СОЦИАЛЬНО-ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ
ЧАСТНОЕ УЧРЕЖДЕНИЕ
ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«УТВЕРЖДАЮ»
Директор ЧУ ПО «СТК»
_____ Е. А. Карпова
27.01.2022 г.

Основы информационной безопасности

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Цикловая комиссия по информатике и информационной безопасности**

Учебный план КОМПЬЮТЕРНЫЕ СИСТЕМЫ И КОМПЛЕКСЫ

Учебный год начала подготовки 2022-2023

Квалификация **Техник по компьютерным системам**

Форма обучения **очная**

Часов по учебному плану 102
в том числе:
аудиторные занятия 68
самостоятельная работа 34

Виды контроля в семестрах:
зачеты с оценкой 8

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		**8 (4.2)**		Итого	
Недель	10		7			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	20	20	14	14	34	34
Практические	20	20	14	14	34	34
Итого ауд.	40	40	28	28	68	68
Контактная работа	40	40	28	28	68	68
Сам. работа	20	20	14	14	34	34
Итого	60	60	42	42	102	102

Рабочая программа дисциплины

Основы информационной безопасности

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования по специальности 09.02.01 КОМПЬЮТЕРНЫЕ СИСТЕМЫ И КОМПЛЕКСЫ (уровень подготовки кадров высшей квалификации). (приказ Минобрнауки России от 28.07.2014 г. № 849)

составлена на основании учебного плана:

КОМПЬЮТЕРНЫЕ СИСТЕМЫ И КОМПЛЕКСЫ

утвержденного на заседании Педагогического Совета ЧУ ПО "СТК" 24.01.2022 протокол № 1.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Цель дисциплины: ознакомить студентов с принципами и методами создания, хранения, редактирования, представления и защиты информации, а также с по-следними достижениями в этих областях, при этом особое внимание акцентируется на изучение специализированного применения технологий обработки информации, необхо-димого студентам в последующей профессиональной деятельности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	ОП
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Вычислительные системы, сети и телекоммуникации
2.1.2	Информационные системы и технологии
2.1.3	Теория вероятностей и математическая статистика
2.1.4	Экономика фирмы (предприятия)
2.1.5	Безопасность жизнедеятельности
2.1.6	Право
2.1.7	История (история России, всеобщая история)
2.1.8	Физическая культура и спорт
2.1.9	Философия
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Менеджмент
2.2.2	Программная инженерия
2.2.3	Производственная практика (технологическая (проектно-технологическая) практика)
2.2.4	Подготовка к сдаче и сдача государственного экзамена

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОК 1: Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	
Знать:	
1	возможные траектории профессионального развития и самообразования
2	сущность и понятие информационной безопасности, характеристику ее составляющих;
Уметь:	
1	источники угроз информационной безопасности и меры по их предотвращению;
2	жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
Владеть:	
1	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
2	Использовать информационно-коммуникационные технологии в профессиональной деятельности

ОК 2: Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	
Знать:	
1	сущность и понятие информационной безопасности, характеристику ее составляющих;
2	место информационной безопасности в системе национальной безопасности страны;
Уметь:	
1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
2	применять основные правила и документы системы сертификации Российской Федерации;
Владеть:	
1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
2	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 3: Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	
Знать:	
1	сущность и понятие информационной безопасности, характеристику ее составляющих;

2	место информационной безопасности в системе национальной безопасности страны;
Уметь:	
1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
2	применять основные правила и документы системы сертификации Российской Федерации;
Владеть:	
1	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность
2	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 4: Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	
Знать:	
1	сущность и понятие информационной безопасности, характеристику ее составляющих;
2	место информационной безопасности в системе национальной безопасности страны;
Уметь:	
1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
2	применять основные правила и документы системы сертификации Российской Федерации;
Владеть:	
1	Реализовывать методы и технологии защиты информации в базах данных
2	Производить инспектирование компонент программного продукта на предмет соответствия стандартам кодирования.

ОК 5: Использовать информационно-коммуникационные технологии в профессиональной деятельности.	
Знать:	
1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
2	применять основные правила и документы системы сертификации Российской Федерации;
Уметь:	
1	- сущность и понятие информационной безопасности, характеристику ее составляющих;
2	место информационной безопасности в системе национальной безопасности страны;
Владеть:	
1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 6: Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.	
Знать:	
1	- место информационной безопасности в системе национальной безопасности страны;
2	- источники угроз информационной безопасности и меры по их предотвращению;
Уметь:	
1	- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
2	применять основные правила и документы системы сертификации Российской Федерации;
Владеть:	
1	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
2	Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7: Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.	
Знать:	
1	- сущность и понятие информационной безопасности, характеристику ее составляющих;
2	место информационной безопасности в системе национальной безопасности страны
Уметь:	
1	классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
2	- применять основные правила и документы системы сертификации Российской Федерации;
Владеть:	
1	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
2	Использовать информационно-коммуникационные технологии профессиональной деятельности

ОК 8: Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	
Знать:	
1	- современные средства и способы обеспечения информационной безопасности. освоить общие компетенции
2	жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;
Уметь:	
1	фундаментальные положения теории информационного кодирования;
2	теоретические основы системного анализа
Владеть:	
1	использовать междисциплинарные системные связи наук;
2	анализировать и оценивать философские проблемы при решении социальных и профессиональных задач;

ОК 9: Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	
Знать:	
1	применять математический инструментарий к решению социальных и профессиональных проблем.
2	использовать междисциплинарные системные связи наук;
Уметь:	
1	фундаментальные положения теории информационного кодирования;
2	теоретические основы системного анализа
Владеть:	
1	навыками математической формализации экономических и социальных процессов
2	навыками выбора наиболее актуальных направлений научных исследований, ставить задачи исследования и определять способы решения поставленных задач;

ПК 1.1: Выполнять требования технического задания на проектирование цифровых устройств.	
Знать:	
1	сущность и значение информации в развитии современного информационного общества;
2	основные виды опасностей и угроз, возникающие в процессе хранения и передачи информации;
Уметь:	
1	решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий
2	решать нестандартные задачи в сфере защиты информации с учетом основных требований информационной безопасности
Владеть:	
1	техническими средствами и методами защиты информации;
2	методами применения криптографических средств защиты информации;

ПК 1.5: Выполнять требования нормативно-технической документации.	
Знать:	
1	сущность и значение информации в развитии современного информационного общества;
2	основные виды опасностей и угроз, возникающие в процессе хранения и передачи информации;
Уметь:	
1	- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
2	основные виды опасностей и угроз, возникающие в процессе хранения и передачи информации;
Владеть:	
1	техническими средствами и методами защиты информации;
2	использования инструментов обеспечения информационной безопасности организации.

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	- сущность и понятие информационной безопасности, характеристику ее составляющих;
3.1.2	- место информационной безопасности в системе национальной безопасностистраны;
3.1.3	- источники угроз информационной безопасности и меры по их предотвращению;
3.1.4	- жизненные циклы конфиденциальной информации в процессе ее создания,обработки, передачи;
3.1.5	- современные средства и способы обеспечения информационной безопасности.

3.2	**Уметь:**
3.2.1	- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
3.2.2	- применять основные правила и документы системы сертификации Российской Федерации;
3.2.3	- классифицировать основные угрозы безопасности информации;
3.3	**Владеть:**
3.3.1	- выполнять полный объем работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;
3.3.2	- к анализу материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации;
3.3.3	- выполнять оперативное управление деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик.
3.3.4	- выполнять полный объем работ, связанных с комплексным обеспечением информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик, в том числе с обеспечением требований нормативных документов, регламентирующих режим соблюдения государственной тайны;
3.3.5	- к анализу материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации;
3.3.6	- выполнять оперативное управление деятельностью организаций по комплексному обеспечению информационной безопасности конкретных автоматизированных систем на основе разработанных программ и методик.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов
	Раздел 1.		
1.1	Информационная безопасность и ее аспекты. /Лек/	7	5
1.2	Общие положения теории информационной безопасности. /Лек/	7	5
1.3	Стратегии защиты информации. /Лек/	7	5
1.4	Угрозы информационной безопасности. /Лек/	7	5
1.5	Методы криптографии. /Пр/	7	7
1.6	Центр обеспечения безопасности Windows. /Пр/	7	7
1.7	Локальная политика безопасности при администрировании Windows. /Пр/	7	6
1.8	Информационная безопасность и ее аспекты. /Ср/	7	4
1.9	Общие положения теории информационной безопасности. /Ср/	7	4
1.10	Стратегии защиты информации. /Ср/	7	4
1.11	Нарушители и нарушения информационной безопасности. /Ср/	7	4
1.12	Защита информационной безопасности. /Ср/	7	2
1.13	Угрозы информационной безопасности. /Ср/	7	2
1.14	Стандарты и спецификации в области информационной безопасности. /Лек/	8	4
1.15	Административный уровень информационной безопасности /Лек/	8	4
1.16	Общие сведения о стандартах и спецификациях в области информационной безопасности. /Лек/	8	4
1.17	Безопасность локальных объектов и локальных сетей. /Лек/	8	2
1.18	Информационная безопасность в условиях локальных сетей. /Пр/	8	6
1.19	Сеансовое конфигурирование Windows. /Пр/	8	6
1.20	Информационная безопасность в СУБД Access. /Пр/	8	2
1.21	Стандарты и спецификации в области информационной безопасности. /Ср/	8	2
1.22	Административный уровень информационной безопасности. /Ср/	8	2
1.23	Общие сведения о стандартах и спецификациях в области информационной безопасности. /Ср/	8	2
1.24	Безопасность локальных объектов и локальных сетей. /Ср/	8	2
1.25	Обеспечение информационной безопасности в общемировых сетях. /Ср/	8	2
1.26	/ЗачётСОц/	8	4

5. ОЦЕНОЧНЫЕ СРЕДСТВА

5.1. Вопросы для самоконтроля и текущей аттестации

Понятие информационной безопасности.
Концепция информационной безопасности.
Место информационной безопасности экономических систем в национальной безопасности страны.
Важность и сложность проблемы информационной безопасности.
Информационная безопасность в условиях функционирования в России глобальных сетей.
Теория информационной безопасности информационных систем, ее основные составляющие и задачи.
Моделирование процессов защиты информации.
Модели безопасности и их применение.
Понятие стратегии защиты. Виды стратегий защиты.
Критерии обоснования стратегии защиты.
Понятие угрозы безопасности информации и общие подходы к ее классификации.
Классификация угроз безопасности информации по способам их возможного негативного воздействия.
Угрозы доступности, целостности, конфиденциальности.
Происхождение угроз безопасности информации.
Предпосылки появления угроз.
Понятие нарушителя безопасности информации.
Виды противников или нарушителей безопасности информации.
Виды возможных нарушений информационной системы.
Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
Анализ способов нарушений информационной безопасности.
Вирус как типичное нарушение информационной безопасности. Виды вирусов.
Понятие системы защиты информации.
Типизация и стандартизация систем защиты информации.
Центры защиты информации и их функции.
Основные технологии построения защищенных ЭИС.
Использование защищенных ЭИС.
Понятие криптографии. Методы криптографии.
Политика безопасности.
Программа безопасности.
Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
Международные стандарты информационного обмена.
Стандарты и спецификации в области информационной безопасности и их классификация.
«Оранжевая книга».
Гармонизированные критерии европейских стран.
Спецификация internet-сообщества RFC 1510 «сетевой сервис аутентификации kerberos (v5)».
Руководящие документы (РД) Гостехкомиссии России.
X.800 «архитектура безопасности для взаимодействия открытых систем».
Технические спецификации IPSEC, TLS.
Рекомендация «как выбирать поставщика internet-услуг».
Британский стандарт BS 7799 «управление информационной безопасностью. Практические правила».
Безопасность операционных систем.
Безопасность систем управления базами данных.
Безопасность виртуальных частных сетей.
Безопасность виртуальных локальных сетей.
Безопасность смарт – карт.
Архитектура средств безопасности IP-уровня.
Контексты безопасности и управление ключами.
Обеспечение аутентичности IP-пакетов.
Обеспечение конфиденциальности сетевого трафика.
Роль поставщика internet-услуг в реагировании на нарушения безопасности.
Меры по защите internet-сообщества.
Обеспечение безопасности маршрутизаторов.
Особенности использования управляющих протоколов.
Безопасное размещение сетевого оборудования потребителя.
Защита системной инфраструктуры.

5.2. Темы письменных работ (контрольных и курсовых работ, рефератов)

Учебным планом не предусмотрены.

5.3. Оценочные средства для промежуточной аттестации

ФОС представлен в УМК дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л1.1	Артемов А. В.	Информационная безопасность: курс лекций: Учебная литература для ВУЗов	Орел: МАБИВ, 2014 http://biblioclub.ru/index.php?page=book&id=428605&sr=1
Л1.2	Башлы П. Н. , Баранова Е. К. , Бабаш А. В.	Информационная безопасность: Учебно-практическое пособие	М.: Евразийский открытый институт, 2011 http://biblioclub.ru/index.php?page=book_red&id=90539

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год, эл. адрес
Л2.1	Колябин А.Ю.	Информационная безопасность и защита информации: сборник студенческих работ	Москва: Студенческая наука,, 2012 https://biblioclub.ru/index.php?page=book_red&id=227774&sr=1

6.2.1 Перечень программного обеспечения

6.3.1.1	Microsoft Windows, OpenOffice, доступ в сеть Интернет.

6.2.2 Перечень информационных справочных систем и ресурсов сети Интернет

6.3.2.1	Каталог документов по направлению Информационная безопасность https://cisoclub.ru/doc/
6.3.2.2	Журнал «Информационная безопасность» https://www.itsec.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Специальные помещения представляют собой учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы и помещения для хранения и профилактического обслуживания учебного оборудования. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации, соответствующие примерным программам дисциплин (модулей), рабочим учебным программам дисциплин (модулей). Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно - образовательную среду.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Обучающимся необходимо помнить, что качество полученного образования в немалой степени зависит от активной роли самого обучающегося в учебном процессе. Обучающийся должен быть нацелен на максимальное усвоение подаваемого лектором материала, после лекции и во время специально организуемых индивидуальных встреч он может задать лектору интересующие его вопросы.

Лекционные занятия составляют основу теоретического обучения и должны давать систематизированные основы знаний по дисциплине, раскрывать состояние и перспективы развития соответствующей области науки, концентрировать внимание -обучающихся на наиболее сложных и узловых вопросах, стимулировать их активную познавательную деятельность и способствовать формированию творческого мышления.

Главная задача лекционного курса - сформировать у обучающихся системное представление об изучаемом предмете, обеспечить усвоение будущими специалистами основополагающего учебного материала, принципов и закономерностей развития соответствующей научно-практической области, а также методов применения полученных знаний, умений и навыков.

Основные функции лекций: 1. Познавательно-обучающая; 2. Развивающая; 3. Ориентирующе-направляющая; 4. Активизирующая; 5. Воспитательная; 6. Организующая; 7. информационная.

Выполнение практических заданий служит важным связующим звеном между теоретическим освоением данной дисциплины и применением ее положений на практике. Они способствуют развитию самостоятельности обучающихся, более активному освоению учебного материала, являются важной предпосылкой формирования профессиональных качеств будущих специалистов.

Проведение практических занятий не сводится только к органическому дополнению лекционных курсов и самостоятельной работы обучающихся. Их вместе с тем следует рассматривать как важное средство проверки усвоения обучающимися тех или иных положений, даваемых на лекции, а также рекомендуемой для изучения литературы; как форма текущего контроля за отношением обучающихся к учебе, за уровнем их знаний, а следовательно, и как один из важных каналов для своевременного подтягивания отстающих обучающихся.

При подготовке важны не только серьезная теоретическая подготовка, но и умение ориентироваться в разнообразных практических ситуациях, ежедневно возникающих в его деятельности. Этому способствует форма обучения в виде практических занятий. Задачи практических занятий: закрепление и углубление знаний, полученных на лекциях и приобретенных в процессе самостоятельной работы с учебной литературой, формирование у обучающихся умений и навыков работы с исходными данными, научной литературой и специальными документами. Практическому занятию должно предшествовать ознакомление с лекцией на соответствующую тему и литературой, указанной в плане этих занятий.
При проведении учебных занятий обеспечиваются развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, преподавание дисциплин (модулей) в форме курсов, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).
Самостоятельная работа может быть успешной при определенных условиях, которые необходимо организовать. Ее правильная организация, включающая технологии отбора целей, содержания, конструирования заданий и организацию контроля, систематичность самостоятельных учебных занятий, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.
Для контроля знаний студентов по данной дисциплине необходимо проводить оперативный, рубежный и итоговый контроль.
Оперативный контроль осуществляется путем проведения опросов студентов на семинарских занятиях, проверки выполнения практических заданий, а также учета вовлеченности (активности) студентов при обсуждении мини-докладов, организации ролевых игр и т.п.
Контроль за самостоятельной работой студентов по курсу осуществляется в двух формах: текущий контроль и итоговый.
Рубежный контроль (аттестация) подразумевает проведение тестирования по пройденным разделам курса. В тестирование могут быть включены темы, предложенные студентам для самостоятельной подготовки, а также практические задания.