Смоленский колледж телекоммуникаций (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Санкт-Петербургский государственный университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича»

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
СМОЛЕНСК
Сертификат: 48135A51C268D4BC256D8BA4E03EE7DD
Владелец: Казаков Андрей Викторович
Действителен: с 22.07.2024 до 15.10.2025

Утверждаю
Директор СКТ(ф)СПбГУТ
_____ А.В. Казаков
«30» 08 2024 г.

Фонд оценочных средств по дисциплине
ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

общепрофессионального цикла
основной образовательной программы
среднего профессионального образования
по специальности:

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Смоленск
2024

РАССМОТРЕНО
на заседании методической комиссии
Информационной безопасности и сетевого администрирования
Председатель _____ Скряго О.С.
Протокол №_1_
«_30_»_____08_____ 2024 г.

СОГЛАСОВАНО
Начальник отдела сопровождения
ООО «Бирсек»
_____ А.А. Ефремов
«_30_»_____08_____2024 г.

Разработчик: Смоленский колледж телекоммуникаций (филиал) ФГБОУ ВО «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича»
Составитель: Скряго О.С.– преподаватель СКТ (ф) СПбГУТ высшей квалификационной категории.

Фонд оценочных средств разработан на основе Федерального государственного образовательного стандарта (далее ФГОС) по специальности среднего профессионального образования 10.02.04 – Обеспечение информационной безопасности телекоммуникационных систем, утвержденного приказом Минобрнауки России № 1551 от 09.12.2016 г. (ред. от 03.07.2024), рабочей программы ОП.04 Основы информационной безопасности.

2

Содержание

1. Общие положения

1.1. Место дисциплины в структуре основной образовательной программы

Учебная дисциплина ОП.04 Основы информационной безопасности является обязательной частью математического и общего и естественнонаучного учебного цикла образовательной программы в соответствии с ФГОС по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

ФОС разработаны на основании положений:

- Программы подготовки специалистов среднего звена (ППССЗ) по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.
- рабочей программы учебной дисциплины ОП.04 Основы информационной безопасности

ФОС включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме экзамена.

Итогом экзамена является качественная оценка в баллах от 2-х до 5-ти.

1.2 Планируемые результаты освоения дисциплины:

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания:

Код ОК, ПК	Умения		Знания	
ОК 03, ОК 06, ПК 2.3	У-1	Классифицировать защищаемую информацию по видам тайны и степеням секретности;	З-1	Сущность и понятие информационной безопасности, характеристику ее составляющих;
	У- 2	Классифицировать основные угрозы безопасности информации;	З-2	Место информационной безопасности в системе национальной безопасности страны;
			З-3	Виды, источники и носители защищаемой информации;
			З-4	Источники угроз безопасности информации и меры по их предотвращению;
			З-5	Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах;
			З-6	Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи;
			З-7	Современные средства и способы обеспечения информационной безопасности;
			З-8	Основные методики анализа угроз и рисков информационной безопасности.

2. Результаты освоения учебной дисциплины, подлежащие проверке

В результате аттестации по учебной дисциплине ОП.04 Основы информационной безопасности осуществляется комплексная проверка следующих умений и знаний, а также динамика формирования профессиональных и общих компетенций.

Формы контроля обучения:

- устный опрос;
- самостоятельная работа;
- электронное тестирование;
- практические занятия.

Методы оценивания:

- формализованное наблюдение за деятельностью обучающихся на уроке;
- проверка выполнения индивидуальных заданий (практических занятий).

Методы оценивания результативности обучения:

- традиционная система отметок в баллах за каждую выполненную работу;
- формирование результатов итогового контроля по дисциплине на основе итогового тестирования.

КОНКРЕТИЗАЦИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ УД

Специальность 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

ПК 2.3 Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.	
Умения и знания	**Формы оценивания**
Уметь: У1. Классифицировать защищаемую информацию по видам тайны и степеням секретности	Практическое занятие 1.Определение объектов защиты на типовом объекте информатизации. Практическое занятие 2.Классификация защищаемой информации по видам тайны. Практическое занятие 3.Классификация защищаемой информации по степеням конфиденциальности. Практическое занятие 6.Работа в справочно-правовой системе с нормативными документами по информационной безопасности Практическое занятие 7.Работа в справочно-правовой системе с правовыми документами по информационной безопасности
У2. Классифицировать основные угрозы безопасности информации;	Практическое занятие 4.Определение угроз объекта информатизации Практическое занятие 5. Классификация угроз объекта информатизации Практическое занятие 8.Выбор организационно-технических мер защиты информации для автоматизированного рабочего места Практическое занятие 9.Выбор программно-аппаратных мер защиты информации для автоматизированного рабочего места
Знать: З1. Сущность и понятие информационной безопасности, характеристику ее составляющих;	Тема 1.1. Основные понятия и задачи информационной безопасности Тема 1.2. Основы защиты информации
З2. Место информационной безопасности в системе национальной безопасности страны;	Тема 2.1. Методологические подходы к защите информации Тема 2.2. Нормативно правовое регулирование защиты информации

З3. Виды, источники и носители защищаемой информации; З4. Источники угроз безопасности информации и меры по их предотвращению	Тема 1.3. Угрозы безопасности защищаемой информации
З5. Факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; З6. Жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи	Тема 2.3. Защита информации в автоматизированных (информационных) системах Тема 1.2. Основы защиты информации
З7. Современные средства и способы обеспечения информационной безопасности	Тема 1.2. Основы защиты информации Тема 2.3. Защита информации в автоматизированных (информационных) системах
З8. Основные методики анализа угроз и рисков информационной безопасности.	Тема 2.1. Методологические подходы к защите информации

2.1. Перечень общих компетенций.

Формирование ОК в рамках дисциплины проводится постоянно на всех занятиях через применение различных форм и технологий проведения. Формирующее оценивание производится в конце учебного года на основании наблюдений преподавателя за работой студентов.

Таблица 2.1

Результаты (освоенные общие компетенции)	**Основные показатели результатов подготовки**	**Формы и методы контроля и оценки**
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на практических занятиях. Экзамен.
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- умения описывать значимость своей профессии; − презентовать структуру профессиональной деятельности по профессии (специальности). − знания сущности гражданско-патриотической позиции; − знания общечеловеческих ценностей; − знания правил поведения в ходе выполнения профессиональной деятельности.	

3. Оценка освоения теоретического курса дисциплины.

3.1. Формы и методы оценивания.

Предметом оценки служат умения и знания, предусмотренные ФГОС по дисциплине ОП.04 Основы информационной безопасности, направленные на формирование общих и профессиональных компетенций.

Контроль и оценка освоения учебной дисциплины ОП.04 Основы информационной безопасности
по темам (разделам) для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

Таблица 3.1.

Элемент учебной дисциплины	**Формы и методы контроля**					
	Текущий контроль		**Рубежный контроль**		**Промежуточная аттестация**	
	Форма контроля	**Проверяемые У, З, ОК, ПК**	**Форма контроля**	**Проверяемые ОК, У, З**	**Форма контроля**	**Проверяемые ОК, У, З**
Раздел 1. Теоретические основы информационной безопасности			*Не предусмотрено*		Экзамен	З1, З3,З4,З5, З7, У1, У2, ОК03, ОК 06, ПК 2.3
Тема 1.1. Основные понятия и задачи информационной безопасности	Устный опрос	З1, ОК03, ОК 06,ПК 2.3				
Тема 1.2. Основы защиты информации	Практическое занятие 1. Практическое занятие 2. Практическое занятие 3.	З1, З5, З7, У1, ОК03, ОК 06, ПК 2.3				
Тема 1.3. Угрозы безопасности защищаемой информации.	Тестирование Практическое занятие 4. Практическое занятие 5.	З3,З4, У2, ОК03, ОК 06, ПК 2.3				
Раздел 2. Методология защиты информации			*Не предусмотрено*		Экзамен	З5, З6, З7, У1, У2, ОК03, ОК 06, ПК 2.3
Тема 2.1. Методологические подходы к защите информации	Тестирование	З5, З7, ОК03, ОК 06, ПК 2.3				
Тема 2.2. Нормативно правовое регулирование защиты информации	Практическое занятие 6. Практическое занятие 7.	З2, У1, ОК03, ОК 06, ПК 2.3				
Тема 2.3. Защита информации в автоматизированных (информационных) системах	Устный опрос Практическое занятие 8. Практическое занятие 9.	З5,З6, З7, У2, ОК03, ОК 06, ПК 2.3				

3.2. Типовые задания для оценки освоения учебной дисциплины.
В состав ФОС по дисциплине ОП.04 Основы информационной безопасности входят практические занятия, лабораторные занятия, устные опросы, тестовые задания

Раздел 1. Теоретические основы информационной безопасности
Тема 1.1. Основные понятия и задачи информационной безопасности
Проверяемые результаты обучения: *31, ОК03, ОК 06,ПК 2.3*
1.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе устного опроса
Контрольно-оценочные средства с использованием устного опроса по дисциплине ОП.04 Основы информационной безопасности
Инструкция студенту: дайте устные ответы на поставленные вопросы.
Устный опрос.

1. Что называется объектом защиты информации?
2. На какие категории можно разделить объекты защиты информации?
3. Как возможно охарактеризовать понятие «информационная безопасность».

Время, отведенное на устный опрос:
Подготовка *3* мин.;
выполнение 9 мин.;
всего *12* мин.

Критерии оценки:

- Оценка 2 выставляется при отсутствии ответов на вопросы или полностью неправильные ответы.
- Оценка 3 выставляется при неполных и слабо аргументированных ответах и только в том в том случае, если студент обнаруживает понимание существа поставленных вопросов, владеет понятийным аппаратом.
- Оценка 4 выставляется за свободное владение материалом, при полных, правильных и обоснованных ответах на основные и дополнительные вопросы при незначительных упущениях и неточностях.
- Оценка 5 выставляется за свободное владение материалом, при полных, правильных и обоснованных ответах на основные и дополнительные вопросы.

Тема 1.2. Основы защиты информации
Проверяемые результаты обучения: *31, 35, 37, У1, ОК03, ОК 06, ПК 2.3*
1.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.
Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности
Практическое занятие №1. Время выполнения практического занятия №1 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.
Время выполнения задания
Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.
Критерии оценки практического занятия:
«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.
«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.
«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.
«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.
2.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №2. Время выполнения практического занятия №2 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

3.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №3. Время выполнения практического занятия №3 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

Тема 1.3. Угрозы безопасности защищаемой информации.

Проверяемые результаты обучения: *З3,З4, У2, ОК03, ОК 06, ПК 2.3*

1.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе тестирования

Контрольно-оценочные средства с использованием тестирования по дисциплине ОП.04 Основы информационной безопасности

Инструкция студенту: прочитайте текст вопроса и выберите один правильный ответ или ответьте на вопрос.

Тестирование

1) Прочитайте текст вопроса и выберите один правильный ответ.

Какие угрозы называют искусственными угрозами безопасности информации?

1. Угрозы, вызванные деятельностью человека.
2. Угрозы, вызванные воздействиями на автоматизированную систему и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.
3. Угрозы, вызванные чрезвычайной ситуацией.
4. Угрозы, зависящие от деятельности искусственного интеллекта.

2) Прочитайте текст вопроса и выберите один правильный ответ.

Какие угрозы называют естественными угрозами безопасности информации?

1.Угрозы, вызванные деятельностью человека.

2.Угрозы, вызванные воздействия ми физических процессов или стихийных природных явлений, независящих от человека.

3. Угрозы, вызванные воздействиями физических процессов, зависящими от человека.

4. Угрозы, вызванные воздействиями стихийных природных явлений, зависящими от человека.

3) Прочитайте текст и к каждой позиции первого столбца подберите соответствующую позицию из второго столбца.

Установите соответствие между определениями и понятиями.

	Определения		Понятия
1.	Любая информация, которая относится к конкретному человеку, или субъекту персональных данных	А.	Коммерческая тайна.
2.	Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.	Б.	Государственная тайна.
3.	Любые данные, не подлежащие разглашению.	В.	Конфиденциальная информация.
4.	Информация, которую компания не разглашает, чтобы увеличить доходы, избежать неоправданных расходов, сохранить или улучшить своё положение на рынке либо получить любую другую коммерческую выгоду.	Г.	Персональные данные.

4) Прочитайте текст вопроса и выберите один правильный ответ.

Какое свойство информации нарушено, если в результате действий злоумышленников легитимный пользователь не может получить доступ к социальной сети?

1. Доступность.
2. Целостность.
3. Отказоустойчивость.
4. Конфиденциальность.

5) Прочитайте текст и ответьте на вопрос.

Как классифицируются угрозы по аспекту информационной безопасности?

Время, отведенное на тестирование:

Подготовка *4* мин.;

выполнение *11* мин.;

всего *15* мин.

Критерии оценки:

Критерии оценивания

«5» - получают студенты, справившиеся с работой 100-90%;

«4» - ставится в том случае, если верные ответы составляют 89-75% от общего количества;

«3» - соответствует работа, содержащая 74-60 % правильных ответов;

«2» - соответствует работа, содержащая менее 60% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
«отлично»	Студент набрал 5 баллов
«хорошо»	Студент набрал 4 балла
«удовлетворительно»	Студент набрал 3 балла

«неудовлетворительно»	Студент набрал 0-2 балла

2.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №4. Время выполнения практического занятия №4 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

3.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №5. Время выполнения практического занятия №5 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

Раздел 2. Методология защиты информации

Тема 2.1. Методологические подходы к защите информации

Проверяемые результаты обучения: *35,37, ОК03, ОК 06, ПК 2.3*

1.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе тестирования

Контрольно-оценочные средства с использованием тестирования по дисциплине ОП.04 Основы информационной безопасности

Инструкция студенту: почитайте текст вопроса и выберите один правильный ответ или ответьте на вопрос.

Тестирование

1) Прочитайте текст вопроса и выберите один правильный ответ.

Как называется действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц?

1. Уничтожение информации.
2. Распространение информации.
3. Предоставление информации.
4. Конфиденциальность информации.
5. Доступ к информации.

2) Прочитайте текст вопроса и выберите один правильный ответ.

Как называется процесс возможности получения информации и ее использования?

1. Сохранение информации.
2. Распространение информации.
3. Предоставление информации.
4. Конфиденциальность информации.
5. Доступ к информации.

3) Прочитайте текст вопроса и выберите один правильный ответ.

Какие действия относятся к несанкционированному доступу к информации?

1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально.
2. Работа на чужом компьютере без разрешения его владельца.
3. Вход на компьютер с использованием данных другого пользователя.
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей.

4) Прочитайте текст вопроса и выберите один правильный ответ.

Охарактеризуйте окно опасности в рамках информационной безопасности?

1. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.
2. Промежуток времени, за который злоумышленник проводит атаку.
3. Промежуток времени, в течение которого устанавливается новое ПО.
4. Промежуток времени от момента, когда администратор безопасности узнает об угрозе, и до момента, когда департаментом информационной безопасности будет разработано решение.

5) Прочитайте текст вопроса и выберите один правильный ответ.

Как классифицируется информация по доступности?

1. Открытую информацию и государственную тайну.
2. Конфиденциальную информацию и информацию свободного доступа.
3. Информацию с ограниченным доступом и общедоступную информацию.
4. Общую и личную информацию.

Время, отведенное на тестирование:

Подготовка *5* мин.;
выполнение *10* мин.;
всего *15* мин.

Критерии оценки:

Критерии оценивания

«5» - получают студенты, справившиеся с работой 100-90%;
«4» - ставится в том случае, если верные ответы составляют 89-75% от общего количества;
«3» - соответствует работа, содержащая 74-60 % правильных ответов;
«2» - соответствует работа, содержащая менее 60% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
«отлично»	Студент набрал 5 баллов
«хорошо»	Студент набрал 4 балла
«удовлетворительно»	Студент набрал 3 балла
«неудовлетворительно»	Студент набрал 0-2 балла

Тема 2.2. Нормативно правовое регулирование защиты информации

Проверяемые результаты обучения: З2, У1, *ОК03, ОК 06, ПК 2.3*

1.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №6. Время выполнения практического занятия №6 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

2.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №7. Время выполнения практического занятия №7 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

Тема 2.3. Защита информации в автоматизированных (информационных) системах

Проверяемые результаты обучения: З5,З6, З7, У2, *ОК03, ОК 06, ПК 2.3*

1.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе устного опроса

Контрольно-оценочные средства с использованием устного опроса по дисциплине ОП.04 Основы информационной безопасности

Инструкция студенту: дайте устные ответы на поставленные вопросы.

Устный опрос.

1. На сколько групп подразделяются классы защищенности автоматизированных систем?
2. Какой процесс характеризует авторизацию в информационной системе?
3. На какие виды делятся информация, обрабатываемая в информационных системах?

Время, отведенное на устный опрос:

Подготовка 3 мин.;
выполнение 9 мин.;
всего 12 мин.

Критерии оценки:

- Оценка 2 выставляется при отсутствии ответов на вопросы или полностью неправильные ответы.
- Оценка 3 выставляется при неполных и слабо аргументированных ответах и только в том в том случае, если студент обнаруживает понимание существа поставленных вопросов, владеет понятийным аппаратом.
- Оценка 4 выставляется за свободное владение материалом, при полных, правильных и обоснованных ответах на основные и дополнительные вопросы при незначительных упущениях и неточностях.
- Оценка 5 выставляется за свободное владение материалом, при полных, правильных и обоснованных ответах на основные и дополнительные вопросы.

2.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №8. Время выполнения практического занятия №8 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

3.Форма контроля и оценивания - формализованное наблюдение за работой студента в процессе выполнения практического занятия.

Контрольно-оценочные средства с использованием практического занятия по дисциплине ОП.04 Основы информационной безопасности

Практическое занятие №9. Время выполнения практического занятия №9 - 2 академических часа. Методические рекомендации по выполнению практического занятия и оформлению отчета представлены в сборнике практических занятий по дисциплине.

Время выполнения задания

Подготовка 10 мин.;
выполнение 55 мин.;
оформление и сдача 25 мин.;
всего 1 час 30 мин.

Критерии оценки практического занятия:

«5» (отлично): выполнены все задания практического занятия, студент четко и без ошибок ответил на все вопросы домашней подготовки и контрольные вопросы.

«4» (хорошо): выполнены все задания практического занятия; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«3» (удовлетворительно): выполнены все задания практического занятия с замечаниями; студент ответил на все вопросы домашней подготовки и контрольные вопросы с замечаниями.

«2» (не зачтено): студент не выполнил или выполнил неправильно задания практического занятия; студент ответил на контрольные вопросы с ошибками или не ответил вопросы домашней подготовки и на контрольные вопросы.

4. Контрольно-оценочные материалы для промежуточной аттестации по учебной дисциплине

Контрольно-оценочные материалы для промежуточной аттестации по учебной дисциплине ОП.04 Основы информационной безопасности для специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Экзамен является промежуточной формой контроля, подводит итог освоения дисциплины ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

В результате освоения дисциплины студент должен освоить следующие общие компетенции:

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ПК 2.3 Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.

Экзамен по дисциплине ОП.04 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ проводится в форме тестирования.

Тест содержит 20 вопросов (суммарно тестовых позиций и теоретических вопросов с кратким ответом), выбираемых случайным образом программой из каждого блоков (состоящих первый блок 25 вопросов, второй блок 30 вопросов) заданий по 10 вопросов. Время тестирования – 50 минут для каждой подгруппы (по 2 минуты на каждый вопрос из первого блока, по 3 минуты на каждый вопрос второго блока). Для прохождения тестирования, студенты разбиваются на подгруппы (по количеству персональных компьютеров в сдаваемой аудитории). Время на подготовку и проверку тестирования – 30 мин.

Критерии оценивания

«5» - получают студенты, справившиеся с работой 100-90%;
«4» - ставится в том случае, если верные ответы составляют 89-80% от общего количества;
«3» - соответствует работа, содержащая 60-79% правильных ответов;
«2» - соответствует работа, содержащая менее 60% правильных ответов.

Шкала оценивания образовательных результатов:

Оценка	Критерии
«отлично»	Студент набрал 5 баллов
«хорошо»	Студент набрал 4 балла
«удовлетворительно»	Студент набрал 3 балла
«неудовлетворительно»	Студент набрал 0-2 балла

Первый блок заданий

Формируемые ОК 03, ОК 06, ПК 2.3

1) Прочитайте текст вопроса и выберите один правильный ответ.

Что называется объектом защиты информации?

1. Информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.
2. Информационный процесс, которые необходимо защищать в соответствии с законом РФ.
3. Носитель информации, которого необходимо защищать.
4. Информация, которую необходимо защищать на уровни организации.

2) Прочитайте текст вопроса и выберите один правильный ответ.

На какие категории можно разделить объекты защиты информации?

1. Информация, ресурсные объекты, физические объекты, пользовательские объекты.
2. Ресурсные объекты, физические объекты, пользовательские объекты.

3. Информация, ресурсные объекты, пользовательские объекты.
4. Информация, ресурсные объекты.

3) Прочитайте текст вопроса и выберите один правильный ответ.

Что такое доступ к информации?

1. Возможность получения информации.
2. Возможность изменения информации и ее передачи.
3. Возможность передачи информации третьему лицу.
4. Возможность получения информации и ее использования.

4) Прочитайте текст вопроса и выберите один правильный ответ.

На какие виды делятся информация, обрабатываемая в информационных системах?

1. Открытую (общедоступную) информацию.
2. Информацию ограниченного доступа (персональные данные).
3. Закрытую информацию.
4. Информация без доступа.

5) Прочитайте текст вопроса и выберите один правильный ответ.

Сколько категорий персональных данных обрабатывается в типовых информационных системах?

1. Одна категория.
2. Две категории.
3. Три категории.
4. Четыре категории.

6) Прочитайте текст вопроса и выберите один правильный ответ.

Что относится к конфиденциальной информации?

1. Государственная тайна.
2. Законодательные акты.
3. "Ноу-хау".
4. Сведения о золотом запасе страны.

7) Прочитайте текст вопроса и выберите один правильный ответ.

Каким Законом определяется система защиты государственных секретов?

1. "Об информации, информатизации и защите информации".
2. "Об органах ФСБ".
3. "О государственной тайне".
4. "О безопасности".

8) Прочитайте текст вопроса и выберите один правильный ответ.

Что такое угроза информационной безопасности?

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.
4. Атака на информацию.

9) Прочитайте текст вопроса и выберите один правильный ответ.

Что является защитой информации?

1. Комплекс мероприятий, направленных на обеспечение информационной безопасности.
2. Процесс разработки структуры защищенной базы данных в соответствии с требованиями пользователей.
3. Небольшая программа для выполнения определенной задачи защиты информации.
4. Процесс разработки документов об информационной защите.

10) Прочитайте текст и к каждой позиции первого столбца подберите соответствующую позицию из второго столбца.

Установите соответствие между определениями и понятиями.

Определения	Понятия
1. Процесс идентификации пользователя или устройства, позволяющий установить его подлинность и право доступа к определённым ресурсам или функционалу системы	А. Авторизация.
2. Процесс определения личности или объекта в системе.	Б. Аутентификация.

3.	Предоставление определённому лицу или группе лиц прав на выполнение определённых действий, а также процесс проверки (подтверждения) этих прав при попытке выполнения этих действий.	В.	Идентификация.
4.	Условное слово или произвольный набор знаков, состоящий из букв, цифр и других символов, предназначенный для подтверждения личности или полномочий.	Г.	Пароль.

11) Прочитайте текст вопроса и выберите один правильный ответ.

Как называется действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц?

1. Уничтожение информации.
2. Распространение информации.
3. Предоставление информации.
4. Конфиденциальность информации.
5. Доступ к информации.

12) Прочитайте текст вопроса и выберите один правильный ответ.

Как называется процесс возможности получения информации и ее использования?

1. Сохранение информации.
2. Распространение информации.
3. Предоставление информации.
4. Конфиденциальность информации.
5. Доступ к информации.

13) Прочитайте текст вопроса и выберите один правильный ответ.

Какие действия относятся к несанкционированному доступу к информации?

1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально.
2. Работа на чужом компьютере без разрешения его владельца.
3. Вход на компьютер с использованием данных другого пользователя.
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей.

14) Прочитайте текст вопроса и выберите один правильный ответ.

Охарактеризуйте окно опасности в рамках информационной безопасности?

1. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется.
2. Промежуток времени, за который злоумышленник проводит атаку.
3. Промежуток времени, в течение которого устанавливается новое ПО.
4. Промежуток времени от момента, когда администратор безопасности узнает об угрозе, и до момента, когда департаментом информационной безопасности будет разработано решение.

15) Прочитайте текст вопроса и выберите один правильный ответ.

Как классифицируется информация по доступности?

1. Открытую информацию и государственную тайну.
2. Конфиденциальную информацию и информацию свободного доступа.
3. Информацию с ограниченным доступом и общедоступную информацию.
4. Общую и личную информацию.

16) Прочитайте текст вопроса и выберите два правильных ответа.

На какие виды подразделяются источники угроз информационной безопасности Российской Федерации?

1. Внешние.
2. Основные.
3. Внутренние.
4. Личные.

17) Прочитайте текст вопроса и выберите один правильный ответ.

Охарактеризуйте понятие «информационная безопасность».

1.Состояние защищѐнности информационной среды.
2.Сохранность информационных ресурсов.
3. Защита конфиденциальности, целостности и доступности информации.

4. Защита доступа.

18) Прочитайте текст вопроса и выберите три правильных ответа.

Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?

1. Доступность.
2. Целостность.
3. Конфиденциальность.
4. Управляемость.
5. Надежность.

19) Прочитайте текст вопроса и выберите один правильный ответ.

Какие угрозы называют искусственными угрозами безопасности информации?

1. Угрозы, вызванные деятельностью человека.
2. Угрозы, вызванные воздействиями на автоматизированную систему и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека.
3. Угрозы, вызванные чрезвычайной ситуацией.
4. Угрозы, зависящие от деятельности искусственного интеллекта.

20) Прочитайте текст вопроса и выберите один правильный ответ.

Какие угрозы называют естественными угрозами безопасности информации?

1. Угрозы, вызванные деятельностью человека.
2. Угрозы, вызванные воздействия ми физических процессов или стихийных природных явлений, независящих от человека.
3. Угрозы, вызванные воздействиями физических процессов, зависящими от человека.
4. Угрозы, вызванные воздействиями стихийных природных явлений, зависящими от человека.

21) Прочитайте текст и к каждой позиции первого столбца подберите соответствующую позицию из второго столбца.

Установите соответствие между определениями и понятиями.

	Определения		Понятия
1.	Любая информация, которая относится к конкретному человеку, или субъекту персональных данных	А.	Коммерческая тайна.
2.	Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.	Б.	Государственная тайна.
3.	Любые данные, не подлежащие разглашению.	В.	Конфиденциальная информация.
4.	Информация, которую компания не разглашает, чтобы увеличить доходы, избежать неоправданных расходов, сохранить или улучшить своё положение на рынке либо получить любую другую коммерческую выгоду.	Г.	Персональные данные.

22) Прочитайте текст вопроса и выберите один правильный ответ.

Какое свойство информации нарушено, если в результате действий злоумышленников легитимный пользователь не может получить доступ к социальной сети?

1. Доступность.
2. Целостность.
3. Отказоустойчивость.
4. Конфиденциальность.

23) Прочитайте текст вопроса и выберите один правильный ответ.

Какой процесс характеризует авторизацию в информационной системе?

1. Процесс предоставления легальным пользователем дифференцированных прав доступа к ресурсам системы.

2. Процесс предоставления всем пользователем прав доступа к ресурсам системы.

3. Процесс проверки подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы.

4. Процесс проверки подлинности пользователя.

24) Прочитайте текст вопроса и выберите один правильный ответ.

К какому виду меры по обеспечению безопасности является процесс установки аппаратного межсетевого экрана?

1.Техническим мерам обеспечения безопасности.

2.Морально-этическим мерам обеспечения безопасности.

3.Физическим мерам обеспечения безопасности.

4.Организационным мерам обеспечения безопасности.

25) Прочитайте текст вопроса и выберите один правильный ответ.

На какой срок выдается лицензия на техническую защиту конфиденциальной информации?

1. 1 год.
2. 5 лет.
3. 3 года.
4. Бессрочно.

Второй блок заданий

Формируемые ОК03, ОК 06, ПК2.3

1) Прочитайте текст и ответьте на вопрос.

Как называется информация, которую предприниматель относит к конфиденциальной и использует ее для получение прибыли?

2) Прочитайте текст и ответьте на вопрос.

Как называется документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности?

3) Прочитайте текст и ответьте на вопрос.

Как называется юридическое лицо или индивидуальный предприниматель, имеющие лицензию на осуществление конкретного вида деятельности?

4) Прочитайте текст и ответьте на вопрос.

Какой участник системы сертификации создает системы сертификации в целом?

5) Прочитайте текст и ответьте на вопрос.

Какой участник системы сертификации проводит сертификационные испытания средств защиты информации и по их результатам оформляют заключения и протоколы?

6) Прочитайте текст и ответьте на вопрос.

На какие два класса делятся угрозы по степени мотивации?

7) Прочитайте текст и ответьте на вопрос.

Что такое риск информационной безопасности?

8) Прочитайте текст и ответьте на вопрос.

На какой срок выдается аттестат соответствия объекта информатизации требованиям безопасности информации?

9) Прочитайте текст и ответьте на вопрос.

На сколько групп подразделяются классы защищенности автоматизированных систем?

10) Прочитайте текст и ответьте на вопрос.

Что такое атака в рамках информационной безопасности?

11) Прочитайте текст и ответьте на вопрос.

Какие Вы знаете каналы утечки информации?

12) Прочитайте текст и ответьте на вопрос.

Что такое государственная тайна?

13) Прочитайте текст и ответьте на вопрос.

Что такое профессиональная тайна?

14) Прочитайте текст и ответьте на вопрос.
Что такое целостность информации?
15) Прочитайте текст и ответьте на вопрос.
Что такое коммерческая тайна?
16) Прочитайте текст и ответьте на вопрос.
Что такое доступность информации?
17) Прочитайте текст и ответьте на вопрос.
Что такое конфиденциальность информации?
18) Прочитайте текст и ответьте на вопрос.
Кто является субъектом персональных данных?
19) Прочитайте текст и ответьте на вопрос.
Кто является оператором персональных данных?
20) Прочитайте текст и ответьте на вопрос.
Что такое лицензирование в области защиты информации?
21) Прочитайте текст и ответьте на вопрос.
Как классифицируются угрозы по аспекту информационной безопасности?
22) Прочитайте текст и ответьте на вопрос.
Что такое канал утечки информации?
23) Прочитайте текст и ответьте на вопрос.
Что такое источник преднамеренных воздействий?
24) Прочитайте текст и ответьте на вопрос.
Что такое утечка информации?
25) Прочитайте текст и ответьте на вопрос.
Что такое разглашение информации?
26) Прочитайте текст и ответьте на вопрос.
Что такое утечка по техническим каналам?
27) Прочитайте текст и ответьте на вопрос.
Что такое информационная безопасность?
28) Прочитайте текст и ответьте на вопрос.
Что собой представляет технический канал утечки информации?
29) Прочитайте текст и ответьте на вопрос.
Носителем, какой информации являются акустические колебания?
30) Прочитайте текст и ответьте на вопрос.
Какие виды пропусков существуют?