МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ

Филиал государственного бюджетного образовательного учреждения высшего образования
«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ»
в г. Железноводске

Кафедра гуманитарных и социально- экономических дисциплин

УТВЕРЖДАЮ
Заведующий кафедрой
М.Н. Арутюнян
протокол № 11
от 24.06.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

Кибербезопасность

(наименование учебной дисциплины)

Уровень основной образовательной программы

бакалавриат

Направление(я) подготовки (специальность)

44.03.05 Педагогическое образование (с двумя профилями подготовки), профили "Дошкольное образование" и "Начальное образование"

Форма обучения заочная

Срок освоения 5 лет 6 месяцев

Кафедра Кафедра гуманитарных и социально- экономических дисциплин

Год начала подготовки 2022

Железноводск, 2025 г.

Программу составил(-и): кандидат педагогических наук, доцент кафедры гуманитарных и социально-экономических дисциплин, Буракова Ирина Сергеевна

Рабочая программа дисциплины "Кибербезопасность" разработана в соответствии с ФГОС: Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 44.03.05 Педагогическое образование (с двумя профилями подготовки) (приказ Минобрнауки России от 22.02.2018 г. № 125).

Рабочая программа дисциплины составлена на основании учебного плана: 44.03.05 Педагогическое образование (с двумя профилями подготовки), профили "Дошкольное образование" и "Начальное образование", утвержденного учёным советом вуза от 25.06.2025, протокол № 7.

Рабочая программа одобрена на заседании кафедры Кафедра гуманитарных и социально-экономических дисциплин от 24.06.2025 г., протокол № 11 для исполнения в 2025-2026 учебном году.

Зав. кафедрой _____ М.Н. Арутюнян

Рабочая программа дисциплины согласована с заведующим библиотекой.

Зав. библиотекой _____ Клименко А.В. 24.06.2025 г.

Срок действия рабочей программы дисциплины: 2025-2026 учебный год.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

формирование целостного представления о роли современного киберпространства в образовательной среде и педагогической деятельности; формирование системы знаний, умений и навыков для обеспечения кибербезопасности своей профессиональной деятельности.

2. ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

формирование общих представления о безопасности в информационном обществе; изучение общих принципов технологий, применяемых в информационной безопасности; формирование умения применять правила кибербезопасности во всех сферах деятельности; освоение знаний, составляющих начала представлений об информационной картине мира и информационных процессах; овладение умением использовать компьютерную технику как практический инструмент для работы с информацией в повседневной жизни; развитие навыков ориентирования в информационных потоках.

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Цикл (раздел) ООП:	Б1.В.ДВ.01

3.1. Требования к предварительной подготовке обучающегося:

Безопасность жизнедеятельности
Математика и информатика
Методика преподавания русского языка в начальной школе с практикумом
Методика самостоятельной работы студента
Методы исследовательской и проектной деятельности
Методы математической обработки данных
Основы естествознания и обществознания
Основы медицинских знаний
Основы педиатрии и гигиена детей раннего и дошкольного возраста
Русский язык
Технологии цифрового образования
Учебная (ознакомительная) практика
Учебная практика (научно-исследовательская работа (получение первичных навыков научно-
Философия

3.2. Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Выполнение и защита выпускной квалификационной работы
Образовательные программы дошкольного образования
Основы военной подготовки
Подготовка к сдаче и сдача государственного экзамена
Производственная (педагогическая) практика 5
Производственная практика (научно-исследовательская работа)
Теория и методика организации дистанционного обучения в образовательных организациях

4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации,	УК-1.1 Демонстрирует знание особенностей системного и критического мышления,
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной	УК-8.1 Оценивает факторы риска, умеет обеспечивать личную безопасность и

В результате освоения дисциплины обучающийся должен:

знать:	**уметь:**	**владеть:**

особенности системного и критического мышления, аргументированное формирование собственного суждения и оценки информации, принятие обоснованного решения.	применять логические формы и процедуры, способен к рефлексии по поводу собственной и чужой мыслительной деятельности; оценивать факторы риска, обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности.	анализа источников информации с целью выявления их противоречий и поиска достоверных суждений; применения методов защиты в чрезвычайных ситуациях и в условиях военных конфликтов, формирования культуры безопасного и ответственного поведения.

5. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины составляет 2 зачетные (-ых) единиц (-ы) (72), включая промежуточную аттестацию.

Распределение часов дисциплины по курсам

Курс	4		Итого	
Вид занятий	УП	РП		
Лекции	2	2	2	2
Практические	4	4	4	4
Контактная работа на промежуточную аттестацию	0,3	0,3	0,3	0,3
Итого ауд.	6	6	6	6
Контактная работа	6,3	6,3	6,3	6,3
Сам. работа	65,7	65,7	65,7	65,7
Итого	72	72	72	72

6. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ ПО РАЗДЕЛАМ (ТЕМАМ) И ВИДАМ ЗАНЯТИЙ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Примечание
	Раздел 1. Обеспечение информационной безопасности государства и общества					
1.1	Кибербезопасность в системе национальной безопасности РФ /Тема/	4	0			
1.2	Кибербезопасность в системе национальной безопасности РФ /Ср/	4	10	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
1.3	Киберпреступления против личности, общества и государства /Тема/	4	0			
1.4	Киберпреступления против личности, общества и государства /Ср/	4	11	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
	Раздел 2. Понятие информации и информационная безопасности					

2.1	Современное киберпространство Техника безопасности в киберпространстве /Тема/	4	0			
2.2	Современное киберпространство Техника безопасности в киберпространстве /Лек/	4	2	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
2.3	Современное киберпространство Техника безопасности в киберпространстве /Пр/	4	2	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
2.4	Современное киберпространство Техника безопасности в киберпространстве /Ср/	4	14	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
2.5	Проблемы Интернет-зависимости, кибербуллинга /Тема/	4	0			
2.6	Проблемы Интернет-зависимости, кибербуллинга /Пр/	4	2	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
2.7	Проблемы Интернет-зависимости, кибербуллинга /Ср/	4	14	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
2.8	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы /Тема/	4	0			
2.9	Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы /Ср/	4	16,7	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	
2.10	Зачет /КПА/	4	0,3	УК-8.1 УК-8.2 УК-1.1 УК-1.2 УК-1.3	Л1.1Л2.1	

* - Тема изучается с учетом профессиональной направленности

Планы проведения учебных занятий отражены в оценочных материалах (Приложение 2.).

7. КОНТРОЛЬ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль качества освоения учебного материала по дисциплине проводится в форме текущего контроля успеваемости и промежуточной аттестации в соответствии с «Положением о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации

обучающихся в ГБОУ ВО СГПИ и его филиалах».

Для аттестации обучающихся на соответствие их персональных достижений требованиям образовательной программы используются оценочные материалы текущего контроля успеваемости и промежуточной аттестаций (Приложение 2).

Уровень сформированности компетенции			
не сформирована	**сформирована частично**	**сформирована в целом**	**сформирована полностью**
«Не зачтено»	**«Зачтено»**		
«Неудовлетворительно»	**«Удовлетворительно»**	**«Хорошо»**	**«Отлично»**
Описание критериев оценивания			
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания.	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания теоретического материала. - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; Возможны незначительные неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебно-методическое обеспечение дисциплины включает рабочую программу дисциплины, методические материалы, оценочные материалы.

Учебно-методическое обеспечение самостоятельной работы обучающихся включает: учебники, учебные пособия, электронные образовательные ресурсы, методические материалы.

Самостоятельная работа обучающихся является формой организации образовательного процесса по дисциплине и включает следующие виды деятельности: поиск (подбор) и обзор научной и учебной литературы, электронных источников информации по изучаемой теме; работа с конспектом лекций, электронным учебником, со словарями и справочниками и др. источниками информации (конспектирование); составление плана и тезисов ответа; подготовка реферата; выполнение творческих заданий и проблемных ситу-аций; подготовка к коллоквиуму, собеседованию, практическим занятиям; подготовка к зачету и экзамену.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

9.1. Рекомендуемая литература

9.1.1. Основная литература

Л1.1	Голубин Р. В., Исакова И. А., Коротышев А. П., Косарева Н. С., Рыхтик П. П. Кибербезопасность подростков в сети интернет. Противодействие киберугрозам [Электронный ресурс]:учебно-методическое пособие. - Нижний Новгород: ННГУ им. Н. И. Лобачевского, 2022. - 65 с. – Режим доступа: https://e.lanbook.com/book/283286

9.1.2. Дополнительная литература

Л2.1	Ванина А. Г., Орёл Д. В., Аникуев С. В. Персональная кибербезопасность: курс лекций [Электронный ресурс]:учебное пособие. - Ставрополь: СКФУ, 2022. - 137 с. – Режим доступа: https://e.lanbook.com/book/386636

10.1 Интернет-ресурсы (базы данных, информационно-справочные системы и др.)

ЭБС «Лань»	https://e.lanbook.com
Национальная электронная библиотека (НЭБ)	https://rusneb.ru
ЭБС «Юрайт»	https://urait.ru
ЭБС «Журнальный зал»: русский толстый журнал как эстетический феномен	https://magazines.gorky.media
«Электронная библиотека ИМЛИ РАН»	http://biblio.imli.ru
«Электронная библиотека ИРЛИ РАН» (Пушкинский Дом)	http://lib.pushkinskijdom.ru
Научный архив	https://научныйархив.рф
ЭБС «Педагогическая библиотека»	http://pedlib.ru
ЭБС «Айбукс.ру»	https://www.ibooks.ru
Научная электронная библиотека eLibrary.ru	https://elibrary.ru
ЭБС Буконлайм	https://bookonlime.ru
Научная электронная библиотека «Киберленинка»	https://cyberleninka.ru/
Государственная публичная научно-техническая библиотека России. Ресурсы открытого доступа	http://www.gpntb.ru/elektronnye-resursy-udalennogo-dostupa/1874-1024.html
Библиотека академии наук (БАН). Ресурсы открытого доступа	http://www.rasl.ru/e_resours/resursy_otkrytogo_dostupa.php

10.2. Профессиональные базы данных и информационные справочные системы

Университетская информационная система	https://uisrussia.msu.ru

РОССИЯ	
Единое окно доступа к образовательным ресурсам	http://window.edu.ru/catalog
Словари и энциклопедии	https://dic.academic.ru
Педагогическая мастерская «Первое сентября»	https://fond.1sept.ru
Сайт Единой коллекции цифровых образовательных ресурсов	http://school-collection.edu.ru
Национальная платформа «Открытое образование»	https://openedu.ru
Портал «Единая коллекция цифровых образовательных ресурсов»	http://school-collection.edu.ru
Российское образование. Федеральный портал	http://edu.ru
Портал Федеральных государственных образовательных стандартов высшего образования	http://fgosvo.ru
Единая цифровая коллекция первоисточников научных работ удостоверенного качества «Научный архив»	https://научныйархив.рф
Портал проекта «Современная цифровая образовательная среда в РФ»	https://online.edu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Занятия, текущий контроль успеваемости и промежуточная аттестация по дисциплине проводятся в учебных аудиториях, укомплектованных типовой мебелью для обучающихся и преподавателя, техническими и мультимедийными средствами обучения, включенными в локальную сеть вуза и с доступом к информационным ресурсам сети Интернет.

Рабочие места для самостоятельной работы обучающихся оснащены компьютерной техникой с подключением к сети Интернет и обеспечены доступом в электронную информационно-образовательную среду вуза.

Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение:

1. Пакет программного обеспечения общего назначения Microsoft Office (MS Word, MS Microsoft Excel, MS PowerPoint).
2. Adobe Acrobat Reader.
3. Браузер (Internet Explorer, Mozilla Firefox, Google Chrome, Opera и др.).
4. Программа тестирования Айрен.

Приложение 1

Методические материалы по дисциплине «Кибербезопасность»

1. Планы практических работ и методические рекомендации

Тема 3. Современное киберпространство Техника безопасности в киберпространстве
Практическое занятие 3.1.
Вопросы для обсуждения

1. Мошеннические действия в Интернете. Киберпреступления
2. Сетевой этикет. Психология и сеть
3. Правовые аспекты защиты киберпространства
4. Онлайн сервисы для безопасности пользователя в ин-тернете (проверка компьютера и файлов на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС и др.).
5. Настройки безопасности почтовых программ.
6. Защита в поисковых системах (фильтры для ограничения потенци-ально опасного содержимого).
7. Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.).
8. Электронная почта и системы мгновенного обмена сообщениями.
9. Настройки безопасности Скайп, ICQ и пр. Способы обеспечения безопасности веб-сайта.
10. Киберпреступления. Виды интернет-мошенничества (письма, рек-лама, охота за личными данными и т.п.). Опасности мобильной связи. Предложения по установке вредоносных приложений.
11. Мошеннические СМС. Утечка и обнародование личных данных. Подбор и перехват паролей.
12. Взломы аккаунтов в социальных сетях. Виды мошенничества в Интернете. Фишинг (фарминг). Азартные игры.
13. Ложные антивирусы. Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.
14. Электронный кошелек. Мошенничество при распространении «бесплатного» ПО.
15. Технологии манипулирования в Интернете.
16. ТБ при интернет-общении.

Тема 4. Проблемы Интернет-зависимости, кибербуллинга
Практическое занятие 4.1.
Вопросы для обсуждения

1. Гигиена компьютера.
2. Компьютер и кровообращение.
3. Польза и вред компьютерных игр.
4. Компьютер и ЗОЖ.
5. Физическое и психическое здоровье.
6. Правила поведения в компьютерном классе.
7. Интернет в системе безопасности.
8. Техника безопасности при работе с компьютером.
9. Компьютер и мобильные устройства в чрезвычайных ситуациях.
10. Медицинская информация в Интернете. Компьютеры и мобильные устройства в экстремальных условиях.

11. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).
12. Комплекс упражнений при работе за компьютером.
13. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.
14. Компьютер в режиме труда и отдыха.
15. Влияние компьютера на репродуктивную систему.
16. Вредные факторы работы за компьютером и их последствия.

Тема 5. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

Практическое занятие 5.1.

1. Контент-фильтры.
2. Поисковые серверы.
3. Признаки заражения компьютера.
4. Антивирусная защита.
5. Защита файлов. Безопасность при скачивании файлов.
6. Защита программ и данных от несанкционированного копирования.
7. Организационные, юридические, программные и программно-аппаратные меры защиты.
8. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п.
9. Неперемещаемые программы.
10. Защита от копирования контента сайта.
11. Источники заражения ПК.
12. Антивирусное ПО, виды и назначение. Методы защиты от вирусов.

2. Задания для самостоятельной работы

Тема 1. Кибербезопасность в системе национальной безопасности РФ
Подготовить доклад по теме:

1. Информационная война. Информационное оружие.
2. Патриотизм и интернет.
3. Информационное воздействие.

Тема 2. Киберпреступления против личности, общества и государства
Подготовить доклад по теме:

1. Реальная и виртуальная личность.
2. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибермоббинг, троллинг, буллицид.

Тема 3. Современное киберпространство Техника безопасности в киберпространстве
Подготовить доклад по теме:

1. Электронный кошелек.
2. Мошенничество при распространении «бесплатного» ПО.
3. Правила поведения в скайпе.
4. Форум. Правила поведения

Тема 4. Проблемы Интернет-зависимости, кибербуллинга
Подготовить доклад по теме:

1. Виды Интернет-зависимости.
2. Киберкультура (массовая культура в сети) и личность.
3. Психологическое воздействие информации на человека

Тема 5. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы
Подготовить доклад по теме:

1. Меры безопасности для пользователя WiFi. Настройка безопасности.
2. Вирусы для мобильных устройств (мобильные банкеры и др.).

3. Примерные темы рефератов

1. Информация - фактор существования и развития общества. Основные формы проявления информации, её свойства как объекта безопасности.
2. Понятие безопасности и её составляющие. Безопасность информации.
3. Обеспечение информационной безопасности: содержание и структура понятия.
4. Национальные интересы в информационной сфере.
5. Источники и содержание угроз в информационной сфере.
6. Соотношение понятий «информационная безопасность» и «национальная безопасность»
7. Риск работы на персональном компьютере. Планирование безопасной работы на персональном компьютере.
8. Информация - фактор существования и развития общества.
9. Цели и задачи защиты информации.
10. Организация защиты конфиденциальной информации.
11. Виды защищаемой информации в сфере государственного и муниципального управления.
12. Уровни ведения информационной войны. Оперативная маскировка. Радиоэлектронная борьба. Воздействие на сети.
13. Основные положения государственной информационной политики Российской Федерации.

Приложение 2

Оценочные материалы по дисциплине « Кибербезопасность»

1. Оценочные материалы для текущего контроля

1.1. Тестовые материалы

Тест 1

1. Информационная безопасность зависит от:
а) компьютеров, поддерживающей инфраструктуры +
б) пользователей
в) информации
2. Таргетированная атака – это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия +
в) атака на конкретный компьютер пользователя
3. Stuxnet – это:
а) троянская программа
б) макровирус
в) промышленный вирус +
4. Основная масса угроз информационной безопасности приходится на:
а) Троянские программы +
б) Шпионские программы
в) Черви
5. Под какие системы распространение вирусов происходит наиболее динамично:
а) Windows
б) Mac OS
в) Android +
6. Какой вид идентификации и аутентификации получил наибольшее распространение:
а) системы PKI
б) постоянные пароли +
в) одноразовые пароли
7. Какие угрозы безопасности информации являются преднамеренными:
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ +
8. Что такое «оффтоп»:
а) сообщение не по теме форума +
б) часть гардероба
в) футбольный термин
9. Системой криптографической защиты информации является:
а) BFox Pro
б) CAudit Pro
в) Крипто Про +
10. СПАМ:
а) агрессивное поведение на форумах
б) массовая рассылка рекламы и прочих объявлений +
в) цепочка непонятных, нелогичных объяснений
11. Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы +

б) троянцы
в) черви
12. Переведите на язык Интернета выражение «лить воду»:
а) флейм
б) флуд +
в) СПАМ
13. «Словесная война», возникающая иногда на форумах:
а) флейм +
б) СПАМ
в) флуд
14. Для выделения наиболее значимых слов в тексте используют:
а) курсив
б) подчеркивание
в) жирный шрифт +
15. Набор слов ЗАГЛАВНЫМИ буквами служит:
а) для выражения сильных эмоций +
б) для обозначения чего-то большого
в) для привлечения внимания собеседника к главному в высказывании
RELAP
RELAP
16. Нормы общения в сети Интернет:
а) интекет
б) нетикет +
в) этикет
17. Выберите верное утверждение.
Авторские посты, размещаемые пользователями в социальных сетях и блогах:
а) никогда не содержат персональной информации, поэтому их публикация не несет серьезных последствий
б) всегда содержат излишнюю персональную информацию о человеке, что может навредить не только его репутации, но и личной безопасности
в) оцениваются читателями по-разному, поэтому невозможно предсказать, как публикация поста отразится на репутации его автора +
18. Укажите устройство для подключения компьютера к сети:
а) мышь
б) модем +
в) сканер
19. При просмотре веб-сайтов и общении через Интернет:
а) Вы оставляете электронные следы, которые можно удалить самому
б) Вы оставляете электронные следы, которые хранятся только на Вашем компьютере
в) Вы оставляете электронные следы («цифровые отпечатки»), по которым можно определить, какие страницы Вы просматривали и какой IP-адрес компьютера Вы использовали +
20. Главной функцией брандмауэра является:
а) пополнительное офисное приложения для работы с базами данных
б) защита компьютера от взлома хакерами, а также всевозможных вирусов и «троянов» +
в) упрощение и оптимизация работы операционной системы

21. Что НЕ поможет защитить свою электронную почту от взлома:
а) периодически менять адрес электронной почты, менять провайдеров +
б) создавать разные пароли от разных аккаунтов
в) не открывать сообщения с незнакомых и подозрительных адресов

22. Когда можно полностью доверять новым онлайн-друзьям:
а) поговорив по телефону
б) ничего не может дать 100 %-ную гарантию того, что онлайн-другу можно доверять +
в) после обмена фотографиями
23. Что делать, если вам пришло письмо о том, что вы выиграли в лотерее:
а) связаться с отправителем по телефону
б) перейти по ссылке в письме, ведь информация может оказаться правдой
в) удалить его и заблокировать отправителя +
24. Какую информацию о себе можно выкладывать в Интернете в открытом доступе:
а) место работы родителей
б) о своих интересах +
в) номер телефона
25. Как защититься от негативного контента:
а) обратиться к автору негативного контента
б) не обращать на него внимания
в) использовать безопасный поиск Google и безопасный режим на YouTube +
26. В каком случае нарушается авторское право:
а) при использовании материалов Википедии для подготовки доклада со ссылкой на источник
б) при размещении на YouTube собственного видеоролика с концерта какой-либо группы +
в) при просмотре трансляций на официальном сайте телеканала
27. Троянская программа опасна тем, что:
а) проникает на компьютер под видом полезной программы и выполняет вредоносные действия без ведома пользователя +
б) обладает всеми вышеперечисленными возможностями
в) вынуждает пользователя возвращать долги данайцев
28. Клавиатурный шпион:
а) юридический термин, используемый для обозначения правонарушений, связанных с информационной безопасностью
б) физический термин, используемый для обозначения правонарушений, связанных с информационной безопасностью
в) программа, отслеживающая ввод пользователем паролей и пин-кодов +
29. Что не является персональными данными:
а) история болезни +
б) паспортные данные
в) фамилия, имя, отчество
30. Что делать, если вы стали жертвой интернет-травли:
а) сыпать угрозами в ответ, предлагать встретиться и разобраться
б) обратиться в администрацию ресурса с просьбой наказать обидчика +
в) выкинуть компьютер

Тест 2

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы
3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная
4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных
20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
- Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальностьl
23) Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
- Защищаемой
25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети
27) Политика безопасности в системе (сети) – это комплекс:
- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети
28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

Критерии оценки:
Для **оценки результатов тестирования** предусмотрена следующая система оценивания учебных достижений студентов:

За каждый правильный ответ ставится 1 балл,
За неправильный ответ – 0 баллов.

Если студент набирает

от 85 до 100 % правильных ответов ему выставляется оценка «отлично»;
от 72 до 84 % правильных ответов – оценка «хорошо»,
от 51 до 71 % правильных ответов – оценка «удовлетворительно»,
менее 50 баллов – оценка «неудовлетворительно».

1.2. Вопросы для собеседования

Тема 1. Кибербезопасность в системе национальной безопасности РФ

1. Государственная политика в области кибербезопасности компьютерным атакам от 15 января 2013 г.
2. Уголовный кодекс РФ, раздел «Преступления в сфере компьютерной информации».
3. Защита киберпространства государством. Кибервойна.
4. Право на информацию в Конституции РФ.
5. Защита государства и защита киберпространства.
6. Доктрина информационной безопасности.
7. Кибервойска. Защита киберпространства как одна из задач вооруженных сил.
8. Информационная война. Информационное оружие.
9. Патриотизм и интернет.
10. Информационное воздействие.
11. Военная, государственная, коммерческая тайна.
12. Защита сайтов государственных органов (электронное правительство).

Тема 2. Киберпреступления против личности, общества и государства

1. Реальная и виртуальная личность.
2. Психологическая обстановка в Интернете: грифинг, кибербуллинг, кибермоббинг, троллинг, буллицид.
3. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.).

4. Термины сетевого этикета: оверквотинг, флейм, флуд, оффтопик, смайлики и др.
5. Примеры этических нарушений. Значение сетевого этикета.
6. Собственность в Интернете. Авторское право.
7. Интеллектуальная собственность.
8. Платная и бесплатная информация.
9. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера.
10. Ответственность за интернет-мошенничество.
11. Правовые акты в области информационных технологий и защиты киберпространства. Ответственность за киберпреступления.
12. Конституционное право на поиск, получение и распространение информации. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию» (действует с 1 сентября 2012 года).
13. Информационное законодательство РФ.
14. Закон РФ «Об информации, информационных технологиях и о защите информации». Уголовная ответственность за создание, использование и распространение вредоносных компьютерных программ (ст. 237 УК РФ). Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo).
15. Правовые основы для защиты от спама.
16. Правовая охрана программ для ЭВМ и БД. Лицензионное ПО. Виды лицензий (OEM, FPP, корпоративные лицензии, подписка). ПО с открытым кодом (GNU GPL, FreeBSD).
17. Право на информацию, на сокрытие данных, категории информации.
18. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных».

Тема 3. Современное киберпространство Техника безопасности в киберпространстве

1. Мошеннические действия в Интернете. Киберпреступления
2. Сетевой этикет. Психология и сеть
3. Правовые аспекты защиты киберпространства
4. Онлайн сервисы для безопасности пользователя в интернете (проверка компьютера и файлов на вирусы онлайн, онлайн деактивация SMS-вирусов, проверка сайта на вирусы, проверка файлов по e-mail, определение адреса страницы, проверка стоимости СМС и др.).
5. Настройки безопасности почтовых программ.
6. Защита в поисковых системах (фильтры для ограничения потенциально опасного содержимого).
7. Настройки безопасности веб-браузеров (Internet Explorer, Firefox и т.п.).
8. Электронная почта и системы мгновенного обмена сообщениями.
9. Настройки безопасности Скайп, ICQ и пр. Способы обеспечения безопасности веб-сайта.
10. Киберпреступления. Виды интернет-мошенничества (письма, рек-лама, охота за личными данными и т.п.). Опасности мобильной связи. Предложения по установке вредоносных приложений.
11. Мошеннические СМС. Утечка и обнародование личных данных. Подбор и перехват паролей.
12. Взломы аккаунтов в социальных сетях. Виды мошенничества в Интернете. Фишинг (фарминг). Азартные игры.
13. Ложные антивирусы. Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.

14. Электронный кошелек. Мошенничество при распространении «бесплатного» ПО.
15. Технологии манипулирования в Интернете.
16. ТБ при интернет-общении.
17. ТБ при регистрации на веб-сайтах.
18. Компьютерное пиратство. Плагиат.

Тема 4. Проблемы Интернет-зависимости, кибербуллинга

1. Техника безопасности при работе с компьютером.
2. Компьютер и мобильные устройства в чрезвычайных ситуациях.
3. Медицинская информация в Интернете. Компьютеры и мобильные устройства в экстремальных условиях.
4. Воздействие радиоволн на здоровье и окружающую среду (Wi-Fi, Bluetooth, GSM).
5. Комплекс упражнений при работе за компьютером.
6. Воздействие на зрение ЭЛТ, жидкокристаллических, светодиодных, монохромных мониторов.
7. Компьютер в режиме труда и отдыха.
8. Влияние компьютера на репродуктивную систему.
9. Вредные факторы работы за компьютером и их последствия.
10. Организация рабочего места
11. Интернет-сообщество.
12. Интернет-зависимость.
13. Социальные сети. Детские социальные сети.
14. Виртуальная личность.
15. Зависимость от Интернет-общения.
16. Развлечения в Интернете.
17. Признаки игровой зависимости.
18. Сетевые игры.
19. Сайты знакомств. ЗОЖ и компьютер.
20. Виды зависимости. Деструктивная информация в Интернете.
21. Виды Интернет-зависимости.
22. Киберкультура (массовая культура в сети) и личность.
23. Критерии зависимости (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив).
24. Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения).
25. Классификация интернет-зависимостей

Тема 5. Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы

1. Признаки заражения компьютера.
2. Антивирусная защита.
3. Защита файлов. Безопасность при скачивании файлов.
4. Защита программ и данных от несанкционированного копирования.
5. Организационные, юридические, программные и программно-аппаратные меры защиты.
6. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п.
7. Неперемещаемые программы.
8. Защита от копирования контента сайта.
9. Источники заражения ПК.

10. Антивирусное ПО, виды и назначение. Методы защиты от вирусов.
11. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.).
12. Проверка подлинности (аутентификация) в Интернете.
13. Меры безопасности для пользователя WiFi. Настройка безопасности.
14. Вирусы для мобильных устройств (мобильные банкеры и др.).
15. Настройка компьютера для безопасной работы. Ошибки пользователя.
16. Простые и динамически изменяющиеся пароли. Борьба с утечками информации.
17. Средства контроля доступа. Права пользователей. Способы разграничения доступа.
18. Отличия вирусов и закладок.
19. Антивирусные программы для ПК: сканеры, ревизоры и др.

Критерии оценки:
оценка «отлично» выставляется студенту, если он продемонстрировал полноту и глубину знаний по всем вопросам, знает основные термины по контролируемым темам, владеет знаниями об основных особенностях решения задач. Умеет применять полученные знания для решения конкретных практических задач.
оценка «хорошо» выставляется студенту, который продемонстрировал полноту и глубину знаний по всем вопросам раздела, логично излагает материал.
оценка «удовлетворительно» выставляется студенту, при наличии у него знаний основных категорий и понятий по предмету, умения достаточно грамотно изложить материал.
оценка «неудовлетворительно» выставляется студенту, который не освоил основного содержания предмета, не владеет знаниями дисциплине.

1.3. Критерии оценки реферата

Критериями оценки реферата могут выступить следующие моменты:
- в какой мере раскрывается актуальность темы;
- каков теоретический уровень суждений автора, как владеет он современными методологическими основами наук при освещении поставленных в реферате вопросов;
- соответствие структуры и содержания реферата плану;
- целостное, глубокое понимание вопросов темы или разрабатываемой проблемы;
- как удалось автору связать излагаемые в реферате вопросы теории с проблемами сегодняшнего дня, умение использовать теоретические источники и учебно-методическую литературу;
- достаточно ли проявлена автором самостоятельность в постановке вопросов, в трактовке их, есть ли в работе оригинальные мысли, свежие факты, описание лучшего опыта работы, конкретных примеров из практики, соответствующие рекомендации и предложения;
- излагается ли в реферате собственное понимание рассматриваемой проблемы, достаточна ли его аргументация;
- как оформлен реферат или доклад (объем, наличие плана, содержательность введения, полнота списка используемой литературы, наличие приложений, анализа опыта работы, схем, таблиц, диаграмм, планов, анкет и т.д.);
- имеет ли работа определенную ценность, чтобы рекомендовать ее в фонд учебных пособий по курсам.

Реферат оценивается по 4-х балльной системе - «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

1.4. Критерии оценки презентации

Балльное выражение оценки презентации:

№	*Критерии оценки компонентов презентации*	*Баллы (максимальное количество при полной выраженности критерия*
	Структура презентации	
1.	Правильное оформление титульного листа	4
2.	Наличие понятной навигации	4
3.	Отмечены информационные ресурсы	4
4.	Логическая последовательность информации на слайдах	4
	Оформление презентации	
5.	Единый стиль оформления	5
6.	Использование на слайдах разного рода объектов	5
7.	Текст легко читается, фон сочетается текстом и графическими файлами	5
8.	Использование анимационных объектов	5
9.	Правильность изложения текста	5
10.	Использование объектов, сделанных в других программах	5
	Содержание презентации	
11.	Сформулированы проблема и её посылы, раскрыты обстоятельства её проявления, определяющие актуальность рассмотрения вопроса.	7
12.	Понятны задачи, логика и общий алгоритм рассмотрения раскрываемых вопросов	7
13.	Достаточная ёмкость, содержательность и убедительность представляемого материала	7
14.	Не перегруженность представляемого материала второстепенными данными и сведениями	7
15.	Сделаны ясные для восприятия выводы (заключения)	7
16.	Представленный материал и выводы соответствуют поставленной цели	7
	Эффект презентации	
17.	Гармоничное дополнение устного выступления и общее впечатление от просмотра презентации	12
	Сумма баллов	100

Если студент набирает

от 85 до 100 - оценка «отлично»;
от 72 до 84 – оценка «хорошо»,
от 51 до 71 – оценка «удовлетворительно»,
менее 50 баллов – оценка «неудовлетворительно».

2. Оценочные материалы для промежуточной аттестации

2.1. Примерный перечень вопросов для зачета.

1. Конституционное право на поиск, получение и распространение информации. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.07.2012) «О защите детей от информации, причиняющей вред их здоровью и развитию» (действует с 1 сентября 2012 года).
2. Защита государства и защита киберпространства.
3. Доктрина информационной безопасности.
4. Кибервойска. Защита киберпространства как одна из задач вооруженных сил.
5. Информационная война. Информационное оружие.
6. Патриотизм и интернет.
7. Информационное воздействие.
8. Безопасная работа в сети в процессе сетевой коммуникации (чаты, форумы, конференции, скайп, социальные сети и пр.).
9. Примеры этических нарушений. Значение сетевого этикета.
10. Собственность в Интернете. Авторское право.
11. Интеллектуальная собственность.
12. Платная и бесплатная информация.
13. Информационное законодательство РФ.
14. Правовая охрана программ для ЭВМ и БД. Коммерческое ПО. Бесплатное ПО (FreeWare, Free, Free GPL, Adware), условно-бесплатное ПО (Trial, Shareware, Demo).
15. Правовые основы для защиты от спама.
16. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных».
17. Сетевой этикет. Психология и сеть
18. Онлайн сервисы для безопасности пользователя в интернете
19. Защита в поисковых системах (фильтры для ограничения потенциально опасного содержимого).
20. Виды интернет-мошенничества (письма, рек-лама, охота за личными данными и т.п.).
21. Опасности мобильной связи. Предложения по установке вредоносных приложений.
22. Виды мошенничества в Интернете. Фишинг (фарминг).
23. Азартные игры.
24. Ложные антивирусы. Подмена страниц в интернете (сайты-клоны). Фальшивые файлообменники.
25. Электронный кошелек. Мошенничество при распространении «бесплатного» ПО.
26. Интернет-этикет. Правила общения в Интернете.
27. Основы сетевого этикета.
28. Переписка в сети.
29. Правила поведения в скайпе. Форум.
30. Общение в сети и его последствия.
31. Агрессия в сети.
32. Анонимность в сети.
33. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.
34. Гигиена компьютера.
35. Польза и вред компьютерных игр.
36. Техника безопасности при работе с компьютером.
37. Компьютер и мобильные устройства в чрезвычайных ситуациях.

38. Медицинская информация в Интернете. Компьютеры и мобильные устройства в экстремальных условиях.
39. Компьютер в режиме труда и отдыха.
40. Вредные факторы работы за компьютером и их последствия.
41. Интернет-зависимость.
42. Социальные сети. Детские социальные сети.
43. Виртуальная личность.
44. Зависимость от Интернет-общения.
45. Развлечения в Интернете.
46. Признаки игровой зависимости.
47. Сетевые игры.
48. Виды зависимости. Деструктивная информация в Интернете.
49. Виды Интернет-зависимости.
50. Психологическое воздействие информации на человека.
51. Критерии зависимости (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив).
52. Классификация интернет-зависимостей
53. Признаки заражения компьютера.
54. Антивирусная защита.
55. Организационные, юридические, программные и программно-аппаратные меры защиты.
56. Защита программ и данных с помощью паролей, программных и электронных ключей, серийных номеров, переноса в онлайн и т.п.
57. Антивирусное ПО, виды и назначение. Методы защиты от вирусов.
58. Меры безопасности для пользователя WiFi. Настройка безопасности.
59. Вирусы для мобильных устройств (мобильные банкеры и др.).

Критерии оценки

0 баллов – задание не выполнено;

1 балл получает студент, демонстрирующий значительные пробелы в знании базового теоретического материала, и низкий уровень практических умений и навыков, допустивший принципиальные ошибки при выполнении практического задания.

2 балла получает студент, демонстрирующий знания базового теоретического материала, нестабильный уровень умений, испытывающий затруднения в выполнении практической работы.

3 балла получает студент, демонстрирующий глубокое знание теоретического материала, высокий уровень умений и способный к их самостоятельному применению, не испытывающему затруднений при выполнении практической работы.

4 баллов получает студент, демонстрирующий глубокое знание теоретического материала, высокий уровень умений и способный к их самостоятельному применению, проявившему способности при выполнении практической работы.

5 баллов получает студент, демонстрирующий глубокое знание базового теоретического материала, высокий уровень умений и способный к их самостоятельному применению, проявившему творческие способности при выполнении практической работы.