Частное профессиональное образовательное учреждение
«ОМСКИЙ ЮРИДИЧЕСКИЙ КОЛЛЕДЖ»
(ОмЮК)

РАССМОТРЕНА

на заседании ЦМК
информационно-технологических
дисциплин
протокол от «30» января 2021 года № 4

УТВЕРЖДЕНА

Директор ОмЮК

_____ Ю.А. Бурдельная

«01» сентября 2021 года

Рабочая программа дисциплины

ОП.06 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

по специальности среднего профессионального образования
(программа подготовки специалистов среднего звена)

10.02.01 Организация и технология защиты информации

Базовая подготовка

Форма обучения очная

Омск, 2021 г.

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1.1. Область применения программы

Программа учебной дисциплины является частью основной профессиональной образовательной программы (далее – ОПОП) в соответствии с ФГОС СПО по специальности 10.02.01 Организация и технология защиты информации.

1.2. Место учебной дисциплины в структуре ОПОП

Дисциплина входит в обязательную часть профессионального учебного цикла, относится к общим профессиональным дисциплинам.

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины

В результате освоения дисциплины обучающийся должен освоить знания и умения, необходимые для формирования общих и профессиональных компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности.

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 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

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.

ПК 1.6. Обеспечивать технику безопасности при проведении организационно-технических мероприятий.

ПК 3.1. Применять программно-аппаратные и технические средства защиты информации на защищаемых объектах.

ПК 3.2. Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов.

ПК 3.3. Проводить регламентные работы и фиксировать отказы средств защиты.

ПК 3.4. Выявлять и анализировать возможные угрозы информационной безопасности объектов.

В результате освоения учебной дисциплины обучающийся должен

уметь:

– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;

– применять основные правила и документы системы сертификации

Российской Федерации;

– классифицировать основные угрозы безопасности информации;

знать:

– сущность и понятие информационной безопасности, характеристику ее составляющих;

– место информационной безопасности в системе национальной безопасности страны;

– источники угроз информационной безопасности и меры по их предотвращению;

– жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;

– современные средства и способы обеспечения информационной безопасности.

1.4. Активные и интерактивные образовательные технологии, используемые на занятиях

Групповые дискуссии, решение ситуационных задач, метод «круглого стола», семинары, мультимедийные презентации, деловые и ролевые игры, кейс-метод.

1.5. Рекомендуемое количество часов на освоение программы учебной дисциплины:

Максимальной учебной нагрузки обучающегося **90** часов, в том числе:
обязательной аудиторной учебной нагрузки обучающегося – **60** часов;
самостоятельной работы обучающихся – **30** часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	**90**
Обязательная аудиторная учебная нагрузка (всего)	**60**
в том числе: практические работы	 20
Самостоятельная работа обучающихся	**30**
Промежуточная аттестация в форме **дифференцированного зачета**	

2.2. Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся		Объем часов	Уровень освоения
1	2		3	4
Раздел 1. Информационная безопасность и уровни ее обеспечения			**12**	
Тема 1.1. Понятие информационная безопасность.	**Содержание учебного материала**		**2**	
	1	Введение. Проблема информационной безопасности общества. Основные положения государственной политики РФ в информационной сфере.	2	1,2
Тема 1.2. Составляющие информационной безопасности.	**Содержание учебного материала**		**2**	
	1	Доступность информации. Целостность информации. Конфиденциальность информации.	2	3
Тема 1.3. Система формирования режима информационной безопасности.	**Содержание учебного материала**		**2**	
	1	Задачи информационной безопасности общества. Комплексное обеспечение информационной безопасности РФ.	2	2
Тема 1.4. Нормативно-правовые основы информационной безопасности в РФ.	**Содержание учебного материала**		**2**	
	1	Правовые основы информационной безопасности общества. Основные положения важнейших законодательных актов РФ в области информационной безопасности и защиты информации. Ответственность за нарушения в сфере информационной безопасности. Международные нормативно-правовые акты обеспечения ИБ.	2	2
	Самостоятельная работа обучающихся по разделу 1		**4**	
	Систематическая проработка конспектов занятий, учебной и специальной литературы. Написание рефератов на заданные темы: «Понятие государственной тайны», «Отличия функциональных требований от требований доверия», «Категории государственных информационных ресурсов».			
Раздел 2. Стандарты ИБ			**52**	
Тема 2.1. Общие критерии стандартов информационной безопасности.	**Содержание учебного материала**		**6**	
	1	Требования безопасности к информационным системам.	2	1,2
	2	Принцип иерархии: класс – семейство – компонент – элемент.	2	2

	3	Критерии и классы оценки защищённости объектов и деятельности.	2	2
	Практические работы		**8**	
	1	Проверка компьютера на предмет наличия уязвимостей.	2	3
	2	Исследование угроз доступности.	2	
	3	Использование средств администрирования Windows для анализа и настройки безопасности системы.	2	
	4	Использование шифрующей файловой системы.	2	
Тема 2.2. Стандарты информационной безопасности распределенных систем.	**Содержание учебного материала**		**4**	
	1	Сервисы безопасности в вычислительных сетях Программно-аппаратные средства обеспечения ИБ в вычислительных сетях.	2	2,3
	2	Администрирование средств безопасности.	2	2
Тема 2.3. Стандарты информационной безопасности в РФ.	**Содержание учебного материала**		**4**	
	1	Гостехкомиссия и ее роль в обеспечении информационной безопасности в РФ.	2	2
	2	Документы по оценке защищенности автоматизированных систем в РФ Документы, регламентирующие деятельность в области защиты информации.	2	2
Тема 2.4. Административный уровень обеспечения информационной безопасности.	**Содержание учебного материала**		**4**	
	1	Цели, задачи и содержание административного уровня.	2	2
	2	Разработка политики информационной безопасности.	2	2
Тема 2.5. Классификация угроз информационной безопасности.	**Содержание учебного материала**		**4**	
	1	Классы угроз информационной безопасности.	2	2,3
	2	Каналы несанкционированного доступа к информации.	2	2
	Практические работы		**4**	
	1	Аварийное восстановление информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней.	2	3
	2	Защита и восстановление данных на компьютере, используя систему архивации.	2	

	Самостоятельная работа обучающихся по разделу 2		**18**	
	Систематическая проработка конспектов занятий, учебной и специальной литературы. Подготовка к практическим занятиям, оформление результатов работ. Написание рефератов на заданные темы: ««Механизмы безопасности используемые для обеспечения конфиденциальности трафика», «Автоматизация технического контроля защиты потоков информации», «Защита процессов переработки информации в СУБД», «Отечественное нормативно-правовое обеспечение ИБ», «Технологии предотвращения угроз ИБ», «Модели защиты при отказе в обслуживании», «Механизм обеспечения ИБ в вычислительных сетях», «Ключевые системы разграничения доступа и электронная цифровая связь», «Методы и средства ограничения доступа к компонентам ЭВМ».			
Раздел 3. Компьютерные вирусы и защита от них			**24**	
Тема 3.1. Вирусы как угроза информационной безопасности.	**Содержание учебного материала**		**2**	
	1	Компьютерные вирусы и информационная безопасность. Характерные черты компьютерных вирусов.	2	2
Тема 3.2. Классификация компьютерных вирусов.	**Содержание учебного материала**		**2**	
	1	Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по деструктивным возможностям.	2	2
Тема 3.3. Характеристика «вирусоподобных» программ.	**Содержание учебного материала**		**6**	
	1	Виды «вирусоподобных» программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования. «Intended»-вирусы.	2	1
	2	Оптимизация антивирусной программы под определенную систему Задание исключений и требований доверия.	2	2
	3	Борьба с рекламными и шпионскими программами. Настройка межсетевого экрана.	2	2
	Практические работы		**6**	
	1	Исследование реестра, на предмет возможных уязвимостей для вирусов.	2	2,3
	2	Использование брандмауэра для анализа трафика между двумя сетями.	2	
	3	Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	2	

	Самостоятельная работа обучающихся по разделу 3	**8**	
	Систематическая проработка конспектов занятий, учебной и специальной литературы. Подготовка к практическим занятиям, оформление результатов работ. Написание рефератов на заданные темы: «Ответственность за использование и распространение вредоносных программ для ЭВМ», «Хронология развития компьютерных вирусов».		
Дифференцированный зачет		**2**	
Итого		**90**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. ознакомительный (узнавание ранее изученных объектов, свойств);
2. репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3. продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы дисциплины требует наличия учебного кабинета информационной безопасности и лаборатории компьютерной техники и технических средств обучения.

Оборудование учебного кабинета:

– посадочные места по количеству обучающихся;
– рабочее место преподавателя;
– комплект учебно-методической документации;
– комплект учебно-наглядных пособий.

Оборудование лаборатории:

– компьютеры;
– принтер;
– сканер;
– модем;
– проектор;
– плоттер;
– программное обеспечение общего и профессионального назначения;
– комплект учебно-методической документации.

Технические средства обучения:

– компьютеры с лицензионным программным обеспечением;
– мультимедиапроектор;
– специализированное программное обеспечение.

3.2. Информационное обеспечение обучения

Основные источники

1. Казарин О.В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О.В.Казарин, И.Б. Шубинский. — Москва: Издательство Юрайт, 2019. — 342 с. — Текст: электронный // URL: http://biblio-online.ru/bcode/431080

Дополнительные источники:

1. Журнал «Защита информации. Инсайд»

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляются преподавателем в процессе проведения семинарских занятий, обязательного тестирования, заслушивания сообщений, докладов, итогового тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения (освоенные умения, усвоенные знания)	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы контроля и оценки результатов обучения**
Умения:		
– классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности; – применять основные правила и документы системы сертификации Российской Федерации; – классифицировать основные угрозы безопасности информации.	ОК 1 - 5, 8, 9 ПК 1.6, 3.1 - 3.4	Устный и письменный опрос; защита практических работ; контроль деятельности обучающихся на практических занятиях; контроль выполнения обучающимися самостоятельной работы; дифференцированный зачет.
Знания:		
– сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – источники угроз информационной безопасности и меры по их предотвращению; – жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности.	ОК 1 - 5, 8, 9 ПК 1.6, 3.1 - 3.4	Устный и письменный опрос; защита практических работ; контроль деятельности обучающихся на практических занятиях; контроль выполнения обучающимися самостоятельной работы; дифференцированный зачет.