации (АС).
42. Правовые аспекты защиты информации. Общие сведения.

43. Подсистема организационно-правовой защиты.
44. Промышленный шпионаж и законодательство.
45. Стандарты и рекомендации по защите информации. Недостатки существующих стандартов и рекомендаций.
46. Организационно-штатная структура службы безопасности.
47. Структурная схема системы защиты информации.
48. Понятия «стандартизация» и «типизация» СЗИ. Допустимые и целесообразные типы СЗИ различных категорий.
49. Метод морфологического древовидного синтеза.
50. Морфологический метод лабиринтного синтеза.

### 6.5. 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. Безопасность информации в автоматизированных системах – М, Финансы и статистика: 2003- 368с: ил.- Доступ из ЭБС: ISBN 5-279-02560-7 http//studentlibrary.ru/book/ISBN5279025607html

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

3. Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г.Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

4. Мельников В.П. Информационная безопасность: 3е издание – М: Издательский центр «Академия», 2008

5. Гришина Н.В. Организация комплексной защиты информации – М: Гелиос АРВ, 2007

### 7.2 Дополнительная учебная литература:

1. Основы построения автоматизированных информационных систем. Учебник /В.А. Гвоздева, И.Ю. Лаврентьева – М – ИД ФОРУМ: НИЦ ИНФРА – М, 2013 – 320с – Доступ из ЭБС: http//znanium.com/bookread2/php?ищщл=392285/

2. В.А. Тихонов, В.В. Райх / Информационная безопасность: концептуальные, правовые, организационные и технические аспекты / М.: Гелиос АРВ, 2006

3. С.Н. Семкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачок / Основы организационного обеспечения информационной безопасности объектов / М.: Гелиос АРВ, 2005

### 7.3 Нормативные правовые акты

1. Доктрина информационной безопасности Российской Федерации: Утв. Президентом РФ 9 сентября 2000г. № Пр-1895 // Рос. газ. – 2000. – 28 сент.

### 7.4 Учебно-методическая литература

1. Полякова Е.Н. Методические указания к выполнению практических работ по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем» для студентов очной формы обучения направлений 10.05.03 и 10.03.01. Курган, КГУ, 2017 – 4 с.

2. Полякова Е.Н. Оценивание рисков. Технология оценки угроз и уязвимостей. Методические указания к выполнению лабораторных работ по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем» для студентов очной формы обучения направлений 10.05.03 и 10.03.01. Курган, КГУ, 2017 – 16 с.

3. Полякова Е.Н. Методические указания к выполнению контрольной работы по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем»» для студентов очной формы обучения направлений 10.05.03 и 10.03.01. Курган, КГУ, 2017 – 7 с.

4. Полякова Е.Н. Определение показателей защищенности информации при несанкционированном доступе. Оценка показателей качества функционирования комплексной системы защиты информации на предприятии. Расследование инцидентов в области информационной безопасности. Реагирование на инциденты. Методические указания к выполнению лабораторных работ по дисциплине «Комплексное обеспечение информационной безопасности автоматизированных систем» для студентов очной формы обучения направлений 10.05.03 и 10.03.01. Курган, КГУ, 2017 – 34 с.

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

1. ЭБС htt://www.iprbookshop.ru/
2. ЭБС htt://www.znanium.com/
3. ЭБС htt://www.studentlibrary.ru
4. http://www.counsultant.ru - справочная правовая система «Консультант Плюс»;
5. http://www.garant.ru – справочная правовая система «Гарант».
6. http://минобрнауки.рф/ Министерство образования и науки Российской Федерации.
7. http://nio.kgsu.ru/ Сайт КГУ. Научно-исследовательский отдел
8. http://window.edu.ru/. Единое окно доступа к образовательным ресурсам
9. http://elibrary.ru/. Научная электронная библиотека
10. http://dspace.kgsu.ru/xmlui/ Электронная библиотека КГУ

## 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
**«Комплексное обеспечение информационной безопасности автоматизированных систем»**

образовательной программы высшего образования –
программы специалитета
**10.05.03 – Информационная безопасность автоматизированных систем**
Направленность: (специализация №7)
**Обеспечение информационной безопасности распределенных информационных систем**

*Трудоемкость дисциплины:* 4 з.е. (144 академических часа)
*Семестр:* 8 (очная форма обучения)
*Форма промежуточной аттестации:* зачет с оценкой
*Содержание дисциплины. Основные разделы*

Проблемы обеспечения информационной безопасности и пути их решения. Комплексный подход к обеспечению информационной безопасности объекта. Формирование концепции обеспечения информационной безопасности. Управление информационной безопасностью. План обеспечения информационной безопасности предприятия.