

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Кислова Наталья Николаевна

Должность: Проректор по УМР и качеству образования

Дата подписания: 31.08.2023

Уникальный программный ключ:

52802513f5b14a975b7e9b13008093d5726b159bf6064f865ae65b96a966c035

МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

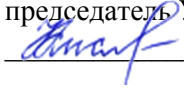
«Самарский государственный социально-педагогический университет»

Кафедра информационно-коммуникационных технологий в образовании

УТВЕРЖДАЮ

Проректор по УМР и КО,

председатель УМС СГСПУ

 Н.Н. Кислова

МОДУЛЬ "ВУЗОВСКИЙ КОМПОНЕНТ"

Информационная безопасность и защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Информационно-коммуникационных технологий в образовании		
Учебный план	ФКИ-626КЦо(4г) Направление подготовки: 44.03.01 Педагогическое образование Направленность (профиль): «Культурологическое образование и цифровая педагогика»		
Квалификация	бакалавр		
Форма обучения	очная		
Общая трудоемкость	2 ЗЕТ		
Часов по учебному плану	72	Виды контроля в семестрах: зачет 3	
в том числе:			
аудиторные занятия	24		
самостоятельная работа	48		

Распределение часов дисциплины по семестрам

Семестр(Курс.Номер семестра на курсе)	3(2.1)		Итого	
	УП	РПД	УП	РПД
Лекции	4	4	4	4
Практические	20	20	20	20
В том числе инт.	6	6	6	6
Итого ауд.	24	24	24	24
Контактная работа	24	24	24	24
Сам. работа	48	48	48	48
Итого	72	72	72	72

Программу составил(и):

Тараканова Е.Н.

При наличии обучающихся из числа лиц с ограниченными возможностями здоровья, которым необходим особый порядок освоения дисциплины (модуля), по их желанию разрабатывается адаптированная к ограничениям их здоровья рабочая программа дисциплины (модуля).

Рабочая программа дисциплины

Информационная безопасность и защита информации

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования – бакалавриат по направлению подготовки 44.03.01 Педагогическое образование. Утвержден приказом Министерства образования и науки Российской Федерации от 22 февраля 2018 г. № 121

составлена на основании учебного плана:

Направление подготовки: 44.03.01 Педагогическое образование

Направленность (профиль): «Культурологическое образование и цифровая педагогика»

утвержденного Учёным советом СГСПУ от 30.04.2026 г. протокол №9

Рабочая программа одобрена на заседании кафедры

Информационно-коммуникационных технологий в образовании

Протокол от 30.06.2026 г. №10

Зав. кафедрой Тараканова Е.Н.

Начальник УОП



Н.А. Доманина

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
Цель изучения дисциплины: обеспечить технологическую и правовую готовность к созданию безопасной информационно-образовательной среды и использованию различных методов и средств защиты информации; профессиональную готовность к реализации деятельности по защите информации и безопасному использованию программных средств при работе с информационными ресурсами. Задачи изучения дисциплины: • формирование знаний в области теоретических основ информационной безопасности, ознакомление с моделями возможных угроз безопасности информации и современными методами защиты информации и программного обеспечения; • освоение правовых основ и способов проектирования профессиональной сетевой среды на основе современных методов и средств защиты информации. Область профессиональной деятельности: 01 Образование и наука	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О.09
2.1 Требования к предварительной подготовке обучающегося:	
Содержание дисциплины базируется на материале:	
Программное обеспечение информационных систем	
2.2 Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Компьютерные сети и Web-проектирование	
Основы функционирования сети Интернет	
Электронные и дистанционные технологии в образовании	

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	
ОПК-9.2. Умеет применять современные информационно-коммуникационные технологии для решения профессиональных задач с учетом специфики предметной области; осуществлять выбор необходимых для осуществления профессиональной деятельности аппаратных и программных средств, мобильных приложений, средств сетевой коммуникации на основе стандартов и норм, принятых в профессиональной среде и с учетом требований информационной безопасности	
Знает: нормативно-правовую базу, методы и средства обеспечения информационной безопасности в профессиональной сетевой среде	
ПК-1. Способен осуществлять педагогическую деятельность по реализации образовательного процесса по предмету	
ПК-1.1. Умеет реализовывать образовательную программу по предмету с учетом специфики содержания, методов и инструментов соответствующей области научного знания	
Умеет: применять методы и средства организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения)	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часов	Интеракт.
	Раздел 1. Методы и средства обеспечения безопасности информации в профессиональной сетевой среде			
1.1	Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности. Нормативно-правовое обеспечение информационной безопасности /Лек/	3	2	0
1.2	Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности. Нормативно-правовое обеспечение информационной безопасности /Пр/	3	4	2
1.3	Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности. Нормативно-правовое обеспечение информационной безопасности /Ср/	3	10	0
1.4	Угрозы безопасности информации, их классификация. Криптографические методы обеспечения информационной безопасности /Лек/	3	2	0
1.5	Угрозы безопасности информации, их классификация. Криптографические методы обеспечения информационной безопасности /Пр/	3	6	2

1.6	Угрозы безопасности информации, их классификация. Криптографические методы обеспечения информационной безопасности /Ср/	3	14	0
Раздел 2. Защита информации в информационно-образовательной среде				
2.1	Технические средства защиты и комплексное обеспечение информационной безопасности. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде /Пр/	3	6	2
2.2	Технические средства защиты и комплексное обеспечение информационной безопасности. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде /Ср/	3	10	0
2.3	Понятие и классификация «вредоносных программ». Защита от «компьютерных вирусов. Программные и аппаратные методы защиты информации (персональной, коллективной, образовательного учреждения) /Пр/	3	4	0
2.4	Понятие и классификация «вредоносных программ». Защита от «компьютерных вирусов. Программные и аппаратные методы защиты информации (персональной, коллективной, образовательного учреждения) /Ср/	3	14	0

5. Оценочные и методические материалы по дисциплине (модулю)	
5.1. Содержание аудиторной работы по дисциплине (модулю)	
3 семестр, 2 лекции, 10 практических занятий Раздел 1. Методы и средства обеспечения безопасности информации в профессиональной сетевой среде Лекция №1 (2 часа) Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности. Нормативно-правовое обеспечение информационной безопасности Вопросы для обсуждения: 1. Понятие информационной безопасности и защищенной системы. Персональные данные как вид защищаемой информации. 2. Актуальность защиты информационных систем и телекоммуникаций. Цели, задачи, направления информационной безопасности. 3. Базовые принципы обеспечения информационной безопасности. 4. Информационная безопасность в условиях функционирования глобальных сетей. 5. Нормативно-правовые и законодательные акты в области информационной безопасности. Авторское право. Интеллектуальная собственность. Практические занятия №1-2 (4 часа) Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности. Нормативно-правовое обеспечение информационной безопасности Вопросы и задания: 1. Понятие информационной безопасности, эволюция понятия. 2. Нормативно-правовые и законодательные акты России в области информационной безопасности. 3. Справочные правовые системы. 4. Практическая работа по теме «Политика государств в области информационной безопасности». Лекция №2 (2 часа) Угрозы безопасности информации, их классификация. Криптографические методы обеспечения информационной безопасности Вопросы для обсуждения: 1. Понятие угрозы. Виды противников или «нарушителей». Виды возможных нарушений информационной системы. 2. Анализ угроз информационной безопасности. 3. Классификация видов угроз информационной безопасности по различным признакам (по природе возникновения, степени преднамеренности и т.п.). 4. Свойства информации: конфиденциальность, доступность, целостность. 5. Угроза раскрытия параметров системы, угроза нарушения конфиденциальности, угроза нарушения целостности, угроза отказа служб. Примеры реализации угроз информационной безопасности. 6. Причины, виды и каналы утечки конфиденциальной информации. 7. Методы и средства несанкционированного доступа к компьютерным ресурсам и программным средствам. 8. Понятие шифра. Симметричное и асимметричное шифрование. Электронная подпись. Практические занятия №3-5 (6 часов) Угрозы безопасности информации, их классификация. Криптографические методы обеспечения информационной безопасности Вопросы и задания: 1. Основные виды угроз информационной безопасности. 2. Последствия нарушения авторских прав на программное обеспечение и роль соответствующих правоохранительных организаций. 3. Практическая работа по теме «Угрозы безопасности информации».	

Раздел 2. Защита информации в информационно-образовательной среде

Практические занятия №6-8 (6 часов)

Технические средства защиты и комплексное обеспечение информационной безопасности. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде

Вопросы для обсуждения:

1. Основные задачи обеспечения защиты информации.
2. Основные методы и средства защиты информационных систем. Классификация способов и средств комплексной защиты информации. Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации.
3. Понятие политики безопасности информационных систем. Разработка и реализация политики безопасности.
4. Защита Интернет-подключений, функции и назначение межсетевых экранов (брандмауэров).
5. Идентификация и аутентификация. Парольные схемы аутентификации. Токены, смарт-карты, их применение. Использование биометрических данных при аутентификации пользователей.
6. Выполнение практической работы «Особенности защиты информации в локальных и глобальных компьютерных сетях».
7. Сервисы управления доступом. Механизмы доступа данных в операционных системах, системах управления базами данных. Ролевая модель управления доступом.
8. Протоколирование и аудит. Задачи и функции аудита. Структура журналов аудита. Активный аудит, методы активного аудита.
9. Парольные методы защиты информации. Программные средства для хранения паролей.
10. Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи.
11. Выполнение практической работы «Меры и методы по защите информации в образовательных организациях».

Практические занятия № 9-10 (4 часа)

Понятие и классификация «вредоносных программ». Защита от «компьютерных вирусов. Программные и аппаратные методы защиты информации (персональной, коллективной, образовательного учреждения)

Вопросы и задания:

1. Классификация «компьютерных вирусов». Общая организация защиты от «компьютерных вирусов». Защита от деструктивных действий и размножения вирусов с использованием средств аппаратного и программного контроля.
2. Антивирусное программное обеспечение. Компьютерные вирусы и антивирусная защита.
3. Парольная защита. Разграничение доступа. Средства родительского контроля.
4. Выполнение практической работы «Антивирусные средства защиты».

5.2. Содержание самостоятельной работы по дисциплине (модулю)

Содержание обязательной самостоятельной работы по дисциплине

№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1	Методы и средства обеспечения безопасности информации в профессиональной сетевой среде	Домашняя работа поисково-аналитического характера по теме «Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности».	Пост в сообществе в социальной сети по теме «Информационная безопасность в РФ»
		Самостоятельное изучение законодательных и нормативно-правовых актов в сфере электронной подписи, цифровых сертификатов, лицензирования деятельности удостоверяющих центров. Создание коллективного облачного документа, отражающего состояние нормативно-правовой базы по изучаемой теме в РФ.	Коллективный облачный документ
2	Защита информации в информационно-образовательной среде	Упорядочивание, приведение в единую систему знаний о современных программных и аппаратных методах защиты информации. Выявление причинно-следственных связей. Представление итогов работы в посте в сообществе в социальной сети.	Пост в сообществе в социальной сети
		Создание сайта на тему «Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде».	Сайт на тему «Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде»

		Классификация «вредоносных программ» и антивирусных программных средств. Составление ментальной карты (кластера, фишбоун-диаграммы и др.) по теме.	Ментальная карта, кластер, диаграмма причинно-следственных связей
Содержание самостоятельной работы по дисциплине на выбор студента			
№ п/п	Темы дисциплины	Содержание самостоятельной работы студентов	Продукты деятельности
1	Методы и средства обеспечения безопасности информации в профессиональной сетевой среде	Домашняя работа поисково-аналитического характера по теме «Информационная безопасность: концептуальные, практические, экономические, правовые, криптологические, математические, психологические, физические, программные и информационные основы».	Облачный документ
		Подготовка инфографики об источниках угроз информационной безопасности и способах совершения компьютерных преступлений.	Инфографика. Публичное выступление
2	Защита информации в информационно-образовательной среде	Подготовка мультимедийной презентации о политике безопасности и механизмах разграничения прав доступа к массивам информации в информационно-образовательной среде.	Презентация. Публичное выступление
		Создание индивидуального блога с обзором правовых и технологических аспектов электронной цифровой подписи и электронных сертификатов.	Индивидуальный блог
		Эссе рефлексивного характера по одной из проблем курса: «Использование методов социальной инженерии для получения доступа к информации»; «Особенности парольной защиты информации»; «О схемах функционирования компьютерных вирусов».	Пост в сообществе в социальной сети

5.3.Образовательные технологии

При организации изучения дисциплины будут использованы следующие образовательные технологии: информационно-коммуникационные технологии, технология организации самостоятельной работы, технология рефлексивного обучения, технология модульного обучения, технология игрового обучения, технологии групповой дискуссии, интерактивные технологии, технология проблемного обучения, технология организации учебно-исследовательской деятельности, технология проектного обучения, технология развития критического мышления.

5.4. Текущий контроль, промежуточный контроль и промежуточная аттестация

Балльно-рейтинговая карта дисциплины оформлена как приложение к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине оформлен отдельным документом.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

Дата обращения к электронным учебным изданиям, электронным образовательным ресурсам, современным базам данных и информационным справочным системам совпадает с датой утверждения рабочей программы

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
ЛП.1	Моргунов, А.В.	Информационная безопасность: учебно-методическое пособие URL: https://biblioclub.ru/index.php?page=book&id=576726	Новосибирск: Новосибирский государственный технический университет, 2019.
ЛП.12	Ищейнов, В. Я.	Информационная безопасность и защита информации: теория и практика: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=571485	Москва, Берлин: Директ-Медиа, 2020

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие, ссылка на электронную библиотечную систему	Издательство, год
--	---------------------	--	-------------------

Л2.1	Косолапов, Ю. В.	Криптографические протоколы на основе линейных кодов: учебное пособие. URL: https://biblioclub.ru/index.php?page=book&id=598671	Ростов-на-Дону; Таганрог: Южный федеральный университет, 2020
Л2.2	Литвиненко, О. В.	Правовые аспекты информационной безопасности: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=694774	Новосибирск: Сибирский государственный университет телекоммуникаций и информатики, 2021
Л2.3	Сидак А. А.	Информационная безопасность. Физические основы технических каналов утечки информации: учебное пособие URL: https://biblioclub.ru/index.php?page=book&id=694670	Москва: Директ-Медиа, 2022
Л2.4	Смирнов, В. И.	Защита информации: лабораторный практикум: практикум URL: https://biblioclub.ru/index.php?page=book&id=476512	Йошкар-Ола: Поволжский государственный технологический университет, 2017.

6.2 Перечень программного обеспечения

- Acrobat reader DC
- Dr.Web Desktop security, Dr.Web Server security
- GIMP
- Мой офис, сервисы Яндекс 360 для образования (почта, Яндекс Диск, Яндекс Телемост, Яндекс документы, Календарь)
- Многофункциональный сервис обмена информацией Max
- Архиватор 7-Zip
- Браузер Яндекс для организаций

6.3 Перечень информационных справочных систем, профессиональных баз данных

- ЭБС «Университетская библиотека онлайн»
- Базы данных Springer eBooks
- Единое содержание общего образования <https://edsoo.ru/>
- Библиотека цифрового образовательного контента <https://моиуроки.рф/>

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1	Наименование специального помещения: учебная аудитория для проведения занятий лекционного типа, практических занятий, групповых консультаций, индивидуальных консультаций, текущего контроля, промежуточной аттестации. Оснащенность: Комплект учебной мебели, меловая доска, ноутбук, переносное проекционное оборудование (мультимедийный проектор и экран на треноге), портативное звукоусиливающее оборудование. Наименование специального помещения: помещение для самостоятельной работы, Читальный зал. Оснащенность: ПК-4шт. с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду СГСПУ, Письменный стол-4 шт., Парты-2 шт. Для практических занятий – компьютерный класс.
-----	---

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Работа над теоретическим материалом происходит кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; пометить важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначить вопросы, термины, материал, который вызывает трудности, пометить и попытаться найти ответ в рекомендуемой литературе. Если самостоятельно не удастся разобраться в материале, необходимо сформулировать вопрос и задать преподавателю. Проработка рабочей программы дисциплины, уделяя особое внимание целям и задачам, структуре и содержанию дисциплины. Конспектирование источников, подготовка ответов к контрольным вопросам, просмотр рекомендуемой литературы, работа с информационными источниками в разных форматах. Также в процессе изучения дисциплины методические рекомендации могут быть изданы отдельным документом.

Балльно-рейтинговая карта дисциплины «Информационная безопасность и защита информации»

Курс 2 Семестр 3

Вид контроля		Минимальное количество баллов	Максимальное количество баллов
Раздел 1. Методы и средства обеспечения безопасности информации в профессиональной сетевой среде			
Текущий контроль по разделу:			
1	Аудиторная работа	8	10
2	Самостоятельная работа (специальные обязательные формы)	8	10
3	Самостоятельная работа (специальные формы на выбор)	4	8
Контрольное мероприятие по разделу		4	12
Промежуточный контроль		24	40
Раздел 2. Защита информации в информационно-образовательной среде			
Текущий контроль по разделу:			
1	Аудиторная работа	8	16
2	Самостоятельная работа (специальные обязательные формы)	10	20
3	Самостоятельная работа (специальные формы на выбор)	8	16
Контрольное мероприятие по разделу		6	8
Промежуточный контроль		32	60
Промежуточная аттестация			
Итого:		56	100

Виды контроля		Перечень или примеры заданий, критерии оценки и количество баллов	Темы для изучения и образовательные результаты
Текущий контроль по разделу «Методы и средства обеспечения безопасности информации в профессиональной сетевой среде»			
1	Аудиторная работа (10 баллов)	Практическая работа по теме «Политика государств в области информационной безопасности». Создание аннотированного каталога интернет-ресурсов по теме занятия. Критерии оценивания: 1. Репрезентативность ресурсов. 2. Соответствие выбранной тематике. 3. Научная новизна, доступность изложения. 4. Качество оформления каталога, выбор средств для его тиражирования. Каждый критерий оценивается в 1 балл. Итого: 4 балла Практическая работа по теме «Угрозы безопасности информации. Компьютерные преступления». Критерии оценивания: 1. Составлена таблица с: • классификаций угроз безопасности информации по различным признакам; • классификацией компьютерных преступлений и др.	Темы для изучения: Основные понятия информационной безопасности: аппаратные и программные средства обеспечения безопасности. Нормативно-правовое обеспечение информационной безопасности Угрозы безопасности информации, их классификация. Криптографические методы обеспечения информационной безопасности Образовательные результаты: Знает: нормативно-правовую базу, методы и средства обеспечения информационной безопасности в профессиональной сетевой среде Умеет: применять методы и средства организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения)

		2. Материал структурирован, информация полная, адекватная и актуальная. 3. Оформление задания соответствует требованиям. Каждый критерий оценивается в 2 балла. Итого: 6 баллов	
2	Самостоятельная работа (обязательные формы) (10 баллов)	Домашняя работа поисково-аналитического характера по теме «Основные понятия информационной безопасности. Нормативно-правовое обеспечение информационной безопасности». Критерии оценивания: 1. Содержание представленной информации осмысленно и интерпретировано в соответствии с поставленной задачей. 2. Результат представлен в лаконичной форме, удобной для восприятия. 3. Визуализированы результаты работы (опубликован пост по теме «Информационная безопасность в РФ» в сообществе в социальной сети). Каждый критерий оценивается по следующему правилу: • 0 баллов - критерий не выполнен; • 1 балл – выполнен частично; • 2 балла – выполнен полностью. Итого: 6 баллов Самостоятельное изучение законодательных и нормативно-правовых актов в сфере электронной подписи, цифровых сертификатов, лицензирования деятельности удостоверяющих центров. Создание коллективного облачного документа, отражающего состояние нормативно-правовой базы по изучаемой теме в РФ. Критерии оценивания: 1. Содержание представленной информации осмысленно и интерпретировано в соответствии с поставленной задачей. 2. Результат представлен в лаконичной форме, удобной для восприятия. Каждый критерий оценивается в 2 балла. Итого: 4 балла	
3	Самостоятельная работа (на выбор) (8 баллов)	Домашняя работа поисково-аналитического характера по теме «Информационная безопасность: концептуальные, практические, экономические, правовые, криптологические, математические, психологические, физические, программные и информационные основы». Составление словаря терминов в области информационной безопасности и перечня нормативных документов по информационной безопасности (облачный документ). Критерии оценивания: 1. Наполнение терминологического словаря. 2. Корректность цитирования источников. Грамотность содержания и оформления.	

		Каждый критерий оценивается в 2 балла. Итого: 4 балла	
		Подготовка инфографики и сообщения об источниках угроз информационной безопасности и способах совершения компьютерных преступлений. Критерии оценивания: 1. Информационная (содержательная) насыщенность продукта. 2. Авторская интерпретация содержания. 3. Уровень структуризации информации. 4. Адекватный выбор выразительных средств. 5. Выбор адекватного сервиса для представления инфографики. 6. Корректность цитирования источников. 7. Реализация технологических возможностей сервиса. 8. Работа выполнена на социальном сервисе (на выбор студента). Каждый критерий оценивается в 0,5 балла Итого: 4 балла	
Контрольное мероприятие по разделу (12 баллов)	Подготовка мультимедийной презентации и сообщения о криптографических методах обеспечения информационной безопасности. Работа выполнена на социальном сервисе (на выбор студента). Критерии оценивания: 1. Информационная (содержательная) насыщенность продукта. 2. Авторская интерпретация содержания. 3. Уровень структуризации информации. 4. Адекватный выбор выразительных средств. 5. Корректность цитирования источников. 6. Реализация технологических возможностей сервиса. Каждый критерий оценивается в 2 балла Итого: 12 баллов	Тема. Угрозы безопасности информации, их классификация. Криптографические методы обеспечения информационной безопасности. Образовательные результаты: Знает: нормативно-правовую базу, методы и средства обеспечения информационной безопасности в профессиональной сетевой среде Умеет: применять методы и средства организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения)	
Текущий контроль по разделу «Защита информации в информационно-образовательной среде»			
1	Аудиторная работа (16 баллов)	Выполнение практической работы «Особенности защиты информации в локальных и глобальных компьютерных сетях». Отчёт о выполнении практической работы. Критерии оценивания: • отчёт содержит полную информацию по изучаемым вопросам; • студент чётко и ясно объясняет методы защиты; • студент демонстрирует знания программных средств защиты информации при работе в компьютерных сетях; • студент демонстрирует навыки организации защиты при работе в компьютерных сетях. Каждый критерий оценивается в 2 балла	Темы для изучения: Технические средства защиты и комплексное обеспечение информационной безопасности. Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде Понятие и классификация «вредоносных программ». Защита от «компьютерных вирусов. Программные и аппаратные методы защиты информации (персональной, коллективной, образовательного учреждения) Образовательные результаты:

		Итого: 8 баллов	Знает: нормативно-правовую базу, методы и средства обеспечения информационной безопасности в профессиональной сетевой среде Умеет: применять методы и средства организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения)
		Выполнение практической работы «Меры и методы по защите информации в образовательных организациях». Отчёт о выполнении практической работы. Критерии оценивания: - отчёт содержит полную информацию по изучаемым вопросам; - студент чётко и ясно объясняет методы защиты; - студент демонстрирует знания программных средств защиты информации при работе в компьютерных сетях; - студент демонстрирует навыки организации защиты при работе в компьютерных сетях. Каждый критерий оценивается в 1 балл. Итого: 4 балла	
		Выполнение практической работы «Антивирусные средства защиты». Отчёт о выполнении практической работы. Критерии оценивания: - отчёт содержит полные ответы на контрольные вопросы; - студент чётко и ясно объясняет алгоритм действий пользователя при заражении компьютера вирусами; - студент демонстрирует знания способов профилактики заражения компьютера вирусами, многообразия антивирусных средств, их возможностей и особенностей приобретения, установки и использования; - студент демонстрирует навыки работы с антивирусной программой. Каждый критерий оценивается в 1 балл Итого: 4 балла	
2	Самостоятельная работа (обязательные формы) (20 баллов)	Составление ментальной карты (кластера, фишбоун-диаграммы и др.) по теме «Понятие и классификация компьютерных вирусов. Защита от компьютерных вирусов». Критерии оценивания: - Работа представляет собой результат изученного в аудитории материала. - В работе использован материал, не рассмотренный на практических занятиях. - Новизна и оригинальность работы. Каждый критерий оценивается в 2 балла. Итого: 6 баллов	
		Упорядочивание, приведение в единую систему знаний о современных программных и аппаратных методах защиты информации, о состоянии нормативно-правовой базы в сфере электронной цифровой подписи, цифровых сертификатов, лицензирования деятельности удостоверяющих центров. Выявление причинно-следственных связей. Представление итогов работы в посте в сообществе в социальной сети.	

		Критерии оценивания: • тема раскрыта полностью; • студент владеет материалом и демонстрирует знания при ответе на вопросы. Каждый критерий оценивается в 2 балла. Итого: 4 балла Создание сайта на тему «Политика безопасности и механизмы разграничения прав доступа к массивам информации в информационно-образовательной среде». Критерии оценивания: 1. Содержание – 5 баллов 1. Ясно ли предназначение сайта? 2. Присутствует ли информация на всех страницах (во всех разделах) сайта? 3. Ориентирован ли сайт на целевую аудиторию? 4. Соответствует ли содержание сайта (текстовое, графическое) его тематике? 5. Есть ли грамматические или синтаксические ошибки? 2. Эргономичность использования – 2 балла 1. Организовано ли содержание логически? 2. Насколько проста и понятна навигация? 3. Расположена ли навигация в одном и том же месте на всех страницах? 4. Позволяет ли навигация вернуться на предыдущие подуровни? 3. Внешний вид (дизайн) – 3 балла 1. Выдержаны ли цвета, шрифты, графика в едином стиле? 2. Сбалансированы ли цвета дизайна страниц? 3. Сбалансирован ли макет страницы (наличие сетки)? 4. Не перегружена ли страница информацией (особенно касается главных страниц)? 5. Качественна ли графика и сочетается ли она с остальными составляющими страницы? 6. Не мешает ли графика пользователю воспринимать информацию Итого: 10 баллов	
3	Самостоятельная работа (на выбор) (16 баллов)	Подготовка мультимедийной презентации о классификации и схемах функционирования компьютерных вирусов или антивирусных программных средствах. Критерии оценивания: 1. Полнота раскрытия темы. 2. Актуальность материалов, отражающих современный уровень состояния вопроса. 3. Оригинальность изложения идеи, наличие интересных фактов. 4. Дизайн оформления визуального ряда (презентации и т.д.). 5. Логичность, последовательность изложения, отсутствие информации, не относящейся к теме. 6. Отсутствие синтаксических, стилистических и орфографических ошибок.	

	Каждый критерий оценивается в 1 балл. Итого: 6 баллов Эссе рефлексивного характера по одной из проблем курса: • «Использование методов социальной инженерии для получения доступа к информации»; • «Особенности парольной защиты информации»; • «О схемах функционирования компьютерных вирусов». Критерии оценивания: 1. Отражена глубина изучения проблемы, проведен ее многофакторный анализ. 2. Работа отражает личное видение автора проблемы и пути ее решения. 3. Соответствие стилю эссе. 4. Содержание эссе опубликовано в сообществе в социальной сети. Каждый критерий оценивается в 1 балл. Итого: 4 балла Создание индивидуального блога с обзором правовых и технологических аспектов электронной цифровой подписи и электронных сертификатов. Критерии оценивания: 1. Технологичность (наличие навигационных элементов (облако тегов, аннотация содержания и пр., целесообразность используемых дополнений, расширений, гаджетов и т.п.). 2. Социальность (блог ориентирован на профессиональную сферу). Каждый критерий оценивается в 3 балла. Итого: 6 баллов	
Контрольное мероприятие по разделу (8 баллов)	Создание поста с обзором и анализом мер и методов по защите информации в образовательных организациях. Итого: 8 баллов	Образовательные результаты: Образовательные результаты: Знает: нормативно-правовую базу, методы и средства обеспечения информационной безопасности в профессиональной сетевой среде Умеет: применять методы и средства организационно-правовой защиты информации в информационно-образовательной среде (персональной, коллективной, образовательного учреждения)
Промежуточная аттестация	Представлены в фонде оценочных средств для промежуточной аттестации по дисциплине	