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 № 14 от 31 марта 2021 г.)

РАБОЧАЯ ПРОГРАММА

Наименование дисциплины ОП.13 Кибербезопасность

Специальность 09.02.04. Информационные системы (по отраслям)

Квалификация (степень) выпускника техник по информационным системам

Самара 2021

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.13 «Кибербезопасность»

1.1. Место дисциплины в структуре образовательной программы:

Дисциплина ОП.13 «Кибербезопасность» является частью программы подготовки специалистов среднего звена (ППССЗ) по специальности 09.02.04 «Информационные системы (по отраслям)» (базовой подготовки).

Рабочая программа по дисциплине ОП.13 «Кибербезопасность» разработана в ФГАОУ ВО «Самарский государственный экономический университет», в соответствии с требованиями ФГОС СПО, компетентностным подходом, реализуемым в системе среднего профессионального образования.

Дисциплина ОП.13 «Кибербезопасность» входит в Профессиональный учебный цикл ОП.07. блока профессиональной подготовки.

Особое значение дисциплина имеет при формировании и развитии следующих компетенций: ОК 1- ОК 3, ОК 8-ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2., ПК 2.3, ПК 2.5.

Общие компетенции (ОК)
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Виды деятельности	**Профессиональные компетенции (ПК)**
Эксплуатация и модификация информационных систем.	ПК 1.3. Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения.
	ПК 1.7. Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.
	ПК 1.8. Консультировать пользователей информационной системы и разрабатывать фрагменты методики обучения пользователей информационной системы.
Участие в разработке информационных систем.	ПК 2.1. Участвовать в разработке технического задания.
	ПК 2.2. Программировать в соответствии с требованиями технического задания.
	ПК 2.3. Применять методики тестирования разрабатываемых приложений
	ПК 2.5. Оформлять программную документацию в соответствии с принятыми стандартами.

1.2. Планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания:

Знать: - действующее законодательство РФ в информационной сфере;
-государственную политику в сфере обеспечения информационной безопасности;
- принципы применения методов обеспечения информационной безопасности;

Уметь: - применять законы и другие нормативно-правовые акты в сфере информационной безопасности;
- выявлять угрозы конфиденциальности, целостности, доступности информации;
- проводить анализ информации с целью подготовки принятия решений по обеспечению информационной безопасности;
- разрабатывать документы организационно-распорядительного характера, регламентирующие работу по обеспечению информационной безопасности.

Иметь практический опыт (владеть): методами обработки, хранения, передачи и накопления информации; защиты информации от несанкционированного доступа; специализированным программным обеспечением для сбора, хранения и обработки информации в соответствии с изучаемыми профессиональными модулями; автоматизированными системами делопроизводства; методами и средствами защиты информации.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Всего часов Семестр 7
Аудиторные занятия	64
В том числе:	
Лекции	32
Практические занятия	32
Самостоятельная работа (всего)	22
Консультации	4
Вид промежуточной аттестации (зачет, экзамен)	экзамен
Общая трудоемкость часы	**90**

2.2. Тематический план и содержание учебной дисциплины

П/П	**Наименование раздела дисциплины**	**Формируемые Компетенции**	**Лек**	**ПЗ**	**Кон-ции**	**СР**	**Всего**
1	Основные понятия и задачи информационной безопасности.	ОК 1, ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	5	5	1	4	15

2	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	ОК 1, ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	5	5	1	4	15
3	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.	ОК 1, ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	5	5	1	4	15
4	Угрозы и уязвимости информационной безопасности.	ОК 1, ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	5	5	1	4	15
5	Стандарты информационной безопасности.	ОК 1, ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	5	5		4	14
6	Меры и средства защиты информации (меры контроля).	ОК 1, ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	7	7		2	16
Итого:			32	32	4	22	90

2.2.1 Содержание разделов и тем

Раздел 1. Основные понятия и задачи информационной безопасности

Основные понятия теории информационной безопасности.

Основные понятия и определения: уязвимость, угроза, атака, эксплойт. Свойства информации: конфиденциальность, целостность, доступность.

Классификация угроз информационной безопасности

Раздел 2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.

Место информационной безопасности в системе национальной безопасности России: понятие, структура и содержание.

Основные руководящие документы, регламентирующие вопросы информационной безопасности.

Современные угрозы информационной безопасности в России

Раздел 3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.

Правовое обеспечение информационной безопасности. Понятие нормативности.

Раздел 4. Угрозы и уязвимости информационной безопасности.

Классификация угроз и уязвимостей информационной безопасности в корпоративных системах. Угроза безопасности объекта, источник угрозы, уязвимость объекта, атака.

Раздел 5. Стандарты информационной безопасности.

Необходимость стандартизации обеспечения безопасности данных. Государственные и международные стандарты информационной безопасности. Стандарты информационной безопасности передачи данных.

Раздел 6. Меры и средства защиты информации (меры контроля).

Защитные меры. Меры обеспечения ИБ. законодательные, административные и процедурные меры обеспечения ИБ.

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 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 распространенной формой самостоятельной работы является подготовка докладов.

Формы самостоятельной работы

№ п/п	Наименование разделов и тем	Часы	Задания для самостоятельной работы	Управление со стороны преподавателя
1.	Основные понятия и задачи информационной безопасности.	4	Подготовка доклада, презентации; домашние задания, подготовка к опросу. Изучение материала к деловым играм и т.д.	Проверка докладов, презентаций; проверка домашних заданий, Оценивание опроса. Проведение деловой игры и оценивание ее результатов
2.	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	4	Подготовка доклада, презентации; домашние задания, подготовка к опросу. Изучение материала к деловым играм и т.д.	Проверка докладов, презентаций; проверка домашних заданий, Оценивание опроса. Проведение деловой игры и оценивание ее результатов

3.	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.	4	Подготовка доклада, презентации; домашние задания, подготовка к опросу. Изучение материала к деловым играм и т.д.	Проверка докладов, презентаций; проверка домашних заданий, Оценивание опроса. Проведение деловой игры и оценивание ее результатов
4.	Угрозы и уязвимости информационной безопасности.	4	Подготовка доклада, презентации; домашние задания, подготовка к опросу. Изучение материала к деловым играм и т.д.	Проверка докладов, презентаций; проверка домашних заданий, Оценивание опроса. Проведение деловой игры и оценивание ее результатов
5.	Стандарты информационной безопасности.	4	Подготовка доклада, презентации; домашние задания, подготовка к опросу. Изучение материала к деловым играм и т.д.	Проверка докладов, презентаций; проверка домашних заданий, Оценивание опроса. Проведение деловой игры и оценивание ее результатов
6.	Меры и средства защиты информации (меры контроля).	2	Подготовка доклада, презентации.	Проверка докладов, презентаций.

Примерная тематика докладов

1. Понятие национальной безопасности.
2. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
3. Виды защищаемой информации.
4. Основные понятия и общеметодологические принципы теории информационной безопасности.
5. Роль информационной безопасности в обеспечении национальной без- опасности государства.
6. Интересы личности в информационной сфере.
7. Интересы общества в информационной сфере.
8. Интересы государства в информационной сфере.
9. Основные составляющие национальных интересов Российской Федерации в информационной сфере.

10. Угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России.
11. Угрозы информационному обеспечению государственной политики Российской Федерации.
12. Угрозы развитию отечественной индустрии информации, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов.
13. Угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России
14. Внешние источники угроз.
15. Внутренние источники угроз.
16. Направления обеспечения информационной безопасности государства.
17. Проблемы региональной информационной безопасности.

5. ЗАДАНИЯ ДЛЯ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

По дисциплине предусмотрены практические занятия с использованием активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой для формирования и развития общих и профессиональных компетенций обучающихся.

№ п/п	Наименование разделов и тем	Формируемые компетенции	Часы	Формы занятий	Форма внеаудиторной работы
1.	Основные понятия и задачи информационной безопасности.	ОК 1,ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	4	Решение практических задач. Устный опрос.	Написание докладов; решение задач
2.	Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	ОК 1,ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	4	Решение практических задач. Устный опрос.	Написание докладов; решение задач
3.	Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.	ОК 1,ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	4	Решение практических задач. Устный опрос.	Написание докладов; решение задач
4.	Угрозы и уязвимости информационной безопасности.	ОК 1,ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	4	Решение практических задач. Устный опрос.	Написание докладов; решение задач

5.	Стандарты информационной безопасности.	ОК 1,ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	4	Решение практических задач. Устный опрос.	Написание докладов; решение задач
6.	Меры и средства защиты информации (меры контроля).	ОК 1,ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.	2	Решение практических задач. Устный опрос.	Написание докладов; решение задач

6. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

6.1. Для реализации программы дисциплины предусмотрены: Студия информационных ресурсов, 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 09.02.04 Информационные системы (по отраслям)

6.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд Университет имеет электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе

6.2.1. Электронные издания:

Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 240 с. — (Профессиональное образование). — ISBN 978-5-534-10711-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/456793

6.2.2. Электронные ресурсы

1. Научная электронная библиотека eLIBRARY.RU https://elibrary.ru/
2. Электронная библиотечная система Юрайт Издательство Юрайт https://biblio-online.ru/
3. Платформа «Библиокомлектатор» http://www.bibliocomplectator.ru/
4. Справочно-правовая система «Консультант Плюс» http://konsultant.ru/

6.2.3. Дополнительные источники

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 ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2020. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451933

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)

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ ОП.13.Основы информационной безопасности.

7.1. Паспорт фонда оценочных средств по дисциплине

Фонд оценочных средств предназначен для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины ОП.13. Кибербезопасность по специальности 09.02.04 «Основы информационной безопасности».

Фонд оценочных средств разработан в соответствии с требованиями ФГОС СПО 09.02.04 Информационные системы (по отраслям) и рабочей программой ОП.13. Кибербезопасность.

В результате освоения учебной дисциплины обучающийся должен:

– ***уметь***

применять законы и другие нормативно-правовые акты в сфере информационной безопасности;

выявлять угрозы конфиденциальности, целостности, доступности информации;

проводить анализ информации с целью подготовки принятия решений по обеспечению информационной безопасности;

разрабатывать документы организационно-распорядительного характера, регламентирующие работу по обеспечению информационной безопасности.

– ***знать***

действующее законодательство РФ в информационной сфере;

государственную политику в сфере обеспечения информационной безопасности;

принципы применения методов обеспечения информационной безопасности;

Приобретаемый практический опыт:

Вид деятельности	Профессиональные компетенции
Эксплуатация и модификация информационных систем.	Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения.
	Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.
	Консультировать пользователей информационной системы и разрабатывать фрагменты методики обучения пользователей информационной системы.
Участие в	Участвовать в разработке технического задания.
	Программировать в соответствии с требованиями технического

разработке информационных систем.	задания.
	Применять методики тестирования разрабатываемых приложений.
	Оформлять программную документацию в соответствии с принятыми стандартами.

Освоить общие и профессиональные компетенции:

Общие компетенции (ОК)
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Виды деятельности	**Профессиональные компетенции (ПК)**
Эксплуатация и модификация информационных систем.	ПК 1.3. Производить модификацию отдельных модулей информационной системы в соответствии с рабочим заданием, документировать произведенные изменения.
	ПК 1.7. Производить инсталляцию и настройку информационной системы в рамках своей компетенции, документировать результаты работ.
	ПК 1.8. Консультировать пользователей информационной системы и разрабатывать фрагменты методики обучения пользователей информационной системы.
Участие в разработке информационных систем.	ПК 2.1. Участвовать в разработке технического задания.
	ПК 2.2. Программировать в соответствии с требованиями технического задания.
	ПК 2.3. Применять методики тестирования разрабатываемых приложений.
	ПК 2.5. Оформлять программную документацию в соответствии с принятыми стандартами.

7.2. Перечень контролирующих мероприятий для проведения текущего контроля и промежуточной аттестации

Перечень контролирующих мероприятий для проведения текущего контроля по дисциплине ОП.13. Кибербезопасность:

Номер семестра	Текущий контроль				
	Тестирование	Опрос	Сквозная задача	Доклад	Формирование портфолио
7	-	+	-	+	-

Перечень контролирующих мероприятий для проведения промежуточной аттестации по дисциплине ОП.13 Кибербезопасность:

Номер семестра	Промежуточная аттестация			
	Курсовая работа	Промежуточное тестирование	Зачет	Экзамен
7	-	-	-	+

7.3. Результаты освоения дисциплины, подлежащие оцениванию

Результат обучения (объект оценивания)	Основные показатели оценивания	Тип задания
Уметь назначение, состав, основные характеристики компьютера; основные компоненты компьютерных сетей, принципы пакетной передачи данных, организацию межсетевого взаимодействия; назначение и принципы использования системного и прикладного программного обеспечения; технологию поиска информации в информационно-телекоммуникационной сети "Интернет" (далее - сеть Интернет); правовые аспекты использования информационных технологий и программного обеспечения; основные понятия автоматизированной обработки информации; назначение, принципы организации и эксплуатации информационных систем; основные угрозы и методы обеспечения информационной безопасности	- Выбор компьютера в соответствии с решаемыми задачами. - Анализ причин возникновения ошибок при работе ОС. - Установка прикладного программного обеспечения. - Систематизация основных источников информационных угроз. - Выбор методов, технологий и аппараты для защиты информации.	Задача, доклад
Знать использовать	-использование информационных ресурсов	Задача, доклад

информационные ресурсы для поиска и хранения информации; обрабатывать текстовую и табличную информацию; использовать деловую графику и мультимедиа-информацию; создавать презентации; применять антивирусные средства защиты информации; читать (интерпретировать) интерфейс специализированного программного обеспечения, находить контекстную помощь, работать с документацией.	для поиска и хранения информации в сети Интернет; - обработка информации любого вида; - использовать современные мультимедийные средства; - работать с документацией и информационно - правовыми системами.	
Иметь практический опыт обработки, хранения, передачи и накопления информации; защиты информации от несанкционированного доступа; специализированным программным обеспечением для сбора, хранения и обработки информации в соответствии с изучаемыми профессиональными модулями; автоматизированными системами делопроизводства; методами и средствами защиты информации	- владеют современными средствами сбора и обработки информации любого вида с использованием современного программного обеспечения - Владеют принципами и методами современного делопроизводства и средствами защиты информации.	Задача

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) образовательных результатов:

Содержание учебного материала по дисциплине	**Тип контрольного задания**		
1. Основные понятия и задачи информационной безопасности.	Вопросы к экзамену	Вопросы к устному или письменному опросу	Задачи, доклад
2. Понятие национальной безопасности, виды безопасности. Информационная безопасность РФ.	Вопросы к экзамену	Вопросы к устному или письменному опросу	Задачи, доклад

3. Международная, национальная и ведомственная нормативная правовая база в области информационной безопасности.	Вопросы к экзамену	Вопросы к устному или письменному опросу	Задачи, доклад
4. Угрозы и уязвимости информационной безопасности.	Вопросы к экзамену	Вопросы к устному или письменному опросу	Задачи, доклад
5. Стандарты информационной безопасности.	Вопросы к экзамену	Вопросы к устному или письменному опросу	Задачи, доклад
6. Меры и средства защиты информации (меры контроля).	Вопросы к экзамену	Вопросы к устному или письменному опросу	Задачи, доклад

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:
- опрос (устный или письменный);
- решение практических задач,
- изучение материала с помощью электронных учебников,
- написание докладов.

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

1. Понятие информационной безопасности.
2. Составляющие информационной безопасности.
3. Задачи информационной безопасности общества.
4. Уровни формирования режима информационной безопасности.
5. Правовые основы информационной бебзопасности общества.
6. Сервисы безопасности в вычислительных сетях.
7. Каналы несанкционированного доступа к информации.
8. «Вирусоподобные» программы.
9. Классификация антивирусных программ.
10. Классы удаленных угроз.

11. Определение понятий «аунтентификация» и «идентификация».
12. Симметричные и ассиметричные методы шифрования.
13. Механизм электронной цифровой подписи.
14. Механизм электронной цифровой подписи.
15. Удаленная атака "подмена доверенного объекта".
16. Удаленная атака "ложный объект".
17. Удаленная атака "отказ в обслуживании".
18. Удаленная атака "Анализ сетевого трафика".
19. Характерные черты компьютерных вирусов.

Перечень практических задач по темам дисциплины

Формируемые компетенции - ОК 1- ОК 3, ОК 8-ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2., ПК 2.3, ПК 2.5.

Практическая работа № 1

«Анализ рисков информационной безопасности»

Цель работы - ознакомиться с алгоритмами оценки риска информационной безопасности.

Задание

1. Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Ч а с т ь 3 «Методы менеджмента безопасности информационных технологий»
2. Ознакомьтесь с **Приложениями C, D** и **E** ГОСТа.
3. Выберите три различных информационных актива организации (см. вариант).
4. Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.
5. Пользуясь **Приложением C** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.
6. Пользуясь одним из методов (см. вариант) предложенных в **Приложении E** ГОСТа произведите оценку рисков информационной безопасности.
7. Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Обоснование выбора информационных активов организации
5. Оценка ценности информационных активов
6. Уязвимости системы защиты информации

7. Угрозы ИБ
8. Оценка рисков
9. Выводы

Практическая работа № 2.

«Обеспечение информационной безопасности в ведущих зарубежных странах»

Цель работы - ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах.

Задание

1. Подготовить краткий доклад по заданному вопросу (см. вариант), используя учебное пособие Аверченкова, В.И. "Системы защиты информации в ведущих зарубежных странах" и другие доступные источники информации.
2. Заполнить таблицу " Системы обеспечения ИБ в ведущих зарубежных странах "(см. вариант) на основе подготовленного материала, а также докладов других студентов.
3. Провести анализ собранной информации и сделать выводы.

Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Таблица "Системы обеспечения ИБ в ведущих зарубежных странах"
5. Выводы

Практическая работа № 3

«Построение концепции информационной безопасности предприятия»

Цель работы -знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Задание

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

1. Общие положения

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

2. Проблемная ситуация в сфере информационной безопасности

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

3. Механизмы обеспечения информационной безопасности Предприятия

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

4. Мероприятия по реализации мер информационной безопасности Предприятия

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.
- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия.
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

5. Программа создания системы информационной безопасности Предприятия

Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Концепция ИБ заданного предприятия по плану, приведенному в задании

7.5. Критерии и шкалы оценивания текущего контроля

Критерии и шкала оценивания (устный опрос, письменный 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, сквозных задач, выполнение и защита практических работ)

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 (доклады)

Оценка	**Критерии оценки доклада**
«отлично»	1. Соблюдение формальных требований к докладу 2. Грамотное и полное раскрытие темы; 3. Самостоятельность в работе над докладом (использование докладов 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 докладу в соответствие с требованиями ГОСТ Р 7.1.-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». 8. Соблюдение требований к оформлению доклада. 9.Умение кратко изложить основные положения доклада при его защите. 10. Иллюстрация защиты доклада презентацией.
«хорошо»	1. Соблюдение формальных требований к докладу 2. Грамотное и полное раскрытие темы; 3. Самостоятельность в работе над докладом (использование докладов 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 докладу 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 доклада. 9. Не четко сформированы краткие основные положения доклада при его защите. 10. Иллюстрация защиты доклада презентацией.
«удовлетворительно»	1. Соблюдение формальных требований к докладу 2. Грамотное и полное раскрытие темы; 3. Самостоятельность в работе над докладом (использование докладов 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 докладу в соответствие с требованиями ГОСТ Р 7.1.- 2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления». 8. Не соблюденны требования к оформлению доклада. 9. Не четко сформированы краткие основные положения доклада при его защите. 10. Иллюстрация защиты доклада презентацией отсутствует
«неудовлетворительно»	Не представил доклад по соответствующим критериям оценивания

7.7. Комплект оценочных средств для промежуточной аттестации

Примерные вопросы к экзамену

Экзамен позволяет оценить сформированность компетенций ОК 1,ОК 2, ОК 3, ОК 8, ОК 9, ПК 1.3, ПК 1.7, ПК 1.8, ПК 2.1, ПК 2.2, ПК 2.3, ПК 2.5.

1. Понятие информационной безопасности.
2. Составляющие информационной безопасности.
3. Задачи информационной безопасности общества.
4. Уровни формирования режима информационной безопасности.
5. Правовые основы информационной бебзопасности общества.
6. Сервисы безопасности в вычислительных сетях.
7. Каналы несанкционированного доступа к информации.
8. «Вирусоподобные» программы.
9. Классификация антивирусных программ.
10. Классы удаленных угроз.
11. Определение понятий «аунтентификация» и «идентификация».
12. Симметричные и ассиметричные методы шифрования.
13. Механизм электронной цифровой подписи.
14. Механизм электронной цифровой подписи.
15. Удаленная атака "подмена доверенного объекта".
16. Удаленная атака "ложный объект".
17. Удаленная атака "отказ в обслуживании".
18. Удаленная атака "Анализ сетевого трафика".
19. Характерные черты компьютерных вирусов.

7.8. Критерии и шкалы оценивания промежуточной аттестации

Критерии и шкала оценивания (экзамен)

Отлично	Хорошо	Удовлетворительно

1. Полно раскрыто содержание вопросов билета; 2. Материал изложен грамотно, в определенной логической последовательности, правильно используется терминология; 3. Показано умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации; 4. Продемонстрировано усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость компетенций, умений и навыков; 5. Ответ прозвучал самостоятельно, без наводящих вопросов.	Ответ удовлетворяет в основном требованиям на оценку «5», но при этом может иметь следующие недостатки: 1. В изложении допущены небольшие пробелы, не исказившие содержание ответа; 2. Допущены один - два недочета при освещении основного содержания ответа, исправленные по замечанию экзаменатора; 3. Допущены ошибка или более двух недочетов при освещении второстепенных вопросов, которые легко исправляются по замечанию экзаменатора.	1. Неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения материала. 2. Имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, исправленные после нескольких наводящих вопросов; 3. При неполном знании теоретического материала выявлена недостаточная сформированность компетенций, умений и навыков.