



ДОКУМЕНТ ПОДПИСАН  
НЕКВАЛИФИРОВАННОЙ  
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ИНФОРМАЦИЯ О СЕРТИФИКАТЕ

S/N: 16E774D691E6E8BB43B90C453EDF6726  
Владелец: Ильяс Таболов Владислав  
Должность: И.о. директора Филиала  
E-mail: pedagogkmv@sspi.ru  
Организация: Филиал СГПИ в г. Железноводске  
Дата подписания: 31.05.2024  
Действителен: с 09.11.2022 до 09.11.2025

МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ

бюджетного образовательного учреждения

высшего образования

«СТАВРОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ»

в г. Железноводске



УТВЕРЖДАЮ

Заместитель директора по учебной  
и научной работе

Т.А. Пономаренко

«28» мая 2024 г.

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

**Б1.В.ДВ.01.01 Кибербезопасность**

(наименование учебной дисциплины)

Уровень основной профессиональной образовательной программы бакалавриат

Направление подготовки

44.03.05 Педагогическое образование (с двумя профилями подготовки),

Направленность профили «Русский язык» и «Литература»

Форма обучения Очная

Срок освоения ОПОП 5 лет.

Год начала обучения 2024

Заведующий кафедрой \_\_\_\_\_/М.Н. Арутюнян /

Декан факультета \_\_\_\_\_/Э.С. Таболова/

Железноводск, 2023 г.

---

Рабочая программа дисциплины составлена в соответствии с учебным планом по соответствующей образовательной программе

Автор (ы)-разработчик (и)

Буракова И.С., доцент кафедры гуманитарных и социально-экономических дисциплин, кандидат педагогических наук

---

*ФИО, должность, ученая степень, звание*

«Согласовано»

Заведующий

выпускающей

кафедры



Краснокутская Л.И., кандидат ист. наук

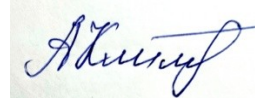
---

*ФИО, ученая степень, звание, подпись*

«28» мая 2024 г.

«Согласовано»

Библиотекарь



И.о. заведующего библиотекой  
Клименко А.В.

---

*ФИО, подпись*

«28» мая 2024 г.

---

## Содержание

1. Цель и задачи, дисциплины.....	4
2. Место дисциплины в структуре образовательной программы.....	4
3. Планируемые результаты обучения по дисциплине.....	4
4. Объем учебной дисциплины и виды учебной работы.....	5
5. Содержание дисциплины по разделам (темам) и видам занятий.....	6
6. Контроль качества освоения дисциплины .....	6
7. Учебно-методическое обеспечение дисциплины.....	8
8. Перечень основной и дополнительной учебной литературы.....	8
9. Материально-техническое обеспечение дисциплины.....	11
Приложения.....	12

### 1. Цель и задачи дисциплины

Целями освоения дисциплины являются: 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.

#### Учебные задачи дисциплины:

- формирование общих представлений 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.

### 2. Место дисциплины в структуре образовательной программы

Дисциплина «Кибербезопасность» относится к части Блока 1, формируемой участниками образовательных отношений, является дисциплиной по выбору.

Для освоения учебного материала по дисциплине используются знания, умения, навыки, сформированные предшествующими дисциплинами: Информатика (школьный курс), Технологии цифрового образования.

Знания, умения, навыки, сформированные в процессе изучения дисциплины необходимы для прохождения учебной и производственной практик, подготовки к государственной итоговой аттестации.

### 3. Планируемые результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
<i>Универсальные компетенции</i>		
УК-1. Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Демонстрирует знание особенностей системного и критического мышления, аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение.	- знает порядок определения источников информации, порядок получения доступа к ним. - знает методы описания и формализации полученной информации. - знает способы верификации получаемой информации. - знает принципы системного подхода. - способен выработать стратегию действий на основе системного подхода используя обработанную полученную информацию.
	УК-1.2 Применяет логические формы и процедуры, способен к рефлексии по поводу собственной и чужой мыслительной деятельности.	- способен провести анализ информации предметной области полученной с использованием ИКТ. - знает основы обработки информации в профессиональной сфере;

		<p>- способен провести выбор необходимой информации предметной области с использованием ПК и пакетов прикладных программ.</p> <p>умеет получать новые знания на основе анализа и синтеза информации; собирать и обобщать данные по научным проблемам, относящимся к профессиональной области;</p> <p>осуществлять поиск информации и применять системный подход для решения поставленных задач; определять и оценивать практические последствия возможных решений задачи.</p>
	<p>УК-1.3. Анализирует источники информации с целью выявления их противоречий и поиска достоверных суждений.</p>	<p>владеет навыками исследования проблем профессиональной деятельности с применением анализа, синтеза и других методов интеллектуальной деятельности; выявления научных проблем и использования адекватных методов для их решения; формулирования оценочных суждений при решении профессиональных задач.</p>
<p>УК-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов</p>	<p>УК-8.1 Оценивает факторы риска, умеет обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности.</p>	<p>Способен создавать и поддерживать необходимые условия безопасности для участников образовательного процесса и личной безопасности. Владеет навыками оценивания, факторов риска, и обеспечения личной безопасности и безопасности участников образовательного процесса.</p>
	<p>УК-8.2 Знает и может применять методы защиты в чрезвычайных ситуациях и в условиях военных конфликтов, формирует культуру безопасного и ответственного поведения.</p>	<p>Знает основные методы создания и поддержания в повседневной жизни и профессиональной деятельности условий в чрезвычайных ситуациях. Применяет на практике методы защиты в чрезвычайных ситуациях, донести принципы культуры безопасного и ответственного поведения обучаемых.</p> <p>Способен обучить навыкам создания и поддержания в повседневной жизни и профессиональной деятельности необходимых условий для ответственного поведения обучаемых.</p>

#### 4. Объем учебной дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы (72 часов), включая промежуточную аттестацию.

Вид учебной работы		Всего часов	Семестры
			7
Контактные часы	<b>Всего:</b>	36,3	72
	Лекции (Лек)	16	16
	Практические занятия (в т.ч. семинары) (Пр/Сем)	20	20
	Лабораторные занятия (Лаб)		
	Индивидуальные занятия (ИЗ)		
Промежуточная аттестация	Зачет, зачет с оценкой, экзамен (КПА)	0,3	0,3
	Консультация к экзамену (Конс)		
	Курсовая работа (Кр)		
Самостоятельная работа студентов (СР)		35,7	35,7
Подготовка к экзамену (Контроль)			
Вид промежуточной аттестации		зачет	зачет
<b>Общая трудоемкость (по плану)</b>		72	72

#### 5. Содержание дисциплины по разделам (темам) и видам занятий

Наименование раздела (темы) дисциплины	Лекции	Практические занятия (в т.ч. семинары)	Лабораторные занятия	СРС	Всего	Планируемые результаты обучения	Формы текущего контроля
<b>Семестр 7</b>							
Кибербезопасность в системе национальной безопасности РФ	2	4		4	10	УК-1 УК-8	Доклад собеседование
Киберпреступления против личности, общества и государства	2	4		6	12	УК-1 УК-8	доклад собеседование
Современное киберпространство Техника безопасности в киберпространстве	4	4		8	16	УК-1 УК-8	доклад собеседование
Проблемы Интернет-зависимости, кибербуллинга	4	4		8	16	УК-1 УК-8	доклад собеседование
Методы обеспечения безопасности ПК и Интернета. Вирусы и антивирусы	4	4		9,7	17,7	УК-1 УК-8	доклад тест собеседование
Форма промежуточной аттестации (зачет)					0,3		собеседование
<b>Всего за семестр:</b>	<b>16</b>	<b>20</b>		<b>35,7</b>	<b>72</b>		

Планы проведения учебных занятий отражены в методических материалах (Приложение 1.).

## 6. 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).

<b>Уровень сформированности компетенции</b>			
<b>не сформирована</b>	<b>сформирована частично</b>	<b>сформирована в целом</b>	<b>сформирована полностью</b>
<b>«Не зачтено»</b>	<b>«Зачтено»</b>		
<b>«Неудовлетворительно»</b>	<b>«Удовлетворительно»</b>	<b>«Хорошо»</b>	<b>«Отлично»</b>
<b>Описание критериев оценивания</b>			
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	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	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

дискуссии и низкая степень контактности.		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.	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.
--	--	--	---

## 7. Учебно-методическое обеспечение дисциплины

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

Полный комплект методических документов размещен на ЭИОС Филиала СГПИ в г. Железноводске.

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, нормативными документами, архивными и др. источниками информации (конспектирование); составление плана и тезисов ответа; подготовка сообщения (реферата); собеседование; презентации; выполнение индивидуальных заданий; подготовка к практическим занятиям и др.; подготовка к зачету.

## 8. Перечень основной и дополнительной учебной литературы

*Основная литература:*

Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2022. — 473 с. — (Высшее образование). — ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/489242>

1. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. — Красноярск : СФУ, 2019. — 206 с. — ISBN 978-



5-7638-4008-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/157578>

*а. Дополнительная литература:*

1. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУ МИРЭА, 2021. — 79 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/182491>
2. Пугин, В. В. Защита информации в компьютерных информационных системах : учебное пособие / В. В. Пугин, Е. Ю. Голубничая, С. А. Лабада. — Самара : ПГУТИ, 2018. — 119 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/182299>
3. Киричек, Ксения Александровна, Как обеспечить информационную защиту авторских прав? Методические рекомендации / К.А. Киричек, О.В. Пелих, А.С. Редванов, В.С. Тоискин – Ставрополь : изд-во «Тимченко О.Г.». 2020.- 51 с.
4. Бибарсова Г.Ш. Правовое обеспечение информационных технологий: Учебное пособие.- Ставрополь: СГПИ, 2010.- 100 с.
5. Формирование информационной гигиены у будущих педагогов: учебное пособие / Бурлакова И.С., Ситак Л.А, и др. Москва, 2020.- Знание –М- 80 с.
6. Тоискин В.С. и др. Информационные технологии безопасная образовательная среда в обществе XXI века – учителям информатики: учебное пособие / В.С. Тоискин, В.В. Красильников, О.В. Пелих.- Ставрополь: Изд-во «Тимченко О.Г.», 2021. – 121 с.

*Интернет-ресурсы:*

**ЭБС**

№ п/п	Наименование	Адрес сайта
1.	ЭБС «Юрайт»	<a href="http://www.biblio-online.ru">www.biblio-online.ru</a>
2.	ЭБС «Юрайт» (раздел «Легендарные книги»)	<a href="http://www.biblio-online.ru">www.biblio-online.ru</a>
3.	Электронно-библиотечная система «Лань»	<a href="http://e.lanbook.com/">http://e.lanbook.com/</a>

**Электронные образовательные ресурсы**

Название ресурса	Ссылка
ЭБС «Журнальный зал»: русский толстый журнал как эстетический феномен	<a href="https://magazines.gorky.media">https://magazines.gorky.media</a>
«Электронная библиотека ИМЛИ РАН»	<a href="http://biblio.imli.ru">http://biblio.imli.ru</a>
«Электронная библиотека ИРЛИ РАН» (Пушкинский Дом)	<a href="http://lib.pushkinskiydom.ru">http://lib.pushkinskiydom.ru</a>
ЭБС «Педагогическая библиотека»	<a href="http://pedlib.ru">http://pedlib.ru</a>
Научная электронная библиотека eLibrary.ru	<a href="https://elibrary.ru">https://elibrary.ru</a>

Научная электронная библиотека «Киберленинка»	<a href="https://cyberleninka.ru/">https://cyberleninka.ru/</a>
Библиотека академии наук (БАН). Ресурсы открытого доступа	<a href="http://www.rasl.ru/e_resours/resursy_otkrytogo_dostupa.php">http://www.rasl.ru/e_resours/resursy_otkrytogo_dostupa.php</a>
Словари и энциклопедии	<a href="https://dic.academic.ru">https://dic.academic.ru</a>
Педагогическая мастерская «Первое сентября»	<a href="https://fond.1sept.ru">https://fond.1sept.ru</a>
Национальная платформа «Открытое образование»	<a href="https://openedu.ru">https://openedu.ru</a>
Российское образование. Федеральный портал	<a href="http://edu.ru">http://edu.ru</a>
Портал Федеральных государственных образовательных стандартов высшего образования	<a href="http://fgosvo.ru">http://fgosvo.ru</a>
Цифровая образовательная платформа «Media» (ЛЕСТА), ГК «Просвещение»	<a href="https://media.prosv.ru/">https://media.prosv.ru/</a>

## 9. Материально-техническое обеспечение дисциплины

Занятия, текущий контроль успеваемости и промежуточная аттестация по дисциплине проводятся в учебных аудиториях, укомплектованных типовой мебелью для обучающихся и преподавателя. По заявке устанавливается мобильный комплект (ноутбук, проектор, экран, колонки).

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

Компьютерное оборудование оснащено комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

1. Пакеты программного обеспечения общего назначения (возможны следующие варианты: «МойОфис», «MicrosoftOffice», «LibreOffice», «ApacheOpenOffice»).
2. Приложение, позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Sumatra PDF Reader», «AdobeAcrobatReaderDC».
3. Приложение, позволяющее сканировать и распознавать текстовые документы (возможны следующие варианты: «ABBYFineReader», «WinScan2PDF»).
4. Программа-файловый архиватор (возможны следующие варианты: «7-zip», «WinRAR»).

---

5. Программа для организации и проведения тестирования (возможны следующие варианты: «Айрен», «MytestX»).

6. Программа просмотра интернет-контента (браузер) (возможен следующий вариант: «Yandex»).

**Методические материалы по дисциплине  
« Кибербезопасность»**

**1. Планы практических работ и методические рекомендации**

**Тема 1. Кибербезопасность в системе национальной безопасности РФ**

**Практическое занятие 1.1.**

Вопросы для обсуждения:

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.

**Практическое занятие 1.2.**

Вопросы для обсуждения

1. Кибервойска. Защита киберпространства как одна из задач вооруженных сил.
2. Информационная война. Информационное оружие.
3. Патриотизм и интернет.
4. Информационное воздействие.
5. Военная, государственная, коммерческая тайна.
6. Защита сайтов государственных органов (электронное правительство).

**Тема 2. Киберпреступления против личности, общества и государства**

**Практическое занятие 2.1.**

Вопросы для обсуждения

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.

**Практическое занятие 2.2.**

Вопросы для обсуждения

1. Ответственность за интернет-мошенничество.
2. Правовые акты в области информационных технологий и защиты киберпространства. Ответственность за киберпреступления.
3. 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).

4. Информационное законодательство РФ.
5. 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).
6. Правовые основы для защиты от спама.
7. Правовая охрана программ для ЭВМ и БД. Лицензионное ПО. Виды лицензий (ОЕМ, FPP, корпоративные лицензии, подписка). ПО с открытым кодом (GNU GPL, FreeBSD).
8. Право на информацию, на сокрытие данных, категории информации.
9. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных».

### **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.

### **Практическое занятие 3.2.**

Вопросы для обсуждения

1. ТБ при регистрации на веб-сайтах.
2. Компьютерное пиратство. Плагиат.
3. Кибернаемники и кибердетективы.
4. Оценка ущерба от киберпреступлений.

5. Интернет-этикет. Правила общения в Интернете.
6. Основы сетевого этикета.
7. Переписка в сети.
8. Правила поведения в скайпе. Форум.
9. Общение в сети и его последствия.
10. Агрессия в сети.
11. Анонимность в сети.
12. Виды этикета (личный, деловой, письменный, дискуссионный и пр.). Различия этикета в разных странах.
13. Этика дискуссий. Взаимное уважение при интернет-общении.
14. Этикет и безопасность.

#### **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.

##### **Практическое занятие 4.2.**

Вопросы для обсуждения

17. Организация рабочего места
  1. Интернет-сообщество.
  2. Интернет-зависимость.
  3. Социальные сети. Детские социальные сети.
  4. Виртуальная личность.
  5. Зависимость от Интернет-общения.
  6. Развлечения в Интернете.
  7. Признаки игровой зависимости.
  8. Сетевые игры.
  9. Сайты знакомств. ЗОЖ и компьютер.
  10. Виды зависимости. Деструктивная информация в Интернете.
  11. Виды Интернет-зависимости.
  12. Киберкультура (массовая культура в сети) и личность.
  13. Психологическое воздействие информации на человека.
  14. Управление личностью через сеть. Интернет и компьютерная зависимость (аддикция).

15. Критерии зависимости (приоритетность, изменения настроения, толерантность, симптом разрыва, конфликт, рецидив).
16. Типы интернет-зависимости (пристрастие к работе с компьютером, к навигации и поиску информации, игромания и электронные покупки, зависимость от сетевого общения).
17. Классификация интернет-зависимостей

## **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.

### **Практическое занятие 5.2.**

#### **Вопросы для обсуждения**

1. Проблемы безопасности инфраструктуры Интернета (протоколы маршрутизации сети, система доменных имен, средства маршрутизации и т.п.).
2. Проверка подлинности (аутентификация) в Интернете.
3. Меры безопасности для пользователя WiFi. Настройка безопасности.
4. Вирусы для мобильных устройств (мобильные банкиры и др.).
5. Настройка компьютера для безопасной работы. Ошибки пользователя.
6. Меры личной безопасности при сетевом общении. Предотвращение несанкционированного доступа к ПК.
7. Пароли, биометрические методы защиты и аутентификация с помощью внешних носителей.
8. Простые и динамически изменяющиеся пароли. Борьба с утечками информации.
9. Средства контроля доступа. Права пользователей. Способы разграничения доступа.
10. Отличия вирусов и закладок.
11. Антивирусные программы для ПК: сканеры, ревизоры и др.
12. Наиболее известные антивирусные программы. Kaspersky Internet Security. Dr.Web Security Space. ESET NOD32 Smart Security. Коммерческое и бесплатное антивирусное ПО.
13. 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.).
14. Настройки безопасности почтовых программ. Защита в поисковых системах (фильтры для ограничения потенциально опасного содержимого).

### **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 банкиры 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.



---

## 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».

## Оценочные материалы по дисциплине « Кибербезопасность »

### 1. Оценочные материалы для текущего контроля

#### 1.1. Тестовые материалы

##### Тест 2

1. К правовым методам, обеспечивающим информационную безопасность, относятся:
  1. Разработка аппаратных средств обеспечения правовых данных
  2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
  3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2. Виды информационной безопасности:
  1. Персональная, корпоративная, государственная
  2. Клиентская, серверная, сетевая
  3. Локальная, глобальная, смешанная
3. Цели информационной безопасности – своевременное обнаружение, предупреждение:
  1. несанкционированного доступа, воздействия в сети
  2. инсайдерства в организации
  3. чрезвычайных ситуаций
4. Основные объекты информационной безопасности:
  1. Компьютерные сети, базы данных
  2. Информационные системы, психологическое состояние пользователей
  3. Бизнес-ориентированные, коммерческие системы
5. Основными рисками информационной безопасности являются:
  1. Искажение, уменьшение объема, перекодировка информации
  2. Техническое вмешательство, выведение из строя оборудования сети
  3. Потеря, искажение, утечка информации
6. К основным функциям системы безопасности можно отнести все перечисленное:
  1. Установление регламента, аудит системы, выявление рисков
  2. Установка новых офисных приложений, смена хостинг-компании
  3. Внедрение аутентификации, проверки контактных данных пользователей
7. К основным типам средств воздействия на компьютерную сеть относится:
  1. Компьютерный сбой
  2. Логические закладки («мины»)
  3. Аварийное отключение питания
8. Когда получен спам по e-mail с приложенным файлом, следует:
  1. Прочитать приложение, если оно не содержит ничего ценного – удалить
  2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
  3. Удалить письмо с приложением, не раскрывая (не читая) его

9. ЭЦП – это:

1. Электронно-цифровой преобразователь
2. Электронно-цифровая подпись
3. Электронно-цифровой процессор

10. Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:

1. Целостность
2. Доступность
3. Актуальность

11. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

1. Программные, технические, организационные, технологические
2. Серверные, клиентские, спутниковые, наземные
3. Личные, корпоративные, социальные, национальные

12. Политика безопасности в системе (сети) – это комплекс:

1. Руководств, требований обеспечения необходимого уровня безопасности
2. Инструкций, алгоритмов поведения пользователя в сети
3. Нормы информационного права, соблюдаемые в сети

### **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: гриффинг, 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 (ОЕМ, 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 банкиры 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.

---

## 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.
- 23

- 
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 банкиры и др.).

**Критерии оценки:**

- оценка «зачтено» выставляется студенту, если он продемонстрировал достаточно полное *знание* материала; продемонстрировал *знание* основных теоретических понятий; достаточно последовательно, грамотно и логически стройно изложил материал; продемонстрировал *умение* ориентироваться в литературе по проблематике дисциплины; *умеет* сделать достаточно обоснованные выводы по излагаемому материалу.

- оценка «не зачтено» выставляется в случае незнания значительной части программного материала; не владения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу.



Лист изменений рабочей программы

№ п/п	Содержание изменений	Реквизиты документа об утверждении изменений	Дата внесения изменений
1.	Утверждена на основании Федерального государственного образовательного стандарта высшего образования по направлению подготовки 44.03.05 Педагогическое образование профили "Русский язык" и "Литература" №125 от 22.02.2018 г.	Протокол заседания кафедры историко-филологических дисциплин № 13 от 28.05.2024	28.05.2024 г.