

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Иванченко Ирина Васильевна

Должность: и.о. директора Филиала СГПИ в г. Железноводске

Дата подписания: 12.09.2024 15:45:13

Уникальный программный ключ:

e192bec1a53c51706141a70b286f0e91498b116

**МИНИСТЕРСТВО ОБРАЗОВАНИЯ СТАВРОПОЛЬСКОГО КРАЯ  
Филиал государственного 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**

### **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ Б1.В.ДВ.02.02**

(наименование учебной дисциплины)

**Уровень основной профессиональной образовательной программы бакалавриат**

**Направление подготовки 44.03.03 Специальное (дефектологическое) образование,**

**Направленность (профиль(и)) "Логопедия"**

**Форма обучения очная**

**Срок освоения ОПОП 4 года.**

**Год начала обучения 2024**

**Факультет психолого-педагогический**

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

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

Железноводск, 2024 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 кафедрой

«Согласовано»  
И.о. заведующего библиотекой

Арутюнян М.Н., к.философ.н.,  
доцент  
*ФИО, ученая степень, звание,*  
*подпись*  
«28» мая 2024г



Клименко А.В.  
*ФИО, подпись*  
«28» мая 2024г.



## 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 системы знаний о современном состоянии проблемы обеспечения информационной безопасности, изучение основных понятий, методов и средств обеспечения информационной безопасности личности, общества и государства. Задачи дисциплины:

- формирование представления о проблеме обеспечения информационной безопасности, ее важность и актуальность;
- изучение основных средств обеспечения информационной безопасности в сетях;
- изучение способов удостоверения и контроля аутентичности входящей и исходящей информации, методов ее проверки;
- изучение общих принципов технологий, применяемых в информационной безопасности;
- формирование навыков эффективного использования доступных методов и средств обеспечения информационной безопасности современных компьютерных систем;
- овладение основными правового обеспечения информационной безопасности и защиты информации;
- развитие навыков ориентирования в информационных потоках.

### 2. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к вариативной части Блока 1, является дисциплиной по выбору.

Для освоения учебного материала по дисциплине используются знания, умения, навыки, сформированные предшествующими дисциплинами: 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 и готовность к нему.	- знает способы верификации получаемой информации. - знает принципы системного подхода. - способен выработать стратегию действий на основе системного подхода используя обработанную полученную информацию.
	УК-1.5 Сопоставляет разные источники информации с целью выявления их противоречий и поиска достоверных суждений.	- знает порядок определения источников информации, порядок получения доступа к ним. - знает методы описания и формализации полученной информации. - способен провести анализ информации предметной области полученной с использованием ИКТ.

		<p>- знает основы обработки информации в профессиональной сфере;</p> <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-1.6. Аргументированно формирует собственное суждение и оценку информации, принимает обоснованное решение.</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>

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

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

Вид учебной работы		Всего часов	Семестры
			5
Контактные часы	<b>Всего:</b>	36	36
	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>	<b>72</b>	<b>72</b>

### 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 5</b>							
Понятие об информационной безопасности общества. Цели и задачи обеспечения информационной безопасности.	2	4		6	10	УК-1.1 УК-1.5 УК-1.6	Доклад собеседование
Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности.	4	6		8	14	УК-1.1 УК-1.5 УК-1.6	практические задания доклад собеседование
Основные угрозы информационной безопасности в информационной образовательной среде	6	6		12	16	УК-1.1 УК-1.5 УК-1.6	практические задания доклад собеседование
Правовое обеспечение информационной безопасности	4	4		9, 7	17,7	УК-1.1 УК-1.5 УК-1.6	практические задания 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.

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»
<b>Описание критериев оценивания</b>			
<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- существенные пробелы в знаниях учебного материала;</li> <li>- допускаются принципиальные ошибки при ответе на основные вопросы билета, отсутствует знание и понимание основных понятий и категорий;</li> <li>- непонимание сущности дополнительных вопросов в рамках заданий билета;</li> <li>- отсутствие умения выполнять практические задания, предусмотренные программой дисциплины;</li> <li>- отсутствие готовности (способности) к дискуссии и низкая степень контактности.</li> </ul>	<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знания теоретического материала;</li> <li>- неполные ответы на основные вопросы, ошибки в ответе, недостаточное понимание сущности излагаемых вопросов;</li> <li>- неуверенные и неточные ответы на дополнительные вопросы;</li> <li>- недостаточное владение литературой, рекомендованной программой дисциплины;</li> <li>- умение без грубых ошибок решать практические задания.</li> </ul>	<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- знание и понимание основных вопросов контролируемого объема программного материала;</li> <li>- твердые знания теоретического материала.</li> <li>- способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития;</li> <li>- правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы;</li> <li>- умение решать практические задания, которые следует выполнить;</li> <li>- владение основной литературой, рекомендованной программой дисциплины;</li> <li>Возможны незначительные неточности в раскрытии отдельных положений вопросов билета, присутствует</li> </ul>	<p>Обучающийся демонстрирует:</p> <ul style="list-style-type: none"> <li>- глубокие, всесторонние и аргументированные знания программного материала;</li> <li>- полное понимание сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий;</li> <li>- способность устанавливать и объяснять связь практики и теории;</li> <li>- логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора;</li> <li>- умение решать практические задания;</li> <li>- наличие собственной обоснованной позиции по обсуждаемым вопросам;</li> <li>- свободное использование в ответах на вопросы материалов рекомендованной</li> </ul>

		неуверенность в ответах на дополнительные вопросы.	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:*

1. Зенков, А. В. Информационная безопасность и защита информации : учебное пособие для вузов / А. В. Зенков. — Москва : Издательство Юрайт, 2022. — 104 с. — (Высшее образование). — ISBN 978-5-534-14590-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/497002>
2. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/496741>

### *Дополнительная литература:*

1. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2022. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/498844>
2. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/495922>
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.

*Периодические издания:*

- 1) Профессиональные психологические тесты - <http://vsetesti.ru>
- 2) Педагогическая библиотека - <http://www.pedlib.ru>
- 3) Журнал "Логопед" <http://www.logoped.sfera.ru/>

*Интернет-ресурсы:*

#### **ЭБС**

№ п/п	Наименование	Адрес сайта
1.	ЭБС «Лань»	<a href="http://www.urait.ru">www.urait.ru</a>
2.	ЭБС «Лань»	<a href="http://e.lanbook.com/">http://e.lanbook.com/</a>
3.	ЭБС «Айбукс.ру/ibooks.ru»	<a href="http://ibooks.ru">http://ibooks.ru</a>
4.	«Национальная электронная библиотека» (НЭБ)	<a href="https://rusneb.ru/">https://rusneb.ru/</a>

#### **ЭОР**

№ п/п	Наименование	Адрес сайта
1.	«Педагогическая библиотека»	<a href="http://pedlib.ru">http://pedlib.ru</a>
2.	Научная электронная библиотека	<a href="https://elibrary.ru">https://elibrary.ru</a>
3.	Научная электронная библиотека «Киберленинка»	<a href="https://cyberleninka.ru/">https://cyberleninka.ru/</a>
4.	Библиотека академии наук (БАН). Ресурсы открытого доступа	<a href="http://www.rasl.ru/e_resours/resursy_otkrytogo_dostu">http://www.rasl.ru/e_resours/resursy_otkrytogo_dostu</a>
5.	Словари и энциклопедии	<a href="https://dic.academic.ru">https://dic.academic.ru</a>
6.	Педагогическая мастерская «Первое сентября»	<a href="https://fond.1sept.ru">https://fond.1sept.ru</a>
7.	Национальная платформа «Открытое образование»	<a href="https://openedu.ru">https://openedu.ru</a>
8.	Российское образование. Федеральный портал	<a href="http://edu.ru">http://edu.ru</a>
9.	Портал Федеральных государственных образовательных стандартов высшего образования	<a href="http://fgosvo.ru">http://fgosvo.ru</a>
10.	Портал проекта «Современная цифровая образовательная среда в РФ»	<a href="https://online.edu.ru">https://online.edu.ru</a>
11.	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: «ABBYYFineReader», «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  
« Информационная безопасность»**

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

**Тема 1. Понятие об информационной безопасности общества. Цели и задачи обеспечения информационной безопасности**

**Практическое занятие 1.1.**

Вопросы для обсуждения:

1. Информационная безопасность – важнейшая составляющая национальной безопасности современной России.
2. Национальные интересы РФ в информационной сфере и их правовое и организационно-техническое обеспечение.
3. Основные составляющие национальных интересов в сфере информационной безопасности РФ.
4. Соблюдение прав и свобод человека и гражданина в области получения информации.
5. Информация как стратегический национальный ресурс.
6. Группы угроз в сфере информационной безопасности.
7. Виды уголовного преследования.
8. Роль информационной сферы.
9. Осведомленность человека и защита личной информации от несанкционированного доступа.
10. Основные цели и задачи обеспечения информационной безопасности общества, группы, личности, регламентируемые государством.
11. Информационная среда общества как системообразующий фактор во всех сферах национальной безопасности.

**Практическое занятие 1.2.**

Вопросы для обсуждения

1. Обеспечение прав граждан на получение адекватной информации о жизнедеятельности общества.
2. Определение информации в научно-технической области и в области права.
3. Социальные и технические свойства информации.
4. Внешние и внутренние признаки информации.
5. Жизненный цикл информации.
6. Информационное пространство.
7. Информационные ресурсы базы данных.
8. Информационные технологии.
9. Интеллектуальные информационные системы.
10. Проблемы организации электронного визирования документов в системах электронного документооборота.
11. Информационная культура.

**Тема 2. Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности**

### **Практическое занятие 2.1.**

Вопросы для обсуждения

1. Доктрина информационной безопасности РФ.
2. Правовое обеспечение информационной безопасности РФ, обучение и воспитание кадров, обеспечивающих информационно-коммуникационные процессы в обществе.
3. Организационно-технические методы обеспечения информационной безопасности РФ.
4. Усиление контроля и ответственности за соблюдение законодательства в информационной сфере.
5. Экономические методы информационной безопасности РФ.

### **Практическое занятие 2.2.**

Вопросы для обсуждения

1. Классификация и краткая характеристика каналов утечки информации.
2. Установление целей источника угроз информационной безопасности, установление задач информационной безопасности общества, социальной группы, личности.
3. Виды и источники угроз информационной безопасности РФ.
4. Перехват информации через естественные каналы утечки и путем несанкционированного доступа.
5. Актуальные каналы утечки информации и их характеристика.
6. 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.).

### **Практическое занятие 2.3.**

Вопросы для обсуждения

1. Собственность в Интернете. Авторское право.
2. Интеллектуальная собственность.
3. Платная и бесплатная информация.
4. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера.
5. Киберпреступления. Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.). Опасности мобильной связи. Предложения по установке вредоносных приложений.
6. Право на информацию, на сокрытие данных, категории информации.
7. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных».
8. Электронный кошелек. Мошенничество при распространении «бесплатного» ПО.

## **Тема 3. Основные угрозы информационной безопасности в информационной образовательной среде. Обеспечение безопасности информационной образовательной среды школы**

### **Практическое занятие 3.1.**

Вопросы для обсуждения

1. Классификация рисков в соответствии с объектом (субъектом) образовательного процесса на который они воздействуют.

2. Педагогические риски – отрицательные воздействия на учебный процесс.
3. Психолого-медицинские риски – отрицательные воздействия на жизнь и здоровье учащихся и педагогов.
4. Управленческие (или организационные) риски – отрицательное влияние на управленческие процессы.
5. Финансовые риски – отрицательные воздействия на финансовое состояние учреждения (прямые финансовые потери).
6. Политические риски - отрицательные воздействия на репутацию учреждения

### **Практическое занятие 3.2.**

Вопросы для обсуждения

1. Принципы классификации информационных угроз.
2. Информационная безопасность детей с позиций психологического подхода
3. Безопасность социальной ситуации развития
4. Влияние СМИ на психическое развитие, здоровье и психологическое благополучие детей и подростков
5. Социальные сети. Детские социальные сети.
6. Признаки игровой зависимости.
7. Сетевые игры.

### **Практическое занятие 3.2.**

Вопросы для обсуждения

1. Критерии оценки состояния информационной безопасности проблемы детей и подростков (рекомендации для родителей, педагогов, психологов)
2. Формы работы по формированию информационной безопасности
3. Концепция информационной безопасности школьников и педагогические условия ее реализации
4. Организация информационно-безопасного образовательного процесса в школе, взаимосвязь с родителями школьников в решении
5. Медицинская информация в Интернете. Компьютеры и мобильные устройства в экстремальных условиях.

## **Тема 4. Информационно-правовые нормы и информационные правоотношения**

### **Практическое занятие 4.1.**

Вопросы для обсуждения

1. Информационная политика.
2. Информационное общество: становление и развитие.
3. Тенденции развития международного информационного общества.
4. Проблемы становления информационного права в России.
5. Конституционно-правовые основы информационного законодательства.
6. Конституция Российской Федерации как источник прав в информационной области и источник правовых ограничений в сфере поиска информации и доступа к информации.
7. Информационно-психологическая безопасность.
8. Информационная безопасность общества, понятие информационной войны.

### **Практическое занятие 4.2.**

Вопросы для обсуждения

1. Средства массовой информации (СМИ) как институт современного общества; понятие, виды. Законодательство о СМИ в Российской Федерации. органов, осуществляющих государственное регулирование в сфере массовой информации. Полномочия государственных органов в отношении СМИ.
2. Процесс регистрации СМИ. Лицензирование в области СМИ, контроль за распространением СМИ.
3. Существующие ограничения свободы информации.
4. Информация в Глобальной информационной сети Интернет.
5. Защита интеллектуальной собственности в Интернет.
6. Порядок регистрации доменных имен.
7. Проблема идентификации пользователей.
8. Концепция Российского законодательства в области Интернета.

## **2. Задания для самостоятельной работы**

### **Тема 1. Понятие об информационной безопасности общества. Цели и задачи обеспечения информационной безопасности.**

Подготовить доклад по теме:

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

### **Тема 2. Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности**

Подготовить доклад по теме:

1. Доктрина информационной безопасности РФ.
2. Психологическая обстановка в Интернете: гриффинг, кибербуллинг, кибермоббинг, троллинг, буллицид.
3. Классификация и краткая характеристика каналов утечки информации.

### **Тема 3. Основные угрозы информационной безопасности в информационной образовательной среде. Обеспечение безопасности информационной образовательной среды школы**

Подготовить доклад по теме:

1. Критерии оценки состояния информационной безопасности детей и подростков (рекомендации для родителей, педагогов, психологов)
2. Формы работы по формированию информационной безопасности детей в сети

### **Тема 4. Информационно-правовые нормы и информационные правоотношения**

Подготовить доклад по теме:

1. Существующие ограничения свободы информации.
2. Информация в Глобальной информационной сети Интернет.
3. Защита интеллектуальной собственности в Интернет.

## **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.

## **Оценочные материалы по дисциплине « Информационная безопасность»**

### **1. Оценочные материалы для текущего контроля**

#### **1.1. Тестовые материалы**

**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-компания
- 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 нелегального 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

**тест\_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, характеризующаяся:**

- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

**22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:**

- Целостность
- Доступность
- Актуальность

**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 перечисленные 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. Понятие об информационной безопасности общества. Цели и задачи обеспечения информационной безопасности**

1. Информационная безопасность – важнейшая составляющая национальной безопасности современной России.
2. Национальные интересы РФ в информационной сфере и их правовое и организационно-техническое обеспечение.
3. Основные составляющие национальных интересов в сфере информационной безопасности РФ.
4. Соблюдение прав и свобод человека и гражданина в области получения информации.
5. Информация как стратегический национальный ресурс.
6. Группы угроз в сфере информационной безопасности.
7. Виды уголовного преследования.
8. Роль информационной сферы.
9. Осведомленность человека и защита личной информации от несанкционированного доступа.
10. Основные цели и задачи обеспечения информационной безопасности общества, группы, личности, регламентируемые государством.
11. Информационная среда общества как системообразующий фактор во всех сферах национальной безопасности.
12. Обеспечение прав граждан на получение адекватной информации о жизнедеятельности общества.
13. Определение информации в научно-технической области и в области права.
14. Социальные и технические свойства информации.
15. Внешние и внутренние признаки информации.
16. Жизненный цикл информации.
17. Информационное пространство.
18. Информационные ресурсы базы данных.
19. Информационные технологии.
20. Интеллектуальные информационные системы.
21. Проблемы организации электронного визирования документов в системах электронного документооборота.
22. Информационная культура.

### **Тема 2. Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности**

1. Доктрина информационной безопасности РФ.
2. Правовое обеспечение информационной безопасности РФ, обучение и воспитание кадров, обеспечивающих информационно-коммуникационные процессы в обществе.
3. Организационно-технические методы обеспечения информационной безопасности РФ.
4. Усиление контроля и ответственности за соблюдение законодательства в информационной сфере.
5. Экономические методы информационной безопасности РФ.
6. Классификация и краткая характеристика каналов утечки информации.
7. Установление целей источника угроз информационной безопасности, установление задач информационной безопасности общества, социальной группы, личности.
8. Виды и источники угроз информационной безопасности РФ.
9. Перехват информации через естественные каналы утечки и путем несанкционированного доступа.
10. Актуальные каналы утечки информации и их характеристика.
11. 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.).
12. Собственность в Интернете. Авторское право.
13. Интеллектуальная собственность.
14. Платная и бесплатная информация.
15. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера.
16. Киберпреступления. Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.). Опасности мобильной связи. Предложения по установке вредоносных приложений.
17. Право на информацию, на сокрытие данных, категории информации.
18. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных».
19. Электронный кошелек. Мошенничество при распространении «бесплатного» ПО.

### **Тема 3. Основные угрозы информационной безопасности в информационной образовательной среде. Обеспечение безопасности информационной образовательной среды школы**

1. Классификация рисков в соответствии с объектом (субъектом) образовательного процесса на который они воздействуют.
2. Педагогические риски – отрицательные воздействия на учебный процесс.
3. Психолого-медицинские риски – отрицательные воздействия на жизнь и здоровье учащихся и педагогов.
4. Управленческие (или организационные) риски – отрицательное влияние на управленческие процессы.
5. Финансовые риски – отрицательные воздействия на финансовое состояние учреждения (прямые финансовые потери).
6. Политические риски - отрицательные воздействия на репутацию учреждения
7. Принципы классификации информационных угроз.
8. Информационная безопасность детей с позиций психологического подхода
9. Безопасность социальной ситуации развития

10. Влияние СМИ на психическое развитие, здоровье и психологическое благополучие детей и подростков
11. Социальные сети. Детские социальные сети.
12. Признаки игровой зависимости.
13. Сетевые игры.
14. Критерии оценки состояния информационной безопасности проблемы детей и подростков (рекомендации для родителей, педагогов, психологов)
15. Формы работы по формированию информационной безопасности
16. Концепция информационной безопасности школьников и педагогические условия ее реализации
17. Организация информационно-безопасного образовательного процесса в школе, взаимосвязь с родителями школьников в решении
18. Медицинская информация в Интернете. Компьютеры и мобильные устройства в экстремальных условиях.

#### **Тема 4. Информационно-правовые нормы и информационные правоотношения**

Информационная политика.

1. Информационное общество: становление и развитие.
2. Тенденции развития международного информационного общества.
3. Проблемы становления информационного права в России.
4. Конституционно-правовые основы информационного законодательства.
5. Конституция Российской Федерации как источник прав в информационной области и источник правовых ограничений в сфере поиска информации и доступа к информации.
6. Информационно-психологическая безопасность.
7. Информационная безопасность общества, понятие информационной войны.
8. Средства массовой информации (СМИ) как институт современного общества; понятие, виды. Законодательство о СМИ в Российской Федерации. органов, осуществляющих государственное регулирование в сфере массовой информации. Полномочия государственных органов в отношении СМИ.
9. Процесс регистрации СМИ. Лицензирование в области СМИ, контроль за распространением СМИ.
10. Существующие ограничения свободы информации.
11. Информация в Глобальной информационной сети Интернет.
12. Защита интеллектуальной собственности в Интернет.
13. Порядок регистрации доменных имен.
14. Проблема идентификации пользователей.
15. Концепция Российского законодательства в области Интернета.

#### **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 дисциплины.

### 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:

<i>№</i>	<i>Критерии оценки компонентов презентации</i>	<i>Баллы (максимальное количество при полной выраженности критерия)</i>
<b>Структура презентации</b>		
1.	Правильное оформление титульного листа	4
2.	Наличие понятной навигации	4
3.	Отмечены информационные ресурсы	4
4.	Логическая последовательность информации на слайдах	4
<b>Оформление презентации</b>		
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
<b>Содержание презентации</b>		
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
<b>Эффект презентации</b>		
17.	Гармоничное дополнение устного выступления и общее впечатление от просмотра презентации	12
	<b>Сумма баллов</b>	<b>100</b>

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. Информационная безопасность – важнейшая составляющая национальной безопасности современной России.
2. Национальные интересы РФ в информационной сфере и их правовое и организационно-техническое обеспечение.
3. Основные составляющие национальных интересов в сфере информационной безопасности РФ.
4. Соблюдение прав и свобод человека и гражданина в области получения информации.
5. Информация как стратегический национальный ресурс.
6. Группы угроз в сфере информационной безопасности.
7. Виды уголовного преследования.
8. Роль информационной сферы.
9. Осведомленность человека и защита личной информации от несанкционированного доступа.
10. Основные цели и задачи обеспечения информационной безопасности общества, группы, личности, регламентируемые государством.
11. Информационная среда общества как системообразующий фактор во всех сферах национальной безопасности.
12. Обеспечение прав граждан на получение адекватной информации о жизнедеятельности общества.
13. Определение информации в научно-технической области и в области права.
14. Социальные и технические свойства информации.
15. Интеллектуальные информационные системы.
16. Проблемы организации электронного визирования документов в системах электронного документооборота.
17. Информационная культура.
18. Классификация и краткая характеристика каналов утечки информации.
19. Установление целей источника угроз информационной безопасности, установление задач информационной безопасности общества, социальной группы, личности.
20. Виды и источники угроз информационной безопасности РФ.
21. перехват информации через естественные каналы утечки и путем несанкционированного доступа.
22. Актуальные каналы утечки информации и их характеристика.
23. Собственность в Интернете. Авторское право.

24. Интеллектуальная собственность.
25. Платная и бесплатная информация.
26. Защита прав потребителей при использовании услуг Интернет. Защита прав потребителей услуг провайдера.
27. Киберпреступления. Виды интернет-мошенничества (письма, реклама, охота за личными данными и т.п.). Опасности мобильной связи. Предложения по установке вредоносных приложений.
28. Право на информацию, на сокрытие данных, категории информации.
29. Персональные и общедоступные данные, ограниченный доступ. Закон «О персональных данных».
30. Электронный кошелек. Мошенничество при распространении «бесплатного» ПО.
31. Классификация рисков в соответствии с объектом (субъектом) образовательного процесса на который они воздействуют.
32. Педагогические риски – отрицательные воздействия на учебный процесс.
33. Психолого-медицинские риски – отрицательные воздействия на жизнь и здоровье учащихся и педагогов.
34. Управленческие (или организационные) риски – отрицательное влияние на управленческие процессы.
35. Финансовые риски – отрицательные воздействия на финансовое состояние учреждения (прямые финансовые потери).
36. Политические риски - отрицательные воздействия на репутацию учреждения
37. Принципы классификации информационных угроз.
38. Информационная безопасность детей с позиций психологического подхода
39. Безопасность социальной ситуации развития
40. Влияние СМИ на психическое развитие, здоровье и психологическое благополучие детей и подростков
41. Социальные сети. Детские социальные сети.
42. Признаки игровой зависимости.
43. Сетевые игры.
44. Критерии оценки состояния информационной безопасности проблемы детей и подростков (рекомендации для родителей, педагогов, психологов)
45. Формы работы по формированию информационной безопасности
46. Концепция информационной безопасности школьников и педагогические условия ее реализации
47. Организация информационно-безопасного образовательного процесса в школе, взаимосвязь с родителями школьников в решении
48. Медицинская информация в Интернете. Компьютеры и мобильные устройства в экстремальных условиях.
49. Информационное общество: становление и развитие.
50. Тенденции развития международного информационного общества.
51. Проблемы становления информационного права в России.
52. Конституционно-правовые основы информационного законодательства.
53. Конституция Российской Федерации как источник прав в информационной области и источник правовых ограничений в сфере поиска информации и доступа к информации.
54. Информационно-психологическая безопасность.
55. Информационная безопасность общества, понятие информационной войны.
56. Средства массовой информации (СМИ) как институт современного общества; понятие, виды. Законодательство о СМИ в Российской Федерации. органов, осуществляющих государственное регулирование в сфере массовой информации. Полномочия государственных органов в отношении СМИ.



57. Процесс регистрации СМИ. Лицензирование в области СМИ, контроль за распространением СМИ.
58. Существующие ограничения свободы информации.
59. Информация в Глобальной информационной сети Интернет.
60. Защита интеллектуальной собственности в Интернет.

#### **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.

## Лист изменений рабочей программы дисциплины

№ п\п	Содержание изменений	Реквизиты документа об утверждении изменений	Дата внесения изменений
1.	Актуализирована в части учебно-методического и информационного обеспечения дисциплины в связи с продлением контракта с ЭБС и в части перечня основной и дополнительной литературы в связи с его изменением. Актуализирована в части лицензионного программного обеспечения в связи с его ежегодным обновлением.	Протокол заседания кафедры гуманитарных и социально-экономических дисциплин № 11 от «28» мая 2024 г.	28.05.2024 г.