МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Направление подготовки 09.03.03 Прикладная информатика
Профиль подготовки:
Прикладная информатика в гуманитарной сфере
Уровень квалификации выпускника – бакалавр

Форма обучения – очная

Москва 2017

Информационная безопасность
Рабочая программа дисциплины
Составитель(и):
Старший преподаватель Кафедры КЗИ Г.Н. Гудов

Ответственный редактор
Доктор технических наук, старший научный сотрудник, зав. кафедрой КЗИ О.В. Казарин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 10 от 29.06.2017 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1 *Цель и задачи дисциплины*

Цель дисциплины – подготовить выпускника, умеющего разрабатывать систему по обеспечению безопасности информационных ресурсов, как для автономных и распределенных вычислительных системах.

Задачи дисциплины:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения информационной безопасности в информационных системах различного назначения;
- изучение теоретических основ информационной безопасности;
- формирование умений использовать основные достижения в области информационной безопасности при реализации своей профессиональной деятельности;
- владение навыками обеспечения защиты информации в информационных системах различного назначения;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

1.2. Формируемые компетенции, соотнесенные с планируемыми результатами обучения по дисциплине

Дисциплина направлена на формирование следующих компетенций:

ПК-18: способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью		
Владение	**Умение**	**Знание**
навыками использования стандартов для защиты информации в ИС.	выполнять анализ требований к системе защиты информации.	назначения и видов подлежащих защите ресурсов ИС, моделей и процессов жизненного цикла системы защиты информации.
навыками работы с инструментальными средствами проектирования баз данных и знаний, управления проектами ИС и защиты информации.	анализировать и контролировать уровень организационной и технологической защищенности информации в ИС.	видов угроз ИС и методов обеспечения ИБ.
ОПК-4: Способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности		
Владение	**Умение**	**Знание**
навыками разработки тех-	определять направления и	содержания основных уров-

нологической документации.	виды защиты информации с учетом характера защищаемой информации.	ней обеспечения ИБ.
навыками использования методов организации и контроля функционирования системы защиты информации.	выявлять угрозы ИБ, обосновывать организационно-технические мероприятия по защите информации в ИС .	основных законодательных и нормативных документов федерального уровня в области ИБ и защиты информации.

1.3. Место дисциплины в структуре основной образовательной программы

Дисциплина «Информационная безопасность» относится к блоку дисциплин базовой части учебного плана.

Для освоения дисциплины необходимы компетенции, формируемые в ходе изучения дисциплин: «Информатика» «Вычислительные системы, сети и телекоммуникации», «Информационные системы» «Информационные технологии».

В результате освоения дисциплины формируются компетенции, необходимые для изучения следующих дисциплин: «Разработка и внедрение информационных систем», «Управление проектами информационных систем».

2. Структура дисциплины

Общая трудоемкость дисциплины составляет 2 (две) зачетные единицы, 72 часов, в том числе контактная работа 28 часа, самостоятельная работа 44 часов.

№ п/п	Раздел дисциплины/темы	Семестр	Виды учебной работы (в часах)						Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
			контактная					Самостоятельная работа	
			Лекции	Семинар	Практические занятия	Лабораторные занятия	Промежуточная аттестация		
1.	***Методологические аспекты информационной безопасности (ИБ)***	**4**	**1**	---		4	---	**4**	
1.1.	*Введение в дисциплину, термины и определения, понятие и сущность ИБ.*	**4**	0	---		2	---	2	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной работы.
1.2.	*Базовые угрозы информационной безопасности.*	**4**	0	---		2	---	2	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной работы.
2.	***Законодательный, уровень обеспечения ИБ***	**4**	**1**	---		4	---	**8**	
2.1.	*Стандарты и спецификации в области ИБ.*	**4**	0,5	---		2	---	4	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной работы.
2.2.	*Стандарты РФ в области ИБ, Руководящие документы ФСТЭКа России.*	**4**	0,5	---		2	---	4	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной

									работы
3.	***Раздел 3. Административный и процедурный уровень обеспечения ИБ***	**4**	**2**	**---**		4	**---**	**12**	
3.1.	*Административный уровень, цели, задачи ИБ, управление рисками.*	**4**	1	**---**		2	**---**	6	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной работы.
3.2.	*Процедурный уровень, назначение, основные направления организации работ, цели, задачи, принципы построения.*	**4**	1	**---**		2	**---**	6	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной работы..
4.	***Программно-технический уровень обеспечения информационной информации***	**4**	**4**	**---**		4	**---**	**12**	
4.1.	*Технология обеспечения ИБ, цели и принципы построения архитектуры ИБ.*	**4**	2	**---**		2	**---**	6	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной работы.
4.2.	*Сервисы ИБ, назначение, функции, методы реализации сервисов ИБ.*	**4**	2	**---**		2	**---**	6	Устный опрос. Проверка домашнего задания. Выполнение и защита лабораторной работы.
5.	*Текущий контроль*	**4**	**---**	**---**		4	**---**	**8**	
5.1.	*Контрольное тестирование*	**4**	**---**	**---**		2	**---**	2	Тестирование
5.2.	*Промежуточная аттестация (зачет с оценкой).*	**4**	**---**	**---**		2	**---**	6	Зачет с оценкой по билетам
	Итого:	**---**	**8**	**---**		20	**---**	**44**	

3. Содержание дисциплины

Раздел 1. Методологические аспекты информационной безопасности

Тема 1. Введение в дисциплину, термины и определения, понятие и сущность ИБ

Понятие безопасности объекта (государства, предприятия и информационной системы). Основные компоненты безопасности государства и доминирующая роль информационной безопасности (ИБ). Становление и развитие понятия «информационная безопасность». Сущность и понятия ИБ и защиты информации. Необходимость и значение нормативно-правового определения основных понятий. Связь ИБ с информатизацией общества. Базовые уровни обеспечения информационной безопасности и защиты информации.

Тема 2. Базовые угрозы информационной безопасности

Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в ИС. Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите информационных систем от реализации угроз.

Раздел 2. Законодательный, уровень обеспечения информационной безопасности

Тема 3. Стандарты и спецификации в области ИБ

Предпосылки создания международных стандартов по обеспечению информационной безопасности. Назначение стандартов и какие задачи решатся при использовании стандартов в области информационной безопасности: в определении цели обеспечения информационной безопасности компьютерных систем, создания эффективной система управления информационной безопасностью, критерии оценки соответствия информационной безопасности заявленным целям, создания условий применения имеющегося инструментария (программных средств) обеспечения информационной безопасности и оценки ее текущего состояния.

Назначение и основные положения международных стандартов: «Критерии оценки надежности компьютерных систем» («Оранжевая книга»), «Информационная безопасность распределенных систем. Рекомендации X.800», ISO 15408 – «Общие критерии». Международные стандарты семейства 27000.

Тема 4. Стандарты РФ в области информационной безопасности (ИБ), Руководящие документы ФСТЭКа России

Основные федеральные органы, генерирующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации. Государственная система по

обеспечению безопасности и защиты информации (ГСЗИ). Основные законодательные акты РФ в области информационной безопасности и защиты информации. Руководящие документы ФСБ, ФСТЭКа России в области информационной безопасности и защиты информации от несанкционированного доступа при ее обработке с использованием СВТ.

Раздел 3. Административный и процедурный уровень обеспечения информационной безопасности

Тема 5. Административный уровень, цели, задачи ИБ, управление рисками

Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки ПИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ.

Тема 6. Процедурный уровень, назначение, основные направления организации работ, цели, задачи, принципы построения

Назначение и задачи процедурного уровня по обеспечению информационной безопасности. Основные классы мер процедурного уровня: управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ.

Раздел 4. Программно-технический уровень обеспечения информационной информации

Тема 7. Технология обеспечения ИБ, цели и принципы построения архитектуры ИБ

Основные понятия программно-технического уровня обеспечения информационной безопасности. Особенности современных информационных систем, существенные с точки зрения обеспечения информационной безопасности. Архитектурная безопасность.

Меры безопасности: превентивные, препятствующие нарушениям информационной безопасности, меры обнаружения нарушений, меры локализующие, сужающие зону воздействия нарушений, меры по прослеживанию нарушителя, меры восстановления режима безопасности.

Тема 8. Сервисы информационной безопасности, назначение, функции, методы реализации сервисов

Программные сервисы защиты информации в информационных системах. Идентификация и аутентификация пользователей. Базовые методы парольной аутентификации.

Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) информационной системы, их основные цели и особенности. Базовые методы криптографического преобразования данных. Потоковое и блочное шифрование. Процедура формирования электронной подписи. Экранирование информации в сетях. Основные сервисы защиты в информационно-телекоммуникационных сетях (ИТС). Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.

4. Образовательные технологии

№ п/п	*Наименование раздела*	*Виды учебной работы*	*Образовательные технологии*
1.	**Раздел 1.** Методологические аспекты информационной безопасности (ИБ) **Тема 1.** Введение в дисциплину, термины и определения, понятие и сущность ИБ.	*Лекция 1. Введение в дисциплину, термины и определения, понятие и сущность ИБ.* *Содержание занятия:* 1. Определение основных понятий и терминов дисциплины. 2. Цели, задачи и принципы ИБ и ЗИ. *Лабораторная работа:* Задание 1. *Домашнее задание №1.* 1. Выбор методологии для построения вербального объекта защиты. *Самостоятельная работа:* 1.Связь ИБ с информатизацией общества. 2.Нормативно-правового определения основных понятий.	*Вводная лекция с использованием видеоматериалов.* *Изучение материала по теме.* *Выполнение и защита лабораторной работы* *Проверка домашнего задания.* *Консультация с использованием электронной почты (ЭП).*
2.	**Раздел 1.** Методологические аспекты информационной безопасности (ИБ) **Тема 2.** Базовые угрозы информационной безопасности.	*Лекция 2. Базовые угрозы информационной безопасности.* *Содержание занятия:* 1.Базовые объекты и субъекты защиты информации. 1.Источники угроз и угрозы ИБ. Домашнее задание №2. 1.Определение источников угроз по отношению к вербальному объекту защиты ИР. 2.Определение потенциальных угроз безопасной информации ИР. *Лабораторная работа:* Задание 2. *Самостоятельная работа:* *1.* Какие объекты защиты в информационных системах (ИС). *2.* Основные источники угроз для ИС. *3.* Характерные угрозы для информационных ресурсов (ИР).	*Лекция-визуализация с применением проектора.* *Изучение материала по теме* *Проверка домашнего задания.* *Выполнение и защита лабораторной работы* *Консультация с использованием электронной почты.*

3.	**Раздел 2.** Законодательный, уровень обеспечения информационной безопасности **Тема 3.** Стандарты и спецификации в области ИБ.	*Лекция 3. Стандарты и спецификации в области ИБ.* *Содержание занятия:* 1. Значение стандартов в использовании информационных технологий. 2. Структура и основные положения международных актов в сфере ИБ. *Лабораторная работа:* Задание 3. *Домашнее задание №3:* *1.*Выбор критерия требований по отношению доверительной базы ИС. *Самостоятельная работа:* 1. Понятие и назначение стандартов. 2.Виды стандартов и критерии оценки состояния информационной безопасности.	*Лекция-визуализация с применением проектора* *Изучение материала по теме.* *Выполнение и защита лабораторной работы* *Проверка домашнего задания.* *Консультация с использованием электронной почты.*
4.	**Раздел 2.** Законодательный, уровень обеспечения информационной безопасности **Тема 4.** Стандарты РФ в области ИБ, Руководящие документы ФСТЭКа России.	*Лекция 4. Стандарты РФ в области ИБ, руководящие документы ФСТЭКа РФ.* *Содержание занятия:* 1.Российские нормативно-правовые акты в области ИБ. 2.Базовые принципы защиты информации от несанкционированного доступа (НСД) в соответствии с нормативно-правовыми документами. *Лабораторная работа:* Задание 4. *Домашнее задание №4:* 1.Определение возможных каналов доступа злоумышленника к вербальному объекту защиты. 2.Треугольник злоумышленных действий. *Самостоятельная работа:* 1.Основные федеральные органы РФ, генерирующие нормативно-правовые акты в сфере ИБ. 2.Категории ценности и важности информации в государственных учреждениях России.	*Лекция-визуализация с применением проектора.* *Изучение материала по тем.* *Выполнение и защита лабораторной работы* *Проверка домашнего задания.* *Консультация с использованием электронной почты.*
5.	**Раздел 3.** Административный и процедурный уровень обеспечения информационной безопасности. **Тема 5.** Административный уровень, цели, задачи ИБ, управление рисками.	*Лекция 5. Административный уровень: цели, задачи ИБ, управление рисками.* *Содержание занятия:* 1. Концепция ИБ. 2. Политика и программа ИБ. 3. Анализ рисков ИБ. *Лабораторная работа:* Задание 5. *Домашнее задание №5.* 1.Опишите содержание основных этапов формирования концепции ИБ. 2.Опишите содержание основных этапов формирования политики ИБ. *Самостоятельная работа:*	*Лекция-визуализация с применением проектора.* *Изучение материала по теме.* *Выполнение и защита лабораторной работы* *Занятие с использованием специализированного ПО.* *Проверка домашнего задания.*

		1.Основные разделы политики ИБ. 2.Базовые инструментальные средства для анализа рисков. 3.Стратегии управления рисками.	*Консультация с использованием электронной почты.*
6	**Раздел 3.** Административный и процедурный уровень обеспечения информационной безопасности. **Тема 6.** Процедурный уровень, назначение, основные направления организации работ, цели, задачи, принципы построения.	*Лекция 6. Процедурный уровень: назначение, основные направления организации работ, цели, задачи, принципы построения.* *Содержание занятия:* овные классы мер процедурного уровня. 1.Управление персоналом. 2.Физическая защита. 3.Поддержание работоспособности. 4.Реагирование на нарушения режима безопасности. 5.Планирование восстановительных работ. *Лабораторная работа:* Задание 6. *Домашнее задание №6.* 1.Разработка требований по работе с персоналом, владеющие конфиденциальной информацией. 2.Типовые правила реагирования на нарушения ИБ в чрезвычайных ситуациях. *Самостоятельная работа:* 1.Минимизация привилегий и распределение обязанностей между персоналом, как основной принцип исключения от случайных ошибок и реализации преднамеренных угроз 2.Основные требования к персоналу по поддержанию работоспособности. ИС. 3.Основные правила по исключении дестабилизирующих факторов нарушения состояния ИБ. 4.Действия персонала по минимизации ущерба при планировании восстановительных работ**.**	*Лекция-визуализация с применением проектора.* *Изучение материала по теме.* *Выполнение и защита лабораторной работы* *Занятие с использованием специализированного ПО.* *Проверка домашнего задания.* *Консультация с использованием электронной почты..*
7	**Раздел 4.** Программно-технический уровень обеспечения информационной информации **Тема 7.** Технология обеспечения ИБ, цели и принципы построения архитектуры ИБ.	*Лекция 7. Технология обеспечения ИБ, цели и принципы построения архитектуры ИБ.* *Содержание занятия:* 1. Основные понятия программно-технического уровня обеспечения ИБ. 2. Особенности современных информационных систем, с точки зрения обеспечения ИБ. 3. Архитектурная безопасность. *Лабораторная работа:* Задание 7. *Домашнее задание №7.* 1.Построение архитектуры безопасности для вербального объекта защиты. *Самостоятельная работа:* 1.Основные проблемы в построении СЗИ,	*Лекция-визуализация с применением проектора.* *Изучение материала по теме.* *Выполнение и защита лабораторной работы* *Занятия с использованием специализированного ПО.* *Проверка домашнего*

		связанных с развитием информационных технологий. 2.Перечислите принципы архитектурной безопасности для обеспечения конфиденциальности ИР. 3.Перечислите принципы архитектурной безопасности для обеспечения высокой доступности (непрерывности функционирования) к ИС.	*задания.*
8	**Раздел 4.** Программно-технический уровень обеспечения информационной информации **Тема 8.** Сервисы ИБ, назначение, функции, методы реализации сервисов ИБ.	*Лекция 8. Сервисы ИБ: назначение, функции, методы реализации сервисов ИБ.* *Содержание занятия:* 1.Идентификация и аутентификация пользователей. 2.Управление доступом к информации. 3.Протоколирование и аудит ИБ. 4.Базовые методы криптографического преобразования данных. 5.Экранирование как защита информации в сетях. *Лабораторная работа:* Задание 8,9. *Домашнее задание №7:* 1. Классификация компьютерных вирусов. 2. Выбор метода криптографического преобразования данных. *Самостоятельная работа:* 1.Основные группы методов аутентификации. 2.Особенности протоколирования аудита. 3.Основные группы классов защищенности ИС. 4.Симметричные и ассиметричные криптосистемы. 5.Компьютерная стеганография. 6.Основные классы межсетевых экранов.	*Лекция-визуализация с применением проектора.* *Изучение материала по теме.* *Выполнение и защита лабораторной работы* *Занятия с использованием специализированного ПО.* *Проверка домашнего задания.* *Консультация с использованием электронной почты.*

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	Макс. количество баллов	
	За одну работу	Всего
Текущий контроль:		
- опрос;	*5 баллов*	*30 баллов*
-защита лабораторных работ;	*5 баллов*	*20 баллов*
- тестирование;	*10 баллов*	*10 баллов*
Промежуточная аттестация *(зачет с оценкой);*		*40 баллов*
Итого за семестр (дисциплину).		*100 баллов*

Текущий контроль

При оценивании устного опроса и участия в дискуссии на семинаре учитываются:

- степень раскрытия содержания материала (0-2 балла);
- изложение материала (грамотность речи, точность использования терминологии и символики, логическая последовательность изложения материала (0-2 балла);
- знание теории изученных вопросов, сформированность и устойчивость используемых при ответе умений и навыков (0-1 балл).

При оценивании практических работ учитываются:

- полнота выполненной работы (задание выполнено не полностью и/или допущены две и более ошибки или три и более неточности) – 1-4 балла;
- обоснованность содержания и выводов работы (задание выполнено полностью, но обоснование содержания и выводов недостаточны, но рассуждения верны) – 5-8 баллов;
- работа выполнена полностью, в рассуждениях и обосновании нет пробелов или ошибок, возможна одна неточность -9-10 баллов.

При оценивании письменных работ (рефератов, докладов):

Оценка «отлично»:

- наличие четкого плана реферата доклада;
- раскрытие в реферате, докладе сути проблемы;
- самостоятельность в подборе фактического материала и аналитического его осмысления;
- свободное изложение материала и четкие ответы на поставленные вопросы.

Оценка «хорошо»:

- умение изложить сжато основные положения реферата, доклада;
- раскрытие в реферате, докладе сути проблемы;

- самостоятельность в подборе фактического материала и аналитического его осмысления;
- свободное изложение материала и ответы на поставленные вопросы с несущественными, но быстро исправляемыми докладчиком ошибками.

Оценка «удовлетворительно»:

- докладчик затрудняется изложить основные положения реферата, доклада;
- не достаточно полных знаний по теме реферата, доклада, отсутствие аргументации при ответе;
- не структурированное изложение материала реферата, доклада, при ответе на вопросы допускает ошибки.

Оценка «неудовлетворительно»:

- реферат, доклад не подготовлен.

Критерии оценивания при тестировании.

При тестировании студент должен ответить на 20 вопросов.

При оценивании ответа на вопрос учитывается:

- ответ содержит менее 20% правильного ответа (1-4 балла);
- ответ содержит 21-50 % правильного ответа (5-9 баллов);
- ответ содержит 51-80 % правильного ответа (10-14 баллов);
- ответ содержит 90% и более правильного ответа (15-20 баллов).

Критерии оценивания при сдаче зачета с оценкой.

При сдаче зачета с оценкой студент должен ответить на 2 вопроса теоретического характера.

При оценивании ответа на вопрос теоретического характера учитывается:

- теоретическое содержание не освоено, знание материала носит фрагментарный характер, наличие грубых ошибок в ответе (1-3 балла);
- теоретическое содержание освоено частично, допущено не более двух-трех недочетов (4-7 баллов);
- теоретическое содержание освоено почти полностью, допущено не более одного-двух недочетов, но обучающийся смог бы их исправить самостоятельно (8-11 баллов);
- теоретическое содержание освоено полностью, ответ построен по собственному плану (12-15 баллов).

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

<table>
<tr><td>100-балльная шкала</td><td colspan="2">Традиционная шкала</td><td>Шкала ECTS</td></tr>
<tr><td>95 – 100</td><td rowspan="2">отлично</td><td rowspan="5">зачтено</td><td>A</td></tr>
<tr><td>83 – 94</td><td>B</td></tr>
<tr><td>68 – 82</td><td>хорошо</td><td>C</td></tr>
<tr><td>56 – 67</td><td rowspan="2">удовлетворительно</td><td>D</td></tr>
<tr><td>50 – 55</td><td>E</td></tr>
<tr><td>20 – 49</td><td rowspan="2">неудовлетворительно</td><td rowspan="2">не зачтено</td><td>FX</td></tr>
<tr><td>0 – 19</td><td>F</td></tr>
</table>

5.2. Критерии выставления оценок

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»/ «зачтено (хорошо)»/ «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетворительно»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
49-0/ F,FX	«неудовлетворительно»/ не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объема знаний обучающегося по определенному разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

1. Основные составляющие информационной безопасности (ИБ).
2. Характеристика проблем ИБ.
3. Концепция объектно-ориентированного подхода к обеспечению ИБ.
4. Недостатки традиционного подхода к обеспечению ИБ.
5. Характеристика наиболее распространенных угроз.
6. Критерии классификации угроз.
7. Примеры угроз доступности.
8. Вредоносное программное обеспечение.
9. Основные угрозы целостности
10. Основные угрозы конфиденциальности.
11. Что такое законодательный уровень ИБ и почему он важен?
12. Основные законы РФ в области ИБ.
13. Основные зарубежные стандарты в области ИБ.
14. Что такое оценочные стандарты и технические спецификации?

15. Что такое оранжевая книга и для чего она применяется?
16. Рекомендации X.800.
17. Стандарт ISO/ IEC.
18. Что такое политика безопасности и ее актуальность?
19. Что такое программа безопасности и ее актуальность?
20. В чем проявляется административный уровень ИБ?
21. Как синхронизируется политика безопасности с жизненным циклом ИС?
22. Этапы управления рисками в системе защиты информации.
23. Основные программно-технические меры защиты.
24. Технология идентификации и аутентификации.
25. Технология управления доступом.
26. Протоколирование и аудит.
27. Технология шифрования.
28. Архитектурные аспекты экранирования.
29. Классификация межсетевых экранов.
30. Анализ защищенности.
31. Возможности типичные схем туннелирования.
32. Задачи управления системой ИБ.

Контрольное тестирование

Контрольное тестирование имеет ряд преимуществ перед традиционными формами и методами контроля. Оно позволяет более рационально использовать время урока, охватить больший объем содержания, быстро установить обратную связь со студентами и определить результаты усвоения материала, сосредоточить внимание на пробелах в знаниях и умениях и внести в них коррективы.

Тесты - могут использоваться для всесторонней оценки состояния испытуемых, например, до начала процесса обучения с целью оценки их отношения к учению, ровня их интеллектуального развития, способностей к конкретному учебному предмету, установления уровня обучаемости, уровня достижений в рассматриваемой области знаний.

Тестирование – это система, обладающая двумя главными системными факторами: содержательным составом тестовых заданий, образующих наилучшую целостность, и нарастанием трудности от задания к заданию.

Принцип нарастания трудности и позволяет определить уровень знаний и умений по контролируемой дисциплине, а обязательное ограничение времени тестирования – выявить наличие навыков и умений.

Именно трудность задания как субъективное понятие определяется эмпирически, по величине доли неправильных ответов. Трудность отличается от объективного показателя – сложности, под которой понимают совокупность числа понятий, вошедших в задание, числа логических связей между ними и числа операций, необходимых для выполнения задания. Задания теста представляют собой не вопросы и не задачи, а утверждения, которые в зависимости от ответов испытуемых превращаются в истинные или ложные.

Примерные тестовые задания:

1. В соответствии с действующим законом РФ понятие «информация», которая подлежит защите, определяется как:

1) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

2) сведения (сообщения, данные) независимо от формы их представления;

3) сведения, рассматриваемые в процессе их передачи или восприятия, позволяющие расширить знания об интересующем объекте;

4) сведения, передаваемые одними людьми другим людям устным, письменным или каким-либо другим способом.

2. Конфиденциальность информации:

1) сведения, в установленном порядке отнесенные руководителем к информации ограниченного доступа;

2) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ;

3) отдельные закрытые документы (массивы документов в закрытых информационных системах);

4) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

3. В соответствии с действующим законом РФ информационная безопасность определяется как:

1) процесс организации защищённости информационной среды от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства;

2) состояние защищённости информационной среды от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства;

3) состояние защищённости информационных ресурсов от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства;

4) состояние защищённости информационных систем от воздействия источников угроз, обеспечивающее её формирование, использование, развитие в интересах граждан, общества, государства.

4. Защита информации от несанкционированного доступа:

защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением требований нормативных и правовых документов;

защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением прав обладателями информации;

защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации;

предотвращение получения защищаемой информации с нарушением установленных требований к защищаемой информации.

5. Источник угрозы безопасности информации:

1) субъект (физическое лицо), являющийся непосредственной причиной возникновения угрозы безопасности информации;

2) субъект (физическое лицо, материальный объект), меняющий состояние информационной безопасности;

3) субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации;

4) субъект (физическое лицо, материальный объект или физическое явление), создающих потенциальную или реально существующую опасность нарушения безопасности информации.

6. Угроза безопасности информации:

1) совокупность условий и факторов, создающих потенциальную опасность нарушения безопасности информации;

2) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;

3) субъект (физическое лицо, материальный объект), являющийся непосредственной причиной возникновения угрозы безопасности информации;

4) субъект (физическое лицо, материальный объект), являющийся причиной изменения состояния безопасности информации.

7. К основным методам реализации НСД к информации не относится:

1) «маскарад»;

2) «подкладывание свиньи»;

3) «карнавал»;

4) «атака»;

8. Борьбу с компьютерными преступлениями в России не ведут:

1) структуры ФСБ;

2*) отделы департамента «С» МЧС России;*

3) отделы «К» МВД России;

4) спецподразделения Управления по борьбе с экономическими преступлениями МВД России.

9. Какой из видов компьютерных преступлений наиболее распространен в настоящее время?

1) кража средств компьютерной техники;

2) несанкционированный доступ к информации;

3) изготовление или распространение вредоносных программ;

4) перехват информации.

10. К основным свойствам информации, подлежащим защите, не относится:

1) доступность;

2) конфиденциальность;

3) достоверность;

4) целостность**.**

11. В соответствии с действующим законом «конфиденциальность информации» определяется как:

1) свойство информации, позволяющее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду;

2) обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия обладателя;

3) свойство информации, доступ к которой ограничивается в соответствии с законодательством РФ;

4) обязательное для соблюдения физическим или юридическим лицом требование не допускать распространение информации без согласия её обладателя.

12. При реализации мандатной политики доступа не реализуется следующий критерий:

1) все субъекты и объекты системы должны быть идентифицированы;

2) права доступа субъекта к объекту системы определяются на основании некоторого правила;

3) каждому объекту системы присваивается метка критичности;

4) каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

13. Что не представлено в матрице доступа к информации:

1) субъект доступа;

2) вид доступа;

3) правило доступа;

4) объект доступа.

14. Новое семейство международных стандартов на системы управления информационной безопасностью имеет код:

1) 17000;

2) 27000;

3) 37000;

4) 47000.

15. В криптосистемах используется в основном следующий тип шифрования:

1) блочный;

2) потоковый;

3) символьный;

4) смешанный.

16. Какое из ниже перечисленных направлений не входит в состав физической защиты:

1) физическое управление доступом;

2) разделение доступа пользователей;

3) защита от перехвата данных;

4) защита поддерживающей инфраструктуры.

17. Гаммирование – это:

1) один из функциональных методов аутентификации;

2) разновидность стеганографического метода защиты информации;

3) способ шифрования информации;

4) метод подготовки сообщения для преодоления межсетевого экрана.

18. Что является объектом защиты в области информационной безопасности и защиты информации:

1) информация;

2) носители информации;

3) информационные процессы;

4) информация, носители информации, информационные процессы.

19. Какого средства для защиты информации или её уничтожения не существует:

1) «информационный сейф»;

2) «цунами»*;*

3) «торнадо»;

4) «тень».

20. Программные вирусы не классифицируются по следующему признаку:

1) по среде обитания вируса;

2) по способу заражения;

3) по деструктивным возможностям;

4) по способу размножения.

21. Преимуществом мандатного метода управления доступом не является:

1) обеспечение более высокой надежности работы самой ИС;

2) простота определения правил разграничения доступа;

3) широкое распространение данного метода для работы с конфиденциальной информацией;

4) предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности.

22. Современная криптография не включает следующий раздел*:*

1) симметричные криптосистемы;

2) криптосистемы с открытым ключом;

3) системы формирования хэш-функций;

4) управление ключами.

23. Симметричные криптосистемы не используют следующий алгоритм шифрования:

1) DES;

2) IDEA;

3) ГОСТ 28147-89;

4) алгоритм Диффи-Хеллмана;

24. Укажите, какой из указанных методов закрытия информации наиболее трудоёмок:

1) перестановка;

2) аналитические преобразования;

3) гаммирование;

4) замена.

25. В число основных принципов, необходимых для достижения архитектурной безопасности защищаемых систем, не входит следующий:

1) невозможность миновать защитные средства;

2) ликвидация самого слабого звена;

3) невозможность перехода системы в небезопасное состояние;

4) эшелонированность обороны.

26. Какой из указанных функций не является сервисом для аппаратно-программных средств защиты информации:

1) идентификация и аутентификация;

2) криптографическая защита;

3) управление персоналом;

4) экранирование.

27. Количество классов защищенности для межсетевых экранов:

1) три;

2) четыре;

3) пять;

4) шесть.

28. К основным мерам по защите криптографических ключей не относится следующая:

1) ограничение круга лиц, допущенных к работе с ключами;

2) регламентация рассылки, хранения и уничтожения ключей;

3) регламентация порядка смены ключей;

4) применение метода конгруэнтных сечений для хранения ключей.

29. В настоящее время брандмауэр - это:

1) специализированный программный комплекс;

2) специальное техническое средство;

3) специализированный программно-аппаратный комплекс;

4) разновидность криптографического средства защиты информации.

30. Цель защиты информации:

1) заранее намеченный результат защиты информации по предотвращению ущерба обладателю информации;

2) заранее намеченный результат защиты информации по предотвращению ущерба обладателю информации из-за возможной утечки информации и (или) несанкционированного и непреднамеренного воздействия на информацию;

3) исключение (недопущения) реализации угроз безопасности информации;

4) защита информации от её утечки.

31. Эффективность защиты информации:

1) выполнение требований нормативных документов по защите информации;

2) выполнение рекомендаций руководящих документов по защите информации;

3) степень соответствия результатов защиты информации требования по защите информации;

4) степень соответствия результатов защиты информации цели защиты информации.

рабочего дня.

32. Минимизация привилегий для работника:

1) минимизация полномочий по исполнению свих служебных обязанностей;

2) выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей;

3) так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс;

4) минимизация поставленных задач для достижения поставленных целей.

33. Разделение обязанностей для работника:

1) минимизация полномочий по исполнению свих служебных обязанностей;

2) выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей;

3) так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс;

4) минимизация полномочий по исполнению свих служебных обязанностей.

34. Основной целью контроля (проверки) состояния защиты конфиденциальной информации на предприятии является:

1) установление правил по защите сведений ограниченного доступа;

2) проверка наличия носителей сведений конфиденциального характера и соблюдения установленного порядка обращения с ними;

3) проверка соблюдения требований по порядку засекречивания сведений и присвоению грифа секретности носителям;

4) проверка правильности учета, хранения, размножения, уничтожения носителей сведений.

35. Контроль эффективности защиты информации:

1) проверка соответствия качественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации;

2) проверка соответствия качественных и количественных показателей эффективности мероприятий по защите информации требованиям или нормам эффективности защиты информации;

3) проверка соответствия эффективности мероприятий по защите информации на объекте защиты требованиям или нормам эффективности защиты информации;

4) проверка соответствия выполнения на объекте защите требований по защите информации.

36. В соответствии с УК РФ неправомерный доступ к компьютерной информации:

1) ст.271;

2) ст.272;

3) ст.273;

4) ст.274.

Контрольные вопросы к зачету с оценкой

1. Основные понятия информации, источники информации, свойства информации.
2. Классификация информации в правовой системе от порядка ее предоставления или распространения.
3. Понятие информационной безопасности.
4. Основные составляющие информационной безопасности.
5. Важность и сложность проблемы информационной безопасности.
6. Потенциальные источники угроз и способы нарушения информационной безопасности.
7. Основные определения и критерии классификации угроз безопасности информации.
8. Наиболее распространенные угрозы доступности.
9. Основные угрозы целостности.
10. Основные угрозы конфиденциальности.
11. Нормативное правовое обеспечение информационной безопасности Российской Федерации.
12. Стандарты и спецификации в области информационной безопасности, основные понятия.

13. Стандарты и спецификации в области информационной безопасности: стандарт «Критерии оценки доверенных компьютерных систем».
14. Стандарты и спецификации в области информационной безопасности: стандарт ISO/IEC 15408 «Критерии оценки безопасности информационных технологий».
15. Стандарты и спецификации в области информационной безопасности: информационная безопасность распределенных систем, рекомендации X.800.
16. Стандарты и спецификации в области информационной безопасности: руководящие документы ФСТЭК (Гостехкомиссии) России.
17. Административный уровень информационной безопасности: основные понятия, цели и задачи, политика безопасности.
18. Административный уровень информационной безопасности: программа безопасности.
19. Управления рисками: основные понятия по анализу рисков, основные этапы управления рисками.
20. Процедурный уровень информационной безопасности: основные классы мер процедурного уровня.
21. Процедурный уровень информационной безопасности: управление персоналом.
22. Процедурный уровень информационной безопасности: физическая защита, поддержание работоспособности.
23. Процедурный уровень информационной безопасности: реагирование на нарушения режима безопасности, планирование восстановительных работ.
24. Основные понятия программно-технического уровня информационной безопасности.
25. Особенности современных информационных систем, существенные с точки зрения безопасности.
26. Принципы построения архитектурной безопасности информационных систем.
27. Идентификация и аутентификация: основные понятия.
28. Идентификация и аутентификация: парольная аутентификация, одноразовые пароли.
29. Идентификация и аутентификация: сервер аутентификации Kerberos.
30. Идентификация/аутентификация с помощью биометрических данных.
31. Управление доступом: основные понятия, ролевое управление доступом.
32. Управление доступом: возможный подход к управлению доступом в распределенной объектной среде.
33. Компьютерные вирусы: определение компьютерного вируса, виды и способы размножения, степень нанесения ущерба компьютерного вируса.
34. Компьютерные вирусы: методы и средства нейтрализации программных вирусов.

35. Протоколирование и аудит: назначение, задачи, функции.
36. Шифрование информации: назначение, методы и способы шифрования информации.
37. Контроль целостности данных: назначение, задачи, функции.
38. Межсетевые экраны: архитектурные аспекты межсетевых экранов.
39. Межсетевые экраны: классификация межсетевых экранов.
40. Сервиз анализа защищенности: задачи, назначение.
41. Туннелирование и управление: назначение, задачи, функциональные области управления.
42. Обеспечение высокой доступности: основные понятия, основы мер обеспечения высокой доступности.
43. Обеспечение высокой доступности: отказоустойчивость и зона риска.
44. Обеспечение высокой доступности: обеспечение отказоустойчивости информационных систем.

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Нормативно-правовые акты Российской Федерации

1. Доктрина информационной безопасности РФ. Утверждена Президентом Российской Федерации от 05.12.2016г. №646. [Электронный ресурс]: Режим доступа: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html, свободный. - Загл. с экрана.

2. Федеральный закон РФ Об информации, информационных технологиях и о защите информации» от 27 июля 2006 № 149-ФЗ. [Электронный ресурс]: Режим доступа: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

3. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_50922-2006, свободный. - Загл. с экрана.

4. ГОСТ Р ИСО/МЭК 17799-2005 Практические правила управления информационной безопасностью. [Электронный ресурс]: Режим доступа: https://meganorm.ru/Index2/1/4293850/4293850664.htm6 свободный. Загл. с экрана.

5. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

6. РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации, Решение Председателя Гостехкомиссии России от 30.03.1992. [Электронный ресурс]: Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

7. РД. АС. Защита от НСД к информации. Классификация АС и требования по защите информации. Решение Председателя Гостехкомиссии России от 30. 03.1992**.. [Электронный ресурс]: Режим доступа:** https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

Печатные издания, имеющиеся в наличии в Научной библиотеке РГГУ (на всех территориях) в бумажном виде.

Рекомендуемая литература (основная)

1. А.П. Зайцев и др, Технические средства и методы защиты информации, учебник / 7 изд. - М. 2014 — 442 с., полоч.индекс 681 317.

Рекомендуемая литература (дополнительная)

1. Олифер В.Г. Компьютерные сети : принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – 3-е изд. – М. [и др.] : Питер, 2008. – 957 с. полоч.индекс 600 О54

2. А.П. Росенко Внутренние угрозы безопасности конфиденциальной информации Б М. 2010 — 156 с., полоч. индекс 681 Р747.

Печатные издания, имеющиеся в наличии в Научной библиотеке РГГУ (на всех территориях) в электронном виде.

Рекомендуемая литература (основная)

1. Словарь терминов и определений по информационной безопасности и защите информации [Электронный ресурс] : учебно-справочное пособие : для бакалавриата по направлению 090900.62 "Информационная безопасность" / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. информац. безопасности ; [сост.: Ищейнов В. Я., Мецатунян М. В.]. - Москва : РГГУ, 2014. - 117 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009502. - Загл. с экрана.

2. Теория информации [Электронный ресурс] : учебно-методический комплекс для бакалавриата по направлению подготовки 090900 – «Информационная безопасность»**,** про-

фили: Организация и технология защиты информации ; Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджет. образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. защиты информ., Каф. орг.-правовой защиты информ. ; [сост.: Е. И. Познякова, отв. ред.: А. А. Тарасов]. - Электрон. дан. - М. : РГГУ, 2013. - 27 с. - Режим доступа : http://elib.lib.rsuh.ru/elib/000007392. - Загл. с экрана.

3. Организационное и правовое обеспечение информационной безопасности [Электронный ресурс] : Часть II. Организационное обеспечение информационной безопасности; Учебно-методический комплекс для бакалавриата по направлению подготовки 090900 – «Информационная безопасность»; профили: Организация и технология защиты информации. Комплексная защита объектов информатизации. Ч. 2 / Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информ. наук и технологий безопасности, Фак. защиты информ., Каф. орг.-правовой защиты информ. ; [сост.: Г. А. Шевцова]. - Электрон. дан. - М. : РГГУ, 2012. - 55 с. - Режим доступа : http://elib.lib.rsuh.ru/elib/000007393.pdf. - Загл. с экрана.

4. Основы информационной безопасности. Части I-II. [Электронный ресурс] : Учебно-методический комплекс для бакалавриата по направлению подготовки 090900 – «Информационная безопасность» по профилям: Организация и технология защиты информации. Комплексная защита объектов информатизации / Федер. агентство по образованию, Гос. образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ) Ин-т информ. наук и технологий безопасности, Фак. защиты информ., Каф. методологии защиты информ. ; [сост.: И. А. Русецкая]. - Электрон. дан. - М. : РГГУ, 2012. - 52 с. - Режим доступа : http://elib.lib.rsuh.ru/elib/000007265.pdf. - Загл. с экрана..

5. Проблемы управления безопасностью сложных систем [Электронный ресурс] : труды XII Междунар. конф., Москва, декабрь 2004 г. / Рос. акад. наук [и др. ; под ред.: Н. И. Архиповой и В. В. Кульбы]. - Электрон. дан. - М. : РГГУ, 2004. - 507 с. : рис. - Режим доступа : http://elib.lib.rsuh.ru/elib/B04010.pdf. - Загл. с экрана.

Рекомендуемая литература (дополнительная):

1. Методы и средства защиты программного обеспечения [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подготовки 090900 «Информационная безопасность»: по профилям: Организация и технология защиты информации, Комплексная защита объектов информатизации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. компьютерной безопасности ; [сост.: Казарин О.

В. ; отв. ред. А. А. Тарасов]. - Электрон. дан. - Москва : РГГУ, 2013. - 30 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009341. - Загл. с экрана.

2. Методы информационного противоборства [Электронный ресурс] : учеб.-метод. комплекс : для бакалавриата по направлению подгот. 090900 «Информационная безопасность»: по профилю Организация и технология защиты информации / Минобрнауки России, Федер. гос. бюджетное образоват. учреждение высш. проф. образования "Рос. гос. гуманитарный ун-т" (РГГУ), Ин-т информац. наук и технологий безопасности, Фак. информац. систем и безопасности, Каф. методологии защиты информации ; [сост.: В. В. Арутюнов]. - Электрон. дан. - Москва : РГГУ, 2013. - 32 с. - Режим доступа: http://elib.lib.rsuh.ru/elib/000009324. - Загл. с экрана.

3. Лобашев А.К., Халяпин Д.Б., Гудов Г.Н. Противодействие экономическому шпионажу (Информационное пособие, электрон. информ.-метод. Пособие, – СПб.: Издательский дом «Афина», 2013. 1элктрон.опт. (CD-ROM) полоч.индекс 681 П 83 (только библиотека ФЗИ).

4. Яновский Г.Г. Сети связи: Учебник / Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. – СПб:БХВ-Петербург, 2014. – 401с. – Режим доступа: http://znanium.com/catalog /product/944261- Загл. с экрана.

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Информационный бюллетень Jet Info [Электронный ресурс]. - Электрон. дан. - [М., 2014]. - Режим доступа свобод.: http://www.jetinfo.ru/ .

2. Официальный сайт Российской государственной библиотеки [Электронный ресурс]. - Электрон. дан. - [М., 2013]. - Режим доступа свобод.: http://www.rsl.ru/ .

3. Официальный сайт Российской национальной библиотеки [Электронный ресурс]. - Электрон. дан. - [М., 2014]. - Режим доступа свобод.: http://www.nlr.ru/ .

4. Glossary Commander. Служба тематических толковых словарей [Элек-тронный ресурс]. - Электрон. дан. - [М., 2008]. - Режим доступа свобод.: http://glossary.ru/ .

5. Сайт справочно-правовой системы по федеральному и региональным законодательствам России - Режим доступа свобод.:http://pravo.ru/.

6. Официальный интернет-портал правовой информации - Режим доступа свобод.:http://pravo.gov.ru.

7. Информационный портал в области защиты информации - Режим доступа свобод.: http://www.securitylab.ru

8. Портал ФСТЭК - Режим доступа свобод.: http://www.fstec.ru

9. Сайт электронной библиотеки - Режим доступа свобод.: http://www.iprbookshop.ru

7. Материально-техническое обеспечение дисциплины

Для проведения занятий по дисциплине необходимо:

1. Сервер – 1.
2. ПЭВМ – 25 комплектов, объединенные в локальную сеть, с установленным ПО MS WINDOS.
3. Мультимедийный видеопроектор.
4. Экран со стойкой.

Лекционных занятий - аудитория с компьютером и проектором,

Практических занятий – компьютерный класс с установленным ПО MS WINDOS, CSS, объединенный локальной информационной сетью по технологии клиент-сервер, интегрированной в домен с выходом в Интернет

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса лицам с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого от студента требуется представить заключение психолого-медико-педагогической комиссии (ПМПК) и личное заявление (заявление законного представителя).

В заключении ПМПК должно быть прописано:

- рекомендуемая учебная нагрузка на обучающегося (количество дней в неделю, часов в день);
- оборудование технических условий (при необходимости);
- сопровождение и (или) присутствие родителей (законных представителей) во время учебного процесса (при необходимости);
- организация психолого-педагогического сопровождение обучающегося с указанием специалистов и допустимой нагрузки (количества часов в неделю).

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся при необходимости могут быть созданы фонды оценочных средств, адаптированные для лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе.

Форма проведения текущей и итоговой аттестации для лиц с ограниченными возможностями здоровья устанавливается с учетом индивидуальных психофизических осо-

бенностей (устно, письменно (на бумаге, на компьютере), в форме тестирования и т.п.). При необходимости студенту предоставляется дополнительное время для подготовки ответа на зачете.

9. Методические материалы

Успешное освоение дисциплины студентом определяется, несколькими факторами: посещение аудиторных занятий, подготовка и выполнение домашних заданий, практических работ, своевременное выполнение запланированных форм отчетности.

9.1. Планы самостоятельных занятий

Самостоятельные занятия направлены на закрепление полученных навыков и для приобретения новых теоретических и фактических знаний, выполняется в читальном зале библиотеки и в домашних условиях, подкрепляется учебно-методическим и информационным обеспечением (учебники, учебно-методические пособия, конспекты лекций).

Самостоятельные занятия выполняется с использованием ПК в домашних условиях, либо в библиотеке института по специальным заданиям в соответствии с методическими материалами, выданными преподавателем. Самостоятельные занятия включает отработку навыков анализа ситуации, создание модели ситуации, которая используется в данном конкретном методе, и решение задачи, также к самостоятельной работе относится выполнение заданий по пройденному материалу. Подготовка по темам пропущенных занятий.

Начиная с первого занятия, преподаватель объявляет студентам тему следующего занятия и список литературы. Студент должен ознакомиться с предложенными источниками, в таком случае он на следующем занятии будет готов к восприятию нового материала.

Студент для самостоятельной работы должен иметь программу курса, вопросы к экзамену, список основной и дополнительной литературы по курсу.

После каждого занятия, перед следующим, студент должен ознакомиться с пройденным материалом. При возникновении вопросов или непонимания, студент должен изучить рекомендованную и дополнительную литературу по курсу.

Процесс изучения дисциплины предусматривает выполнение обучающимися следующих видов самостоятельной работы:

- подготовка к лекциям,
- практическим занятиям, устным опросам,
- выполнение письменных работ,

- подготовка к итоговой аттестации.

Вопросы для самостоятельной проработки и самоконтроля.

Раздел № 1 Методологические аспекты информационной безопасности (ИБ) и защиты информации (ЗИ)

1. Освоение основных терминов и определений, понятий в области ИБ и ЗИ.
2. Связь ИБ с информатизацией общества.
3. Необходимость и значение нормативно-правового определения основных понятий.
4. Классификация угроз ИБ, каналов НСД к информации в ИС. Подготовка к тестированию.
5. Какие объекты защиты в информационных системах (ИС).
6. Основные источники угроз для ИС.
7. Характерные угрозы для информационных ресурсов (ИР).
8. Подготовка домашней работы по заданию преподавателя.

Раздел № 2 Законодательный, уровень обеспечения информационной безопасности

1. Понятие и назначение стандартов.
2. Виды стандартов и критерии оценки состояния информационной безопасности.
3. Освоение основных действующих в России международных стандартов в области ИБ.
4. Освоение основных действующих в России нормативно-правовых актов в области ИБ.
5. Российские нормативно-правовые акты в области ИБ.
6. Базовые принципы защиты информации от несанкционированного доступа (НСД) в соответствии с нормативно-правовыми документами
7. Основные группы классов защищенности ИС.
8. Подготовка домашней работы по заданию преподавателя.

Раздел № 3 Административный и процедурный уровень обеспечения информационной безопасности.

1. Основные разделы и содержание политики ИБ.
2. Основные разделы и содержание программы ИБ.
3. Базовые инструментальные средства для анализа рисков.
4. Стратегии управления рисками.
5. Минимизация привилегий и распределение обязанностей между персоналом, как основной принцип исключения от случайных ошибок и реализации преднамеренных угроз

6. Основные требования к персоналу по поддержанию работоспособности. ИС,
7. Основные правила по исключении дестабилизирующих факторов нарушения состояния ИБ
8. Действия персонала по минимизации ущерба при планирование восстановительных работ
9. Подготовка домашней работы по заданию преподавателя.

Раздел № 4 Программно-технический уровень обеспечения информационной информации

1. Основные проблемы в построении СЗИ, связанных с развитием информационных технологий.
2. Перечислите принципы архитектурной безопасности для обеспечения конфиденциальности ИР.
3. Перечислите принципы архитектурной безопасности для обеспечения высокой доступности (непрерывности функционирования) к ИС.
4. Основные группы методов аутентификации.
5. Особенности протоколирования и аудита. ИБ.
6. Симметричные и ассиметричные криптосистемы.
7. Компьютерная стеганография.
8. Основные классы межсетевых экранов.
9. Подготовка домашней работы по заданию преподавателя.

9.2. Планы практических занятий

Методические указания по организации и проведению практических занятий.

Практические задания – это задания, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины.

Практические занятия проводятся в учебных группах (подгруппах) и имеют своей целью:

1) закрепление теоретических основ дисциплины, излагаемых в лекционном курсе, а также самостоятельно изучаемых студентами;

2) формирование практических навыков по использованию средств защиты информации;

Методическая ценность использования практических заданий в том, что студенту надо глубже вникать в сущность задания, выделять главные моменты, учитывая связи между компонентами, и т. д. Благодаря этому учебный навык, на формирование которого

направлены эти задания, вырабатывается быстрее, ибо он связан с продуктивной мыслительной деятельностью обучаемого.

При выборе практических заданий преподаватель, в первую очередь, должен руководствоваться их потенциальной пригодностью для достижения поставленных целей занятия. Наиболее значимыми целями для преподавателя информационных дисциплин являются формирование теоретических знаний, умений добывать, систематизировать знания, развитие мышления, способность выражать мысли, воспитание информационной и коммуникативной культуры.

Тематика практических занятий соответствует программе дисциплины.

Оформление лабораторной работы.

Лабораторная работа выполняется в отдельной тетради (на отдельных листах) в рукописном или печатном вариантах включает следующие разделы:

- наименование лабораторной работы и учебные вопросы;
- описание и схема объекта защиты;
- таблицы с измеряемыми параметрами;
- расчеты (по необходимости);
- разработанные предложения;
- общее выводы по работе.

Защита полученных результатов

Оформленная лабораторная работа представляется преподавателю.

Студент должен быть готовым к ответу на вопросы преподавателя по теоретическим материалам данной работы, по порядку ее выполнения и оформления.

Тематика лабораторных занятий

Раздел № 1 Методологические аспекты информационной безопасности (ИБ) и защиты информации (ЗИ)

Задание № 1. (2часа) Определение понятия «система защита информации»

Ниже даны 9 понятий система из различных источников. Прочитайте каждое из этих понятий и проделайте следующее:

1. Проанализируйте приведённые и выделите основные свойства систем.

2. Сформулируйте свой вариант определения понятия «система защиты информации» (СЗИ).

3. Сформуйте свой вариант определения понятия «цель организации и функционирования СЗИ».

4. Разработайте пирамиду целей СЗИ.

5. Определите основные классы задач СЗИ и дайте их краткую и обобщенную характеристику.

Существующие определения понятия «система»

1. «...все, состоящее из связанных друг с другом частей, мы будем называть системой» (Ст. Бир).

2. «Система — это комплекс взаимодействующих компонентов» (Л. Берталанфи).

3. «Система — это множество взаимосвязанных элементов... не существует одного подмножества элементов, не связанного с другим подмножеством» (Р. Акофф).

4. «Система — это не просто совокупность единиц... а совокупность отношений между этими единицами» (А. Рапорт).

5. «И хотя понятие системы определяется по-разному, обычно все-таки имеется в виду, что система представляет собой определенное множество взаимосвязанных элементов, образующих устойчивое единство и целостность, обладающее интегральными свойствами и закономерностями» (В. П. Кузьмин).

6. «Мы можем определить систему как нечто целое, абстрактное или реальное, состоящее из взаимосвязанных взаимодействующих или взаимозависимых частей» (Ф. Ханика).

7. «Любой комплекс, любая форма распределения активности в цепи, рассматриваемая каким-либо наблюдателем как закономерное, является системой» (Г. Паск).

8. «Система — это то, что получается в результате оптимизации конструкций путем всестороннего анализа взаимосвязанных факторов, влияющих на ее существенные характеристики» (Б. Байцер).

9. «Системой можно назвать только такой комплекс избирательно вовлеченных компонентов, у которых взаимодействие и взаимоотношение приобретают характер взаимодействия компонентов на получение фокусированного полезного результата» (П. К. Анохин).

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017-wireshark-kak-i-dlya.htm, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Задание №2. (2часа) Разработайте модель системы защиты информации на предприятии.

1. Представить состав основных функций и организационных элементов КСЗИ.
2. Объяснить, как содержательно взаимосвязаны функциональная и организационная структуры КСЗИ.
3. Построить и графически представить функциональную и организационную модели системы защиты информации объекта, описание которого приведено в приложении к заданию.

Приложение к заданию

Оцениваемый объект представляет собой научно-производственное предприятие, ориентированное на выпуск сложных, дорогостоящих изделий специального назначения. Предприятие обладает высоким техническим потенциалом, имеет сложное оборудование и квалифицированных специалистов. В состав предприятия входит специальное конструкторское бюро с собственной гражданской и оборонной тематикой.

В условиях резкого сокращения оборонных заказов предприятие вынуждено было начать поиск внебюджетных источников инвестиций. Одним из таких источников стало производство электрохромных активных зеркал заднего вида для легковых автомобилей, предназначенных на свободную реализацию. Такие зеркала являются уникальными для России, обладают «ноу-хау» и имеют конкурентные преимущества высокого порядка, преодоление которых для конкурентов является сложной проблемой. Аналогичные изделия, которые поставляются в Россию, производятся еще только двумя американскими фирмами (Донелли и Гентакс). Потребителем их продукции в России является представительство фирмы Альфа-Ромео, офис которого находится рядом с центральным административным корпусом здания рассматриваемого предприятия.

Основные производственные помещения (цеха), где изготавливаются изделия, находятся в г. Чехове. Что касается представительства (центральный офис), в котором располагается руководящий аппарат, то он находится в центре Москвы. Рядом с основным корпусом административного здания находится строение, которое одновременно выполняет функции хранилища готовой продукции и выставочного комплекса.

Система защиты объекта построена по принципу выделения защищаемых зон и их декомпозиции. Внешняя зона защиты охватывает территорию от ограждения до периметра зданий (включая автостоянку).

Внутренняя зона разделена:

1) на сектор защиты выделенных помещений в 1 комнату;
2) сектор защиты хранилища и выставочного комплекса.

3) Для обеспечения безопасности внешней зоны установлено металлическое ограждение высотой 3 метра.

4) Безопасность внутренней зоны обеспечивается следующими средствами, методами и мероприятиями:

5) при входе в каждый корпус осуществляется электронный контроль. Посетители и сотрудники проходят через специальные ворота, где определяется, нет ли при них оружия и опасных предметов. Кроме того, у сотрудника проверяется пропуск, а у посетителей — документ, удостоверяющий личность;

6) имеется система теленаблюдения. Сигналы с ТВ-камер выводятся на цифровые анализаторы. При срабатывании сигналов тревоги изображения с тревожных камер выводятся на видеомагнитофон;

7) установлена система охранной сигнализации с резервным и аварийным источниками питания;

8) выделенные помещения оборудованы магнитными датчиками, реагирующими на прохождение человека с металлическим предметом достаточно большой массы;

9) применяются заранее оговоренные условные фразы и кодовые выражения при ведении телефонных разговоров по городским каналам связи о времени и месте проведения важных деловых встреч и совещаний;

10) в Устав и правила трудового распорядка, а также в контракты сотрудников внесены специальные разделы и пункты, касающиеся правил обеспечения защиты информации;

11) ежегодно проводится обучение сотрудников правилам и процедурам работы с конфиденциальной информацией;

12) определен круг лиц, которые в силу занимаемого служебного положения на предприятии имеют доступ к защищаемой информации;

13) осуществляется взаимодействие с органами внутренних дел по вопросам обеспечения безопасности;

14) в выделенных помещениях применяются звукопоглощающие облицовки и двойные оконные переплеты для защиты от прослушивания;

15) используются светонепроницаемые стекла, занавески, драпировки и другие защитные материалы для защиты от наблюдения и фотографирования.

16) Для защиты локально-вычислительной сети предусмотрено следующее:

17) идентификация технических средств, файлов и аутентификация пользователей;

18) регистрация и контроль работы технических средств и пользователей;

19) уничтожение информации в ЗУ после использования;

20) установлены специальные антивирусные средства;

21) ведется учет носителей.

Координирует действия по обеспечению безопасности служба защиты информации, являющаяся самостоятельным структурным подразделением.

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017-wireshark-kak-i-dlya.htm, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Раздел № 2 (2часа) Законодательный, уровень обеспечения информационной безопасности

Задание №3. Разработайте примерный перечень сведений, составляющих коммерческую тайну предприятия.

1. Укажите разделы данного перечня.

2. Определите критерии, по которым те или иные сведения могут быть отнесены к защищаемым.

3. Определите, какие документы необходимы для внесения изменений и дополнений в сформированный перечень сведений, составляющих коммерческую тайну, и кто эти документы *разрабатывает.*

Список литературы:

1. *Основы работы с Cisco Packet Tracer* [Электронный ресурс] : Режим доступа : http://just-networks.ru/articles/osnovy-raboty-s-cisco-packet-tracer, свободный. – Загл. с экрана.

2. *Как пользоваться Wireshark под Windows* [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017-wireshark-kak-i-dlya.htm, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Задание №4. Определение понятий технология управления и функционирования СЗИ

1. На основе обобщения приведенных интерпретаций определений понятия

«технология» сформулировать свой вариант определения понятия «технология управления СЗИ» и «технология функционирования СЗИ».

2. Провести сравнительный анализ рассматриваемых понятий.

3. Определить, на какие этапы делится процедура принятия решения, учитывая, что оно (принятие решения) составляет основу технологии управления.

Перечень существующих определений понятия «технология»

1. Технология — любое средство преобразования исходных материалов, будь то люди, информация или физические материалы, для получения желаемых продукций или услуг.

2. Технология — (искусство, мастерство, умение) — совокупность методов обработки, изготовления, изменения состояния, свойств, формы сырья, материала или полуфабриката, осуществляемых в процессе производства продукции.

3. Технология — процессы подготовки, передачи, накопления и обработки информации с помощью вычислительных машин.

4. Технология — система взаимосвязанных способов обработки материалов и приемов изготовления продукции в производственном процессе.

5. Технология — совокупность методов, производственных процессов и программно-технических средств, объединенных в технологическую цепочку, обеспечивающую сбор, хранение, обработку, вывод и распространение информации для снижения трудоемкости процессов использования информационного ресурса, повышения их надежности и оперативности.

6. Технология — совокупность технологических элементов, например устройств или методов, используемых людьми для обработки информации.

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017-wireshark-kak-i-dlya.htm, свободный. – Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Раздел № 3. Административный и процедурный уровень обеспечения информационной безопасности.

Задание № 5. (2часа) Определение основных принципов управления сложных организационно -технических систем.

1. Ознакомьтесь с перечнем принципов организации сложных организационно-технических систем.
2. Из предложенного ниже перечня выбрать принципы организации сложных социотехнических систем, обосновать свой выбор и дать интерпретацию выбранных принципов с точки зрения организации СЗИ;
3. Указать, какими еще принципами следует руководствоваться при организации и управлении СЗИ;
4. Выявить приоритетность среди выбранных принципов (обосновать свое мнение, используя практические примеры).

Перечень принципов организации сложных организационно-технических систем:

Целенаправленность — сосредоточение определяющей доли всех видов ресурсов на решении важнейших задач.

Комплексность — учет всех или по крайней мере большинства важнейших факторов, оказывающих влияние на решение поставленной задачи, а также учет возможных последствий реализации принимаемых решений и внутренних взаимосвязей разрабатываемых и осуществляемых мероприятий.

Научная обоснованность — системное рассмотрение проблем, изучение и обобщение передового научного и практического опыта в данной предметной области.

Экономичность — создание и эксплуатация системы, осуществляемые с оптимальным расходованием различных видов ресурсов.

Эргономичность — проектирование системы с учетом психофизиологических особенностей человека, который будет ее эксплуатировать.

Централизованность — организационно-функциональная самостоятельность процессов, обеспечивающих решение всех важнейших задач организации и функционирования системы.

Специализированность — привлечение к проектированию, внедрению и эксплуатации системы специализированных организаций, профессионально подготовленных специалистов, имеющих опыт научной и лабораторной работы в области, соответствующей целевому и функциональному назначению системы, ее техническим и другим особенностям.

Совершенствование — непрерывный анализ и внесение соответствующих корректив в процесс функционирования системы с учетом соответствующих научных и практических достижений и обобщения накопленного опыта.

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Задание № 6. (2часа) Разработайте модель угроз защищаемой информации на предприятии:

1. Представьте графическую схему, отражающую содержание основных этапов процедуры выявления угроз информации и основных категорий нарушителей.
2. Объясните, каким образом действия нарушителей различных категорий оказывают влияние на обеспечение функционирования КСЗИ.
3. Заполните табл. П1.1 следующего вида:

Таблица П1.1

Категории нарушителей	Дестабилизирующие воздействия								
	Объекты защиты (Q_i...Q_n)								
		II					..		VII

Угрозы (A, B, C, ..., Z)

A — вывод из строя основного оборудования;

B — перехват информации;

C — ...;

Z — физическое воздействие на информацию.

Объекты защиты (I, II, ..., X)

I — выделенные помещения;

II — средства обработки информации и связи;

III — ...;

X — системы обеспечения функционирования объекта.

Вербально-числовая оценка степени опасности дестабилизирующего воздействия

1 — незначительная;

2 — малая;

3 — средняя;

4 — высокая.

Категории нарушителей:

1. специалисты функциональных подразделений;
2. специалисты службы безопасности;
3. вспомогательный (технический) персонал.

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.
2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017 – свободный. Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Раздел № 4 Программно-технический уровень обеспечения информационной информации

Задание №7. (2часа) Определение и разработка этапов планирования работ

1. Определить, какие общие этапы включает в себя планирование организации системы защиты информации (система защиты информации).
2. Разработать структуру плана организации СЗИ на основе предложенной общей, поэтапной программы действий (см. Приложение 2), охватывающей процесс организации СЗИ на любом предприятии.
3. Предложить свое содержательное наполнение разработанной структуры плана.

Таблица П1.2

Характеристики видов контроля	Значения характеристик
Периодичность проведения	Оперативный Периодический Эпизодический

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017 – свободный. Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Задание № 8. (2часа) Алгоритм построения контроля системы защиты информации.

1. Сформулировать определение понятия «контроль функционирования КСЗИ».
2. Определить, в чем заключаются особенности организации и контроля функционирования КСЗИ и систем другого назначения (например, производственных, систем связи, АСОД и т. д.);
3. Графически представить алгоритм контроля в КСЗИ;
4. Заполнить классификационную таблицу (табл. П1.2).

Таблица П1.2

Характеристики видов контроля	Значения характеристик
Периодичность проведения	Оперативный Периодический Эпизодический

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017 – свободный. Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

Задание № 9. (2часа) Разработка программы действий в чрезвычайных ситуациях на примере банка.

1. На основе анализа определений различных понятий, относящихся к данной предметной области, сформулировать определение понятия «чрезвычайная ситуация» в

отношении процессов защиты информации;

2. Определить критерии, по которым можно провести классификацию потенциально возможных чрезвычайных ситуаций, способных влиять на функционирование КСЗИ;

3. Разработать программу действий в чрезвычайных ситуациях на примере банка, и самостоятельно сформировать:

а) структуру паспорта риска объекта;

б) структуру группы (комитета) по управлению в условиях ЧС и ликвидации их последствий.

Перечень определений различных понятий, относящихся к категории экстремальных (чрезвычайных) событий:

Авария — опасное происшествие на хозяйствующем субъекте, транспорте или на линиях связи, представляющее угрозу жизни и здоровью людей либо приводящее к разрушению производственных помещений, повреждению или уничтожению оборудования, механизмов, транспортных средств, сырья и готовой продукции, а также к нарушению производственного процесса.

Катастрофа — внезапное бедствие, событие, влекущее за собой тяжелые последствия.

Кризисная ситуация — резкий, крутой перелом в чем-либо, тяжелое переходное состояние.

Риск - тип реализации опасностей определенного класса, который может быть определен как частота или как вероятность возникновения одного события при наступлении другого события.

Чрезвычайная ситуация — комплекс событий, протекание и результат наступления которых приводит к реализации в районе чрезвычайной ситуации, опасной для жизни и здоровья людей, а также материальных ценностей, нарушение экономической деятельности, нормального жизнеобеспечения, функционирования схем управления и связи, а также экологического равновесия.

Список литературы:

1. ГОСТ Р ИСО/МЭК 15408-1 (15408-2, 15408-3) Критерии оценки безопасности информационных технологий. [Электронный ресурс]: Режим доступа: https://standartgost.ru/g/ГОСТ_Р_ИСО/МЭК 15408-1, свободный. Загл. с экрана.

2. Как пользоваться Wireshark под Windows [Электронный ресурс] : Режим доступа : https://www.windxp.com.ru/1017 – свободный. Загл. с экрана.

Материально-техническое обеспечение занятия:

Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной, ППП Cisco Packet Tracer и Wireshark.

9.2. Методические рекомендации по подготовке письменных работ (рефератов, докладов)

Реферат, доклад – продукт самостоятельной работы студента, представляющий собой написание учебный работы и публичное выступление по представлению полученных результатов решения определенной учебно-лабораторной, учебно-исследовательской или научной темы.

Примерный перечень тем рефератов, докладов

1 Основные методики, используемые для оценки рисков.

2 Процедура формирования электронной подписи.

3 Основные каналы несанкционированного доступа (НСД0 к информации при ее обработке с использованием технических средств.

4 Методы, способы несанкционированного доступа (НСД) к информации при ее обработке на СВТ (АС).

5 Основные уровни обеспечения информационной безопасности.

6 Классификация угроз, источников угроз информационной безопасности при обработке информации с использованием технических средств.

7 Основные положения ФЗ «Об информации, информационных технологиях и о защите информации».

8 Концептуальные нормативно-правовые акты России в области защиты информации.

9 Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну.

10 Виды и классификация компьютерных преступлений.

11 Виды компьютерных преступлений, методы противодействия компьютерным преступлениям.

12 Политика информационной безопасности, основные положения и этапы её разработки.

13 Программа информационной безопасности, основные положения и этапы её разработки.

14 Основные угрозы компьютерным системам.

15 Методики оценки рисков для информационных систем.

16 Стандарты в области разработки политики информационной безопасности.

17 Инструментальные средства для анализа рисков и управления ими.

18 Законодательный уровень информационной безопасности, основные нормативно-правовые документы необходимые для обеспечения безопасности информации на предприятии.

19 Административный уровень информационной безопасности, политика и программа информационной безопасности.

20 Административный уровень информационной безопасности, анализ, учет и управления рисками.

21 Процедурный уровень информационной безопасности, назначение, цели и решаемые задачи.

22 Программно-технический уровень информационной безопасности, назначение, цели и решаемые задачи,

23 Принципы построения архитектурной безопасности информационных систем.

24 Основные группы процедурных мер по обеспечению информационной безопасности.

25 Базовые направления поддержки работоспособности информационных систем.

26 Основные сервисы программных средств защиты информации в информационных системах.

27 Базовые группы методов аутентификации.

28 Основные правила парольной защиты в компьютерных системах.

29 Биометрические системы идентификации пользователей.

30 Основные виды управления доступом к информации.

31 Классификация программ-вирусов.

32 Базовые виды антивирусных программ.

33 Классификация вредоносных программ.

34 Основные свойства антивирусного программного продукта Лаборатории Касперского.

35 Классификация методов криптографического преобразования данных.

36 Блочное и потоковое шифрование.

37 Основные методы шифрования данных.

38 Базовые криптографические стандарты.

39 Симметричные и ассиметричные криптосистемы.

40 Стеганографические системы при передаче информации по каналам связи .

41 Базовые ресурсы информационных систем, подлежащих защите.

42 Основные принципы архитектурной безопасности информационных систем.

43 Сервисы безопасности для реализации защитных функций вычислительной сети.

44 Иерархия сервисов безопасности в информационных телекоммуникационных системах (ИТС).

45 Юридическая ответственность за нарушение правовых норм по защите информации.

46 Меры дисциплинарной за нарушение правовых норм по защите информации.

47 Административная ответственность за правонарушения в области защиты информации.

48 Уголовная ответственность за правонарушения и преступления в области конфиденциальной информации.

Аннотация

Дисциплина Б1.Б14 «Информационная безопасность» относится к блоку Б1 дисциплин базовой части учебного плана по направлению подготовки 09.03.03 «Прикладная информатика».

Дисциплина реализуется на факультете Информационных систем и безопасности кафедрой «Комплексной защиты информации».

Цель дисциплины:

- профессиональная подготовка студентов, необходимая для освоения методов и технологий обеспечения информационной безопасности и защиты информации в информационных системах архивов и системах документооборота.

Задачи дисциплины:

- получение систематизированных знаний о современных концепциях, методах и технологиях обеспечения информационной безопасности в информационных системах различного назначения;
- изучение теоретических основ информационной безопасности;
- формирование умений использовать основные достижения в области информационной безопасности при реализации своей профессиональной деятельности;
- владение навыками обеспечения защиты информации в информационных системах различного назначения;
- развитие аналитического мышления, умения строго излагать свои мысли, развитие способностей к обобщению и анализу информации, постановке целей и выбору путей ее достижения.

Дисциплина направлена на формирование следующих компетенциях:

- ОПК-4: способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;
- ПК-18: способен принимать участие в организации ИТ-инфраструктуры и управлении информационной безопасностью.

В результате освоения дисциплины обучающийся должен:

Знать основные понятия, связанных с обеспечением информационной безопасностью и защитой информации, цели и задачи предметной области и компьютерные методы их решения, особенности использования локальных и глобальных информационно-телекоммуникационных сетей, требования к надежности и эффективности информационных систем в области её применения.

Уметь выбирать методы и технологии обеспечения информационной безопасности, использовать системный подход к исследованию и построению информационных систем.

Владеть комплексным подходом к обеспечению информационной безопасности, навыками решения задачи проектирования информационных систем для предметной области с использованием типовых проектных решений и стандартов, навыками постановки задачи системного проектирования и обслуживания программных средств на всем жизненном цикле информационных систем.

Рабочей программой предусмотрены следующие виды контроля: текущий контроль успеваемости в форме тестовых заданий, промежуточная аттестация в форме зачета с оценкой.

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 часа.

Приложение 2

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты
информации РГГУ
№ 20 от 26.06.2018

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины «Информационная безопасность» по направлению подготовки 09.03.03 «Прикладная информатика» (прикладной бакалавриат) на 2018/2019 учебный год

1. В перечень программного обеспечения (ПО) вносятся следующие изменения (табл. 1):

Таблица 1

№ п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2013	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2. В перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) вносятся следующие изменения (табл. 2):

Таблица 2

№ п/п	Наименование
	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2018 г. Web of Science Scopus
	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2018 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам
	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Приложение 3

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты
информации РГГУ
№ 1 от 29.08.2019

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины «Информационная безопасность» по направлению подготовки 09.03.03 «Прикладная информатика» (прикладной бакалавриат) на 2019/2020 учебный год

1. В перечень программного обеспечения (ПО) вносятся следующие изменения (табл. 1):

Таблица 1

№ п/п	Наименование ПО	Производитель	Способ распространения
	Kaspersky Endpoint Security	Kaspersky	лицензионное
	Microsoft Office 2016	Microsoft	лицензионное
	Visual Studio 2019	Microsoft	лицензионное
	Adobe Creative Cloud	Adobe	лицензионное

2. В перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) вносятся следующие изменения (табл. 2):

Таблица 2

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2019 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2019 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis
3	Профессиональные полнотекстовые БД JSTOR Издания по общественным и гуманитарным наукам Электронная библиотека Grebennikon.ru
4	Компьютерные справочные правовые системы Консультант Плюс, Гарант

Приложение 4

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты
информации РГГУ
№ 14 от 23.06.2020

ЛИСТ ИЗМЕНЕНИЙ

в рабочей программе дисциплины «Информационная безопасность» по направлению подготовки 09.03.03 «Прикладная информатика» (прикладной бакалавриат) на 2020/2021 учебный год

1. В перечень программного обеспечения (ПО) вносятся следующие изменения (табл. 1):

Таблица 1

№п/п	Наименование ПО	Производитель	Способ распространения
1	Windows 10 Pro	Microsoft	лицензионное
2	Kaspersky Endpoint Security	Kaspersky	лицензионное
3	Microsoft Office 2016	Microsoft	лицензионное
4	Платформа ZOOM	Zoom	лицензионное

2. В перечень современных профессиональных баз данных (БД) и информационно-справочных систем (ИСС) вносятся следующие изменения (табл. 2):

Таблица 2

№п/п	Наименование
1	Международные реферативные наукометрические БД, доступные в рамках национальной подписки в 2020 г. Web of Science Scopus
2	Профессиональные полнотекстовые БД, доступные в рамках национальной подписки в 2020 г. Журналы Cambridge University Press ProQuest Dissertation & Theses Global SAGE Journals Журналы Taylor and Francis Электронные издания издательства Springer
3	Компьютерные справочные правовые системы Консультант Плюс, Гарант