Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Самарский государственный экономический университет»

Факультет среднего профессионального и предпрофессионального образования

Кафедра факультета среднего профессионального и предпрофессионального образования

Утверждено
Ученым советом университета
(протокол №11 от 30 мая 2023г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины ОП.16 Кибербезопасность

Специальность 09.02.07 Информационные системы и программирование

Квалификация (степень) выпускника специалист по информационным системам

Самара 2023

СОДЕРЖАНИЕ

1. Общая характеристика рабочей программы дисциплины «Кибербезопасность»

1.1. Место дисциплины в структуре основной образовательной программы:

Дисциплина ОП.17 «Кибербезопасность» является обязательной частью общепрофессионального цикла основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 09.02.07 «Информационные системы и программирование».

Дисциплина ОП.17 «Кибербезопасность» обеспечивает формирование общих компетенций в соответствии с ФГОС по специальности СПО 09.02.07 «Информационные системы и программирование».

Особое значение дисциплина имеет при формировании и развитии

ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7

Код	**Наименование общих компетенций**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

Перечень профессиональных компетенций:

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 5	***Проектирование и разработка информационных систем***
ПК 5.1	Собирать исходные данные для разработки проектной документации на информационную систему.
ПК 5.2	Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.
ПК 5.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.
ПК 5.4	Производить разработку модулей информационной системы в соответствии с техническим заданием.
ПК 5.5	Осуществлять тестирование информационной системы на этапе опытной эксплуатации с фиксацией выявленных ошибок кодирования в разрабатываемых модулях информационной системы.
ПК 5.6	Разрабатывать техническую документацию на эксплуатацию информационной системы.
ПК 5.7	Производить оценку информационной системы для выявления возможности ее модернизации.

1.2. Планируемые результаты освоения дисциплины:
В результате изучения дисциплины обучающийся должен:

уметь	– применять законы и другие нормативно-правовые акты в сфере информационной безопасности; – выявлять угрозы конфиденциальности, целостности, доступности информации; – принимать решения по обеспечению информационной безопасности.
знать:	– средства и методы предотвращения и обнаружения вторжений; – технические каналы утечки информации; – возможности технических средств перехвата информации; – способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – действующее законодательство РФ в информационной сфере; – государственную политику в сфере обеспечения информационной безопасности.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов**
Объем образовательной программы учебной дисциплины	**72**
в том числе:	
теоретическое обучение	**32**
практические занятия	**26**
лабораторные занятия	**-**
курсовая работа (проект) *(не предусмотрено*)	
Самостоятельная работа	**14**
Промежуточная аттестация	**Дифференцированный зачет**

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся	Объем в часах
1	*2*	*3*
Раздел 1. Основные положения теории информационной безопасности		**10**
Тема 1.1. Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**6**
	Теоретическое обучение. Стандарты в области кибербезопасности. Международные стандарты информационного обмена. Понятие угрозы, атаки. Глобальные сети и информационная безопасность. Понятие нарушителя кибербезопасности. Хакеры. Виды хакеров. Примеры хакерских атак. Вирусы как класс вредоносного программного обеспечения. Виды вирусов и их классификация.	4
	В том числе практических занятий	**2**
	Практическое занятие. Работа в справочно-правовой системе с нормативными и правовыми документами по кибербезопасности	2
Тема 1.2. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	**Содержание учебного материала**	**4**
	Теоретическое обучение. Понятие государственной, коммерческой, личной тайны. Основные нормативные документы в этой области. Рассекречивание документов. Уровень тайны. Схема построения кибербезопасности на уровне государства. Назначение и задачи в сфере обеспечения безопасности. Специальные отделы и их функции в процессе обеспечения кибербезопасности государства. Военные подразделения в сфере кибербезопасности.	4
Раздел 2. Угрозы кибербезопасности		**18**
Тема 2.1. Классификация нарушений кибербезопасности вычислительной	**Содержание учебного материала**	**8**
	Теоретическое обучение. Понятие нарушения безопасности. Причины нарушения кибербезопасности. Аудит событий в рамках информационной системы. Уязвимости. Методы оценки уязвимости информации.	4
	В том числе практических занятий	**4**

системы и причины, обуславливающие их существование	**Практическое занятие.** Определение угроз объекта информатизации и их классификация.	4
Тема 2.2. Анализ способов нарушений кибербезопасности	**Содержание учебного материала**	**10**
	Теоретическое обучение. Анализ различных способов нарушений кибербезопасности. Хакерские атаки, отказы оборудования в обслуживании, внешние факторы, влияющие прямо на информационную безопасность систем. Каналы и методы несанкционированного доступа к информации.	4
	В том числе практических занятий	**6**
	Практическое занятие. Выполнение индивидуального задания по теме: «Способы нарушений кибербезопасности»	6
Раздел 3. Организационные и технические меры по обеспечению защиты информации		**30**
Тема 3.1. Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**	**8**
	Теоретическое обучение. Основные механизмы защиты информации. Система защиты информации. Меры защиты информации, реализуемые в автоматизированных (информационных) системах. Программные и программно-аппаратные средства защиты информации. Инженерная защита и техническая охрана объектов информатизации. Организационно-распорядительная защита информации. Работа с кадрами и внутриобъектовый режим. Принципы построения организационно-распорядительной системы.	4
	В том числе практических занятий	**4**
	Практическое занятие. Выбор мер защиты информации для автоматизированного рабочего места.	4
Тема 3.2. Методы криптографии	**Содержание учебного материала**	**10**
	Теоретическое обучение. Криптография, Криптоанализ. Основные понятия криптологии. История шифрования. Использование шифрования различными методами. Рассмотрение сокрытия информации таблицей Винжера. Программы для криптографии. Электронная подпись.	4
	В том числе практических занятий	**6**
	Практическое занятие. Выбор мер защиты информации для автоматизированного рабочего места.	6

Тема 3.3. Основные технологии построения защищенных систем	**Содержание учебного материала**	**8**
	Теоретическое обучение. Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.	4
	В том числе практических занятий	**4**
	практическое занятие. Проектирование системы безопасности автоматизированной информационной системы с описанием возможных угроз и оценкой вероятности их возникновения	4
Тема 3.4. Место кибербезопасности экономических систем в национальной безопасности страны	**Содержание учебного материала**	**4**
	Теоретическое обучение. Информационная безопасность страны. Защита экономических систем. Обмен конфиденциальной информацией. Структура банковских информационных систем в области защиты информации. Важность защиты экономических систем. Электронные деньги и безопасность финансовых переводов. Концепция кибербезопасности. Основные сведения и положения.	4
Тематика самостоятельной учебной работы 1. Работа с конспектами, учебной и специальной литературой; 2. Доработка разрабатываемых проектов; 3. Подготовка отчетов по практическим занятиям; 4. Написание рефератов и докладов.		**14**
Курсовой проект (работа) ***(не предусмотрена)***		
Самостоятельная учебная работа обучающегося над курсовым проектом (работой) ***(не предусмотрена)***		
Консультация		-
Промежуточная аттестация (Дифференцированный зачет)		**Дифференцированный зачет**
Всего		**72**

3. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ В ОТНОШЕНИИ ЛИЦ ИЗ ЧИСЛА ИНВАЛИДОВ И ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Обучающиеся с ограниченными возможностями здоровья, в отличие от остальных обучающихся, имеют свои специфические особенности восприятия, переработки материала.

Подбор и разработка учебных материалов должны производится с учетом того, чтобы предоставлять этот материал в различных формах так, чтобы инвалиды с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально (например, с использованием программ-синтезаторов речи) или с помощью тифлоинформационных устройств.

Выбор средств и методов обучения осуществляется самим преподавателям. При этом в образовательном процессе рекомендуется использование социально-активных и рефлексивных методов обучения, технологий социокультурной реабилитации с целью оказания помощи в установлении полноценных межличностных отношений с другими обучающимися, создании комфортного психологического климата в студенческой группе.

Согласно требованиям, установленным Минобрнауки России к порядку реализации образовательной деятельности в отношении инвалидов и лиц с ограниченными возможностями здоровья, необходимо иметь в виду, что:

1) инвалиды и лица с ограниченными возможностями здоровья по зрению имеют право присутствовать на занятиях вместе с ассистентом, оказывающим обучающемуся необходимую помощь.

2) инвалиды и лица с ограниченными возможностями здоровья по слуху имеют право на использование звукоусиливающей аппаратуры.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для инвалидов в одной аудитории совместно с обучающимися, не являющимися инвалидами, если это не создает трудностей для инвалидов и иных обучающихся при прохождении государственной итоговой аттестации;

- присутствие в аудитории ассистента (ассистентов), оказывающего обучающимся инвалидам необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочитать и оформить задание, общаться с экзаменатором);

- пользование необходимыми обучающимся инвалидам техническими средствами при прохождении аттестации с учетом их индивидуальных особенностей;

- обеспечение возможности беспрепятственного доступа обучающихся инвалидов в аудитории, туалетные и другие помещения, а также их пребывания в указанных помещениях.

По письменному заявлению обучающегося инвалида продолжительность сдачи обучающимся инвалидом экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут;

В зависимости от индивидуальных особенностей обучающихся с ограниченными возможностями здоровья организация обеспечивает выполнение следующих требований при проведении аттестации:

а) для слепых:

- задания и иные материалы для сдачи экзамена оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом;

- письменные задания выполняются обучающимися на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых, либо надиктовываются ассистенту;

- при необходимости обучающимся предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

б) для слабовидящих:

- задания и иные материалы для сдачи экзамена оформляются увеличенным шрифтом;

- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

в) для глухих и слабослышащих, с тяжелыми нарушениями речи:

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования;

- по их желанию испытания проводятся в письменной форме;

г) для лиц с нарушениями опорно-двигательного аппарата (тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются обучающимися на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по их желанию испытания проводятся в устной форме.

О необходимости обеспечения специальных условий для проведения аттестации обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).

4. ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

При планировании самостоятельной внеаудиторной работы обучающимся могут быть рекомендованы следующие виды заданий:

– для овладения знаниями: чтение текста (учебника, первоисточника, дополнительной литературы); составление плана текста; графическое изображение структуры текста; конспектирование текста; выписки из текста; работа со словарями и справочниками; ознакомление с нормативными документами; учебно-исследовательская работа; использование аудио- и видеозаписей, компьютерной техники и Интернета и др.;

– для закрепления и систематизации знаний: работа с конспектом лекций (обработка текста); повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио- и видеозаписей); составление плана и тезисов ответа; составление таблиц для систематизации учебного материала; изучение нормативных материалов; ответы на контрольные вопросы; аналитическая обработка текста (аннотирование, рецензирование, реферирование и др.); подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов; составление библиографии, тематических кроссвордов; тестирование и др.;

– для формирования умений: решение задач и упражнений по образцу; решение вариантных задач и упражнений; выполнение чертежей, схем; выполнение расчётно-графических работ; решение ситуационных производственных (профессиональных) задач; подготовка к деловым играм; проектирование и моделирование разных видов и компонентов профессиональной деятельности; подготовка курсовых и дипломных работ (проектов); экспериментально-конструкторская работа; опытно-экспериментальная работа; упражнения на тренажёре; упражнения спортивно-оздоровительного характера; рефлексивный анализ профессиональных умений с использованием аудио- и видеотехники и др.

Наиболее распространенными формами самостоятельной работы являются подготовка докладов и рефератов.

4.1. Вопросы для самостоятельной работы

Наименование разделов и тем дисциплины/ Самостоятельная работа обучающихся	Формируемые компетенции
1	**2**
Раздел 1. Основные положения теории кибербезопасности	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7
Раздел 2. Угрозы кибербезопасности	
Раздел 3. Организационные и технические меры по обеспечению защиты информации	
Подготовка доклада, доклада, презентации; домашние задания, подготовка к опросу. Изучение материала к деловым играм и т.д	

4.2. Примерная тематика докладов/рефератов

1. Угрозы кибербезопасности предприятия (организации) и способы борьбы с ними
2. Современные средства защиты информации
3. Современные системы компьютерной безопасности
4. Современные средства противодействия экономическому шпионажу
5. Современные криптографические системы
6. Криптоанализ, современное состояние
7. Правовые основы защиты информации
8. Технические аспекты обеспечения защиты информации
9. Атаки на систему безопасности и современные методы защиты
10. Современные пути решения проблемы кибербезопасности РФ

5. ЗАДАНИЯ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

По дисциплине предусмотрены практические занятия с использованием активных и интерактивных форм проведения занятий (разбора конкретных ситуаций, групповых дискуссий) в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся.

Наименование разделов и тем дисциплины/практические занятия	Формируемые компетенции
1	*2*
Раздел 1. Основные положения теории кибербезопасности	
Тема 1.1.	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7
Основные понятия и задачи кибербезопасности	
Раздел 2. Угрозы кибербезопасности	
Тема 2.1.	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7
Классификация нарушений кибербезопасности вычислительной системы и причины, обуславливающие их существование	
Тема 2.2.	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7
Анализ способов нарушений кибербезопасности	
Раздел 3. Организационные и технические меры по обеспечению защиты информации	
Тема 3.1.	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1

Защита информации в автоматизированных (информационных) системах	ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7
Тема 3.2. Методы криптографии	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7
Тема 3.3. Основные технологии построения защищенных систем	ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7

6. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

6.1. Для реализации программы дисциплины предусмотрены лаборатория инструментальных средств разработки, учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная набором демонстрационного оборудования и учебно-наглядными пособиями; учебная аудитория для текущего контроля и промежуточной аттестации, оснащенная набором демонстрационного оборудования и учебно-наглядными пособиями; библиотека, читальный зал с выходом в интернет; помещение для хранения и профилактического обслуживания учебного оборудования; актовый зал; помещение для самостоятельной работы, оснащенные в соответствии с ОПОП по специальности 09.02.07 «Информационные системы и программирование»

6.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд Университета имеет электронные образовательные и информационные ресурсы, рекомендуемых для использования в образовательном процессе.

6.2.1. Электронные издания

1. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518006

6.2.2. Электронные ресурсы

1. Научная электронная библиотека eLIBRARY.RU [Электронный ресурс]. - Режим доступа: https://elibrary.ru/
2. Платформа «Библиокомлектатор» [Электронный ресурс]. - Режим доступа: http://www.bibliocomplectator.ru/
3. Справочно-правовая система «Консультант Плюс» [Электронный ресурс]. - Режим доступа: http://konsultant.ru/
4. Единое окно доступа к образовательным ресурсам: портал [Электронный ресурс].- Режим доступа: http://window.edy.ru./

6.2.3. Дополнительные источники

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN

978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512861

6.3. Обязательное программное обеспечение

1. Microsoft Windows 10 Education / Microsoft Windows 7 / Windows Vista Business
2. Office 365 ProPlus, Microsoft Office 2019, Microsoft Office 2016 Professional Plus (Word, Excel, Access, PowerPoint, Outlook, OneNote, Publisher) / Microsoft Office 2007 (Word, Excel, Access, PowerPoint)
3. Linux Ubuntu / Debian
4. Kali Linux
5. VirtualBox

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ ОП.17 «Кибербезопасность»

7.1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ

Фонд оценочных средств предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП.16 «Кибербезопасность» по специальности СПО 09.02.07 «Информационные системы и программирование».

Фонд оценочных средств разработан в соответствии с требованиями ФГОС СПО 09.02.07 «Информационные системы и программирование» и рабочей программой дисциплины ОП.16 «Кибербезопасность».

В результате освоения дисциплины обучающийся должен:

- освоить общие компетенции:

Код	**Наименование общих компетенций**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях.

Перечень профессиональных компетенций:

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 5	***Проектирование и разработка информационных систем***
ПК 5.1	Собирать исходные данные для разработки проектной документации на информационную систему.
ПК 5.2	Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.
ПК 5.3	Разрабатывать подсистемы безопасности информационной системы в соответствии с техническим заданием.
ПК 5.4	Производить разработку модулей информационной системы в соответствии с техническим заданием.
ПК 5.5	Осуществлять тестирование информационной системы на этапе опытной эксплуатации с фиксацией выявленных ошибок кодирования в разрабатываемых модулях информационной системы.
ПК 5.6	Разрабатывать техническую документацию на эксплуатацию информационной системы.
ПК 5.7	Производить оценку информационной системы для выявления возможности ее модернизации.

- получить умения и знания:

уметь	– применять законы и другие нормативно-правовые акты в сфере кибербезопасности; – выявлять угрозы конфиденциальности, целостности, доступности информации; – принимать решения по обеспечению кибербезопасности.
знать:	– средства и методы предотвращения и обнаружения вторжений; – технические каналы утечки информации; – возможности технических средств перехвата информации; – способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – действующее законодательство РФ в информационной сфере; – государственную политику в сфере обеспечения кибербезопасности.

7.2. ПЕРЕЧЕНЬ КОНТРОЛИРУЮЩИХ МЕРОПРИЯТИЙ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Перечень контролирующих мероприятий для проведения текущего контроля по дисциплине ОП.17 «Кибербезопасность»:

Номер семестра	**Текущий контроль**				
	Тестирование	**Опрос**	**Практические задания**	**Реферат/ доклад**	**Формирование портфолио**
3	-	+	+	+	

Перечень контролирующих мероприятий для проведения промежуточной аттестации по дисциплине ОП.17 «Кибербезопасность»:

Номер семестра	**Промежуточная аттестация**			
	Курсовая работа	**Промежуточное тестирование**	**Диф. зачет**	**Экзамен**
3			+	

7.3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Результаты обучения	***Критерии оценки***	***Методы оценки***
Уметь – применять законы и другие нормативно-правовые акты в сфере кибербезопасности; – выявлять угрозы конфиденциальности, целостности, доступности информации; – принимать решения по обеспечению кибербезопасности.	- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; - применять основные правила и документы по кибербезопасности	Экспертная оценка практических и лабораторных работ, умения применять на практике изученный теоретический материал
Знать – средства и методы предотвращения и обнаружения вторжений; – технические каналы утечки информации; – возможности технических средств перехвата информации; – способы и средства защиты информации от утечки по техническим каналам и контроля эффективности защиты информации; – действующее законодательство РФ в информационной сфере; – государственную политику в сфере обеспечения кибербезопасности.	- сущность и понятие кибербезопасности, характеристика её составляющих; - место кибербезопасности в системе национальной безопасности страны; - источники угроз кибербезопасности и меры по их предотвращению; - жизненные циклы конфиденциальной информации в процессе её создания, обработки, передачи; - современные средства и способы обеспечения кибербезопасности.	Опрос, тестирование, задание, доклад, реферат

7.4. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ НА РАЗЛИЧНЫХ ЭТАПАХ ИХ ФОРМИРОВАНИЯ, ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ.

Текущий контроль знаний представляет собой контроль освоения программного материала учебной дисциплины, с целью своевременной коррекции обучения, активизации самостоятельной работы и проверки уровня знаний и умений обучающихся, сформированности компетенций.

Промежуточная аттестация по дисциплине позволяет оценить степень выраженности (сформированности) компетенций:

Содержание учебного материала по дисциплине	**Тип контрольного задания**		
Раздел 1. Основы теории операционных систем	Вопросы к экзамену	Вопросы к устному опросу Практические задания	Тестирование, доклад, реферат
Раздел 2. Свойства и принципы построения операционных систем	Вопросы к экзамену	Вопросы к устному опросу; Практические задания	Тестирование, задание, доклад, реферат
Раздел 3. Работа в современных операционных системах	Вопросы к экзамену	Вопросы к устному опросу; Практические задания	Тестирование, задание, доклад, реферат

7.4.1. Комплект оценочных средств для текущего контроля

Текущий контроль знаний представляет собой контроль освоения программного материала учебной дисциплины, с целью своевременной коррекции обучения, активизации самостоятельной работы и проверки уровня знаний и умений обучающихся, сформированности компетенций. Результаты текущего контроля заносятся в журналы учебных занятий.

Формы текущего контроля знаний:

- устный опрос;
- письменный опрос;
- тестирование;
-выполнение и защита практических работ;
- выполнение практических заданий;
- написание докладов/рефератов.

Проработка конспекта лекций и учебной литературы осуществляется студентами в течение всего семестра, после изучения новой темы.

Защита практических работ по типам контрольных заданий производится студентом в день их выполнения в соответствии с планом-графиком.

Преподаватель проверяет правильность выполнения практических работ студентом, контролирует знание студентом пройденного материала с помощью контрольных вопросов или тестирования.

Примерная тематика докладов/рефератов
Формируемые компетенции – ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7

1. Классификация информации. Виды данных и носителей. Ценность информации. Цена информации.
2. Количество и качество информации. Виды защищаемой информации.
3. Демаскирующие признаки объектов защиты. Классификация источников и носителей информации.
4. мероприятия по управлению доступом к информации. Функциональные источники сигналов. Опасный сигнал.
5. Основные средства и системы, содержащие потенциальные источники опасных сигналов. Вспомогательные средства и системы, содержащие потенциальные источники опасных сигналов.
6. Виды паразитных связей и наводок, характерные для любых радиоэлектронных средств и проводов, соединяющих их кабелей. Виды угроз безопасности информации.
7. Основные принципы добывания информации. Процедура идентификации, как основа процесса обнаружения объекта.
8. Методы синтеза информации. Методы несанкционированного доступа к информации.
9. Основными способами привлечения сотрудников государственных и коммерческих структур, имеющих доступ к интересующей информации. Способы наблюдения с использованием технических средств.
10. Каналы утечки информации. Технические каналы утечки. Классификация технических каналов утечки по физической природе носителя.
12. Классификация технических каналов утечки по информативности. Классификация технических каналов утечки по времени функционирования.
13. Классификация технических каналов утечки по структуре. Наблюдение в оптическом диапазоне и применяемые для этого средства. Характеристики таких средств.
14. Перехват электромагнитных излучений. Акустическое подслушивание. Эффекты, возникающие при подслушивании.
15. Понятия скрытия информации, виды скрытий. Информационный портрет. Противодействие наблюдению. Способы маскировки.
16. Способы и средства противодействия подслушиванию. Нейтрализация закладных устройств.
17. Состав инженерной защиты и технической охраны объектов. Инженерные конструкции и сооружения для защиты информации. Их классификация.
19. Средства идентификации личности. Классификация датчиков охранной сигнализации.
20. Защита личности как носителя информации. Системный подход к защите информации. Параметры системы защиты информации.

Примерный перечень практических заданий по дисциплине
Формируемые компетенции – ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7

Практическая работа по теме 1.1

Знакомство с терминологией по кибербезопасности. информационные ресурсы. угрозы и уязвимости в информационной системе. критерии: конфиденциальность, целостность, доступность

Практическая работа по теме 2.1

Классификация нарушений кибербезопасности вычислительной системы и выявление причин, обуславливающих их существование

Практическая работа по теме 2.2

Изучение механизмов защиты информации. Анализ способов нарушений кибербезопасности

Практическая работа по теме 3.1

Информационные активы коммерческой организации. угрозы и уязвимости кибербезопасности. Выявление инсайдера в коммерческой организации. социальная инженерия.

Практическая работа по теме 3.2

Изучение принципов построения моноалфавитных и полиалфавитных шифров замены. Исследование свойств подстановочных шифров. Изучение принципов построения шифров перестановки. Исследование свойств перестановочных шифров.

Практическая работа по теме 3.3

Изучение возможностей уничтожения и восстановления электронных документов с помощью специальных программ.

Критерии и шкала оценивания (устный опрос)

Оценка			
«отлично»	**«хорошо»**	**«удовлетворительно»**	**«неудовлетворительно»**
Тема раскрыта в полном объеме, высказывания связанные и логичные, использована научная лексика, приведены примеры. Ответы даны в полном объеме.	Тема раскрыта не в полном объеме, высказывания в основном связанные и логичные, использована научная лексика, приведены примеры. Ответы на вопросы даны не в полном объеме.	Тема раскрыта недостаточно, высказывания несвязанные и нелогичные. Научная лексика не использована, не приведены примеры. Ответы на вопросы зависят от помощи со стороны преподавателя.	Тема не раскрыта. Логика изложения, примеры, выводы и ответы на вопросы отсутствуют.

Критерии и шкала оценивания (выполнение практических заданий)

Оценка			
«отлично»	**«хорошо»**	**«удовлетворительно»**	**«неудовлетворительно»**
По решению задачи дан правильный ответ и развернутый вывод	По решению задачи дан правильный ответ, но не сделан вывод	По решению задачи дан частичный ответ, не сделан вывод	Задача не решена полностью

Критерии и шкала оценивания (тестирование)

Число правильных ответов	**Оценка**
90-100% правильных ответов	Оценка «отлично»
70-89% правильных ответов	Оценка «хорошо»
51-69% правильных ответов	Оценка «удовлетворительно»
Менее 51 % правильных ответов	Оценка «неудовлетворительно»

Критерии и шкала оценивания (доклады/рефераты)

Оценка	Критерии оценки доклада/реферата
«отлично»	1. Соблюдение формальных требований к реферату 2. Грамотное и полное раскрытие темы; 3. Самостоятельность в работе над рефератом (использование рефератов из сети Интернет запрещается). 4. Умение работать с учебной, профессиональной литературой. 5. Умение работать с периодической литературой. 6. Умение обобщать, делать выводы. 7. Умение оформлять библиографические список к реферату в соответствие с требованиями ГОСТ Р 7.1.- 2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». 8. Соблюдение требований к оформлению реферата. 9.Умение кратко изложить основные положения реферата при его защите. 10. Иллюстрация защиты реферата презентацией.
«хорошо»	1. Соблюдение формальных требований к реферату 2. Грамотное и полное раскрытие темы; 3. Самостоятельность в работе над рефератом (использование рефератов из сети Интернет запрещается). 4. Умение работать с учебной, профессиональной литературой. 5. Умение работать с периодической литературой. 6. Не полно обобщен и сделан вывод. 7. Не точно оформлен библиографический список к реферату в соответствие с требованиями ГОСТ Р 7.1.- 2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». 8. Не полно соблюдены требования к оформлению реферата. 9. Не четко сформированы краткие основные положения реферата при его защите. 10. Иллюстрация защиты реферата презентацией.
«удовлетворительно»	1. Соблюдение формальных требований к реферату 2. Грамотное и полное раскрытие темы; 3. Самостоятельность в работе над рефератом (использование рефератов из сети Интернет запрещается). 4. Не полно изучены учебная, профессиональная литература. 5. Не полно изучена периодическая литература. 6. Не обобщены и не конкретизированы выводы. 7. Не точно оформлен библиографический список к реферату в соответствие с требованиями ГОСТ Р 7.1.- 2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». 8. Не соблюденны требования к оформлению реферата. 9. Не четко сформированы краткие основные положения реферата при его защите. 10. Иллюстрация защиты реферата презентацией отсутствует
«неудовлетворительно»	Реферат не представлен по соответствующим критериям оценивания

7.4.2. КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Примерные вопросы к зачету

Контролируемые компетенции – ОК 01 ОК 02 ОК 03 ОК 04 ОК 05 ОК 07 ПК 5.1 ПК 5.2 ПК 5.3 ПК 5.4 ПК 5.5 ПК 5.6. ПК 5.7

1. Защита информации. Общие представления
2. Информационно-манипулятивные технологии (социальная инженерия)
3. Информационная система как объект защиты.
4. Объекты и предметы защиты
5. Виды защищаемой информации
6. Угрозы безопасности информации и их классификация.
7. Основные угрозы конфиденциальности
8. Основные угрозы целостности
9. Основные угрозы доступности
10. Основные источники внутренних угроз в информационной системе коммерческой организации
11. Классификация нарушителей
12. Модель нарушителя
13. Идентификация и аутентификация. Метод пароля и его модификация.
14. Идентификация и аутентификация Защита информации с помощью идентификационных карт
15. Идентификация и аутентификация. Биометрические системы защиты. Основные представления
16. Алгоритм использования биометрического признака при идентификации и аутентификации личности. Ошибки первого и второго рода
17. Стеганография как способ защиты информации. Методы, используемые в программах по стеганографии.
18. Проверка целостности файлов: основные представления
19. Способы восстановлены удаленных данных
20. Способы безвозвратного удаления данных
21. Механизмы защиты информации: основные представления
22. Использование полиграфа для решения задач защиты информации: общие представления
23. Средства защиты информации: общие представления
24. Графический пароль: общие представления
25. Методы шифрования с помощью перестановки букв. Примеры
26. Подсистемы кибербезопасности
27. Защита информации: меры
28. Защита информации: методы
29. Защита информации: этапы реализации механизмов защиты
30. Защита информации: уровни безопасности

Критерии и шкалы оценивания промежуточной аттестации

Шкала и критерии оценки (экзамен)

Зачтено	Незачтено
1. Ответ раскрывает содержание материала, но при этом может иметь следующие недостатки: 2. В изложении допущены небольшие пробелы, не исказившие содержание ответа; 3. Допущены один - два недочета при освещении основного содержания ответа, исправленные по замечанию экзаменатора; 4. Допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию экзаменатора.	1. Содержание материала не раскрыто. 2. Ошибки в определении понятий, не использовалась терминология в ответе.

Разработчик:
Преподаватель ФСППО кафедры факультета среднего профессионального и предпрофессионального образования факультета среднего профессионального и предпрофессионального образования ФГАОУ ВО «СГЭУ» Р.А.Олин