Автономная некоммерческая организация профессиональная образовательная организация «Колледж экономики, права и информационных технологий»

(АНО ПОО «КЭПиИТ»)

УТВЕРЖДАЮ
Директор АНО ПОО «КЭПиИТ»
_____А.Б. Ярощук
«02» марта 2023 г.

Рабочая программа учебной дисциплины

ОП.14 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

для специальности СПО

09.02.08 Интеллектуальные интегрированные системы

(программа подготовки специалистов среднего звена)

Москва, 2023

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1. Место учебной дисциплины в структуре основной профессиональной образовательной программы: обязательная часть общепрофессионального цикла

1.2. Цель и планируемые результаты освоения учебной дисциплины: цель учебной дисциплины – формирование знаний и умений, соответствующих ОК 01, ОК 02, ОК 04, ОК 06, ПК 1.1.

Требования к результатам освоения учебной дисциплины:

Номер /индекс компетен-ции по ФГОС СПО	**Содержание компетенции (или ее части)**	**В результате изучения дисциплины обучающиеся должны:**	
		знать	**уметь**
ОК 01	Выбирать способы решения задач профес сиональной деятель-ности применительно к различным кон-текстам.	Актуальный профессиональный и социальный контекст, вкотором приходится работать и жить; основные источники информации и ресурсы для решения задач ипроблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональнойи смежных сферах; структуру плана для решения задач;порядок оценки результатов решения задач профессиональной деятельности.	Распознавать задачу и/или проблему в профессиональн ом и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/илипроблемы; составить план действия; определить необходимые ресурсы; владеть актуальными м тодами работы в профессио-нальной и смежных сферах; реализовать со-ставленный план; оцени-

			вать результат и последствия своих действий (самостоятельно или с помощью наставника).
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	Номенклатуру информационных источников, применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации	Определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска.
ОК 04	Эффективно взаимодействоватьи работать в коллективе и команде	Психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности	Организовывать работуколлектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональ--ной деятельности
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанноеповедение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетомгармонизации межнациональныхи межрелигиозных	Сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности;стандарты антикоррупционного поведения и последствия его нарушения.	Проявлять сущность гражданско-патриотической позиции, общечеловеческих ценностей; значимость профессиональной деятельности по специальности; стандарты антикоррупционного поведения и

	отношений, применять стандарты антикоррупционного поведения		последствия его нарушения.
ПК 1.1	Выявлять, разрабатывать и сопровождать требования к отдельным функциям системы.	Модели процесса разработки программного обеспечения. Основные принципы процесса разработки программного обеспечения. Основные программные модули.	Умения: анализировать проектную и техническую документацию. Использовать специализированные графические средства построения и анализа архитектуры программных продуктов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем часов по видам учебной работы**
Общий объем учебной нагрузки	**82**
Работа обучающихся во взаимодействии с преподавателем	**82**
в том числе:	
лекционные занятия	56
лабораторные занятия	26
Самостоятельная работа студента	
в том числе:	
подготовка к лабораторным занятиям подготовка к текущему контролю	
Консультации	
Промежуточная аттестация в форме дифференцированного зачета	

2.2. Тематический план и содержание учебной дисциплины «Информационная безопасность»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1. Информация как объекта защиты			
Тема 1.1. Общие сведения о защите информации	Понятие об опасной информации. Виды опасной информации. Способы защиты человека от излишней, назойливой, недобросовестной информации. Вредная информация в формах обмана и злоупотребления доверием. Ценность информации.	2	1
Тема 1.2. Основные понятия и определения информационной безопасности	Основные понятия в информационной безопасности.	2	1
	Практическая работа обучающихся Национальные интересы и безопасность	1	
Тема 1.3. Базовая модель нарушителя	Структура базовой модели нарушителя. Описание нарушителей (субъектов атак).	2	1
	Практическая работа обучающихся Анализ действий нарушителя информационной безопасности предприятия	1	
Тема 1.4. Агенты угроз информационной безопасности	Информационные нарушители. Цели нарушителей. Оценка опасности нарушителя на основании его осведомленности, оснащенности и подготовленности. Ресурсы нарушителя. Оценка рисков неправомерного доступа для объекта атаки и нарушителя. Сложившиеся приоритеты в выборе тактики действий нарушителя.	4	**1**
	Практическая работа обучающихся Элементы и объекты защиты в автоматизированных системах обработки данных	**2**	
Раздел 2. Направления информационной защиты			
Тема 2.1. Виды мер и основные принципы обеспечения информационной безопасности	Характеристика нормативно-правовой защиты. Виды информации по категории доступа. Правовой режим защиты государственной тайны. Правовой режим защиты конфиденциальной информации. Виды конфиденциальной информации и режимы ее защиты. Ответственность за право нарушения в сфере защиты конфиденциальной информации.	4	1
	Практическая работа Проблемы реализации применения основных принципов информационной безопасности	**2**	
Тема 2.2. Классификация угроз информационной безопасности	Основные понятия об источниках угроз, факторах и последствиях. Виды проявления ущерба. Классификация угроз информационной безопасности. Классификация источников угроз. Классификация уязвимостей безопасности.	2	**1**

Тема 2.3. **Возможные каналы утечки информации**	Угрозы и возможные каналы утечки конфиденциальной информации. Виды угроз. Предпосылки появления угроз. Обобщенный перечень угроз и перечень мероприятий по защите данных. Рекомендуемые мероприятия по защите.	4	**1**
	Практическая работа Сравнительный анализ возможных каналов утечки информации	2	
Тема 2.4. **Правовые основы защиты персональных данных**	Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных». Основные понятия в законе. Защита персональных данных работников по Трудовому кодексу РФ.	2	**1**
Тема 2.5. **Уголовный кодекс РФ глава 28. Преступления в сфере компьютерной информации**	Уголовный кодекс Российской Федерации № 63-ФЗ от 13.06.1996 (с изм. и доп. от 07.07.2007). Уголовно-процессуальный кодекс Российской Федерации № 174-ФЗ от 18.12.2001 (с изм. и доп. от 07.07.2003). Кодекс РФ об административных нарушениях № 195-ФЗ от 30.12.2001 (с изм. и доп. от 4.07.2003). Гражданский кодекс РФ. Часть четвертая. ТК Велби, Изд-во Проспект, 2007. ФЗ «Об информации, информационных технологиях и защите информации», № 149-ФЗ от 27.07.2006. ФЗ «О связи», № 126-ФЗ от 07.07.2003.	2	**1**
	Практическая работа Сравнительный анализ преступлений в сфере компьютерной безопасности в странах ближнего зарубежья.	2	
Раздел 3. Методы и средства защиты программного обеспечения			
Тема 3.1. **Методы защиты программного обеспечения**	Аппаратные ключи защиты. Ключи с памятью. Ключи с неизвестным алгоритмом. Ключи с таймером. Ключи с известным алгоритмом. Ключи с программируемым алгоритмом. Программные средства защиты программного обеспечения. Алгоритмы запутывания (обфускация). Метод шифрования программного кода. Метод проверки целостности кода программы. Метод эмуляции процессора. Выполнение на стороне сервера.	6	1
	Практическая работа Анализ современного программного обеспечения в области информационной безопасности предприятий и частных лиц.	4	
Тема 3.2. **Регистрационные коды для программ**	Требования и классификация. Методы проверки регистрационных кодов. «Черный ящик». Сложная математическая задача. Табличные методы. Выбор метода.	4	1

Тема 3.3. **Методы и средства защиты программ от компьютерных вирусов и средств исследования программ**	Инструменты динамического исследования ПО. Инструменты статического исследования ПО. Защита от отладчиков. Защита от эмулирующих отладчиков. Защита от дизассемблеров.	4	1
Тема 3.4. **Криптография**	Участники взаимодействия. Объекты и операции. Симметричные алгоритмы. Алгоритмы шифрования. Криптографические хэш-функции. Криптографические генераторы псевдослучайных чисел. Модели основных криптоаналитических атак. Атака на основе только шифртекста. Атака на основе открытого текста. Атака на основе подобранного открытого текста. Модели распространения программного обеспечения. Бесплатные программы (Freeware). Почти бесплатные программы. Программы, показывающие рекламу (Adware). Коммерческие программы (Commercial). Почти работоспособные программы. Условно бесплатные продукты (Shareware).	4	1,2
	Практическая работа Проблемы реализации методов криптографической защиты в автоматизированных системах обработки данных Актуальные задачи защиты программ Особенности защиты информации в персональных ЭВМ	2	
Раздел 4. Механизмы обеспечения информационной безопасности программного обеспечения и баз данных			
Тема 4.1. **Привязка программного обеспечения к аппаратным средствам**	Основные способы и виды привязки программного обеспечения к аппаратным средствам.	4	***1,2***
	Практическая работа Цели, функции и задачи защиты информации в сетях ЭВМ Технические средства защиты	2	
Тема 4.2. **Шифрование RSA**	Описание алгоритма. История создания. Шифрование и расшифрование. Цифровая подпись.	2	***1***
	Практическая работа Достоинства и недостатки программного обеспечения, используемого для защиты данных Вредоносные закладки в ПК и борьба с ними	2	
Тема 4.3. **Безопасность web-приложений**	Особенности XSS-атак. Виды SQL-инъекций. Локальные и удаленные инклуды.	2	***1***
Тема 4.4.	История. Классификация. Распространение. Механизм. Каналы. Противодействие.	2	***1***

Компьютерные вирусы			
Тема 4.5. **Антивирусные средства.** **Компьютерные вирусы**	Классификация. Работа антивирусных средств. База. Целевые платформы антивирусных средств.	2	***1***
	Практическая работа Сравнительный анализ современных антивирусных комплексов, используемых в РФ	2	
Тема 4.6. **Уязвимость компьютерных сетей**	Проблемы безопасности протоколов TCP/IP. Методы и инструменты. Прослушивание сети. Сканирование сети. Генерация пакетов. Перехват данных. Ложные ARP-ответы. Навязывание ложного маршрутизатора. Имперсонация. Несанкционированное подключение к сети. Туннелирование. Атака крошечными фрагментами (Tiny Fragment Attack). Принуждение к ускоренной передаче данных. Отказ в обслуживании. Ложные DHCP-клиенты.	2	***1***
	Практическая работа Архитектура механизмов защиты информации в сетях ЭВМ	2	
Тема 4.7. **Защита баз данных**	Причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Соотношение защищенности и доступности данных. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.	2	***1***
Итого:			
Максимальная учебная нагрузка обучающегося (всего):		***82***	

**Для характеристики уровня освоения учебного материала используются следующие обозначения:
ознакомительный -узнавание ранее изученных объектов, свойств;
репродуктивный - выполнение деятельности по образцу, инструкции или под руководством;
продуктивный - планирование и самостоятельное выполнение деятельности, решение проблемных задач.

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация учебной дисциплины требует наличия учебных аудиторий (для проведения занятий всех видов, в том числе групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации), мастерские, помещения для самостоятельной работы, оснащенные компьютерной техникой с возможностью подключения к ин формационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронно-телекоммуникационную среду образовательной организации.

Технические средства обучения: проектор, экран, компьютеры.

Программное обеспечение: Microsoft Windows; Microsoft Office (или аналог); Mozilla Firefox (или Google Chrome, или любой другой браузер), обслуживающие программы и среды разработки программ по выбору преподавателей из числа свободно распространяемых и отечественных разработок.

Учебные занятия для обучающихся с ограниченными возможностями здоровья и инвалидов проводятся с учетом особенностей их психофизического развития, индивидуальных возможностей и состояния здоровья.

3.2. Информационное обеспечение обучения

Основная литература

1. Щербак, А. В. Информационная безопасностьебник для среднего офессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2022. — Э с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст: ектронный // Образовательная платформа Юрайт [сайт]. — RL: https://urait.ru/bcode/497642

2. Казарин, О. В. Основы информационной безопасности: надежность и безопасность ограммного обеспечения: учебное пособие для среднего профессионального образования / В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — рофессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // разовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524

3. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее разование). — ISBN 978-5-534-13960-0. — Текст: электронный // Образовательная атформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741

Дополнительная литература

4. Чернова, Е. В. Информационная безопасность человека: учебное пособие для зов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 3 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст: электронный // разовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495922

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

6. Казарин, О. В. Основы информационной безопасности: надежность и безопасность

ограммного обеспечения : учебное пособие для среднего профессионального образования / В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — рофессиональное образование). — ISBN 978-5-534-10671-8. — Текст: электронный // ЭБС райт [сайт]. — URL: https://urait.ru/bcode/456792

Интернет-ресурсы

1.Федеральный портал «Российское образование». Форма доступа: http://www.edu.ru

2.www.consultant.ru – Консультант Плюс

3.Доступ к открытым базам цитирования, в т.ч. springer.com, scholar.google.com, th-net.ru

4.Пржиялковский В. К каждой строке охранника приставишь! . Режим доступа: p://www.citforum.ru/database/oracle/l security

5.Пржиялковский В. Изучаем метки доступа к строкам: задание свойств столбца ступа к таблице. Режим доступа: http://www.citforum.ru/database/oracle/LearnOLS

6.Пржиялковский В. Изучаем метки доступа к строкам: правка обычных столбцов блицы. Режим доступа: http://www.citforum.ru/database/ oracle/LearnOL S 3.

7.Специализированный сайт по вопросам информационной безопасности. Режим ступа: http://www.securitylab.ru

8.Электронные версии журналов Сети, Открытые системы. Режим доступа: p://cisco.netacad.net

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе тестирования, а также выполнения обучающимися внеаудиторных и самостоятельных заданий.

Результаты обучения (освоенные компетенции)	**Результаты обучения (освоенные умения, усвоенные знания)**	**Формы и методы контроля и оценки результатов обучения**
ОК 1. Выбирать способы решения задач профес сиональной деятель-ности применительно к различным кон-текстам. ОК 2. Использовать современные средства поиска, анализа и ин-терпретации информации, и информационные технологии для выполнения задач профес сиональной деятельности ОК 4. Эффективно взаимодействоватьи работать в коллективе и команде ОК 6. Проявлять гражданско-	**Умения:** — выявлять потенциальных нарушителей информационной 1 безопасности; — производить оценку угроз информации; — применять алгоритмы криптографии для защиты данных; — использовать методы и средства защиты данных в зависимости от потенциальных пользователей системы; — применять методы шифрования организованных структур данных;	Экспертная оценка внеаудиторной самостоятельной работы; экспертная оценка при фронтальном опросе; наблюдение и оценка результата выполнения практических работ; дифференцированный зачет

патриотическую позицию, демонстрировать осознанноеповедение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетомгармонизации межнациональныхи межрелигиозных отношений, применять стандарты антикоррупционного поведения ПК 1.1. Выявлять, разрабатывать и сопровождать требования к отдельным функциям системы.	— создавать дополнительные средства защиты, опираясь на персональные данные компьютера пользователя; — пользоваться современными приложениями защиты авторских прав: — проводить анализ и оценивать механизмы защиты; — выбирать формы и критерии информационной безопасности; — использовать средства защиты от вредоносного программного обеспечения; — разрабатывать предложения по совершенствованию политики безопасности. **Знания:** - терминологию в сфере безопасности информационного контента; — понятия политики безопасности, существующие типы политик безопасности; — существующие 1 стандарты информационной безопасности; — виды угроз информационной безопасности; — средства борьбы с угрозами информационной безопасности; — о современных концепциях безопасности программного обеспечения и баз данных;	

	— методы защиты информации; — критерии защищенности программного обеспечения и баз данных; — угрозы безопасности программного обеспечения и баз данных; — критерии и методы оценивание механизмов защиты; — организационно-правовое обеспечение информационной безопасности.	