**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Проректор по УР

Документ подписан электронной подписью
Сертификат: a1119608-cdff-4455-b54e-5235117c185c
Владелец: Сенченко Павел Васильевич
Действителен: с 17.09.2019 по 16.09.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Уровень образования: **высшее образование - магистратура**
Направление подготовки / специальность: **10.04.01 Информационная безопасность**
Направленность (профиль) / специализация: **Информационная безопасность объектов критической информационной инфраструктуры**
Форма обучения: **очная**
Факультет: **Факультет безопасности (ФБ)**
Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**
Курс: **2**
Семестр: **3**
Учебный план набора 2023 года

Объем дисциплины и виды учебной деятельности

| Виды учебной деятельности | 3 семестр | Всего | Единицы |
|---|---|---|---|
| Лекционные занятия | 28 | 28 | часов |
| Практические занятия | 28 | 28 | часов |
| Лабораторные занятия | 12 | 12 | часов |
| Самостоятельная работа | 40 | 40 | часов |
| Подготовка и сдача экзамена | 36 | 36 | часов |
| Общая трудоемкость (включая промежуточную аттестацию) | 144 | 144 | часов |
| | 4 | 4 | з.е. |

| Формы промежуточной аттестация | Семестр |
|---|---|
| Экзамен | 3 |

Томск

## 1. Общие положения

### 1.1. Цели дисциплины

1. Овладение основными принципами управления уровнем информационной безопасности защищаемых ресурсов организации.

### 1.2. Задачи дисциплины

1. Получение студентами знаний о структуре и принципах построения политики информационной безопасности организации.
2. Получение студентами умений и навыков по построению моделей угроз и нарушителей и по оценке рисков информационной безопасности в организации.
3. Получение студентами знаний об основных методах контроля обеспечения информационной безопасности в организации.

## 2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).
Часть блока дисциплин: Обязательная часть.
Модуль дисциплин: Модуль направления подготовки (hard skills – HS).
Индекс дисциплины: Б1.О.2.5.
Реализуется с применением электронного обучения, дистанционных образовательных технологий.

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

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):
Таблица 3.1 – Компетенции и индикаторы их достижения

| Компетенция | Индикаторы достижения компетенции | Планируемые результаты обучения по дисциплине |
|---|---|---|
| **Универсальные компетенции** | | |
| - | - | - |
| **Общепрофессиональные компетенции** | | |

| | | |
|---|---|---|
| ОПК-1. Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание; | ОПК-1.1. Знает меры (организационные, технические) и технологии обеспечения информационной безопасности | Знает организационные меры по управлению информационной безопасностью на объектах критической информационной инфраструктуры |
| | ОПК-1.2. Знает уязвимости систем и угрозы информационной безопасности | Знает методы выявления уязвимостей систем и угрозы информационной безопасности объектов критической информационной инфраструктуры. |
| | ОПК-1.3. Знает нормативную базу и ГОСТы, регламентирующие процесс разработки технических заданий на создание систем обеспечения информационной безопасности объектов | Знает нормативную базу и ГОСТы, регламентирующие процесс управления информационной безопасностью объектов критической информационной инфраструктуры. |
| | ОПК-1.4. Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности | Умеет обосновывать требования к процессам и технологиям обеспечения информационной безопасности объектов критической информационной инфраструктуры |
| | ОПК-1.5. Умеет осуществлять выбор подсистем, реализующих технологии обеспечения информационной безопасности | Умеет осуществлять выбор средств защиты информации объектов критической информационной инфраструктуры. |
| | ОПК-1.6. Умеет обосновывать требования к мерам обеспечения информационной безопасности | Умеет обосновывать требования к мерам обеспечения информационной безопасности объектов критической информационной инфраструктуры |
| | ОПК-1.7. Умеет разрабатывать техническое задание на создание подсистемы обеспечения информационной безопасности | Умеет разрабатывать техническое задание на создание средств защиты информации объектов критической информационной инфраструктуры. |
| | ОПК-1.8. Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности | Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности объектов критической информационной инфраструктуры |
| | ОПК-1.9. Знает нормативную и правовую базу в области обеспечения информационной безопасности, нормативные методические документы ФСБ России, ФСТЭК России и иных регуляторов в области обеспечения информационной безопасности | Знает нормативную и правовую базу в области обеспечения информационной безопасности объектов критической информационной инфраструктуры |
| | ОПК-1.10. Знает основы управления рисками информационной безопасности | Знает основы управления рисками информационной безопасности объектов критической информационной инфраструктуры |
| | ОПК-1.11. Умеет оценивать риски информационной безопасности | Умеет оценивать риски информационной безопасности объектов критической информационной инфраструктуры |

| | | |
|---|---|---|
| ОПК-3. Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности | ОПК-3.1. Знает нормативную и правовую базу в области обеспечения информационной безопасности, нормативные методические документы ФСБ России, ФСТЭК России и иных регуляторов в области обеспечения информационной безопасности | Знает нормативную и правовую базу в области управления информационной безопасностью объектов критической информационной инфраструктуры |
| | ОПК-3.2. Знает отечественные и зарубежные стандарты в области обеспечения информационной безопасности | Знает отечественные и зарубежные стандарты в области управления информационной безопасностью объектов критической информационной инфраструктуры |
| | ОПК-3.3. Знает структуру политик обеспечения информационной безопасности и требования к их содержанию | Знает структуру политик обеспечения информационной безопасности объектов критической информационной инфраструктуры и требования к их содержанию |
| | ОПК-3.4. Умеет разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности | Умеет разрабатывать проекты нормативных и организационно-распорядительных документов по обеспечению информационной безопасности объектов критической информационной инфраструктуры |
| | ОПК-3.5. Умеет разрабатывать политику информационной безопасности различных уровней | Умеет разрабатывать политику информационной безопасности объектов критической информационной инфраструктуры различных уровней |
| **Профессиональные компетенции** | | |
| - | - | - |

## 4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 4 зачетных единиц, 144 академических часов.

Распределение трудоемкости дисциплины по видам учебной деятельности представлено в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины по видам учебной деятельности

| Виды учебной деятельности | Всего часов | Семестры |
|---|---|---|
| | | 3 семестр |
| **Контактная аудиторная работа обучающихся с преподавателем, всего** | 68 | 68 |
| Лекционные занятия | 28 | 28 |
| Практические занятия | 28 | 28 |
| Лабораторные занятия | 12 | 12 |
| **Самостоятельная работа обучающихся, в т.ч. контактная внеаудиторная работа обучающихся с преподавателем, всего** | 40 | 40 |
| Подготовка к тестированию | 20 | 20 |
| Написание отчета по практическому занятию (семинару) | 14 | 14 |
| Подготовка к лабораторной работе, написание отчета | 6 | 6 |
| **Подготовка и сдача экзамена** | 36 | 36 |
| **Общая трудоемкость (в часах)** | 144 | 144 |
| **Общая трудоемкость (в з.е.)** | 4 | 4 |

## 5. Структура и содержание дисциплины

### 5.1. Разделы (темы) дисциплины и виды учебной деятельности

Структура дисциплины по разделам (темам) и видам учебной деятельности приведена в таблице 5.1.

Таблица 5.1 – Разделы (темы) дисциплины и виды учебной деятельности

| Названия разделов (тем) дисциплины | Лек. зан., ч | Прак. зан., ч | Лаб. раб. | Сам. раб., ч | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|---|
| **3 семестр** | | | | | | |
| 1 Анализ объекта защиты | 8 | 8 | - | 8 | 24 | ОПК-1, ОПК-3 |
| 2 Внутренние угрозы ИБ | 4 | 10 | - | 8 | 22 | ОПК-1, ОПК-3 |
| 3 Подбор и увольнение сотрудников | 2 | - | - | 2 | 4 | ОПК-1, ОПК-3 |
| 4 Текущая работа с персоналом | 2 | - | - | 2 | 4 | ОПК-1, ОПК-3 |
| 5 Разграничение доступа и контроль работы сотрудников | 2 | - | - | 2 | 4 | ОПК-1, ОПК-3 |
| 6 Управление инцидентами ИБ | 4 | - | 12 | 8 | 24 | ОПК-1, ОПК-3 |
| 7 Системы менеджмента ИБ | 2 | 10 | - | 6 | 18 | ОПК-1, ОПК-3 |
| 8 Свод правил по управлению ИБ | 2 | - | - | 2 | 4 | ОПК-1, ОПК-3 |
| 9 Обеспечение защиты информации в экстренных ситуациях | 2 | - | - | 2 | 4 | ОПК-1, ОПК-3 |
| Итого за семестр | 28 | 28 | 12 | 40 | 108 | |
| Итого | 28 | 28 | 12 | 40 | 108 | |

### 5.2. Содержание разделов (тем) дисциплины

Содержание разделов (тем) дисциплины (в т.ч. по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов (тем) дисциплины (в т.ч. по лекциям)

| Названия разделов (тем) дисциплины | Содержание разделов (тем) дисциплины (в т.ч. по лекциям) | Трудоемкость (лекционные занятия), ч | Формируемые компетенции |
|---|---|---|---|
| **3 семестр** | | | |
| 1 Анализ объекта защиты | Технология анализа объекта защиты. Типы информационных систем. Методы оценки ущерба от реализации угроз информационной безопасности. Комплекс стандартов в области информационной безопасности. | 8 | ОПК-1, ОПК-3 |
| | Итого | 8 | |
| 2 Внутренние угрозы ИБ | Подходы к формированию модели нарушителя и модели угроз. Требования регуляторов к формированию модели нарушителя и модели угроз | 4 | ОПК-1, ОПК-3 |
| | Итого | 4 | |

| | | | |
|---|---|---|---|
| 3 Подбор и увольнение сотрудников | Проверка персонала при приеме на работу. Сбор и анализ информации о физическом лице по методу SMICE. Использование информационных ресурсов Интер-нет для сбора информации о кандидате на работу в компанию. Получение информации о физическом лице с использованием поисковых систем, социальных сетей, баз данных, годовых отчетов акционерных обществ и иных источников. Порядок взаимодействия подразделений и должностных лиц компании по вопросам увольнения персонала. Проведение внутренних проверок и расследований происшествий. | 2 | ОПК-1, ОПК-3 |
| | Итого | 2 | |
| 4 Текущая работа с персоналом | Основные положения стандартов в области управления рисками информационной безопасности | 2 | ОПК-1, ОПК-3 |
| | Итого | 2 | |
| 5 Разграничение доступа и контроль работы сотрудников | Основные положения стандартов по проектированию, реализации и аудиту системы управления информационной безопасностью. Организация управления персоналом в контексте обеспечения информационной безопасности. | 2 | ОПК-1, ОПК-3 |
| | Итого | 2 | |
| 6 Управление инцидентами ИБ | Основные положения стандартов в области управления инцидентами информационной безопасности. Регламентация действий сотрудников при возникновении нештатных ситуаций. | 4 | ОПК-1, ОПК-3 |
| | Итого | 4 | |
| 7 Системы менеджмента ИБ | Понятие бизнес-рисков. Этапы внедрения систем менеджмента информационной безопасности (СМИБ). Определение должностных лиц, отвечающих за аспекты ИБ на этапах внедрения СМИБ. | 2 | ОПК-1, ОПК-3 |
| | Итого | 2 | |
| 8 Свод правил по управлению ИБ | Основные положения стандартов в области регламентации обеспечения информационной безопасности. | 2 | ОПК-1, ОПК-3 |
| | Итого | 2 | |
| 9 Обеспечение защиты информации в экстренных ситуациях | Изучение требований в части поддержания (и восстановления) функционирования защитных мер (функций и механизмов) обеспечения информационной безопасности (ИБ) информационно-телекоммуникационных систем (ИТС) организации в условиях чрезвычайной ситуации в контексте роли и места защитных мер ИБ ИТС в обеспечении непрерывности деятельности организации. | 2 | ОПК-1, ОПК-3 |
| | Итого | 2 | |

| | | |
|---|---|---|
| Итого за семестр | 28 | |
| Итого | 28 | |

### 5.3. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 5.3.

Таблица 5.3. – Наименование практических занятий (семинаров)

| Названия разделов (тем) дисциплины | Наименование практических занятий (семинаров) | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| **3 семестр** | | | |
| 1 Анализ объекта защиты | Формальное описание структуры информационной системы | 8 | ОПК-1, ОПК-3 |
| | Итого | 8 | |
| 2 Внутренние угрозы ИБ | Составление модели угроз информационной системе. Формирование требований к системе защиты информации. | 10 | ОПК-1, ОПК-3 |
| | Итого | 10 | |
| 7 Системы менеджмента ИБ | Формирование требований к политике информационной без-опасности. Формирование регламента действий при возникновении нештатных ситуаций. | 10 | ОПК-1, ОПК-3 |
| | Итого | 10 | |
| Итого за семестр | | 28 | |
| Итого | | 28 | |

### 5.4. Лабораторные занятия

Наименование лабораторных работ приведено в таблице 5.4.

Таблица 5.4 – Наименование лабораторных работ

| Названия разделов (тем) дисциплины | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| **3 семестр** | | | |
| 6 Управление инцидентами ИБ | Анализ рисков информационной безопасности на основе построения модели информационных потоков. | 4 | ОПК-1, ОПК-3 |
| | Анализ рисков на основе модели угроз и уязвимостей. | 4 | ОПК-1, ОПК-3 |
| | Анализ рисков на основе международного стандарта ISO 17799. | 4 | ОПК-1, ОПК-3 |
| | Итого | 12 | |
| Итого за семестр | | 12 | |
| Итого | | 12 | |

### 5.5. Курсовой проект / курсовая работа

Не предусмотрено учебным планом

### 5.6. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 5.6.

Таблица 5.6. – Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов (тем) дисциплины | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| **3 семестр** | | | | |
| 1 Анализ объекта защиты | Подготовка к тестированию | 4 | ОПК-1, ОПК-3 | Тестирование |
| | Написание отчета по практическому занятию (семинару) | 4 | ОПК-1, ОПК-3 | Отчет по практическому занятию (семинару) |
| | Итого | 8 | | |
| 2 Внутренние угрозы ИБ | Подготовка к тестированию | 3 | ОПК-1, ОПК-3 | Тестирование |
| | Написание отчета по практическому занятию (семинару) | 5 | ОПК-1, ОПК-3 | Отчет по практическому занятию (семинару) |
| | Итого | 8 | | |
| 3 Подбор и увольнение сотрудников | Подготовка к тестированию | 2 | ОПК-1, ОПК-3 | Тестирование |
| | Итого | 2 | | |
| 4 Текущая работа с персоналом | Подготовка к тестированию | 2 | ОПК-1, ОПК-3 | Тестирование |
| | Итого | 2 | | |
| 5 Разграничение доступа и контроль работы сотрудников | Подготовка к тестированию | 2 | ОПК-1, ОПК-3 | Тестирование |
| | Итого | 2 | | |
| 6 Управление инцидентами ИБ | Подготовка к тестированию | 2 | ОПК-1, ОПК-3 | Тестирование |
| | Подготовка к лабораторной работе, написание отчета | 6 | ОПК-1, ОПК-3 | Лабораторная работа |
| | Итого | 8 | | |
| 7 Системы менеджмента ИБ | Подготовка к тестированию | 1 | ОПК-1, ОПК-3 | Тестирование |
| | Написание отчета по практическому занятию (семинару) | 5 | ОПК-1, ОПК-3 | Отчет по практическому занятию (семинару) |
| | Итого | 6 | | |
| 8 Свод правил по управлению ИБ | Подготовка к тестированию | 2 | ОПК-1, ОПК-3 | Тестирование |
| | Итого | 2 | | |
| 9 Обеспечение защиты информации в экстренных ситуациях | Подготовка к тестированию | 2 | ОПК-1, ОПК-3 | Тестирование |
| | Итого | 2 | | |
| Итого за семестр | | 40 | | |

| | | | | |
|---|---|---|---|---|
| | Подготовка и сдача экзамена | 36 | | Экзамен |
| Итого | | 76 | | |

### 5.7. Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности

Соответствие компетенций, формируемых при изучении дисциплины, и видов учебной деятельности представлено в таблице 5.7.

Таблица 5.7 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

| Формируемые компетенции | Виды учебной деятельности | | | | Формы контроля |
|---|---|---|---|---|---|
| | Лек. зан. | Прак. зан. | Лаб. раб. | Сам. раб. | |
| ОПК-1 | + | + | + | + | Лабораторная работа, Отчет по практическому занятию (семинару), Тестирование, Экзамен |
| ОПК-3 | + | + | + | + | Лабораторная работа, Отчет по практическому занятию (семинару), Тестирование, Экзамен |

## 6. Рейтинговая система для оценки успеваемости обучающихся

### 6.1. Балльные оценки для форм контроля

Балльные оценки для форм контроля представлены в таблице 6.1.

Таблица 6.1 – Балльные оценки

| Формы контроля | Максимальный балл на 1-ую КТ с начала семестра | Максимальный балл за период между 1КТ и 2КТ | Максимальный балл за период между 2КТ и на конец семестра | Всего за семестр |
|---|---|---|---|---|
| **3 семестр** | | | | |
| Лабораторная работа | 10 | 10 | 10 | 30 |
| Тестирование | 10 | 15 | 0 | 25 |
| Отчет по практическому занятию (семинару) | 0 | 0 | 15 | 15 |
| Экзамен | | | | 30 |
| Итого максимум за период | 20 | 25 | 25 | 100 |
| Нарастающим итогом | 20 | 45 | 70 | 100 |

### 6.2. Пересчет баллов в оценки за текущий контроль

Пересчет баллов в оценки за текущий контроль представлен в таблице 6.2.

Таблица 6.2 – Пересчет баллов в оценки за текущий контроль

| Баллы на дату текущего контроля | Оценка |
|---|---|
| ≥ 90% от максимальной суммы баллов на дату ТК | 5 |
| От 70% до 89% от максимальной суммы баллов на дату ТК | 4 |
| От 60% до 69% от максимальной суммы баллов на дату ТК | 3 |
| < 60% от максимальной суммы баллов на дату ТК | 2 |

### 6.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 6.3.

Таблица 6.3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|---|---|---|
| 5 (отлично) (зачтено) | 90 – 100 | A (отлично) |
| 4 (хорошо) (зачтено) | 85 – 89 | B (очень хорошо) |
| | 75 – 84 | C (хорошо) |
| | 70 – 74 | D (удовлетворительно) |
| 3 (удовлетворительно) (зачтено) | 65 – 69 | |
| | 60 – 64 | E (посредственно) |
| 2 (неудовлетворительно) (не зачтено) | Ниже 60 баллов | F (неудовлетворительно) |

## 7. Учебно-методическое и информационное обеспечение дисциплины

### 7.1. Основная литература

1. Основы информационной безопасности : учебное пособие / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — Москва : Горячая линия-Телеком, 2011. — 558 с. — ISBN 5-93517-292-5. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/111016.

2. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. [Электронный ресурс]: — Режим доступа: https://urait.ru/bcode/497002 .

3. Андрианов, В. И. Инновационное управление рисками информационной безопасности : учебное пособие / В. И. Андрианов, А. В. Красов, В. А. Липатников. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2012. — 396 с. — ISBN 978-5-91891-092-4. пользователей. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/181472.

### 7.2. Дополнительная литература

1. ГОСТ Р ИСО/МЭК ТО 18044-2007. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности. М., 2009, 50 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=173886 .

2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М., 2022, 28 с. [Электронный ресурс]: — Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=242006.

3. ГОСТ Р ИСО/МЭК 27002-2021. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. М., 2021, 74 с. [Электронный ресурс]: — Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=240766.

4. ГОСТ Р ИСО/МЭК 27003-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации. М., 2021, 46с. [Электронный ресурс]: — Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=240709.

5. ГОСТ Р ИСО/МЭК 27004-2021. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание. М., 2021, 50 с. [Электронный ресурс]: — Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=240761.

6. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. М., 2011, 51 с. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=177398 .

7. ГОСТ Р ИСО/МЭК 27006-2020. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. М., 2021, 42 с. [Электронный ресурс]: — Режим доступа: https://protect.gost.ru/document.aspx?control=7&id=238756.

8. ГОСТ Р ИСО/МЭК 27007-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187871 .
9. ГОСТ Р ИСО/МЭК 27011-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководства по менеджменту информационной безопасности для телекоммуникационных организаций на основе ИСО/МЭК 27002. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=183954 .
10. ГОСТ Р ИСО/МЭК 27013-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководство по совместному использованию стандартов ИСО/МЭК 27001 и ИСО/МЭК 20000-1. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187948 .
11. ГОСТ Р ИСО/МЭК 27031-2012. Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=184904 .
12. ГОСТ Р ИСО/МЭК 27033-1-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=179072 .
13. ГОСТ Р ИСО/МЭК 27033-3-2011. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187869 .
14. ГОСТ Р ИСО/МЭК 27034-1-2014. Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187929 .
15. ГОСТ Р ИСО/МЭК 27037-2014. Информационная технология. Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, пред-ставленных в цифровой форме. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document.aspx?control=7&id=187854 .
16. ГОСТ Р ИСО/МЭК 27038-2016. Информационные технологии. Методы обеспечения безопасности. Требования и методы электронного цензурирования. [Электронный ресурс]: — Режим доступа: http://protect.gost.ru/document1.aspx?control=31&id=204467 .
17. Ал□шкин, А. С. Аппаратные и программные средства поиска уязвимостей при моделировании и эксплуатации информационных систем (обеспечение информационной безопасности) : учебное пособие / А. С. Ал□шкин, С. А. Лесько, Д. О. Жуков. — Москва : РТУ МИРЭА, 2020. — 152 с. [Электронный ресурс]: — Режим доступа: https://e.lanbook.com/book/167600.

### 7.3. Учебно-методические пособия

#### 7.3.1. Обязательные учебно-методические пособия

1. Конев, А. А. Управление информационной безопасностью: учебно-методическое пособие [Электронный ресурс] / А. А. Конев, А. Ю. Якимук. — Томск: ТУСУР, 2022. — 124 с. [Электронный ресурс]: — Режим доступа: https://edu.tusur.ru/publications/9989.

#### 7.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

**Для лиц с нарушениями зрения:**

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

– в форме электронного документа;

– в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

– в форме электронного документа;

– в печатной форме.

### 7.4. Современные профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется обращаться к современным базам данных, информационно-справочным и поисковым системам, к которым у ТУСУРа открыт доступ: https://lib.tusur.ru/ru/resursy/bazy-dannyh.

## 8. Материально-техническое и программное обеспечение дисциплины

### 8.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с достаточным количеством посадочных мест для учебной группы, оборудованная доской и стандартной учебной мебелью. Имеются мультимедийное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

### 8.2. Материально-техническое и программное обеспечение для практических занятий

Аудитория Интернет-технологий и информационно-аналитической деятельности: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

### 8.3. Материально-техническое и программное обеспечение для лабораторных работ

Аудитория Интернет-технологий и информационно-аналитической деятельности: учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа; 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 402 ауд.

Описание имеющегося оборудования:

- Интерактивная доска IQBoard DVT TN100;
- Проектор Optoma EH400;
- Веб-камера Logitech C920s;
- Акустическая система Yamaha;
- Комплект беспроводных микрофонов Clevermic;
- Магнитно-маркерная доска;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

### 8.4. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 209 ауд.;

- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Описание имеющегося оборудования:
- учебная мебель;
- компьютеры;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду ТУСУРа.

Перечень программного обеспечения:
- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;
- Google Chrome.

### 8.5. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися с **нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися с **нарушениями зрения** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися с **нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

## 9. Оценочные материалы и методические рекомендации по организации изучения дисциплины

### 9.1. Содержание оценочных материалов для текущего контроля и промежуточной аттестации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы, представленные в таблице 9.1.

Таблица 9.1 – Формы контроля и оценочные материалы

| Названия разделов (тем) дисциплины | Формируемые компетенции | Формы контроля | Оценочные материалы (ОМ) |
|---|---|---|---|
| 1 Анализ объекта защиты | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| | | Отчет по практическому занятию (семинару) | Темы практических занятий |

| | | | |
|---|---|---|---|
| 2 Внутренние угрозы ИБ | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| | | Отчет по практическому занятию (семинару) | Темы практических занятий |
| 3 Подбор и увольнение сотрудников | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| 4 Текущая работа с персоналом | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| 5 Разграничение доступа и контроль работы сотрудников | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| 6 Управление инцидентами ИБ | ОПК-1, ОПК-3 | Лабораторная работа | Темы лабораторных работ |
| | | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| 7 Системы менеджмента ИБ | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| | | Отчет по практическому занятию (семинару) | Темы практических занятий |
| 8 Свод правил по управлению ИБ | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |
| 9 Обеспечение защиты информации в экстренных ситуациях | ОПК-1, ОПК-3 | Тестирование | Примерный перечень тестовых заданий |
| | | Экзамен | Перечень экзаменационных вопросов |

Шкала оценки сформированности отдельных планируемых результатов обучения по дисциплине приведена в таблице 9.2.

Таблица 9.2 – Шкала оценки сформированности планируемых результатов обучения по дисциплине

| Оценка | Баллы за ОМ | Формулировка требований к степени сформированности планируемых результатов обучения | | |
|---|---|---|---|---|
| | | знать | уметь | владеть |
| 2 (неудовлетворительно) | < 60% от максимальной суммы баллов | отсутствие знаний или фрагментарные знания | отсутствие умений или частично освоенное умение | отсутствие навыков или фрагментарные применение навыков |
| 3 (удовлетворительно) | от 60% до 69% от максимальной суммы баллов | общие, но не структурированные знания | в целом успешно, но не систематически осуществляемое умение | в целом успешное, но не систематическое применение навыков |
| 4 (хорошо) | от 70% до 89% от максимальной суммы баллов | сформированные, но содержащие отдельные проблемы знания | в целом успешное, но содержащие отдельные пробелы умение | в целом успешное, но содержащие отдельные пробелы применение навыков |
| 5 (отлично) | ≥ 90% от максимальной суммы баллов | сформированные систематические знания | сформированное умение | успешное и систематическое применение навыков |

Шкала комплексной оценки сформированности компетенций приведена в таблице 9.3.

Таблица 9.3 – Шкала комплексной оценки сформированности компетенций

| Оценка | Формулировка требований к степени компетенции |
|---|---|
| 2 (неудовлетворительно) | Не имеет необходимых представлений о проверяемом материале<br>или<br>Знать на уровне **ориентирования**, представлений. Обучающийся знает основные признаки или термины изучаемого элемента содержания, их отнесенность к определенной науке, отрасли или объектам, узнает в текстах, изображениях или схемах и знает, к каким источникам нужно обращаться для более детального его усвоения. |
| 3 (удовлетворительно) | Знать и уметь на **репродуктивном** уровне. Обучающихся знает изученный элемент содержания репродуктивно: произвольно воспроизводит свои знания устно, письменно или в демонстрируемых действиях. |
| 4 (хорошо) | Знать, уметь, владеть на **аналитическом** уровне. Зная на репродуктивном уровне, указывать на особенности и взаимосвязи изученных объектов, на их достоинства, ограничения, историю и перспективы развития и особенности для разных объектов усвоения. |
| 5 (отлично) | Знать, уметь, владеть на **системном** уровне. Обучающийся знает изученный элемент содержания системно, произвольно и доказательно воспроизводит свои знания устно, письменно или в демонстрируемых действиях, учитывая и указывая связи и зависимости между этим элементом и другими элементами содержания дисциплины, его значимость в содержании дисциплины. |

### 9.1.1. Примерный перечень тестовых заданий

1. Какие ресурсы используют при построении модели информационных потоков в ГРИФ?
   a) Группы пользователей и права доступа
   b) Пользователи и группы
   c) Сервер и рабочая станция
   d) Риски и контрмеры

2. По каким угрозам в системе ГРИФ не оценивается ущерб?
   a) Конфиденциальности
   b) Целостности
   c) Достоверность
   d) Доступность

3. Какой категории угроз не представлено в системе ГРИФ?
   a) Физические угрозы человека
   b) Угрозы персонала
   c) Системные ошибки
   d) Физические угрозы

4. Какого типа экономического ущерба не существует?
   a) Долговременный экономический ущерб
   b) Кратковременный экономический ущерб
   c) Отсроченный экономический ущерб
   d) Немедленный экономический ущерб

5. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «нарушение бизнес-деятельности»?
   a) Кратковременный экономический ущерб
   b) Отсроченный экономический ущерб
   c) Немедленный экономический ущерб
   d) Долговременный экономический ущерб

6. Как повлияет на веса средств защиты ответ «Положения политики внедрены частично» на первый вопрос раздела о политике безопасности?
   a) Не повлияет
   b) Приравняет к нулю
   c) Вызовет уменьшение
   d) Вызовет рост

7. Какая из перечисленных выполняемых проверок не входит в перечень обязательных действий, входящих в руководство по реализации средств управления против злонамеренного кода?
   a) Проверка любых файлов на электронном или оптическом носителе, а также файлов, полученных по сетям, на наличие злонамеренного кода перед использованием
   b) Проверка web-страниц на наличие злонамеренного кода
   c) Проверка обновлений средства управления против злонамеренного кода
   d) Проверка приложений к электронным письмам и загрузок на наличие злонамеренного кода перед использованием

8. По какой причине для класса группы авторизованных интернет-пользователей в системе ГРИФ не предлагается никаких средств защиты рабочего места?
   a) Для данной группы характерна минимальная вероятность реализации угрозы
   b) Для группы по умолчанию выбран набор средств защиты рабочего места
   c) Для группы неизвестно, откуда будет осуществляться доступ
   d) Для группы неизвестна степень влияния на систему

9. Какие данные нельзя указать при задании контрмер в системе ГРИФ?
   a) Стоимость внедрения

b) Возможное снижение затрат на ИБ
c) Срок внедрения контрмеры
d) Название для отчета

10. Какие параметры нельзя включить в состав отчета по проекту в системе КОНДОР?
a) Выполненные требования
b) Невыполненные требования
c) Риски
d) Контрмеры

11. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «подрыв репутации»?
a) Кратковременный экономический ущерб
b) Отсроченный экономический ущерб
c) Долговременный экономический ущерб
d) Немедленный экономический ущерб

12. Какой тип экономического ущерба должен быть присвоен при обнаружении критерия «снижение розничных продаж»?
a) Отсроченный экономический ущерб
b) Немедленный экономический ущерб
c) Кратковременный экономический ущерб
d) Долговременный экономический ущерб

13. Какой информации не содержится в отчете по периоду, формируемом системой КОНДОР?
a) Количество выполненных и невыполненных требований в целом по системе для выбранного периода аудита
b) Уровень риска невыполнения требований стандарта в целом по системе для выбранного периода аудита
c) Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
d) Затраты на контрмеры в целом по системе для выбранного периода аудита

14. Чему по умолчанию равны вероятность в течение года и критичность реализации для только что созданной угрозы?
a) 25 %
b) 15 %
c) %
d) 0 %

15. Какой информации не содержится в отчете по проекту, формируемом системой КОНДОР?
a) Изменения количества выполненных требований в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
b) Изменения уровня риска в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита
c) Текст выполненных требований по каждому разделу
d) Изменения затрат на контрмеры в целом по системе, по всем разделам или для каждого раздела в выбранных периодах аудита

16. Какое количество мер защиты содержит в себе «Оценка уровня обеспечения ИБ организации БС РФ в соответствии с требованиями СТО БР ИББС-1.0»?
a) 32
b) 33
c) 34
d) 35

17. В каком формате выводятся результаты оценки объекта на предмет обеспечения требований из СТО БР ИББС-1.2?
    a) Диаграмма Ганта
    b) Гистограмма
    c) Круговая диаграмма
    d) Срез структуры

18. Что понимается под базовым временем простоя ресурсов?
    a) Время необходимое на обработку информации после запроса
    b) Время отклика системы на запрос
    c) Время, в течение которого доступ к информации ресурса невозможен
    d) Время, в течение которого система загружает необходимые для работы службы

19. Фактором, значимым для использования уязвимости не является?
    a) Время, затрачиваемое на идентификацию уязвимости
    b) Техническая компетентность специалиста
    c) Программное средство, требуемое для анализа
    d) Знание проекта и функционирования объекта

20. Что понимается под эффективностью средства защиты информации?
    a) Показатель быстродействия системы в условиях использования средств защиты информации
    b) Коэффициент снижения уровня риска по отношению к первоначальному уровню
    c) Степень влияния на защищенность информации и рабочего места группы пользователей
    d) Субъективная оценка экспертами корректности функционирования средства защи-ты информации

21. Что понимается под базовой вероятностью конфиденциальности?
    a) Вероятность огласки информации минимального уровня конфиденциальности в системе
    b) Минимальная вероятность реализации угрозы
    c) Максимальная вероятность реализации угрозы
    d) Вероятность огласки информации максимального уровня конфиденциальности в системе

22. Какой тип внутренних нарушителей наиболее подвержен социальной инженерии?
    a) Подрабатывающий
    b) Внедренный
    c) Манипулируемый
    d) Нелояльный

23. К внешним чрезвычайным ситуациям не относятся?
    a) Стихийные бедствия
    b) Преступные действия
    c) Техногенные аварии и сбои
    d) Диверсии

24. Что не входит перечень того, что для любой организации, серьезно относящейся к информационной безопасности, важно применять в структурном и плановом подходе ГОСТ Р ИСО/МЭК ТО 18044–2007?
    a) Обнаружение, оповещение об инцидентах информационной безопасности и их оценка
    b) Реагирование на инциденты информационной безопасности, включая активацию защитных мер для предотвращения, уменьшения последствий и (или) восстановление после негативных воздействий
    c) Предотвращение инцидентов информационной безопасности

d) Извлечение уроков из инцидентов информационной безопасности, введение превентивных защитных мер и улучшение общего подхода к менеджменту инцидентов информационной безопасности

25. Что понимается под инцидентом информационной безопасности?
    a) Процесс сравнения количественно оцененного риска с заданными критериями рис-ка для определения его значимости
    b) Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности
    c) Появление одного или нескольких нежелательных или неожиданных событий информационной безопасности, с которыми связана значительная вероятность компрометации бизнес-операций и создания угрозы информационной безопасности
    d) Процесс обеспечения восстановления операции в случае возникновения какого-либо неожиданного или нежелательного инцидента, способного негативно воздействовать на непрерывность важных функций бизнеса и поддерживающих его эле-ментов

26. К какому варианту неработоспособности относится болезнь сотрудника?
    a) Полное прекращение выполнения сотрудником своих обязанностей
    b) Опасность для жизни персонала
    c) Прекращение выполнения сотрудником рутинных операций
    d) Саботаж

27. К какой группе внешних чрезвычайных ситуаций относится скупка контрольного па-кета акций?
    a) Общественные
    b) Правовые
    c) Экономические
    d) Стихийные бедствия

28. Какому из перечисленных типов внутренних нарушителей характерна постановка за-дачи извне?
    a) Халатный
    b) Манипулируемый
    c) Подрабатывающий
    d) Обиженный

29. Что понимается под характеристиками группы пользователей?
    a) Состав группы пользователей
    b) Название группы пользователей
    c) Вид доступа группы пользователей
    d) Описание группы пользователей

30. Какая статья расходов не входит в расходы на информационную безопасность?
    a) Затраты на приобретение систем защиты информации
    b) Затраты на управление системой защиты информации
    c) Затраты на разработку политики безопасности
    d) Затраты на обучение персонала

31. Что произойдет, если задать пороговое значение риска в 50% в системе КОНДОР?
    a. Будут отображены все положения стандартов, риски для которых ниже 50%
    b. Будут отображены все положения стандартов, риски для которых выше 50%
    c. Будут отображены только критичные положения стандартов, которые не выполнены
    d. Будут отображены только критичные положения стандартов, которые выполнены

### 9.1.2. Перечень экзаменационных вопросов

1. Цель и этапы анализа объектов защиты.
2. Перечислите этапы оценки рисков информационной безопасности автоматизированных систем.
3. Идентификация и классификация объектов защиты.
4. Типизация информационных систем. Данные об информационной системе, необходимые для построения модели документооборота.
5. Подходы к разграничению доступа в рамках организации. Структура документов, регламентирующих разграничение доступа.
6. Подходы к построению модели нарушителя.
7. Классификация нарушителей (ФСТЭК).
8. Классификация угроз безопасности персональных данных (ФСТЭК).
9. Методика определения актуальных угроз (ФСТЭК).
10. Методика оценки ущерба, нанесённого при реализации угроз информационной безопасности.
11. Угрозы, источником которых является персонал организации.
12. Методы «социальной инженерии» и способы защиты от них.
13. Обязанности сотрудников Службы безопасности при приёме сотрудников на работу.
14. Нормативная документация, обязательная к ознакомлению и подписанию при приёме на работу.
15. Предоставление сотруднику доступа к конфиденциальной информации. Основные разделы Инструкции по внесению изменений в списки пользователей.
16. Обязанности сотрудников Службы безопасности при обучении и увольнении сотрудников.
17. Упрощённая модель классификации субъектов.
18. Основные положения инструкции по установке, модификации и техническому обслуживанию программного обеспечения и аппаратных средств автоматизированной системы организации.
19. Основные положения регламента контроля использования технических средств обработки и передачи информации.
20. Основные положения инструкции по организации парольной защиты.
21. Основные положения документов, регламентирующих использование средств аутентификации и носителей ключевой информации.
22. Основные положения инструкции по организации антивирусной защиты.
23. Основные положения инструкции по работе с электронной почтой.
24. Типы чрезвычайных ситуаций. Структура аварийного плана. Причины изменения аварийного плана.
25. Классификация объектов при составлении аварийного плана.
26. Требования к различным классам объектов и их резервированию.
27. Основные положения плана обеспечения непрерывной работы и восстановления работоспособности.
28. Приведите примеры источников информации об инцидентах информационной безопасности.
29. Перечислите аспекты анализа инцидентов информационной безопасности, направленные на совершенствование системы управления информационной безопасностью.
30. Приведите требования к формированию политики информационной безопасности организации и учитываемые в ней категории безопасности.

### 9.1.3. Темы практических занятий

1. Формальное описание структуры информационной системы
2. Составление модели угроз ин-формационной системе. Формирование требований к системе защиты информации.
3. Формирование требований к политике информационной без-опасности. Формирование регламента действий при возникновении нештатных ситуаций.

### 9.1.4. Темы лабораторных работ

1. Анализ рисков информационной безопасности на основе построения модели информационных потоков.

2. Анализ рисков на основе модели угроз и уязвимостей.
3. Анализ рисков на основе международного стандарта ISO 17799.

### 9.2. Методические рекомендации

Учебный материал излагается в форме, предполагающей самостоятельное мышление студентов, самообразование. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.

Начать изучение дисциплины необходимо со знакомства с рабочей программой, списком учебно-методического и программного обеспечения. Самостоятельная работа студента включает работу с учебными материалами, выполнение контрольных мероприятий, предусмотренных учебным планом.

В процессе изучения дисциплины для лучшего освоения материала необходимо регулярно обращаться к рекомендуемой литературе и источникам, указанным в учебных материалах; пользоваться через кабинет студента на сайте Университета образовательными ресурсами электронно-библиотечной системы, а также общедоступными интернет-порталами, содержащими научно-популярные и специализированные материалы, посвященные различным аспектам учебной дисциплины.

При самостоятельном изучении тем следуйте рекомендациям:

– чтение или просмотр материала осуществляйте со скоростью, достаточной для индивидуального понимания и освоения материала, выделяя основные идеи; на основании изученного составить тезисы. Освоив материал, попытаться соотнести теорию с примерами из практики;

– если в тексте встречаются незнакомые или малознакомые термины, следует выяснить их значение для понимания дальнейшего материала;

– осмысливайте прочитанное и изученное, отвечайте на предложенные вопросы.

Студенты могут получать индивидуальные консультации, в т.ч. с использованием средств телекоммуникации.

По дисциплине могут проводиться дополнительные занятия, в т.ч. в форме вебинаров. Расписание вебинаров и записи вебинаров публикуются в электронном курсе / электронном журнале по дисциплине.

### 9.3. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 9.4.

Таблица 9.4 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

| Категории обучающихся | Виды дополнительных оценочных материалов | Формы контроля и оценки результатов обучения |
|---|---|---|
| С нарушениями слуха | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы | Преимущественно письменная проверка |
| С нарушениями зрения | Собеседование по вопросам к зачету, опрос по терминам | Преимущественно устная проверка (индивидуально) |
| С нарушениями опорно-двигательного аппарата | Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету | Преимущественно дистанционными методами |
| С ограничениями по общемедицинским показаниям | Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы | Преимущественно проверка методами, определяющимися исходя из состояния обучающегося на момент проверки |

### 9.4. Методические рекомендации по оценочным материалам для лиц с ограниченными

**возможностями здоровья и инвалидов**

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух;

– предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

**Для лиц с нарушениями зрения:**

– в форме электронного документа;

– в печатной форме увеличенным шрифтом.

**Для лиц с нарушениями слуха:**

– в форме электронного документа;

– в печатной форме.

**Для лиц с нарушениями опорно-двигательного аппарата:**

– в форме электронного документа;

– в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

**ЛИСТ СОГЛАСОВАНИЯ**

Рассмотрена и одобрена на заседании кафедры КИБЭВС
протокол № 1 от «25» 1 2022 г.

**СОГЛАСОВАНО:**

| Должность | Инициалы, фамилия | Подпись |
|---|---|---|
| Заведующий выпускающей каф. КИБЭВС | А.А. Шелупанов | Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d |
| Заведующий обеспечивающей каф. КИБЭВС | А.А. Шелупанов | Согласовано, c53e145e-8b20-45aa-9347-a5e4dbb90e8d |
| Начальник учебного управления | Е.В. Саврук | Согласовано, fa63922b-1fce-4a6a-845d-9ce7670b004c |

**ЭКСПЕРТЫ:**

| | | |
|---|---|---|
| Доцент, каф. КИБЭВС | Е.Ю. Костюченко | Согласовано, c6235dfe-234a-4234-88f9-e1597aac6463 |
| Доцент, каф. КИБЭВС | А.А. Конев | Согласовано, 81687a04-85ce-4835-9e1e-9934a6085fdd |

**РАЗРАБОТАНО:**

| | | |
|---|---|---|
| Доцент, каф. КИБЭВС | А.Ю. Якимук | Разработано, 4ffdf265-fb78-4863-b293-f03438cb07cc |