

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Иванченко Ирина Васильевна
Должность: директор Филиала в г. Железноводске
Дата подписания: 04.07.2025 16:43:19
Уникальный программный ключ:
6ed79967cd09433ac580691de3e3e95b564cf0da

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

Кафедра гуманитарных и социально- экономических дисциплин

УТВЕРЖДАЮ

Заведующий кафедрой



М.Н. Арутюнян

протокол № 11

от 24.06.2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

Информационная безопасность

(наименование учебной дисциплины)

Уровень основной образовательной программы

бакалавриат

Направление(я) подготовки (специальность)

44.03.05 Педагогическое образование (с двумя профилями подготовки), профили
"Физическая культура" и "Безопасность жизнедеятельности"

Форма обучения

очная

Срок освоения

5 лет 0 месяцев

Кафедра

Кафедра гуманитарных и социально- экономических
дисциплин

**Год начала
подготовки**

2023

Железноводск, 2025 г.

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

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

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

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

Зав. кафедрой _____  М.Н. Арутюнян

Рабочая программа дисциплины согласована с заведующим библиотекой.

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

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

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
формирование системы знаний о современном состоянии проблемы обеспечения информационной безопасности, изучение основных понятий, методов и средств обеспечения информационной безопасности личности, общества и государства.	
2. ЗАДАЧИ ОСВОЕНИЯ 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.	
3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ООП:	Б1.В.ДВ.01
3.1. Требования к предварительной подготовке обучающегося:	
Безопасность жизнедеятельности	
Биохимия	
Концептуальные основы безопасности жизнедеятельности	
Методы исследовательской и проектной деятельности	
Методы математической обработки данных	
Основы медицинских знаний	
Первая помощь пострадавшим	
Природные опасности и защита от них	
Технологии цифрового образования	
Учебная практика (научно-исследовательская работа (получение первичных навыков научно-Философия	
3.2. Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:	
Безопасный отдых и туризм	
Выполнение и защита выпускной квалификационной работы	
Гражданская оборона	
Методика оздоровительной физической культуры	
Основы военной подготовки	
Основы научно-методической деятельности в физической культуре и спорте	
Производственная (педагогическая) практика 5	
Производственная практика (научно-исследовательская работа)	
Теория и методика организации дистанционного обучения в образовательных организациях	
Экологическая безопасность	
Этика. Эстетика	
4. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ	
Код и наименование компетенции	Код и наименование индикатора достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации,	УК-1.1 Демонстрирует знание особенностей системного и критического мышления,
УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной	УК-8.1 Оценивает факторы риска, умеет обеспечивать личную безопасность и

В результате освоения дисциплины обучающийся должен:

знать: особенности системного и критического мышления, принципы аргументированного формирования собственного суждения и оценки информации, принятие обоснованных решений.	уметь: анализировать источники информации с целью выявления их противоречий и поиска достоверных суждений.	владеть: применения логических форм и процедур, рефлексии по поводу собственной и чужой мыслительной деятельности; оценки факторов риска, умение обеспечивать личную безопасность и безопасность окружающих в повседневной жизни и в профессиональной деятельности.
5. ОБЪЕМ УЧЕБНОЙ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ		

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

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Се местр на курсе>)	7 (4.1)		Итого	
Неделя	16 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	16	16	16	16
Практические	20	20	20	20
Контактная работа на промежуточную аттестацию	0,3	0,3	0,3	0,3
Итого ауд.	36	36	36	36
Контактная работа	36,3	36,3	36,3	36,3
Сам. работа	35,7	35,7	35,7	35,7
Итого	72	72	72	72

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

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Основные понятия информационной безопасности					
1.1	Понятие об информационной безопасности общества. Цели и задачи обеспечения информационной безопасности. /Тема/	7	0			
1.2	Понятие об информационной безопасности общества. Цели и задачи обеспечения информационной безопасности. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.3	Понятие об информационной безопасности общества. /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	

1.4	Цели и задачи обеспечения информационной безопасности. /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.5	Цели и задачи обеспечения информационной безопасности. /Ср/	7	6	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.6	Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности. /Тема/	7	0			
1.7	Основные методы и средства обеспечения информационной безопасности. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.8	Установление целей и задач источника угрозы информационной безопасности. /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.9	Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности. /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.10	Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности. /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.11	Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности. /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
1.12	Основные методы и средства обеспечения информационной безопасности. Установление целей и задач источника угрозы информационной безопасности. /Ср/	7	12	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
	Раздел 2. Организация системы защиты информации					

2.1	Основные угрозы информационной безопасности в информационной образовательной среде /Тема/	7	0			
2.2	Основные угрозы информационной безопасности в информационной образовательной среде /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.3	Основные угрозы информационной безопасности в информационной образовательной среде /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.4	Основные угрозы информационной безопасности в информационной образовательной среде /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.5	Основные угрозы информационной безопасности в информационной образовательной среде /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.6	Основные угрозы информационной безопасности в информационной образовательной среде /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.7	Основные угрозы информационной безопасности в информационной образовательной среде /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.8	Основные угрозы информационной безопасности в информационной образовательной среде /Ср/	7	10	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.9	Правовое обеспечение информационной безопасности /Тема/	7	0			
2.10	Правовое обеспечение информационной безопасности /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	

2.11	Правовое обеспечение информационной безопасности /Лек/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.12	Правовое обеспечение информационной безопасности /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.13	Правовое обеспечение информационной безопасности /Пр/	7	2	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.14	Правовое обеспечение информационной безопасности /Ср/	7	7,7	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	
2.15	Зачет /КПА/	7	0,3	УК-1.1 УК-1.2 УК-1.3 УК-8.1 УК-8.2	Л1.1 Л1.2Л2.1 Л2.2	

* - Тема изучается с учетом профессиональной направленности

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

7. КОНТРОЛЬ КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль качества освоения учебного материала по дисциплине проводится в форме текущего контроля успеваемости и промежуточной аттестации в соответствии с «Положением о формах, периодичности и порядке текущего контроля успеваемости и промежуточной аттестации обучающихся в ГБОУ ВО СГПИ и его филиалах».

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

Уровень сформированности компетенции			
не сформирована	сформирована частично	сформирована в целом	сформирована полностью
«Не зачтено»	«Зачтено»		
«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
Описание критериев оценивания			
Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - допускаются принципиальные ошибки при ответе на	Обучающийся демонстрирует: - знания теоретического материала; - неполные ответы на основные вопросы, ошибки в ответе, недостаточное	Обучающийся демонстрирует: - знание и понимание основных вопросов контролируемого объема программного материала; - твердые знания	Обучающийся демонстрирует: - глубокие, всесторонние и аргументированные знания программного материала; - полное понимание

основные вопросы билета, отсутствует знание и понимание основных понятий и категорий; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие умения выполнять практические задания, предусмотренные программой дисциплины; - отсутствие готовности (способности) к дискуссии и низкая степень контактности.	понимание сущности излагаемых вопросов; - неуверенные и неточные ответы на дополнительные вопросы; - недостаточное владение литературой, рекомендованной программой дисциплины; - умение без грубых ошибок решать практические задания.	теоретического материала. - способность устанавливать и объяснять связь практики и теории, выявлять противоречия, проблемы и тенденции развития; - правильные и конкретные, без грубых ошибок, ответы на поставленные вопросы; - умение решать практические задания, которые следует выполнить; - владение основной литературой, рекомендованной программой дисциплины; Возможны незначительные неточности в раскрытии отдельных положений вопросов билета, присутствует неуверенность в ответах на дополнительные вопросы.	сущности и взаимосвязи рассматриваемых процессов и явлений, точное знание основных понятий в рамках обсуждаемых заданий; - способность устанавливать и объяснять связь практики и теории; - логически последовательные, содержательные, конкретные и исчерпывающие ответы на все задания билета, а также дополнительные вопросы экзаменатора; - умение решать практические задания; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.
---	---	---	---

8. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

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

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

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

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ ЛИТЕРАТУРЫ

9.1. Рекомендуемая литература

9.1.1. Основная литература

ЛП.1	Суворова Г. М. Информационная безопасность [Электронный ресурс]: учебное пособие для вузов. - Москва: Юрайт, 2024. - 277 с – Режим доступа: https://urait.ru/bcode/544029
------	---

9.1.2. Дополнительная литература

Л2.1	Коллеров А. С. Информационная безопасность [Электронный ресурс]: учебное пособие. - Екатеринбург: ЕАСИ, 2014. - 183 с. – Режим доступа: https://e.lanbook.com/book/136383
------	---

9.1.1. Основная литература

Л1.2	Лойко В. И., Лаптев В. Н., Аршинов Г. А., Лаптев С. Н. Информационная безопасность [Электронный ресурс]: учебное пособие. - Краснодар: КубГАУ, 2020. - 332 с. – Режим доступа: https://e.lanbook.com/book/254168
------	--

9.1.2. Дополнительная литература

Л2.2	Тимофеева Т. Ф. Защита интеллектуальной собственности и информационная безопасность [Электронный ресурс]: учебно-методическое пособие. - Чебоксары: ЧГУ им. И.Н. Ульянова, 2023. - 172 с. – Режим доступа: https://e.lanbook.com/book/388823
------	--

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

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

10.2. Профессиональные базы данных и информационные справочные системы

Университетская информационная система РОССИЯ	https://uisrussia.msu.ru
Единое окно доступа к образовательным ресурсам	http://window.edu.ru/catalog
Словари и энциклопедии	https://dic.academic.ru
Педагогическая мастерская «Первое сентября»	https://fond.1sept.ru
Сайт Единой коллекции цифровых образовательных ресурсов	http://school-collection.edu.ru
Национальная платформа «Открытое образование»	https://openedu.ru
Портал «Единая коллекция цифровых образовательных ресурсов»	http://school-collection.edu.ru
Российское образование. Федеральный портал	http://edu.ru

Портал Федеральных государственных образовательных стандартов высшего образования	http://fgosvo.ru
Единая цифровая коллекция первоисточников научных работ удостоверенного качества «Научный архив»	https://научныйархив.рф
Портал проекта «Современная цифровая образовательная среда в РФ»	https://online.edu.ru

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

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

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

Компьютерное оборудование имеет соответствующее лицензионное программное обеспечение:

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

**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.

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
«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-компаний

- 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.

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:

- 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.