**МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**Федеральное государственное бюджетное образовательное учреждение высшего образования**

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

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# Комплексные системы защиты информации в сетях и системах связи

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **11.03.02 Инфокоммуникационные технологии и системы связи**
Направленность (профиль) / специализация: **Защищенные системы и сети связи**
Форма обучения: **очная**
Факультет: **РТФ, Радиотехнический факультет**
Кафедра: **РСС, Кафедра радиоэлектроники и систем связи**
Курс: **4**
Семестр: **7, 8**
Учебный план набора 2016 года

Распределение рабочего времени

| № | Виды учебной деятельности | 7 семестр | 8 семестр | Всего | Единицы |
|---|---|---|---|---|---|
| 1 | Лекции | 36 | 0 | 36 | часов |
| 2 | Практические занятия | 12 | 14 | 26 | часов |
| 3 | Лабораторные работы | 36 | 0 | 36 | часов |
| 4 | Контроль самостоятельной работы (курсовой проект / курсовая работа) | 0 | 10 | 10 | часов |
| 5 | Всего аудиторных занятий | 84 | 24 | 108 | часов |
| 6 | Самостоятельная работа | 60 | 84 | 144 | часов |
| 7 | Всего (без экзамена) | 144 | 108 | 252 | часов |
| 8 | Подготовка и сдача экзамена | 36 | 0 | 36 | часов |
| 9 | Общая трудоемкость | 180 | 108 | 288 | часов |
| | | 5.0 | 3.0 | 8.0 | З.Е. |

Экзамен: 7 семестр
Зачет: 8 семестр
Курсовой проект / курсовая работа: 8 семестр

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Шелупанов А.А.
Должность: Ректор
Дата подписания: 23.08.2017
Уникальный программный ключ:
c53e145e-8b20-45aa-9347-a5e4dbb90e8d

Томск 2018

Согласована на портале № 40606

Рассмотрена и одобрена на заседании кафедры
протокол № 11 от « 3 » 7 2018 г.

# ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 11.03.02 Инфокоммуникационные технологии и системы связи, утвержденного 06.03.2015 года, рассмотрена и одобрена на заседании кафедры РСС «___» _____ 20__ года, протокол №_____.

Разработчик:

доцент кафедра Радиоэлектроники и систем связи (РСС) _____ Д. В. Дубинин

Заведующий обеспечивающей каф. РСС _____ А. В. Фатеев

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан РТФ _____ К. Ю. Попова

Заведующий выпускающей каф. РСС _____ А. В. Фатеев

Эксперты:

Профессор кафедры радиоэлектроники и систем связи (РСС) _____ А. С. Задорин

Старший преподаватель кафедры радиоэлектроники и систем связи (РСС) _____ Ю. В. Зеленецкая

Согласована на портале № 40606

## 1. Цели и задачи дисциплины

### 1.1. Цели дисциплины

Целью преподавания дисциплины является формирование у студентов устойчивых основ знаний организации комплексных систем защиты информации в сетях и системах связи и методов ее управления, приобретения при этом необходимых умений и навыков.

### 1.2. Задачи дисциплины

- Основными задачами изучения дисциплины являются:
- изучение сущности и задач комплексной системы защиты информации (КСЗИ);
- изучение принципов организации и этапов разработки КСЗИ, факторов, влияющих на организацию КСЗИ;
- определение и нормативное закрепление состава защищаемой информации;
- определение объектов защиты;
- анализ и оценка угроз безопасности информации: выявление и оценка источников,
- способов и результатов дестабилизирующего воздействия на информацию;
- определение потенциальных каналов и методов несанкционированного доступа к информации, определение возможностей несанкционированного доступа к защищаемой информации;
- определение компонентов и условий функционирования КСЗИ, разработка модели, технологического и организационного построения КСЗИ;
- кадровое, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ;
- назначение, структура и содержание управления КСЗИ, изучение принципов и методы планирования, сущности и содержание контроля функционирования КСЗИ;
- изучение особенностей управления КСЗИ в условиях чрезвычайных ситуаций;
- изучение состава методов и моделей оценки эффективности КСЗИ.

## 2. Место дисциплины в структуре ОПОП

Дисциплина «Комплексные системы защиты информации в сетях и системах связи» (Б1.В.ОД.12) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Введение в профиль "Защищенные системы связи", Вычислительная техника и информационные технологии, Защита информационных процессов в сетях и системах связи, Информатика, Общая теория связи, Организация и управление службой защиты информации на предприятиях связи, Основы криптографии, Основы организационно-правового обеспечения информационной безопасности сетей и систем, Основы построения защищенных инфокоммуникационных систем и сетей, Сетевые технологии высокоскоростной передачи данных, Сети связи и системы коммутации, Схемотехника телекоммуникационных устройств, Комплексные системы защиты информации в сетях и системах связи.

Последующими дисциплинами являются: Преддипломная практика, Программно-аппаратные средства защиты сетей и систем связи, Программно-аппаратные средства связи, Техническая защита информации в сетях и системах связи, Комплексные системы защиты информации в сетях и системах связи.

## 3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ПК-13 способностью осуществлять подготовку типовых технических проектов на различные инфокоммуникационные объекты;
- ПК-14 умением осуществлять первичный контроль соответствия разрабатываемых проектов и технической документации национальным и международным стандартам и техническим регламентам;

В результате изучения дисциплины обучающийся должен:

- **знать** Основы организации и управления комплексной системой защиты информации в сетях и системах связи.

Согласована на портале № 40606

– **уметь** На концептуальном и практическом уровне разрабатывать и внедрять комплексные системы защиты информации в сетях и системах связи.

– **владеть** Навыками внедрения комплексных систем защиты информации в сетях и системах связи.

## 4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 8.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

| Виды учебной деятельности | Всего часов | Семестры | |
|---|---|---|---|
| | | 7 семестр | 8 семестр |
| Аудиторные занятия (всего) | 108 | 84 | 24 |
| Лекции | 36 | 36 | 0 |
| Практические занятия | 26 | 12 | 14 |
| Лабораторные работы | 36 | 36 | 0 |
| Контроль самостоятельной работы (курсовой проект / курсовая работа) | 10 | 0 | 10 |
| Самостоятельная работа (всего) | 144 | 60 | 84 |
| Оформление отчетов по лабораторным работам | 80 | 24 | 56 |
| Проработка лекционного материала | 15 | 15 | 0 |
| Подготовка к практическим занятиям, семинарам | 49 | 21 | 28 |
| Всего (без экзамена) | 252 | 144 | 108 |
| Подготовка и сдача экзамена | 36 | 36 | 0 |
| Общая трудоемкость, ч | 288 | 180 | 108 |
| Зачетные Единицы | 8.0 | 5.0 | 3.0 |

## 5. Содержание дисциплины

### 5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

| Названия разделов дисциплины | Лек., ч | Прак. зан., ч | Лаб. раб., ч | КП/КР, ч | Сам. раб., ч | Всего часов (без экзамена) | Формируемые компетенции |
|---|---|---|---|---|---|---|---|
| 7 семестр | | | | | | | |
| 1 Введение. | 1 | 2 | 0 | 0 | 4 | 7 | ПК-13, ПК-14 |
| 2 Содержание и этапы проведения работ по организации комплексной системы защиты информации. | 5 | 0 | 0 | 0 | 4 | 9 | ПК-13, ПК-14 |
| 3 Определение компонентов КСЗИ. | 9 | 4 | 0 | 0 | 4 | 17 | ПК-13, ПК-14 |
| 4 Технология определения и клас- | 7 | 2 | 0 | 0 | 3 | 12 | ПК-13, ПК- |

Согласована на портале № 40606

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| сификации состава и защищенности информации. | | | | | | | 14 |
| 5 Построение комплексной системы защиты информации. | 4 | 2 | 0 | 0 | 8 | 14 | ПК-13, ПК-14 |
| 6 Управление комплексной системой защиты информации. | 2 | 2 | 0 | 0 | 6 | 10 | ПК-13, ПК-14 |
| 7 Служба защиты информации. | 4 | 0 | 0 | 0 | 2 | 6 | ПК-13, ПК-14 |
| 8 Особенностей управления КСЗИ в условиях чрезвычайных ситуаций. | 2 | 0 | 0 | 0 | 2 | 4 | ПК-13, ПК-14 |
| 9 Состав методов и моделей оценки эффективности КСЗИ. | 2 | 0 | 0 | 0 | 3 | 5 | ПК-13, ПК-14 |
| 10 Экзамен. | 0 | 0 | 36 | 0 | 24 | 60 | ПК-13, ПК-14 |
| Итого за семестр | 36 | 12 | 36 | 0 | 60 | 144 | |
| 8 семестр | | | | | | | |
| 11 Зачёт. | 0 | 14 | 0 | 10 | 84 | 98 | ПК-13, ПК-14 |
| Итого за семестр | 0 | 14 | 0 | 10 | 84 | 108 | |
| Итого | 36 | 26 | 36 | 10 | 144 | 252 | |

### 5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

| Названия разделов | Содержание разделов дисциплины (по лекциям) | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 7 семестр | | | |
| 1 Введение. | Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса. | 1 | ПК-13, ПК-14 |
| | Итого | 1 | |
| 2 Содержание и этапы проведения работ по организации комплексной системы защиты информации. | Цели комплексной защиты информации (ЗИ) и способы ее обеспечения. Системный метод при решении задач обеспечения комплексной защиты информации.Определение возможных каналов утечки информации. Определение объектов и элементов защиты.Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации. Выбор методов и средств защиты информации. | 5 | ПК-13, ПК-14 |
| | Итого | 5 | |

Согласована на портале № 40606

| | | | |
|---|---|---|---|
| 3 Определение компонентов КСЗИ. | Правовая защита информации. Законодательная база по ЗИ. Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ. Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации.Техническая защита информации. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг. Криптографическая защита информации. Средства и методы.Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии. Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации. | 9 | ПК-13, ПК-14 |
| | Итого | 9 | |
| 4 Технология определения и классификации состава и защищенности информации. | Охраняемые сведения и объекты защиты.Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и государственную тайну к различным степеням и категориям доступа. | 7 | ПК-13, ПК-14 |
| | Итого | 7 | |
| 5 Построение комплексной системы защиты информации. | Разработка моделей комплексной системы защиты информации. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. Архитектурное построение комплексной системы защиты информации. | 4 | ПК-13, ПК-14 |
| | Итого | 4 | |
| 6 Управление комплексной системой защиты информации. | Структура и содержание технологии управления комплексной системой защиты информации. Планирование и оперативное управление системой | 2 | ПК-13, ПК-14 |

Согласована на портале № 40606

| | | | |
|---|---|---|---|
| | ЗИ, управление КСЗИ в условиях чрезвычайных ситуаций.Анализ надежности функционирования комплексной системы защиты информации. | | |
| | Итого | 2 | |
| 7 Служба защиты информации. | Организация службы защиты информации (СЗИ) и организационное проектирование деятельности СЗИ. Порядок создания СЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации. | 4 | ПК-13, ПК-14 |
| | Итого | 4 | |
| 8 Особенностей управления КСЗИ в условиях чрезвычайных ситуаций. | Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение КСЗИ. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ. Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер КСЗИ.Восстановление после чрезвычайной ситуации функций и механизмов КСЗИ организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации. | 2 | ПК-13, ПК-14 |
| | Итого | 2 | |
| 9 Состав методов и моделей оценки эффективности КСЗИ. | Основные термины и определения, характеризующие эффективность защиты информации. Содержание и особенности методологии оценки эффективности КСЗИ. Основные модели оценки эффективности КСЗИ. | 2 | ПК-13, ПК-14 |
| | Итого | 2 | |
| Итого за семестр | | 36 | |
| Итого | | 36 | |

### 5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

| Наименование дисциплин | № разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| Предшествующие дисциплины | | | | | | | | | | | |
| 1 Введение в профиль | + | | | | | | | | | | |

Согласована на портале № 40606

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| "Защищенные системы связи" | | | | | | | | | | | |
| 2 Вычислительная техника и информационные технологии | | + | + | | | | | | | | |
| 3 Защита информационных процессов в сетях и системах связи | | | + | + | + | + | | | | | |
| 4 Информатика | | + | | | | | | | | | |
| 5 Общая теория связи | | | + | + | + | + | | | | | |
| 6 Организация и управление службой защиты информации на предприятиях связи | | | | | | | + | + | | | |
| 7 Основы криптографии | | | + | | | | | | | | |
| 8 Основы организационно-правового обеспечения информационной безопасности сетей и систем | | | | | | + | + | + | + | | |
| 9 Основы построения защищенных инфокоммуникационных систем и сетей | | | | | + | | | | + | | |
| 10 Сетевые технологии высокоскоростной передачи данных | | | | + | + | | | | | | |
| 11 Сети связи и системы коммутации | | | | + | + | | | | + | | |
| 12 Схемотехника телекоммуникационных устройств | | | + | + | + | | | | + | | |
| 13 Комплексные системы защиты информации в сетях и системах связи | + | + | + | + | + | + | + | + | + | + | + |
| Последующие дисциплины | | | | | | | | | | | |
| 1 Преддипломная практика | | | | | | + | + | + | + | | |
| 2 Программно-аппаратные средства защиты сетей и систем связи | | | + | | | | | | | | |
| 3 Программно-аппаратные средства связи | | | + | + | | | | | | | |
| 4 Техническая защита информации в сетях и системах связи | | + | + | + | + | + | | | + | | |
| 5 Комплексные системы | + | + | + | + | + | + | + | + | + | + | + |

Согласована на портале № 40606

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| защиты информации в сетях и системах связи | | | | | | | | | | | |

**5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий**

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

| Компетенции | Виды занятий | | | | | Формы контроля |
|---|---|---|---|---|---|---|
| | Лек. | Прак. зан. | Лаб. раб. | КСР (КП/КР) | Сам. раб. | |
| ПК-13 | + | + | + | + | + | Экзамен, Конспект самоподготовки, Защита отчета, Опрос на занятиях, Защита курсовых проектов / курсовых работ, Зачет, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию |
| ПК-14 | + | + | + | + | + | Экзамен, Конспект самоподготовки, Защита отчета, Опрос на занятиях, Защита курсовых проектов / курсовых работ, Зачет, Выступление (доклад) на занятии, Тест, Отчет по практическому занятию |

## 6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

## 7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Таблица 7.1 – Наименование лабораторных работ

| Названия разделов | Наименование лабораторных работ | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 7 семестр | | | |
| 10 Экзамен. | Система защиты информации от несанкционированного доступа SecretNet. | 6 | ПК-13, ПК-14 |
| | Система защиты информации от несанкционированного доступа Dallas Lock. | 6 | |
| | Система защиты информации от несанкциониро- | 6 | |

Согласована на портале № 40606

| | | | |
|---|---|---|---|
| | ванного доступа Страж NT. | | |
| | DLP-решения по защите информации в информационных системах. | 6 | |
| | Защита информации от программных воздействий на базе антивируса Dr.Web. | 6 | |
| | Защита информации от программных воздействий на базе антивируса KAV. | 6 | |
| | Итого | 36 | |
| Итого за семестр | | 36 | |
| Итого | | 36 | |

## 8. Практические занятия (семинары)

Наименование практических занятий (семинаров) приведено в таблице 8.1.

Таблица 8.1 – Наименование практических занятий (семинаров)

| Названия разделов | Наименование практических занятий (семинаров) | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|---|
| 7 семестр | | | |
| 1 Введение. | Сущность и понятие системы защиты информации с позиции системного подхода. | 2 | ПК-13, ПК-14 |
| | Итого | 2 | |
| 3 Определение компонентов КСЗИ. | Определение, понятие и физический смысл технического канала утечки информации (ТКУИ). Методология защиты информации от утечки по техническим каналам. | 2 | ПК-13, ПК-14 |
| | Сущность и понятие объекта защиты информации, объекта информатизации. | 2 | |
| | Итого | 4 | |
| 4 Технология определения и классификации состава и защищенности информации. | Помещения, предназначенные для конфиденциальных переговоров. ТКУИ, характерные для объекта защиты. Определения и понятия. Методика защиты информации.Обработка защищаемой информации с использованием технических средств и систем. ТКУИ, характерные для объекта защиты. Определения и понятия. Методика защиты информации. | 2 | ПК-13, ПК-14 |
| | Итого | 2 | |
| 5 Построение комплексной системы защиты информации. | Защита информации от несанкционированного доступа (НСД). Основные определения и понятия. Особенности защиты от НСД к информации в автоматизированных системах и средствах вычислительной техники. Модель угроз и нарушителя. Понятие и основные практические подходы к разработке.Средства защиты информации по ТКУИ. Особенности выбора и обоснования. | 2 | ПК-13, ПК-14 |

Согласована на портале № 40606

| | | | |
|---|---|---|---|
| | Итого | 2 | |
| 6 Управление комплексной системой защиты информации. | Аттестация объектов информатизации по требованиям безопасности информации.Основные понятия и особенности практической реализации. Состав примерного комплекта документов. | 2 | ПК-13, ПК-14 |
| | Итого | 2 | |
| Итого за семестр | | 12 | |
| 8 семестр | | | |
| 11 Зачёт. | Договор на проведение аттестации объекта информатизации по требованиям безопасности информации. Сущность, состав и особенности. | 4 | ПК-13, ПК-14 |
| | Техническое задание на проведение аттестации объекта информатизации по требованиям безопасности информации. Сущность, состав и особенности. | 4 | |
| | Технический паспорт защищаемого объекта информатизации. Сущность, состав и особенности.Особенности подготовки технического паспорта объекта вычислительной техники (ОВТ). | 4 | |
| | Особенности разработки системы защиты информации персональных данных в информационных системах. | 2 | |
| | Итого | 14 | |
| Итого за семестр | | 14 | |
| Итого | | 26 | |

## 9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

| Названия разделов | Виды самостоятельной работы | Трудоемкость, ч | Формируемые компетенции | Формы контроля |
|---|---|---|---|---|
| 7 семестр | | | | |
| 1 Введение. | Подготовка к практическим занятиям, семинарам | 3 | ПК-13, ПК-14 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 4 | | |
| 2 Содержание и этапы проведения работ по организации комплексной системы защиты информации. | Подготовка к практическим занятиям, семинарам | 3 | ПК-13, ПК-14 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Проработка лекционного материала | 1 | | |

Согласована на портале № 40606

| | | | | |
|---|---|---|---|---|
| | Итого | 4 | | |
| 3 Определение компонентов КСЗИ. | Подготовка к практическим занятиям, семинарам | 3 | ПК-13, ПК-14 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 4 | | |
| 4 Технология определения и классификации состава и защищенности информации. | Подготовка к практическим занятиям, семинарам | 2 | ПК-13, ПК-14 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Проработка лекционного материала | 1 | | |
| | Итого | 3 | | |
| 5 Построение комплексной системы защиты информации. | Подготовка к практическим занятиям, семинарам | 6 | ПК-13, ПК-14 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Проработка лекционного материала | 2 | | |
| | Итого | 8 | | |
| 6 Управление комплексной системой защиты информации. | Подготовка к практическим занятиям, семинарам | 4 | ПК-13, ПК-14 | Выступление (доклад) на занятии, Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Проработка лекционного материала | 2 | | |
| | Итого | 6 | | |
| 7 Служба защиты информации. | Проработка лекционного материала | 2 | ПК-13, ПК-14 | Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Итого | 2 | | |
| 8 Особенностей управления КСЗИ в условиях чрезвычайных ситуаций. | Проработка лекционного материала | 2 | ПК-13, ПК-14 | Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Итого | 2 | | |
| 9 Состав методов и моделей оценки эффективности КСЗИ. | Проработка лекционного материала | 3 | ПК-13, ПК-14 | Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Итого | 3 | | |
| 10 Экзамен. | Оформление отчетов по лабораторным работам | 24 | ПК-13, ПК-14 | Конспект самоподготовки, Опрос на занятиях, Тест, Экзамен |
| | Итого | 24 | | |
| Итого за семестр | | 60 | | |
| | Подготовка и сдача экзамена | 36 | | Экзамен |
| 8 семестр | | | | |
| 11 Зачёт. | Подготовка к практическим занятиям, семинарам | 7 | ПК-13, ПК-14 | Выступление (доклад) на занятии, Зачет, Защита отчета, Конспект само- |

Согласована на портале № 40606

| | | | | |
|---|---|---|---|---|
| | Подготовка к практическим занятиям, семинарам | 7 | | подготовки, Опрос на занятиях, Отчет по практическому занятию, Тест |
| | Подготовка к практическим занятиям, семинарам | 7 | | |
| | Подготовка к практическим занятиям, семинарам | 7 | | |
| | Оформление отчетов по лабораторным работам | 56 | | |
| | Итого | 84 | | |
| Итого за семестр | | 84 | | |
| Итого | | 180 | | |

## 10. Курсовой проект / курсовая работа

Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы представлены таблице 10.1.

Таблица 10.1 – Трудоемкость аудиторных занятий и формируемые компетенции в рамках выполнения курсового проекта / курсовой работы

| Наименование аудиторных занятий | Трудоемкость, ч | Формируемые компетенции |
|---|---|---|
| 8 семестр | | |
| Получение технического задания на курсовую работу. Обсуждение технического задания. Подписание технического задания. | 2 | ПК-13, ПК-14 |
| Разработка алгоритма решения задачи. Определение составных частей системы связи. Формулирование требований к составным частям системы. | 4 | |
| Реализация подсистемы технической защиты информации объекта информатизации предприятия. | 4 | |
| Итого за семестр | 10 | |

### 10.1. Темы курсовых проектов / курсовых работ

Примерная тематика курсовых проектов / курсовых работ:

- Разработка подсистемы технической защиты выделенного помещения предприятия.
- Разработка подсистемы технической защиты объекта вычислительной техники.
- Разработка подсистемы технической защиты персональных данных, обрабатываемых в информационной системе предприятия.

## 11. Рейтинговая система для оценки успеваемости обучающихся

### 11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

| Элементы учебной деятельности | 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 | Всего за семестр |
|---|---|---|---|---|

Согласована на портале № 40606

| | | | | |
|---|---|---|---|---|
| | | | конец семестра | |
| 7 семестр | | | | |
| Выступление (доклад) на занятии | 5 | 5 | 5 | 15 |
| Конспект самоподготовки | 5 | 5 | 5 | 15 |
| Опрос на занятиях | 5 | 5 | 5 | 15 |
| Тест | 5 | 5 | 15 | 25 |
| Итого максимум за период | 20 | 20 | 30 | 70 |
| Экзамен | | | | 30 |
| Нарастающим итогом | 20 | 40 | 70 | 100 |
| 8 семестр | | | | |
| Выступление (доклад) на занятии | 2 | 2 | 2 | 6 |
| Зачет | 2 | 2 | 2 | 6 |
| Защита курсовых проектов / курсовых работ | | | 45 | 45 |
| Защита отчета | 5 | 5 | 5 | 15 |
| Конспект самоподготовки | 2 | 2 | 2 | 6 |
| Опрос на занятиях | 2 | 2 | 2 | 6 |
| Отчет по практическому занятию | 2 | 2 | 2 | 6 |
| Тест | 5 | 5 | | 10 |
| Итого максимум за период | 20 | 20 | 60 | 100 |
| Нарастающим итогом | 20 | 40 | 100 | 100 |

### 11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

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

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

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

| Оценка (ГОС) | Итоговая сумма баллов, учитывает успешно сданный экзамен | Оценка (ECTS) |
|---|---|---|

Согласована на портале № 40606

| | | |
|---|---|---|
| 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) |

## 12. Учебно-методическое и информационное обеспечение дисциплины

### 12.1. Основная литература

1. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2015. 284 с. - Режим доступа: https://edu.tusur.ru/publications/5262 (дата обращения: 25.07.2018).

### 12.2. Дополнительная литература

1. Защита информации от утечки по техническим каналам [Электронный ресурс]: Учебное пособие / А. М. Голиков - 2015. 256 с. - Режим доступа: https://edu.tusur.ru/publications/5263 (дата обращения: 25.07.2018).

### 12.3. Учебно-методические пособия

#### 12.3.1. Обязательные учебно-методические пособия

1. Защита информации в инфокоммуникационных системых и сетях [Электронный ресурс]: Учебное пособие для практических и семинарских занятий (Часть 1) / А. М. Голиков - 2015. 103 с. - Режим доступа: https://edu.tusur.ru/publications/5330 (дата обращения: 25.07.2018).
2. Защита информации в инфокоммуникационных системах и сетях [Электронный ресурс]: Сборник лабораторных работ / А. М. Голиков - 2015. 373 с. - Режим доступа: https://edu.tusur.ru/publications/5378 (дата обращения: 25.07.2018).
3. Информационные технологии в управлении качеством и защита информации [Электронный ресурс]: Методические рекомендации к курсовым работам и организации самостоятельной работы студентов / Е. Г. Годенова - 2011. 35 с. - Режим доступа: https://edu.tusur.ru/publications/290 (дата обращения: 25.07.2018).

#### 12.3.2. 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.

### 12.4. Профессиональные базы данных и информационные справочные системы

1. При изучении дисциплины рекомендуется использовать базы данных и информационно-справочные системы, к которым у ТУСУРа есть доступ https://lib.tusur.ru/ru/resursy/bazydannyh

Согласована на портале № 40606

## 13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

### 13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

#### 13.1.1. 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 количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

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

Учебная лаборатория радиоэлектроники / Лаборатория ГПО

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634034, Томская область, г. Томск, Вершинина улица, д. 47, 407 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Коммутатор D-Link Switch 24 port;
- Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. (12 шт.);
- Вольтметр В3-38 (7 шт.);
- Генератор сигналов специальной формы АКИП ГСС-120 (2 шт.);
- Кронштейн PTS-4002;
- Осциллограф EZ Digital DS-1150C (3 шт.);
- Осциллограф С1-72 (4 шт.);
- Телевизор плазменный Samsung;
- Цифровой генератор сигналов РСС-80 (4 шт.);
- Цифровой осциллограф GDS-810C (3 шт.);
- Автоматизированное лабораторное место по схемотехнике и радиоавтоматике (7 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

- 7-Zip
- Adobe Acrobat Reader
- Far Manager
- Google Chrome
- LibreOffice
- Microsoft Windows
- Mozilla Firefox
- PDFCreator
- WinDjView

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

Учебная лаборатория радиоэлектроники / Лаборатория ГПО

учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа

634034, Томская область, г. Томск, Вершинина улица, д. 47, 407 ауд.

Описание имеющегося оборудования:

- Доска магнитно-маркерная;
- Коммутатор D-Link Switch 24 port;
- Компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. (12 шт.);
- Вольтметр В3-38 (7 шт.);

Согласована на портале № 40606

- Генератор сигналов специальной формы АКИП ГСС-120 (2 шт.);
- Кронштейн PTS-4002;
- Осциллограф EZ Digital DS-1150C (3 шт.);
- Осциллограф С1-72 (4 шт.);
- Телевизор плазменный Samsung;
- Цифровой генератор сигналов РСС-80 (4 шт.);
- Цифровой осциллограф GDS-810C (3 шт.);
- Автоматизированное лабораторное место по схемотехнике и радиоавтоматике (7 шт.);
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:
- 7-Zip
- Adobe Acrobat Reader
- Far Manager
- Google Chrome
- LibreOffice
- Microsoft Windows
- Mozilla Firefox
- PDFCreator
- WinDjView

### 13.1.4. 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, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:
- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

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

### 13.2. 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 зрениями** предусмотрено использование в

Согласована на портале № 40606

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.

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

### 14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

#### 14.1.1. Тестовые задания

1. Информация это -
1) сведения, поступающие от СМИ
2) только документированные сведения о лицах, предметах, фактах, событиях
3) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
4) только сведения, содержащиеся в электронных базах данных

2. Информация
1) не исчезает при потреблении
2) становится доступной, если она содержится на материальном носителе
3) подвергается только "моральному износу"
4) характеризуется всеми перечисленными свойствами

3. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
1) достоверной
2) конфиденциальной
3) документированной
4) коммерческой тайной

4. Формы защиты интеллектуальной собственности -
1) авторское, патентное право и коммерческая тайна
2) интеллектуальное право и смежные права
3) коммерческая и государственная тайна
4) гражданское и административное право

5. По принадлежности информационные ресурсы подразделяются на
1) государственные, коммерческие и личные
2) государственные, не государственные и информацию о гражданах
3) информацию юридических и физических лиц
4) официальные, гражданские и коммерческие

6. К негосударственным относятся информационные ресурсы
1) созданные, приобретенные за счет негосударственных учреждений и организаций
2) созданные, приобретенные за счет негосударственных предприятий и физических лиц
3) полученные в результате дарения юридическими или физическими лицами
4) все указанное в пунктах 1-3

8. По доступности информация классифицируется на
1) открытую информацию и государственную тайну
2) конфиденциальную информацию и информацию свободного доступа

Согласована на портале № 40606

3) информацию с ограниченным доступом и общедоступную информацию
4) виды информации, указанные в остальных пунктах

9. К конфиденциальной информации относятся документы, содержащие
1) государственную тайну
2) законодательные акты
3) "ноу-хау"
4) сведения о золотом запасе страны

10. Запрещено относить к информации ограниченного доступа
1) информацию о чрезвычайных ситуациях
2) информацию о деятельности органов государственной власти
3) документы открытых архивов и библиотек
4) все, перечисленное в остальных пунктах

11. К конфиденциальной информации не относится
1) коммерческая тайна
2) персональные данные о гражданах
3) государственная тайна
4) "ноу-хау"

12. Вопросы информационного обмена регулируются (...) правом
1) гражданским
2) информационным
3) конституционным
4) уголовным

13. Согласно ст.132 ГК РФ интеллектуальная собственность это
1) информация, полученная в результате интеллектуальной деятельности индивида
2) литературные, художественные и научные произведения
3) изобретения, открытия, промышленные образцы и товарные знаки
4) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

14. Интеллектуальная собственность включает права, относящиеся к
1) литературным, художественным и научным произведениям, изобретениям и открытиям
2) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам
3) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям
4) всему, указанному в остальных пунктах

15. Конфиденциальная информация это
1) сведения, составляющие государственную тайну
2) сведения о состоянии здоровья высших должностных лиц
3) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ
4) данные о состоянии преступности в стране

16. Какая информация подлежит защите?
1) информация, циркулирующая в системах и сетях связи
2) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
3) только информация, составляющая государственные информационные ресурсы
4) любая документированная информация, неправомерное обращение с которой может на-

Согласована на портале № 40606

нести ущерб ее собственнику, владельцу, пользователю и иному лицу

17. Система защиты государственных секретов определяется Законом
1) "Об информации, информатизации и защите информации"
2) "Об органах ФСБ"
3) "О государственной тайне"
4) "О безопасности"

18. Государственные информационные ресурсы не могут принадлежать
1) физическим лицам
2) коммерческим предприятиям
3) негосударственным учреждениям
4) всем перечисленным субъектам

19. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает
1) Указ Президента "Об утверждении перечня сведений, относящихся к государственной тайне"
2) ГК РФ
3) Закон "Об информации, информатизации и защите информации"
4) Конституция

20. Классификация и виды информационных ресурсов определены
1) Законом "Об информации, информатизации и защите информации"
2) Гражданским кодексом
3) Конституцией
4) всеми документами, перечисленными в остальных пунктах

### 14.1.2. Экзаменационные вопросы

1. Системный подход. Определение и понятие.
2. Система обеспечения информационной безопасности организации. Определение и понятие.
3. Система защиты информации организации. Определение и понятие.
4. Объект защиты информации. Определение и понятие.
5. Защищаемая информация. Определение и понятие.
6. Защита информации. Определение и понятие.
7. Организация защиты информации. Определение и понятие.
8. Техника защиты информации. Определение и понятие.
9. Контроль защиты информации. Цели и понятие.
10. Контролируемая зона. Определение и понятие.
11. Технический канал утечки информации (ТКУИ), виды ТКУИ. Определение, физический смысл.
12.Подсистема технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Модель и понятие.
13. Подсистема технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. Модель и понятие.
14. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем.
15. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров.
16. Уязвимости системы обеспечения ИБ организации. Определение и понятие.
17. Нарушитель ИБ организации. Определение и понятие.
18. Модель технической реализации ПТЗИ ОИ.
19. Защита информации от несанкционированного доступа (НСД). Определение и понятие.
20. Основа концепции защиты СВТ и АС от НСД к информации.

Согласована на портале № 40606

21. Классификация АС. Цели и основные понятия.
22. Аттестация объектов информатизации. Понятие.
23. Алгоритм приобретения ПЭВМ в защищенном исполнении.
24. Доктрина ИБ РФ. Общие положения.

### 14.1.3. Темы докладов

1. Особенности разработки подсистемы технической защиты объекта вычислительной техники организации.
2. Особенности разработки подсистемы технической защиты защищаемого помещения организации.
3. Особенности разработки подсистемы технической защиты персональных данных, обрабатываемых в информационной системе организации.

### 14.1.4. Темы опросов на занятиях

Цели, структура и задачи курса. Взаимосвязь курса с другими дисциплинами, системный характер научно-технических проблем при решении задач по организации и управлению комплексной системы защиты информации на предприятии. Специфика курса.

Цели комплексной защиты информации (ЗИ) и способы ее обеспечения. Системный метод при решении задач обеспечения комплексной защиты информации.Определение возможных каналов утечки информации. Определение объектов и элементов защиты.Оценка угроз технических разведок (ТР) и других источников угроз безопасности защищаемой информации. Выбор методов и средств защиты информации.

Правовая защита информации. Законодательная база по ЗИ. Сертификация и лицензирование. Правовые нормы, методы и средства защиты охраняемой информации в РФ. Система юридической ответственности за нарушение норм защиты государственной, служебной и коммерческой тайны в РФ. Правовые основы выявления и предупреждения утечки охраняемой информации.Техническая защита информации. Виды информации, защищаемой техническими средствами. Демаскирующие признаки объектов защиты и их классификация. Каналы утечки информации (оптический, акустический, радиоэлектронный). Методы защиты от несанкционированного перехвата речевой, визуальной, оптической, радиоэлектронной информации. Радиомониторинг. Криптографическая защита информации. Средства и методы.Физическая защита информации. Принципы, силы, средства и условия организационной защиты информации. Организация внутриобъектового и пропускного режима предприятия. Организация системы охраны предприятия (физическая охрана, пожарная и охранная сигнализация, охранное телевидение, системы ограничения доступа). Организация аналитической работы по предупреждению перехвата конфиденциальной информации. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Определение политики защиты информации на предприятии. Особенности организации комплексной защиты информации, отнесенной в установленном порядке к государственной тайне. Определение сил и средств, необходимых для защиты информации.

Охраняемые сведения и объекты защиты.Особенности отнесения сведений, составляющих служебную, конфиденциальную, коммерческую и государственную тайну к различным степеням и категориям доступа.

Разработка моделей комплексной системы защиты информации. Определение и разработка состава нормативно-технической документации (НТД) по обеспечению защиты информации, материально-техническое и нормативно-методическое обеспечение функционирования КСЗИ. Архитектурное построение комплексной системы защиты информации.

Структура и содержание технологии управления комплексной системой защиты информации. Планирование и оперативное управление системой ЗИ, управление КСЗИ в условиях чрезвычайных ситуаций.Анализ надежности функционирования комплексной системы защиты информации.

Организация службы защиты информации (СЗИ) и организационное проектирование деятельности СЗИ. Порядок создания СЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации.

Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и

Согласована на портале № 40606

обеспечение КСЗИ. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ. Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер КСЗИ.Восстановление после чрезвычайной ситуации функций и механизмов КСЗИ организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации.

Основные термины и определения, характеризующие эффективность защиты информации. Содержание и особенности методологии оценки эффективности КСЗИ. Основные модели оценки эффективности КСЗИ.

### 14.1.5. Зачёт

Архитектурное построение комплексной системы защиты информации. Структура и содержание технологии управления комплексной системой защиты информации. Планирование и оперативное управление системой ЗИ, управление КСЗИ в условиях чрезвычайных ситуаций.Анализ надежности функционирования комплексной системы защиты информации. Организация службы защиты информации (СЗИ) и организационное проектирование деятельности СЗИ. Порядок создания СЗИ, состав нормативных документов, регламентирующих деятельность служб защиты информации. Определение и понятие чрезвычайной ситуации. Аспекты обеспечения условий непрерывности в информационной сфере организации. Роль совета директоров и исполнительных органов организации. Идентификация недостатков. Непрерывность сервисов в изменяющейся среде и обеспечение КСЗИ. Реорганизация и ликвидация СЗИ. Определение должностного состава и численности СЗИ. Планирование и отчетность о деятельности СЗИ. Понимание рисков непрерывности и их влияние на цели деятельности организации и восстановление защитных мер КСЗИ.Восстановление после чрезвычайной ситуации функций и механизмов КСЗИ организации. Организационная основа процессов восстановления, вопросы системы менеджмента информационной безопасности (ИБ) организации и менеджмента непрерывности бизнеса. Восстановление и обеспечение функционирования процессов системы менеджмента ИБ организации. Основные термины и определения, характеризующие эффективность защиты информации. Содержание и особенности методологии оценки эффективности КСЗИ. Основные модели оценки эффективности КСЗИ.

### 14.1.6. Вопросы на самоподготовку

1. Системный подход. Определение и понятие.
2. Система обеспечения информационной безопасности организации. Определение и понятие.
3. Система защиты информации организации. Определение и понятие.
4. Объект защиты информации. Определение и понятие.
5. Защищаемая информация. Определение и понятие.
6. Защита информации. Определение и понятие.
7. Организация защиты информации. Определение и понятие.
8. Техника защиты информации. Определение и понятие.
9. Контроль защиты информации. Цели и понятие.
10. Контролируемая зона. Определение и понятие.
11. Технический канал утечки информации (ТКУИ), виды ТКУИ. Определение, физический смысл.
12. Подсистема технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров. Модель и понятие.
13. Подсистема технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем. Модель и понятие.
14. Модель угроз подсистемы технической защиты информации объектов информатизации, реализующих информационные технологии с использованием технических средств и систем.
15. Модель угроз подсистемы технической защиты информации объектов информатизации, предназначенных для ведения конфиденциальных переговоров.
16. Уязвимости системы обеспечения ИБ организации. Определение и понятие.
17. Нарушитель ИБ организации. Определение и понятие.

Согласована на портале № 40606

18. Модель технической реализации ПТЗИ ОИ.
19. Защита информации от несанкционированного доступа (НСД). Определение и понятие.
20. Основа концепции защиты СВТ и АС от НСД к информации.
21. Классификация АС. Цели и основные понятия.
22. Аттестация объектов информатизации. Понятие.
23. Алгоритм приобретения ПЭВМ в защищенном исполнении.
24. Доктрина ИБ РФ. Общие положения.

### 14.1.7. Вопросы для подготовки к практическим занятиям, семинарам

Договор на проведение аттестации объекта информатизации по требованиям безопасности информации. Сущность, состав и особенности.

Техническое задание на проведение аттестации объекта информатизации по требованиям безопасности информации. Сущность, состав и особенности.

Технический паспорт защищаемого объекта информатизации. Сущность, состав и особенности.Особенности подготовки технического паспорта объекта вычислительной техники (ОВТ).

Особенности разработки системы защиты информации персональных данных в информационных системах.

### 14.1.8. Темы курсовых проектов / курсовых работ

1. Разработка подсистемы технической защиты выделенного помещения предприятия.
2. Разработка подсистемы технической защиты объекта вычислительной техники.
3. Разработка подсистемы технической защиты персональных данных, обрабатываемых в информационной системе предприятия.

## 14.2. 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 14.

Таблица 14 – 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 исходя из состояния обучающегося на момент проверки |

## 14.3. 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.

Согласована на портале № 40606

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.

Согласована на портале № 40606