10.02.05.01.ОП.01-2023-РП

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Кузбасский государственный технический университет имени Т. Ф. Горбачева»
Институт профессионального образования

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: ректорат
Должность: проректор по среднему профессиональному образованию
Дата: 17.05.2023 10:49:02

Попов Иван Павлович

Рабочая программа дисциплины

Основы информационной безопасности

Специальность «10.02.05 Обеспечение информационной безопасности автоматизированных систем»

Присваиваемая квалификация
"Техник по защите информации"

Формы обучения
очная

Кемерово 2023 г.

Рабочую программу составил:

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 16.05.2023 01:40:30

Прокопенко Евгения Викторовна

Рабочая программа обсуждена на заседании кафедры информационной безопасности

Протокол № 3/1 от 16.05.2023

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 16.05.2023 02:52:31

Прокопенко Евгения Викторовна

Согласовано цикловой-методической комиссией по направлению подготовки (специальности) 10.02.05 Обеспечение информационной безопасности автоматизированных систем
Протокол № 4/1 от 16.05.2023

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: начальник управления
Дата: 16.05.2023 06:09:40

Прокопенко Евгения Викторовна

Согласовано заместителем директора по УР ИПО

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: Заместитель директора по учебной работе
Дата: 16.05.2023 06:09:40

Полуэктова Наталья Сергеевна

Согласовано заместителем директора по МР ИПО

ПОДПИСАНО ЭП КУЗГТУ
Подразделение: учебно-методическое управление
Должность: Заместитель директора по методической работе
Дата: 16.05.2023 06:09:40

Сьянова Татьяна Юрьевна

1. Общая характеристика рабочей программы дисциплины

1.1 Место дисциплины в структуре основной образовательной программы

Учебная дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла основной образовательной программы в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».
Учебная дисциплина «Основы информационной безопасности» обеспечивает формирование профессиональных и общих компетенций в соответствии с ФГОС по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем».

1.2 Цель и планируемые результаты освоения дисциплины, соотнесенные с планируемыми результатами освоения образовательной программы

Освоение дисциплины направлено на формирование:
общих компетенций:
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.
Знать: современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности;
Уметь: классифицировать основные угрозы безопасности информации;
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
Знать: место информационной безопасности в системе национальной безопасности страны;
Уметь: классифицировать основные угрозы безопасности информации;
ОК 09. Использовать информационные технологии в профессиональной деятельности.
Знать: сущность и понятие информационной безопасности, характеристику ее составляющих;
Уметь: классифицировать основные угрозы безопасности информации;
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.
Знать: источники угроз безопасности информации и меры по их предотвращению; современные средства и способы обеспечения информационной безопасности;
Уметь: классифицировать основные угрозы безопасности информации;
профессиональных компетенций:
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.
Знать: виды, источники и носители защищаемой информации; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; Уметь: классифицировать защищаемую информацию по видам тайны и степеням секретности; Иметь практический опыт: обработки, хранения и передачи информации;

В результате освоения дисциплины обучающийся в общем по дисциплине должен
Знать:
- современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности;
- место информационной безопасности в системе национальной безопасности страны;
- сущность и понятие информационной безопасности, характеристику ее составляющих;
- источники угроз безопасности информации и меры по их предотвращению; современные средства и способы обеспечения информационной безопасности;
- виды, источники и носители защищаемой информации; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
Уметь:
- классифицировать основные угрозы безопасности информации;
- классифицировать защищаемую информацию по видам тайны и степеням секретности;
Иметь практический опыт:
- обработки, хранения и передачи информации;

2. Структура и содержание дисциплины

2.1 Объем дисциплины и виды учебной работы

Форма обучения	Количество часов		
	ОФ	ЗФ	ОЗФ
Курс 2 / Семестр 3			
Объем дисциплины	68		
в том числе:			
лекции, уроки	32		
лабораторные работы			
практические занятия	32		
Консультации			
Самостоятельная работа	4		
Промежуточная аттестация			
Индивидуальное проектирование			
Форма промежуточной аттестации	дифференцированный зачет		

2.2 Тематический план и содержание дисциплины

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
3 семестр		
Раздел 1. Теоретические основы информационной безопасности		
Тема 1.1. Основные понятия и задачи информационной безопасности		
Лекции		
	Лекция 1.1.1. Понятие информации и информационной безопасности. Информация, сообщения, информационные процессы как объекты информационной безопасности. Обзор защищаемых объектов и систем.	1
	Лекция 1.1.2. Понятие «угроза информации». Понятие «риска информационной безопасности». Примеры преступлений в сфере информации и информационных технологий. Сущность функционирования системы защиты информации. Защита человека от опасной информации и от неинформированности в области информационной безопасности.	1
Тема 1.2. Основы защиты информации		
Лекции		

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
	Лекция 1.2.1. Целостность, доступность и конфиденциальность информации. Классификация информации по видам тайны и степеням конфиденциальности. Понятия государственной тайны и конфиденциальной информации.	2
	Лекция 1.2.2. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.	2
	Лекция 1.2.3. Цели и задачи защиты информации. Основные понятия в области защиты информации.	2
	Лекция 1.2.4. Элементы процесса менеджмента ИБ. Модель интеграции информационной безопасности в основную деятельность организации. Понятие Политики безопасности.	2
Практические занятия		
	Практическое занятие 1.2.1. Определение объектов защиты на типовом объекте информатизации.	4
	Практическое занятие 1.2.2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности.	4
Тема 1.3. Угрозы безопасности защищаемой информации.		
Лекции		
	Лекция 1.3.1. Понятие угрозы безопасности информации	2
	Лекция 1.3.2. Системная классификация угроз безопасности информации.	2
	Лекция 1.3.3. Каналы и методы несанкционированного доступа к информации	2
	Лекция 1.3.4. Уязвимости. Методы оценки уязвимости информации.	2
Практические занятия		
	Практическое занятие 1.3.1. Определение угроз объекта информатизации и их классификация	4
Самостоятельная работа обучающихся		2
4 семестр		
Раздел 2. Методология защиты информации		
Тема 2.1. Методологические подходы к защите информации		
Лекции		
	Лекция 2.1.1. Анализ существующих методик определения требований к защите информации.	1
	Лекция 2.1.2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.	1
	Лекция 2.1.3. Виды мер и основные принципы защиты информации.	1

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах
Тема 2.2. Нормативно правовое регулирование защиты информации		
Лекции		
	Лекция 2.2.1. Организационная структура системы защиты информации	1
	Лекция 2.2.2. Законодательные акты в области защиты информации.	1
	Лекция 2.2.3. Российские и международные стандарты, определяющие требования к защите информации.	1
	Лекция 2.2.4. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации	1
Практические занятия		
	Практическое занятие 2.2.1. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности	10
Тема 2.3. Защита информации в автоматизированных (информационных) системах		
Лекции		
	Лекция 2.3.1. Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах.	1
	Лекция 2.3.2. Программные и программно-аппаратные средства защиты информации	2
	Лекция 2.3.3. Инженерная защита и техническая охрана объектов информатизации	2
	Лекция 2.3.4. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	2
Практические занятия		
	Практическое занятие 2.3.1. Выбор мер защиты информации для автоматизированного рабочего места	10
Самостоятельная работа обучающихся		2
Всего		***68***

3 Материально-техническое и учебно-методическое обеспечение дисциплины (модуля)

3.1 Специальные помещения для реализации программы

Специальное помещение №1146 представляет собой лабораторию информационных технологий,

сетей и систем передачи информации, программирования и баз данных, оснащенную рабочими местами

на базе вычислительной техники, подключенными к локальной вычислительной сети и информационнотелекоммуникационной сети "Интернет"; программным обеспечением сетевого оборудования; обучающим программным обеспечением; эмуляторами активного сетевого оборудования; программным обеспечением

межсетевого экранирования и мониторинга технического состояния активного сетевого оборудования.

Перечень основного оборудования:

Комплект мебели (столы и стулья).

Мультимедиа-проектор BenQ MP721C; Ноутбук AcerAspire5102WLM.; Проектор Aser P1383W с

кронштейном, видео кабелем 20 м; Сейф металлический; Сплинг-система RODA RS\RU-A 18B серия Arctic;

Сплинг-система RU-A07B серия Arctic; Экран настенный рулонный Projicta ProScreen 183*240 см.;

Системный блок MK Office (Intel Core i3/4Гб/500Гб); IP-камера ZQ-IPC3-DAS-36VI Камера внутр., купольная,

1/2.8 "SONY; Моноблок Powercool, Россия; Многофункциональное устройство (МФУ) PANTUM M6500;

Принтер лазерный Kyosera Ecosys P2040dn.A4 ч\б) 1200*1200dpi. дуплэкс, сетевой; Перечень

программного обеспечения: Libre Office. Mozilla Firefox. Google Chrome. 7-zip .Microsoft Windows. ESET

NOD32 Smart Security Business Edition. Kaspersky Endpoint Security. Браузер Спутник.

3.2 Информационное обеспечение реализации программы

3.2.1 Основная литература

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для СПО / Внуков А. А.. – 3-е изд., пер. и доп. – Москва : Юрайт, 2020. – 161 с. – ISBN 978-5-534-13948-8. – URL: https://urait.ru/book/osnovy-informacionnoy-bezopasnosti-zaschita-informacii-467356 (дата обращения: 26.09.2023). – Текст : электронный.

2. Сычев, Ю. Н. Защита информации и информационная безопасность : Учебное пособие / Ю. Н. Сычев ; Российский экономический университет им. Г.В. Плеханова. – Москва : НИЦ ИНФРА-М, 2021. – 201 с. – ISBN 978-5-16-016583-7. – URL: http://znanium.com/catalog/document?id=366835 (дата обращения: 26.09.2023). – Текст : электронный.

3. Бубнов, А. А. Основы информационной безопасности : учебник для студентов, обучающихся по специальностям укрупненной группы специальностей среднего профессионального образования "Информационная безопасность" / А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. – 3-е изд. стер. – Москва : Академия, 2020. – 254 с. – (Профессиональное образование). – URL: https://academia-library.ru/catalogue/4831/471592/ (дата обращения: 26.09.2023). – Текст : электронный.

3.2.2 Дополнительная литература

1. Гультяева, Т. А. Основы информационной безопасности / Т. А. Гультяева. – Новосибирск : Новосибирский государственный технический университет, 2018. – 79 с. – ISBN 9785778236400. – URL: http://biblioclub.ru/index.php?page=book_red&id=574729 (дата обращения: 26.09.2023). – Текст : электронный.

2. Емельянова, Н. З. Защита информации в персональном компьютере : Учебное пособие / Н. З. Емельянова, Т. Л. Попов И. И. Партыка. – Москва : НИЦ ИНФРА-М, 2021. – 368 с. – ISBN 978-5-00091-466-3. – URL: https://znanium.com/catalog/document?id=365335 (дата обращения: 26.09.2023). – Текст : электронный.

3. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : Учебное пособие / Ю. Н. Сычев ; Российский экономический университет им. Г.В. Плеханова. – Москва : НИЦ ИНФРА-М, 2021. – 223 с. – ISBN 978-5-16-015718-4. – URL: https://znanium.com/catalog/document?id=364478 (дата обращения: 26.09.2023). – Текст : электронный.

3.2.3 Методическая литература

1. Основы информационной безопасности : методические материалы для обучающихся направления подготовки 10.02.05 "Обеспечение информационной безопасности автоматизированных систем" / Кузбасский государственный технический университет им. Т. Ф. Горбачева ; Кафедра информационной безопасности, составители: Е. В. Прокопенко, А. В. Медведев, А. Г. Киренберг. – Кемерово : КузГТУ, 2020. – 7 с. – URL: http://library.kuzstu.ru/meto.php?n=9963 (дата обращения: 26.09.2023). – Текст : электронный.

3.2.4 Интернет ресурсы

1. ЭИОС КузГТУ:

a) Электронная библиотека КузГТУ. – Текст: электронный // Научно-техническая библиотека Кузбасского государственного технического университета им. Т. Ф. Горбачева : сайт. – Кемерово, 2001 – . – URL: https://elib.kuzstu.ru/ . – Текст: электронный.

b) Портал.КузГТУ : Автоматизированная Информационная Система (АИС) : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://portal.kuzstu.ru/. – Режим доступа: для авториз. пользователей. – Текст: электронный.

c) Электронное обучение : [сайт] / Кузбасский государственный технический университет им. Т. Ф. Горбачева. – Кемерово : КузГТУ, [б. г.]. – URL: https://el.kuzstu.ru/ . – Режим доступа: для авториз. пользователей КузГТУ. – Текст: электронный.

2. ФСТЭК России : Федеральная служба по техническому и экспортному контролю : официальный сайт / ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – Москва, 2004 – . – URL: www.fstec.ru. – Текст: электронный.

3. SecurityLab.ru : информационный портал по безопасности : сайт. – Москва. – URL: https://www.securitylab.ru/ . – Текст: электронный.

4. Департамент образования Вологодской области : официальный сайт. – Вологда. – URL: http://depobr.gov35.ru/ . – Текст: электронный.

5. BIOMETRICS.RU : Российский биометрический портал : сайт. – Москва, 2000 – . – URL: www.biometrics.ru . – Текст: электронный.

6. InformationSecurity/Информационная безопасность : сайт. – Москва. – URL: http://www.itsec.ru. – Текст: электронный.

7. eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.

8. Гарант. ру : информационно-правовой портал : сайт. – Москва, 1990 – . – URL: https://www.garant.ru/ . – Текст: электронный.

9. КонсультантПлюс : компьютерная справочно-правовая система : сайт. – Москва, 1992 – . – URL: www.consultant.ru . – Текст: электронный.

10. Единое окно доступа к образовательным ресурсам : информационная система : сайт / ФГАУ ГНИИ ИТТ «Информика» . – Москва, 2005 – . – URL: http://window.edu.ru/ . – Текст: электронный.

11. Российское образование. Федеральный образовательный портал : сайт / ФГАОУ ДПО ЦРГОП и ИТ. – Москва, 2002 – . – URL: www.edu.ru . – Текст: электронный.

4. Организация самостоятельной работы обучающихся

Самостоятельная работа обучающихся осуществляется в объеме, установленном в разделе 2 настоящей программы дисциплины (модуля).

Для самостоятельной работы обучающихся предусмотрены специальные помещения, оснащенные компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети "Интернет" с обеспечением доступа в электронную информационно-образовательную среду КузГТУ.

5. Фонд оценочных средств для проведения текущего контроля, промежуточной аттестации обучающихся по дисциплине

5.1 Паспорт фонда оценочных средств

Планируемые результаты обучения по дисциплине.

Дисциплина направлена на формирование следующих компетенций выпускника:

5.1 Паспорт фонда оценочных средств

№	Наименование разделов дисциплины	Содержание (темы) раздела	Код компетенции	Знания, умения, практический опыт, необходимые для формирования соответствующей компетенции	Форма текущего контроля знаний, умений, практического опыта, необходимых для формирования соответствующей компетенции
1	Раздел 1. Теоретические основы информационной безопасности	Тема 1.1. Основные понятия и задачи информационной безопасности Тема 1.2. Основы защиты информации Тема 1.3. Угрозы безопасности защищаемой информации.	ОК 03	Знать: современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности; Уметь:классифицировать основные угрозы безопасности информации;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 06	Знать: место информационной безопасности в системе национальной безопасности страны; Уметь: классифицировать основные угрозы безопасности информации;	
			ОК 09	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; Уметь: классифицировать основные угрозы безопасности информации;	
			ПК 2.4	Знать: виды, источники и носители защищаемой информации; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; Уметь: классифицировать защищаемую информацию по видам тайны и степеням секретности; Иметь опыт: обработки, хранения и передачи информации;	

2	Раздел 2. Методология защиты информации	Тема 2.1. Методологические подходы к защите информации Тема 2.2. Нормативно правовое регулирование защиты информации Тема 2.3. Защита информации в автоматизированных (информационных) системах	ОК 03	Знать: современные средства и способы обеспечения информационной безопасности; основные методики анализа угроз и рисков информационной безопасности; Уметь:классифицировать основные угрозы безопасности информации;	опрос обучающихся по контрольным вопросам, защита отчетов по практическим заданиям, тестирование
			ОК 06	Знать: место информационной безопасности в системе национальной безопасности страны; Уметь: классифицировать основные угрозы безопасности информации;	
			ОК 09	Знать: сущность и понятие информационной безопасности, характеристику ее составляющих; Уметь: классифицировать основные угрозы безопасности информации;	
			ОК 10	Знать: источники угроз безопасности информации и меры по их предотвращению; современные средства и способы обеспечения информационной безопасности; Уметь: классифицировать основные угрозы безопасности информации;	
			ПК 2.4	Знать: виды, источники и носители защищаемой информации; факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; Уметь: классифицировать защищаемую информацию по видам тайны и степеням секретности; Иметь опыт: обработки, хранения и передачи информации;	

5.2 Типовые контрольные задания или иные материалы

Текущий контроль успеваемости и аттестационные испытания обучающихся могут быть организованы с использованием ресурсов ЭИОС КузГТУ. Полный перечень оценочных материалов расположен в ЭИОС КузГТУ.: https://el.kuzstu.ru/login/index.php.

Текущий контроль успеваемости и аттестационные испытания могут проводиться в письменной и (или) устной, и (или) электронной форме.

5.2.1 Оценочные средства при текущем контроле

Текущий контроль по темам дисциплины заключается в опросе обучающихся по контрольным вопросам, защите отчетов по лабораторным и(или) практическим заданиям, тестировании.

Опрос по контрольным вопросам:

При проведении текущего контроля обучающимся будет письменно, либо устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Методологические подходы к оценке уязвимости информации
2. Понятие атаки

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень контрольных вопросов:

Раздел 1. Теоретические основы информационной безопасности

Тема 1.1. Основные понятия и задачи информационной безопасности

1. Термин "информационная безопасность".
2. Понятие конфиденциальность информации.
3. Понятие целостность информации.
4. Понятие доступность информации.
5. Понятие атаки.
6. Понятие угрозы.
7. Угрозы информационной безопасности.
8. Классификация угроз.
9. Уровни защиты информации
10. Законы РФ в области информационной безопасности

Тема 1.2. Основы защиты информации

1. Концепция информационной безопасности. Основные концептуальные положения системы защиты информации.
2. Понятие системы безопасности. Составляющие системы безопасности.
3. Направления обеспечения информационной безопасности.
4. Понятие правовой защиты информации.
5. Понятие конфиденциальной информации и содержание этого понятия.
6. Формы защиты информации.
7. Перечень собственных нормативно-правовых документов организации, ориентированных на обеспечение информационной безопасности.
8. Понятие организационной защиты информации. Основные организационные мероприятия по защите информации на предприятии (организации).
9. Понятие инженерно-технической защиты информации. Классификация средств инженерно-технической защиты по функциональному назначению.
10. Понятие физических средств защиты информации, назначение, классификация.

Тема 1.3. Угрозы безопасности защищаемой информации.

1. Классификация конфиденциальной информации. Защищаемая информация
2. Системы контроля доступа.
3. Компоненты модели информационной безопасности.
4. Виды угроз конфиденциальной информации.
5. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
6. Протоколирование и аудит как средство и метод защиты информации на предприятии
7. Классификация конфиденциальной информации. Защищаемая информация. Каналы утечки информации. Примеры
8. Классификация угроз информационной безопасности
9. Защита электронного документооборота
10. Защита от несанкционированного доступа
11. Защита информации при работе с Интернетом

Раздел 2. Методология защиты информации

Тема 2.1. Методологические подходы к защите информации

1. Методологические подходы к оценке уязвимости информации.
2. Модель защиты системы с полным перекрытием.
3. Рекомендации по использованию моделей оценки уязвимости информации.

4. Допущения в моделях оценки уязвимости информации.
5. Методы определения требований к защите информации.
6. Требования к защите, обусловливаемые видом защищаемой информации.
7. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
8. Анализ существующих методик определения требований к защите информации.

Тема 2.2. Нормативно правовое регулирование защиты информации

1. Законодательство РФ в области защиты информации (перечень документов и их основные положения)
2. Классификация способов и действий по обеспечению информационной безопасности.
3. Понятие «разглашение конфиденциальной информации», пути и способы разглашения.
4. Меры противодействия разглашению конфиденциальной информации.
5. Требования законодательства к средствам защиты ПД
6. Требования законодательства к ИСПД
7. Лицензирование деятельности по защите персональных данных
8. Контроль в области защиты персональных данных
9. Регуляторы в области защиты персональных данных
10. Проверки Роскомнадзора
11. Проверки ФСБ

Тема 2.3. Защита информации в автоматизированных (информационных) системах

1. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
2. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой автоматизированной обработки информации.
3. Классификация требований к средствам защиты информации.
4. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
5. Требования к защите, обусловливаемые видом защищаемой информации.
6. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.

Отчеты по лабораторным и (или) практическим заданиям(далее вместе - задания):

По каждой работе обучающиеся самостоятельно оформляют отчеты в электронном формате

Содержание отчета:

1.Тема работы.

2. Задачи задания.

4. Краткое описание хода выполнения.

5. Ответы на задания или полученные результаты по окончании выполнения работы (в зависимости от задач, поставленных в п. 2).

6. Выводы

Критерии оценивания:

- 60 – 100 баллов – при раскрытии всех разделов в полном объеме

- 0 – 59 баллов – при раскрытии не всех разделов, либо при оформлении разделов в неполном объеме.

Количество баллов	0–59	60–100
Шкала оценивания	Не зачтено	Зачтено

Процедура защиты отчетов по заданиям:

Оценочными средствами для текущего контроля по защите отчетов являются контрольные вопросы. Обучающимся будет устно задано два вопроса, на которые они должны дать ответы.

Например:

1. Классификация способов и действий по обеспечению информационной безопасности.

2. Требования к защите, обусловливаемые видом защищаемой информации.

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;

- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;

- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;

- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень заданий:

1.Задание к практическому занятию 1.2.1. Определение объектов защиты на типовом объекте информатизации.

1. Составить таблицу в Excel, в которую внести все объекты офиса для информационной защиты.
2. С помощью стандартов ФСТЭК внести для каждого объекта критерии и методы оценки его защищенности.
3. Внести в таблицу виду информационных угроз по каждому объекту.
4. Произвести оценку каждого объекта на предмет оценки риска возникновения угрозы, вероятность угрозы в % указать в таблице для каждого объекта.
5. Указать приоритеты по защите объектов.

Результаты зафиксировать в отчете.

2. Задание к практическому занятию 1.2.2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности

1. Составить таблиц Excel и внести в нее типы информации, с которой работает каждый сотрудник офиса.
2. В строке с каждой позиции указать информация для внутреннего использования или внешнего, а также тип информации (графическая, текстовая, табличная, мультимедийная).
3. Произвести средствами Excel / инструмент Фильтрация группировку (классификацию) внешней информации по видам тайны (стратегическая, ключевая, обеспечивающая, высокопотенциальная) и степени конфиденциальности (руководство, руководство+сотрудники, руководство+стотрудники+партнеры контрагенты), например: кадровые дела сотрудников; список клиентов и контрагентов; уникальные разработки фирмы) и выделить ее цветом.

Результаты зафиксировать в отчете.

3. Задание к практическому занятию 1.3.1. Определение угроз объекта информатизации и их классификация

1. В Excel составить таблицу объектов информатизации (ПК сотрудников, сервера, интернет-шлюзы, шкафы с бухгалтерскими и кадровыми документами, сеть Wi-Fi (если есть), внешние носители информации – USB-внешние диски, флэшки, ноутбуки….
2. Для каждой позиции указать кто имеет доступ к информации и возможные каналы утечки
3. Для каждой позиции указать угрозу и последствия в случае совершения угрозы.
4. Используя соответствующие стандарты и методики оценить степени рисков (вероятность совершения угрозы. в %), в отношении каждого объекта информации, и наиболее подверженные выделить цветом.
5. Средствами Excel произвести сортировку (группировку) или выделить цветом по степени вероятности наступления угрозы.

Результаты зафиксировать в отчете.

4. Задание к практическому занятию 2.2.1. Работа в справочно-правовой системе с нормативными и правовыми документами по информационной безопасности

С помощью СПС Гарант найдите текст и ознакомьтесь с содержанием ФЗ «Об информации, информационных технологиях и защите информации»

Найдите ответы на следующие вопросы:

1) Какие отношения в информационной сфере регулируются ФЗ «Об информации, информационных технологиях и защите информации»

2) На каких принципах основывается регулирование отношений в информационной сфере

3) На какие виды подразделяется информация по категориям доступа:

4) На какие виды подразделяется информация в зависимости от порядка предоставления?

5) Какие права имеет обладатель информации?

6) Каковы обязанности обладателя информации?

7) К какой информации не может быть ограничен доступ?

8) Какие требования по защите информации в информационной системе должны быть обеспечены?

9) Может ли государственный орган отказать гражданину в предоставлении информации, непосредственно затрагивающей его права и свободы?

Результаты зафиксировать в отчете.

5. Задание к практическому занятию 2.3.1. Выбор мер защиты информации для автоматизированного рабочего места

1. В таблице Excel создать паспорт для каждого конкретного АРМ, в котором указать:

ФИО сотрудника
основное ПО
характер информации, используемой в работе с ПО
степень сложности пароля и частота его обновления
наличие дополнительных средств защиты (токены, чипы, пластиковые карты, флэшки)
вид ОС и возможность ее регулярного обновления
канал подключения к офисной сети и Интернету
наличие и тип антивирусной защиты и возможность регулярного обновления, межсетевого экрана
права пользователя (доменные и рабочей группы)
кто кроме основного сотрудника данного АРМ имеет доступ в кабинет, где хранятся ключи
наличие охранной и пожарной сигнализации в кабинете
наличие ИБП для данного АРМ
наличие круглосуточных камер в кабинете.
возможность автоматического архивирования информации АРМ на внешнее хранилище, регулярность (частота архивации)
используется ли внешний носитель информации сотрудником в служебных целях за пределами кабинета АРМ

2. Возле каждой позиции расставить оценку качества защиты по шкале от 0 до 10 (например)

3. Определить угрозы для информации и АРМ в целом и каналы ее совершения, наиболее критические, т.е. с высоким % совершения выделить цветом

4. Для каждой позиции из п.2. указать меры по защите информации и АРМ в целом

5. произвести классификацию мер:

технические,
программные
организационные

6. Результаты оценки и рекомендуемые меры по каждой критической позиции внести в таблицу.

Результаты зафиксировать в отчете.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80…89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0…59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример тестовых заданий:

Раздел 1. Теоретические основы информационной безопасности

Тема 1.1. Основные понятия и задачи информационной безопасности

1. Под информационной безопасностью понимается…

1. защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
2. программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
3. нет правильного ответа

2. Основные составляющие информационной безопасности:

1. целостность
2. достоверность
3. конфиденциальность

3. Доступность – это…

1. возможность за приемлемое время получить требуемую информационную услугу.
2. логическая независимость
3. нет правильного ответа

4. Целостность – это..

1. целостность информации
2. непротиворечивость информации
3. защищенность от разрушения

5. Конфиденциальность – это..

1. защита от несанкционированного доступа к информации
2. программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
3. описание процедур

6. Для чего создаются информационные системы?

1. получения определенных информационных услуг
2. обработки информации
3. все ответы правильные

7. Целостность можно подразделить:

1. статическую
2. динамичную
3. структурную

8. Угроза – это…

1. потенциальная возможность определенным образом нарушить информационную безопасность
2. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
3. процесс определения отвечает на текущее состояние разработки требованиям данного этапа

9. Атака – это…

1. попытка реализации угрозы
2. потенциальная возможность определенным образом нарушить информационную безопасность
3. программы, предназначенные для поиска необходимых программ.

10. Источник угрозы – это..

1. потенциальный злоумышленник
2. злоумышленник
3. нет правильного ответа

11. Окно опасности – это…

1. промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется.
2. комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
3. формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере

Тема 1.2. Основы защиты информации

1. Защита информации – это..

1. комплекс мероприятий, направленных на обеспечение информационной безопасности.

2. процесс разработки структуры базы данных в соответствии с требованиями пользователей
3. небольшая программа для выполнения определенной задачи

2. От чего зависит информационная безопасность?

1. от компьютеров
2. от поддерживающей инфраструктуры
3. от информации

3. Где применяются средства контроля динамической целостности?

1. анализе потока финансовых сообщений
2. обработке данных
3. при выявлении кражи, дублирования отдельных сообщений

4. Какие трудности возникают в информационных системах при конфиденциальности?

1. сведения о технических каналах утечки информации являются закрытыми
2. на пути пользовательской криптографии стоят многочисленные технические проблемы
3. все ответы правильные

5. Какие события должны произойти за время существования окна опасности?

1. должно стать известно о средствах использования пробелов в защите.
2. должны быть выпущены соответствующие заплаты.
3. заплаты должны быть установлены в защищаемой И.С.

Тема 1.3. Угрозы безопасности защищаемой информации.

1. Угрозы можно классифицировать по нескольким критериям:

1. по спектру И.Б.
2. по способу осуществления
3. по компонентам И.С.

2. По каким компонентам классифицируется угрозы доступности:

1. отказ пользователей
2. отказ поддерживающей инфраструктуры
3. ошибка в программе

3. Основными источниками внутренних отказов являются:

1. отступление от установленных правил эксплуатации
2. разрушение данных
3. все ответы правильные

4. Основными источниками внутренних отказов являются:

1. ошибки при конфигурировании системы
2. отказы программного или аппаратного обеспечения
3. выход системы из штатного режима эксплуатации

5. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

1. невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности
2. обрабатывать большой объем программной информации
3. нет правильного ответа

6. Какие существуют грани вредоносного П.О.?

1. вредоносная функция
2. внешнее представление
3. способ распространения

7. По механизму распространения П.О. различают:

1. вирусы
2. черви
3. все ответы правильные

8. Вирус – это…

1. код обладающий способностью к распространению путем внедрения в другие программы
2. способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
3. небольшая программа для выполнения определенной задачи

9. Черви – это…

1. код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения
2. код обладающий способностью к распространению путем внедрения в другие программы
3. программа действий над объектом или его свойствами

10. Конфиденциальную информацию можно разделить:

1. предметную
2. служебную
3. глобальную

11. Природа происхождения угроз:

1. случайные
2. преднамеренные
3. природные

12. Предпосылки появления угроз:

1. объективные
2. субъективные
3. преднамеренные

13. К какому виду угроз относится присвоение чужого права?

1. нарушение права собственности
2. нарушение содержания
3. внешняя среда

14. Отказ, ошибки, сбой – это:

1. случайные угрозы
2. преднамеренные угрозы
3. природные угрозы

15. Отказ - это…

1. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
2. некоторая последовательность действий, необходимых для выполнения конкретного задания
3. структура, определяющая последовательность выполнения и взаимосвязи процессов

16. Ошибка – это…

1. неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния
2. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
3. негативное воздействие на программу

17. Сбой – это…

1. такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
2. неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
3. объект-метод

18. Побочное влияние – это…

1. негативное воздействие на систему в целом или отдельные элементы
2. нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
3. нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

Раздел 2. Методология защиты информации

Тема 2.1. Методологические подходы к защите информации

1. СЗИ (система защиты информации) делится:

1. ресурсы автоматизированных систем
2. организационно-правовое обеспечении
3. человеческий компонент

2. Что относится к человеческому компоненту СЗИ?

1. системные порты
2. администрация
3. программное обеспечение

3. Что относится к ресурсам А.С. СЗИ?

1. лингвистическое обеспечение
2. техническое обеспечение
3. все ответы правильные

4. По уровню обеспеченной защиты все системы делят:

1. сильной защиты
2. особой защиты
3. слабой защиты

5. По активности реагирования СЗИ системы делят:

1. пассивные
2. активные
3. полупассивные

Тема 2.2. Нормативно правовое регулирование защиты информации

1. Правовое обеспечение безопасности информации – это…

1. совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
2. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
3. нет правильного ответа

2. Правовое обеспечение безопасности информации делится:

1. международно-правовые нормы
2. национально-правовые нормы
3. все ответы правильные

3. Информацию с ограниченным доступом делят:

1. государственную тайну
2. конфиденциальную информацию

3. достоверную информацию

4. Что относится к государственной тайне?

1. сведения, защищаемые государством в области военной, экономической … деятельности
2. документированная информация
3. нет правильного ответа

5. Вредоносная программа - это…

1. программа, специально разработанная для нарушения нормального функционирования систем
2. упорядочение абстракций, расположение их по уровням
3. процесс разделения элементов абстракции, которые образуют ее структуру и поведение

6. Основополагающие документы для обеспечения безопасности внутри организации:

1. трудовой договор сотрудников
2. должностные обязанности руководителей
3. коллективный договор

7. К организационно - административному обеспечению информации относится:

1. взаимоотношения исполнителей
2. подбор персонала
3. регламентация производственной деятельности

8. Что относится к организационным мероприятиям:

1. хранение документов
2. проведение тестирования средств защиты информации
3. пропускной режим

9. Какие средства используется на инженерных и технических мероприятиях в защите информации:

1. аппаратные
2. криптографические
3. физические

10. Первый шаг в анализе угроз — это:

1. идентификация угроз;
2. аутентификация угроз;
3. ликвидация угроз.

11. Управление рисками включает в себя следующие виды деятель ности:

1. определение ответственных за анализ рисков;
2. оценка рисков;
3. выбор эффективных защитных средств.

12. Оценка рисков позволяет ответить на следующие вопросы:

1. чем рискует организация, используя информационную систе му?
2. чем рискуют пользователи информационной системы?
3. чем рискуют системные администраторы?

12. В число классов мер процедурного уровня входят:

1. поддержание работоспособности;
2. поддержание физической формы;
3. физическая защита.

13. В число принципов управления персоналом входят:

1. минимизация привилегий;

2. минимизация зарплаты;
3. максимизация зарплаты.

14. В число этапов процесса планирования восстановительных ра бот входят:

1. выявление критически важных функций организации;
2. определение перечня возможных аварий;
3. проведение тестовых аварий.

15. В число направлений повседневной деятельности на процедур ном уровне входят:

1. ситуационное управление;
2. конфигурационное управление;
3. оптимальное управление.

16. Уголовный кодекс РФ не предусматривает наказания за:

1. создание, использование и распространение вредоносных программ;
2. ведение личной корреспонденции на производственной технической базе;
3. нарушение правил эксплуатации информационных систем.

17. Под определение средств защиты информации, данное в Законе «О государственной тайне», подпадают:

1. средства выявления злоумышленной активности;
2. средства обеспечения отказоустойчивости;
3. средства контроля эффективности защиты информации.

18. Уровень безопасности В согласно «Оранжевой книге» характеризуется:

1. произвольным управлением доступом;
2. принудительным управлением доступом;
3. верифицируемой безопасностью.

19. В число классов требований доверия безопасности «Общих критериев» входят:

1. разработка;
2. оценка профиля защиты;
3. сертификация.

20. Согласно «Оранжевой книге» политика безопасности включает в себя следующие элементы:

1. периметр безопасности;
2. метки безопасности;
3. сертификаты безопасности.

21. Согласно рекомендациям X.800 выделяются следующие сервисы безопасности:

1. управление квотами;
2. управление доступом;
3. экранирование.

22. Уровень безопасности А согласно «Оранжевой книге» характеризуется:

1. произвольным управлением доступом;
2. принудительным управлением доступом;
3. верифицируемой безопасностью.

23. Согласно рекомендациям X.800 аутентификация может быть реализована на:

1. сетевом уровне;
2. транспортном уровне;
3. прикладном уровне.

24. В число целей политики безопасности верхнего уровня входят:

1. решение сформировать или пересмотреть комплексную программу безопасности;
2. обеспечение базы для соблюдения законов и правил;
3. обеспечение конфиденциальности почтовых сообщений.

25. В число целей политики безопасности верхнего уровня входят:

1. управление рисками;
2. определение ответственных за информационные сервисы;
3. определение мер наказания за нарушения политики безопасности.

26. В рамках политики безопасности нижнего уровня осуществляются:

1. стратегическое планирование;
2. повседневное администрирование;
3. отслеживание слабых мест защиты.

Тема 2.3. Защита информации в автоматизированных (информационных) системах

1. Программные средства – это…

1. специальные программы и системы защиты информации в информационных системах различного назначения
2. структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
3. модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

2. Криптографические средства – это…

1. средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
2. специальные программы и системы защиты информации в информационных системах различного назначения
3. механизм, позволяющий получить новый класс на основе существующего

3. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

1. меры обеспечения целостности;
2. административные меры;
3. меры обеспечения конфиденциальности.

4. Дублирование сообщений является угрозой:

1. доступности;
2. конфиденциальности;
3. целостности.

5. Вредоносное ПО Melissa подвергает атаке на доступность:

1. системы электронной коммерции;
2. геоинформационные системы;
3. системы электронной почты.

4. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.

1. Melissa.
2. Bubble Boy.
3. ILO VE YOU.

5. Самыми опасными источниками внутренних угроз являются:

1. некомпетентные руководители;
2. обиженные сотрудники;

3. любопытные администраторы.

6. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.

1. просчеты при администрировании информационных систем;
2. необходимость постоянной модификации информационных систем;
3. сложность современных информационных систем.

7. Агрессивное потребление ресурсов является угрозой:

1. доступности
2. конфиденциальности
3. целостности

8. Программа Melissa — это:

1. бомба;
2. вирус;
3. червь.

9. Для внедрения бомб чаще всего используются ошибки типа:

1. отсутствие проверок кодов возврата;
2. переполнение буфера;
3. нарушение целостности транзакций.

10. Окно опасности появляется, когда:

1. становится известно о средствах использования уязвимости;
2. появляется возможность использовать уязвимость;
3. устанавливается новое ПО.

11 .Среди ниже перечисленных отметьте две троянские программы:

1. I LOVE YOU;
2. Back Orifice;
3. Netbus.

12. Политика безопасности строится на основе:

1. общих представлений об ИС организации;
2. изучения политик родственных организаций;
3. анализа рисков.

13. В число целей политики безопасности верхнего уровня входят:

1. формулировка административных решений по важнейшим аспектам реализации программы безопасности;
2. выбор методов аутентификации пользователей;
3. обеспечение базы для соблюдения законов и правил.

14. Риск является функцией:

1. размера возможного ущерба;
2. числа пользователей информационной системы;
3. уставного капитала организации.

15. В число этапов управления рисками входят:

1. идентификация активов;
2. ликвидация пассивов;
3. выборобъектов оценки.

16. Протоколирование и аудит могут использоваться для:

1. предупреждения нарушений И Б;
2. обнаружения нарушений;
3. восстановления режима И Б.

17. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

1. выработка и проведение в жизнь единой политики безопасности;
2. унификация аппаратно-программных платформ;
3. минимизация числа используемых приложений.

18. Экранирование может использоваться для:

1. предупреждения нарушений И Б;
2. обнаружения нарушений;
3. локализации последствий нарушений.

19. В число основных принципов архитектурной безопасности входят:

1. следование признанным стандартам;
2. применение нестандартных решений, не известных злоумышленникам;
3. разнообразие защитных средств.

20. В число основных принципов архитектурной безопасности входят:

1. усиление самого слабого звена;
2. укрепление наиболее вероятного объекта атаки;
3. эшелонированность обороны.

21. Для обеспечения информационной безопасности сетевых конфигураций следует руководствоваться следующими принципами:

1. использование собственных линий связи;
2. обеспечение конфиденциальности и целостности при сетевых взаимодействиях;
3. полный анализ сетевого трафика.

22. В число универсальных сервисов безопасности входят:

1. управление доступом;
2. управление информационными системами и их компонентами;
3. управление носителями.

23. Контроль целостности может использоваться для:

1. предупреждения нарушений И Б;
2. обнаружения нарушений;
3. локализации последствий нарушений.

24. В число универсальных сервисов безопасности входят:

1. средства построения виртуальных локальных сетей;
2. экранирование;
3. протоколирование и аудит.

25. В качестве аутентификатора в сетевой среде могут использоваться:

1. кардиограмма субъекта;
2. номер карточки пенсионного страхования;
3. результат работы генератора одноразовых паролей.

26. Аутентификация на основе пароля, переданного по сети в зашифрованном виде, плоха, потому что не обеспечивает защиты от:

1. перехвата;
2. воспроизведения;
3. атак на доступность.

27. В число основных понятий ролевого управления доступом входит:

1. роль;
2. исполнитель роли;
3. пользователь роли.

28. В качестве аутентификатора в сетевой среде могут использоваться:

1. год рождения субъекта;
2. фамилия субъекта;
3. секретный криптографический ключ.

29. Ролевое управление доступом использует следующее средство объектно-ориентированного подхода:

1. инкапсуляция;
2. наследование;
3. полиморфизм.

30. В число основных понятий ролевого управления доступом входит:

1. объект;
2. субъект;
3. метод.

31. Цифровой сертификат содержит:

1. открытый ключ пользователя;
2. секретный ключ пользователя;
3. имя пользователя.

5.2.2 Оценочные средства при промежуточной аттестации

Формой промежуточной аттестации в четвертом семестре является дифференцированный зачет, в процессе которого определяется сформированность обозначенных в рабочей программе компетенций.

Инструментом измерения сформированности компетенций являются:
- зачтенные отчеты по заданиям,
- ответы на вопросы во время опроса,
- зачтенное компьютерное тестирование.

При проведении промежуточного контроля обучающийся отвечает на 2 вопроса выбранных случайным образом и на 10 тестовых заданий формирующихся случайным образом.

Тестирование может проводиться в письменной и (или) устной, и (или) электронной форме. Банк вопросов на тестирование находится в ЭИОС КузГТУ "Moodle".

Ответ на вопросы:

Критерии оценивания:

- 90–100 баллов – при правильном и полном ответе на два вопроса;
- 80–89 баллов – при правильном и полном ответе на один из вопросов и правильном, но не полном ответе на другой из вопросов;
- 60–79 баллов – при правильном и неполном ответе только на один из вопросов;
- 0–59 баллов – при отсутствии правильных ответов на вопросы.

Количество баллов	0-59	60-79	80-89	90-100
Шкала оценивания	неуд	удовл	хорошо	отлично

Примерный перечень вопросов к зачету:

1. Термин "информационная безопасность".
2. Понятие конфиденциальность информации.

3. Понятие целостность информации.
4. Понятие доступность информации.
5. Понятие атаки.
6. Понятие угрозы.
7. Угрозы информационной безопасности.
8. Классификация угроз.
9. Уровни защиты информации
10. Законы РФ в области информационной безопасности
11. Концепция информационной безопасности. Основные концептуальные положения системы защиты информации.
12. Понятие системы безопасности. Составляющие системы безопасности.
13. Направления обеспечения информационной безопасности.
14. Понятие правовой защиты информации.
15. Понятие конфиденциальной информации и содержание этого понятия.
16. Формы защиты информации.
17. Перечень собственных нормативно-правовых документов организации, ориентированных на обеспечение информационной безопасности.
18. Понятие организационной защиты информации. Основные организационные мероприятия по защите информации на предприятии (организации).
19. Понятие инженерно-технической защиты информации. Классификация средств инженерно-технической защиты по функциональному назначению.
20. Понятие физических средств защиты информации, назначение, классификация.
21. Классификация конфиденциальной информации. Защищаемая информация
22. Системы контроля доступа.
23. Компоненты модели информационной безопасности.
24. Виды угроз конфиденциальной информации.
25. Действия, приводящие к неправомерному овладению конфиденциальной информацией.
26. Протоколирование и аудит как средство и метод защиты информации на предприятии
27. Классификация конфиденциальной информации. Защищаемая информация. Каналы утечки информации. Примеры
28. Классификация угроз информационной безопасности
29. Защита электронного документооборота
30. Защита от несанкционированного доступа
31. Защита информации при работе с Интернетом
32. Методологические подходы к оценке уязвимости информации.
33. Модель защиты системы с полным перекрытием.
34. Рекомендации по использованию моделей оценки уязвимости информации.
35. Допущения в моделях оценки уязвимости информации.
36. Методы определения требований к защите информации.
37. Требования к защите, обусловливаемые видом защищаемой информации.
38. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.
39. Анализ существующих методик определения требований к защите информации.
40. Законодательство РФ в области защиты информации (перечень документов и их основные положения)
41. Классификация способов и действий по обеспечению информационной безопасности.
42. Понятие «разглашение конфиденциальной информации», пути и способы разглашения.
43. Меры противодействия разглашению конфиденциальной информации.
44. Требования законодательства к средствам защиты ПД
45. Требования законодательства к ИСПД
46. Лицензирование деятельности по защите персональных данных
47. Контроль в области защиты персональных данных
48. Регуляторы в области защиты персональных данных
49. Проверки Роскомнадзора
50. Проверки ФСБ
51. Структурированная схема потенциально возможных злоумышленных действий в автоматизированных системах обработки данных.
52. Факторы, обусловливающие конкретные требования к защите, обусловленные спецификой

автоматизированной обработки информации.

53. Классификация требований к средствам защиты информации.
54. Требования к защите, определяемые структурой автоматизированной системы обработки данных.
55. Требования к защите, обусловливаемые видом защищаемой информации.
56. Требования, обусловливаемые взаимодействием пользователя с комплексом средств автоматизации.

Тестирование:

Критерии оценивания при тестировании:

- 90-100 баллов – при правильном и полном ответе на 10 вопроса;
- 80…89 баллов – при правильном ответе на 8-9 вопросов;
- 60…79 баллов – правильном ответе на 5-7 вопросов;
- 0…59 – при правильном ответе только на 4 вопроса;

Количество баллов	0–59	60–79	80–89	90–100
Шкала оценивания	неуд	удовл	хорошо	отлично

Пример вариантов тестовых заданий:

1 вариант

1. СЗИ (система защиты информации) делится:

1. ресурсы автоматизированных систем
2. организационно-правовое обеспечении
3. человеческий компонент

2. Что относится к человеческому компоненту СЗИ?

1. системные порты
2. администрация
3. программное обеспечение

3. Правовое обеспечение безопасности информации – это…

1. совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации
2. система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
3. нет правильного ответа

4. Правовое обеспечение безопасности информации делится:

1. международно-правовые нормы
2. национально-правовые нормы
3. все ответы правильные

5. Информацию с ограниченным доступом делят:

1. государственную тайну
2. конфиденциальную информацию
3. достоверную информацию

6. Агрессивное потребление ресурсов является угрозой:

1. доступности
2. конфиденциальности
3. целостности

7. Программа Melissa — это:

1. бомба;
2. вирус;
3. червь.

8. Для внедрения бомб чаще всего используются ошибки типа:

1. отсутствие проверок кодов возврата;
2. переполнение буфера;
3. нарушение целостности транзакций.

9. Окно опасности появляется, когда:

1. становится известно о средствах использования уязвимости;
2. появляется возможность использовать уязвимость;
3. устанавливается новое ПО.

10 .Среди ниже перечисленных отметьте две троянские программы:

1. I LOVE YOU;
2. Back Orifice;
3. Netbus.

2 вариант

1. Что относится к ресурсам А.С. СЗИ?

1. лингвистическое обеспечение
2. техническое обеспечение
3. все ответы правильные

2. По уровню обеспеченной защиты все системы делят:

1. сильной защиты
2. особой защиты
3. слабой защиты

3. Что относится к государственной тайне?

1. сведения, защищаемые государством в области военной, экономической … деятельности
2. документированная информация
3. нет правильного ответа

4. Вредоносная программа - это…

1. программа, специально разработанная для нарушения нормального функционирования систем
2. упорядочение абстракций, расположение их по уровням
3. процесс разделения элементов абстракции, которые образуют ее структуру и поведение

5. Основополагающие документы для обеспечения безопасности внутри организации:

1. трудовой договор сотрудников
2. должностные обязанности руководителей
3. коллективный договор

6. Вредоносное ПО Melissa подвергает атаке на доступность:

1. системы электронной коммерции;
2. геоинформационные системы;
3. системы электронной почты.

7. Выберите вредоносную программу, которая открыла новый этап в развитии данной области.

1. Melissa.
2. Bubble Boy.
3. ILO VE YOU.

8. Самыми опасными источниками внутренних угроз являются:

1. некомпетентные руководители;
2. обиженные сотрудники;
3. любопытные администраторы.

9. Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности.

1. просчеты при администрировании информационных систем;
2. необходимость постоянной модификации информационных систем;
3. сложность современных информационных систем.

10. Политика безопасности строится на основе:

1. общих представлений об ИС организации;
2. изучения политик родственных организаций;
3. анализа рисков.

3 вариант

1. По уровню обеспеченной защиты все системы делят:

1. сильной защиты
2. особой защиты
3. слабой защиты

2. По активности реагирования СЗИ системы делят:

1. пассивные
2. активные
3. полупассивные

3. К организационно - административному обеспечению информации относится:

1. взаимоотношения исполнителей
2. подбор персонала
3. регламентация производственной деятельности

4. Что относится к организационным мероприятиям:

1. хранение документов
2. проведение тестирования средств защиты информации
3. пропускной режим

5. Какие средства используется на инженерных и технических мероприятиях в защите информации:

1. аппаратные
2. криптографические
3. физические

6. Программные средства – это…

1. специальные программы и системы защиты информации в информационных системах различного назначения
2. структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
3. модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

7. Криптографические средства – это…

1. средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования
2. специальные программы и системы защиты информации в информационных системах различного назначения
3. механизм, позволяющий получить новый класс на основе существующего

8. В число граней, позволяющих структурировать средства достижения информационной безопасности, входят:

1. меры обеспечения целостности;
2. административные меры;
3. меры обеспечения конфиденциальности.

9. Дублирование сообщений является угрозой:

1. доступности;
2. конфиденциальности;
3. целостности.

10. В число целей политики безопасности верхнего уровня входят:

1. формулировка административных решений по важнейшим аспектам реализации программы безопасности;
2. выбор методов аутентификации пользователей;
3. обеспечение базы для соблюдения законов и правил.

5.2.3 Методические материалы, определяющие процедуры оценивания знаний, умений, практического опыта деятельности, характеризующие этапы формирования компетенций

Порядок организации проведения текущего контроля и промежуточной аттестации представлен в Положении о проведении текущего контроля и промежуточной аттестации обучающихся, осваивающих образовательные программы среднего профессионального образования в КузГТУ (Ип 06/-10

6. Иные сведения и (или) материалы

1. Образовательный процесс осуществляется с использованием как традиционных, так и современных интерактивных технологий. При контактной работе педагогического работника с обучающимися применяются следующие элементы интерактивных технологий:

- совместный разбор проблемных ситуаций;

- совместное выявление причинно-следственных связей вещей и событий, происходящих в повседневной жизни, и их сопоставление с учебным материалом.

2. Проведение групповых и индивидуальных консультаций осуществляется в соответствии с расписанием консультаций по темам, заявленным в рабочей программе дисциплины, в период освоения дисциплины и перед промежуточной аттестацией с учетом результатов текущего контроля.