ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

**«ЛЕНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ИМЕНИ А.С. ПУШКИНА»**

УТВЕРЖДАЮ

Проректор по учебно-методической

работе

\_\_\_\_\_\_\_\_\_\_\_\_ С.Н.Большаков

РАБОЧАЯ ПРОГРАММА

дисциплины

**Б1.В.05.ДВ.02.02 РЕАЛЬНЫЕ УГРОЗЫ ВИРТУАЛЬНОГО ПРОСТРАНСТВА**

Направление подготовки **44.03.05 Педагогическое образование
(с двумя профилями подготовки)**

Направленность (профиль) **Информатика и математика**

(год начала подготовки - 2022)

Санкт-Петербург

2022

**1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ:**

Процесс изучения дисциплины направлен на формирование следующих компетенций:

|  |  |  |
| --- | --- | --- |
| Индекс компетенции | Содержание компетенции (или ее части) | Индикаторы компетенций (код и содержание) |
| ПК-3 | Способен применять предметные знания при реализации образовательного процесса | ИПК-3.1. Знает закономерности, принципы и уровни формирования и реализации содержания образования в области информатики; структуру, состав и дидактические единицы содержания школьного курса информатики.ИПК-3.2. Умеет осуществлять отбор учебного содержания для реализации в различных формах обучения информатике в соответствии с дидактическими целями и возрастными особенностями обучающихся.ИПК-3.3. Владеет предметным содержанием с учетом взаимосвязи урочной и внеурочной форм обучения информатике. |

**2. Место дисциплины в структуре ОП:**

Цель дисциплины: формирование у обучающихся представлений о потенциальных рисках пребывания детей в глобальной сети и способах сохранения безопасности в условиях киберпространства.

Задачи дисциплины:

* характеристика возможностей и препятствий сетевого взаимодействия;
* классификация киберугроз;
* изучение способов защиты детей от вреда киберпространства;
* использования потенциала цифровых технологий в интересах каждого ребенка.

Дисциплина относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, модуль «Документационное обеспечение управления и информационная безопасность». Данной дисциплиной закладываются основы безопасного и полезного использования Интернета в решении практических задач и удовлетворения своих информационных потребностей с помощью интернет-ресурсов, формирование представлений о кибербезопасности, киберугрозах и способах защиты от них. Дисциплина имеет общекультурное значение и носит междисциплинарный характер.

Освоение дисциплины и сформированные при этом компетенции необходимы в последующей деятельности.

**3. Объем дисциплины и виды учебной работы:**

Общая трудоемкость освоения дисциплины составляет 2 зачетные единицы, 72 академических часа *(1 зачетная единица соответствует 36 академическим часам).*

Очная форма обучения

|  |  |
| --- | --- |
| Вид учебной работы | Трудоемкость в акад.час |
|  |  | Практическая подготовка |
| **Контактная работа (аудиторные занятия) (всего):** | 32 |
| в том числе: |  |
| Лекции | 16 | - |
| Лабораторные работы / Практические занятия (в т.ч. зачет) | -/16 | - |
| **Самостоятельная работа (всего)** | 40 |
| **Вид промежуточной аттестации (экзамен):** | - |
| контактная работа | - |
| самостоятельная работа по подготовке к экзамену | - |
| **Общая трудоемкость дисциплины (в час. /з.е.)** | 72/2 |

Заочная форма обучения

|  |  |
| --- | --- |
| Вид учебной работы | Трудоемкость в акад.час |
|  |  | Практическая подготовка |
| **Контактная работа (аудиторные занятия) (всего):** | 8 |
| в том числе: |  |
| Лекции | 4 | - |
| Лабораторные работы/ Практические занятия | -/4 | - |
| **Самостоятельная работа (всего)** | 60 |
| **Вид промежуточной аттестации (зачет):** | 4 |
| контактная работа | 0,25 |
| самостоятельная работа по подготовке к зачету | 3,75 |
| **Вид промежуточной аттестации (экзамен):** | - |
| контактная работа | - |
| самостоятельная работа по подготовке к экзамену | - |
| **Общая трудоемкость дисциплины (в час. /з.е.)** | 72/2 |

**4.СОДЕРЖАНИЕ ДИСЦИПЛИНЫ:**

При проведении учебных занятий обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая при необходимости проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, составленных на основе результатов научных исследований, проводимых организацией, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей**).**

**4.1 Блоки (разделы) дисциплины.**

|  |  |
| --- | --- |
| № | Наименование блока (раздела) дисциплины |
| 1 | Интернет как среда жизни человека, виртуальная реальность и средство коммуникации. Цифровизация системы образования. |
| 2 | Дети в цифровом мире. Воздействие цифровых технологий на детей. Дети и Интернет. |
| 3 | Цифровые возможности (перспективы сетевого взаимодействия), цифровые барьеры и цифровые опасности. |
| 4 | Киберугрозы (киберопасности). Риски, связанные с контентом, контактами и поведением.  |
| 5 | Кибербезопасность. Предупреждение и избегание киберугроз. |
| 6 | Цифровая грамотность как основа безопасности детей при работе в сети. |

**4.2. Примерная тематика курсовых работ (проектов):**

Курсовая работа по дисциплине не предусмотрена учебным планом.

**4.3. Перечень занятий, проводимых в активной и интерактивной формах, обеспечивающих развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств. Практическая подготовка**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование блока (раздела) дисциплины** | **Занятия, проводимые в активной и интерактивной формах** | **Практическая подготовка\*** |
| **Форма проведения занятия** | **Наименование видов занятий** |
| 1. | Интернет как среда жизни человека, виртуальная реальность и средство коммуникации. | лекция | лекция-дискуссия |  |
| практическое занятие | разбор конкретных ситуаций |  |
| 2. | Дети в цифровом мире. Воздействие цифровых технологий на детей. Дети и Интернет. | практическое занятие | разбор конкретных ситуаций |  |
| 3. | Цифровые возможности (перспективы сетевого взаимодействия), цифровые барьеры и цифровые опасности. | лекция | лекция-дискуссия |  |
| практическое занятие | разбор конкретных ситуаций |  |
| 4. | Киберугрозы (киберопасности). Риски, связанные с контентом, контактами и поведением. | практическое занятие | разбор конкретных ситуаций |  |
| 5. | Кибербезопасность. | лекция | лекция-визуализация |  |
| практическое занятие | разбор конкретных ситуаций |  |
| 6. | Цифровая грамотность как основа безопасности детей при работе в сети. | лекция | лекция-дискуссия |  |

**\***Практическая подготовка при реализации учебных предметов, курсов, дисциплин (модулей) организуется путем проведения практических занятий, практикумов, лабораторных работ и иных аналогичных видов учебной деятельности, **предусматривающих участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.**

**5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине:**

**5.1. Темы конспектов:**

Тема 1. Интернет как среда жизни человека, виртуальная реальность и средство коммуникации.

1. Особенности Интернет-среды, личность в виртуальном пространстве.

2. Цифровая социализация личности.

Тема 2. Дети в цифровом мире. Воздействие цифровых технологий на детей. Дети и Интернет.

1. Безопасность детей в Интернете.

2. Признаки негативного воздействия Интернета на ребенка.

3. Глобальный Интернет: угрозы и действия родителей.

**Тема 3. Цифровые возможности (перспективы сетевого взаимодействия), цифровые барьеры и цифровые опасности.**

1. Роль цифровых технологий в жизни человека. Возможности и недостатки сетевого взаимодейтсвия.

**Тема 4. Киберугрозы (киберопасности). Риски, связанные с контентом, контактами и поведением.**

1. Основные виды киберугроз.

2. Интернет-аферы.

3. Киберпреступность, ее классификация и борьба с ней.

**Тема 5. Кибербезопасность.**

1. Характеристика кибербезопасности.

2. Цели системы кибербезопасности.

**Тема 6. Цифровая грамотность как основа безопасности детей при работе в сети.**

1. Безопасность в цифровой среде.

2. Сущность и содержание цифровой грамотности обучающихся.

**5.2. Вопросы для подготовки к практическим занятиям:**

Способы доступа в Интернет. Шифрование данных при передачи информации в Интернет. Протоколы сети Интернет. Опасности Интернет. Типы компьютерных преступлений. Понятие кибербезопасности, основные категории кибербезопасности. Защита информации. Масштабы распространения киберугроз и основные виды киберугроз (киберпреступления, кибератака, кибертерроризм). Вредоносное программное обеспечение и вредоносный код. Виды вредоносного ПО (вирусы, черви, троянские программы, шпионское программное обеспечение, программы-вымогатели, рекламное программное обеспечение, боты, руткиты, баги). SQL-инъекция. Спам. Фишинг. Атаки Man-in-the-Middle («человек посередине»). DoS-атаки (атаки типа «отказ в обслуживании»). Программы-вымогатели и кибершантаж. Стандартные методы заражения и признаки заражения.

Способы защиты от кибератак: советы по кибербезопасности. Роль учителя в предупреждении наступления рисков при использовании Интернет.

Понятия «конфиденциальность», «персональные данные». Идентификация пользователя в сети. Правила создания надежного пароля. Безопасность личных данных в онлайн-играх. Схемы действий кибермошенников по доступу к аккаунту в онлайн-игре. Настройка уровня конфиденциальности личной информации в Google. Двухэтапная аутентификация. Интернет вещей и безопасность умного дома. Типы киберугроз для умного дома.

Понятие и виды контента. Цифровой контент. Классификация контента по уникальности, форме подачи информации, по доступности, по целевой аудитории и др. Организация контента в Сети. Способы поиска информации в сети Интернет. Фейковые (поддельные) новости и правильная реакция на них. Характеристики опасного контента в сети Интернет. Федеральный закон от 29.12.2010 г. №436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Программы родительского контроля. Развитие у ребенка правильной реакции на негативную информацию. Признаки негативного воздействия Интернета на ребенка. Действия педагога по снижению рисков киберугроз для детей. Полезный образовательный контент.

Особенности общения в сети Интернет. Правила безопасного общения и переписки в сети Интернет. Безопасное поведение в социальных сетях. Знакомства в Интернете. Безопасная работа с электронной почтой. Безопасное взаимодействие с мобильными приложениями. Безопасная работа в Скайпе. Правила сетевой этики. Нетикет.

Интернет-зависимость. Формы интернет-зависимости у детей. Признаки интернет-зависимости у ребенка и способы ее профилактики и борьбы с ней. Игровая зависимость. Факторы, оказывающие влияние на развитие игровой зависимости (личностный фактор, дефицит общения, нарушение психики, система вознаграждений). Критерии диагностики игровой зависимости.

Понятие об интернет-мошенничестве и компьютерном хулиганстве. Схемы интернет-мошенничества. Виды компьютерного хулиганства. Кибербуллинг. Признаки кибербуллинга. Профилактика кибербуллинга и противодействие ему учителя. Правила поведения для ребенка при кибербуллинге. Троллинг. Способы противостояния троллингу. Правила поведения для ребенка при троллинге.

Безопасная работа с файлами, ссылками и сайтами сети Интернет. Безопасное использование сети Wi-Fi. Безопасная работа с цифровыми устройствами (смартфонами и планшетами, цифровыми веб-камерами, устройств умного дома). Вирусы и антивирусные программы. Защита компьютера от вирусов.

Объекты авторских прав. Понятие «интеллектуальная собственность», «авторское право». Федеральный закон №149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации». Права автора. Ответственность за нарушение авторских прав. Виды ответственности за нарушение авторских прав. Срок действия авторских прав. Легальное использование контента.

**5.3. Вопросы для устного опроса:**

1. Как Вы думаете, кто может увидеть Вашу персональную информацию, которая плохо защищена?
2. Зачем злоумышленникам нужен доступ к информации о Вас? Что они хотят выяснить? Почему некоторые сайты, где Вы не выполнили вход, пытаются следить за вами?
3. Что такое вредоносное ПО? Каково его предназначение?
4. Как защититься от вредоносного ПО или слежки?
5. Решите для себя, готовы ли вы к тому, что кто-то будет следить за вами? Насколько важна для вас конфиденциальность?
6. Дайте определение понятию «кибербезопасность».
7. Назовите основные категории, в рамках которых актуальна кибербезопасность.
8. Оцените масштабы распространения киберугроз в современном мире.
9. Охарактеризуйте виды киберугроз.
10. Что такое киберпреступления, кибератака, кибертерроризм?
11. Чем отличается вредоносное программное обеспечение и вредоносный код?
12. Охарактеризуйте вирусы, троянцы, шпионское программное обеспечение, программы-вымогатели, рекламное программное обеспечение, ботнеты.
13. Что такое фишинг и как на него реагировать?
14. Какие программы-вымогатели Вы знаете?
15. Опишите SQL-инъекцию как вид кибератак.
16. Что такое спам и фишинг?
17. Охарактеризуйте атаки Man-in-the-Middle.
18. Охарактеризуйте DoS-атаки.
19. Опишите способы защиты от кибератак.
20. Почему одним людям мы готовы сообщить больше информации, чем другим?
21. Какой личной информацией вы готовы делиться с другими людьми?
22. Вся ли личная информация должна быть секретной?
23. Какую информацию Вы бы не стали передавать малознакомым людям?
24. Прокомментируйте, какие требования предъявляются к созданию надежного пароля?
25. В каких ситуациях делиться паролем допустимо?
26. Чем вы рискуете, передавая свой пароль кому-либо?
27. Как самому повысить надёжность пароля?
28. Как часто целесообразно менять пароли?
29. Какие опасности могут возникнуть у ученика в онлайн-играх?
30. Как могут киберпреступники использовать аккаунт онлайн-игрока?
31. Что такое двухэтапная аутентификация?
32. Какие существуют способы сохранения конфиденциальности персональной информации в Google?
33. Как обеспечить безопасность умных устройств?
34. Какие опасности включает интернет вещей?
35. Представьте, что Вы решили выполнить в Интернете поиск по своему имени (например, в поисковой системе или в социальной сети) и нашли о себе негативную информацию. Как Вы поступите?
36. Если возможно, приведите примеры контента о себе, который Вы хотели бы скрыть от окружающих?
37. Какие киберугрозы связаны с контентом в сети Интернет?
38. На основании каких критериев можно оценить информацию в Интернете: как полезную и как вредную?
39. Какие существуют способы защиты детей от негативной информации в Сети?
40. Какая позитивная информация может помочь в борьбе с негативной?
41. Охарактеризуйте наиболее опасные для детей интернет-сервисы.
42. Что такое родительский контроль?
43. Приведите примеры программ родительского контроля.
44. Как Вы считаете, можно запретить ребенку общение в социальных сетях? К чему это может привести?
45. Какие сайты могут оказаться потенциально опасными для детей, от каких сайтов должен уберечь учитель школьников?
46. Охарактеризуйте признаки, по которым можно судить о негативном виртуальном влиянии на ребенка?
47. Как Вы поступите, если заметите хотя бы один из этих признаков?
48. Какие действия должен предпринимать учитель в организации учебного процесса и внеурочной деятельности, чтобы снизить риски киберугроз?
49. Какие полезные и интересные ребенку сайты Вы знаете?
50. Как можно использовать полезный образовательный контент в Вашей профессиональной деятельности?
51. Какие опасности ожидают ребенка при общении в Интернете?
52. Опишите правила безопасного поведения и общения в социальных сетях.
53. Опишите правила безопасности при общении по электронной почте.
54. Как часто Вы знакомитесь в Интернете первыми? Как часто знакомятся с Вами?
55. Приведите примеры мобильных приложений в виде социальных сетей и охарактеризуйте правила безопасной работы с ними.
56. С какими рисками может столкнуться ребенок в социальных сетях?
57. Как организовать безопасную работу в скайпе?
58. Что такое сетевой этикет?
59. Сформулируйте правила сетевой этики при общении в социальных сетях.
60. Сформулируйте правила сетевой этики при общении в чатах и на форумах.
61. Сформулируйте правила сетевой этики при общении в онлайн-играх.
62. Сформулируйте правила сетевой этики при общении по электронной почте.
63. Дайте определение интернет-зависимости.
64. Охарактеризуйте механизм формирования интернет-зависимости.
65. У кого возникает интернет-зависимость?
66. Какие формы интернет-зависимости можно назвать?
67. Назовите признаки и симптомы интернет-зависимости у ребенка.
68. Как следует действовать, если Вы обнаружили у ребенка интернет-зависимость?
69. Что такое игровая зависимость?
70. Как возникает игровая зависимость?
71. Какие стадии можно выделить при возникновении игровой зависимости?
72. Какие факторы оказывают влияние на развитие игровой зависимости?
73. Назовите признаки и симптомы игровой зависимости у ребенка.
74. Охарактеризуйте критерии диагностики игровой зависимости.
75. Дайте определение понятию «мошенничество» и «хулиганство».
76. Назовите основные виды виртуального мошенничества.
77. Кто такие компьютерные хулиганы?
78. Какая ответственность возлагается на виртуальное мошенничество и компьютерное хулиганство?
79. Знаете ли вы, что такое «бомбардировка сообщениями»? Дайте своё определение этому термину.
80. Что Вы посоветуете другу, который попал под «бомбардировку» сообщениями? Будете ли вы принимать меры? Какие?
81. Что такое кибербуллинг?
82. По каким признакам можно определить кибербуллинг как вид хулиганства?
83. Опишите меры профилактики и правила поведения при кибербуллинге.
84. Что такое троллинг?
85. По каким признакам можно определить троллинг как вид хулиганства?
86. Опишите правила поведения при троллинге.
87. Как правильно организовать безопасную работу с файлами в сети Интернет?
88. Можно ли безопасно работать с Wi-Fi?
89. Как осуществить безопасное взаимодействие со смартфонами и планшетами?
90. Как осуществить безопасное взаимодействие с цифровыми веб-камерами?
91. Может ли быть опасным умный дом?
92. Как обеспечить безопасность интернета-вещей?
93. Что такое компьютерные вирусы и как работают антивирусные программы?
94. Приведите примеры компьютерных вирусов и антивирусных программ.
95. Какую опасность таит поддельный сайт, который сложно отличить от настоящего?
96. Назовите средства борьбы с потенциальными угрозами в Сети Интернет.
97. Что необходимо делать, чтобы вредоносные файлы не попали на ваш компьютер?
98. Что означает фраза «соблюдать авторское право»?
99. Какими статьями Гражданского Кодекса регламентируются вопросы авторского права?
100. Что относится к объектам авторского права? Перечислите основные компоненты.
101. Приведите примеры, объектов Вашего авторского права. Есть ли уже у Вас такие объекты?
102. Можно ли свободно использовать и распространять информацию в Интернете, не нарушая чьих-либо прав? Почему?
103. Как Вы считаете, в чём заключаются правила сетевого этикета?
104. Охарактеризуйте, что понимают под использованием произведения.
105. На какой срок распространяется авторское право?
106. Какие объекты не являются объектами авторского права?
107. Что Вам известно по поводу авторского права на программы для компьютера и сайты Интернета, охраняются ли они авторским правом?
108. Что нельзя делать без согласия?
109. Какие существуют способы использования чужого контента?
110. Что понимают под смежными правами?
111. Какие виды ответственности предусмотрены российским законодательством за нарушение авторских прав?

**6 Оценочные средства для текущего контроля успеваемости:**

**6.1. Текущий контроль**

|  |  |  |
| --- | --- | --- |
| №пп | № и наименование блока (раздела) дисциплины | Форма текущего контроля |
| 1 | Темы 1-8 | Проверка конспектов, устный опрос |
| 2 | Темы 1-8 | Тест |

**6.2. Примеры оценочных средств для текущего контроля по дисциплине**

***Темы конспектов.***

Представлены в разделе 5.1.

***Примеры тестовых заданий.***

**1.** Какой из предложенных паролей лучше выбрать?

а) NoTeb!!k

б) qwerty

в) [Дата рождения]

г) 123456

**2.** Что нужно сделать в первую очередь, если компьютер подвергся атаке?

а) Отключить компьютер от Интернета

б) Выйти из браузера

в) Проверить сохранение важных файлов

г) Запустить проверку компьютера антивирусной программой

**3.** Вам пришло письмо: «Чтобы выиграть миллион в нашей лотерее, нужно зарегистрироваться на этом сайте (ссылка на сайт). Регистрация закрывается завтра. Не пропустите!». Что Вы сделаете?

а) Зайду на сайт и посмотрю, что за лотерея

б) Напишу в ответ письмо, где попрошу прислать подробности о лотерее

в) Удалю письмо. Я ничего не знаю об этом сайте и авторе письма. Скорее всего, это спам.

**4.** Что делать, если вы стали жертвой интернет-травли?

а) Сыпать угрозами в ответ, предлагать встретиться и разобраться

б) Выбросить компьютер

в) Ничего не делать, терпеть

г) Обратиться в администрацию ресурса с просьбой наказать обидчика

**5.** При установке приложения обработки фотографий на смартфон приложение просит доступ к СМС-сообщениям и телефонной книге. Согласиться или нет?

а) Согласиться, поскольку это безопасно

б) Не согласиться, поскольку это небезопасно

**6.** Что не является персональными данными?

а) Фамилия, имя, отчество

б) Паспортные данные

в) История болезни

г) Дата и место рождения.

**7.** Клавиатурный шпион – это:

а) Программа, отслеживающая ввод пользователем паролей и пин-кодов

б) Юридический термин, используемый для обозначения правонарушений, связанных с информационной безопасностью.

**8.** Троянская программа опасна тем, что:

а) Проникает на компьютер под видом полезной программы и выполняет вредоносные действия без ведома пользователя

б) Вынуждает пользователя возвращать долги данайцев (древнегреч. миф.)

в) Ищет на доске какого-то коня, снижая производительность системы

г) Обладает всеми вышеперечисленными возможностями

**9.** Главной функцией брандмауэра является

а) Защита компьютера от взлома хакерами, а также всевозможных вирусов и «троянов»

б) Упрощение и оптимизация работы операционной системы

в) Дополнительное офисное приложения для работы с базами данных

**10.** При просмотре веб-сайтов и общении через Интернет:

а) Вы оставляете электронные следы («цифровые отпечатки»), по которым можно определить, какие страницы Вы просматривали и какой IP-адрес компьютера Вы использовали

б) Вы оставляете электронные следы, которые можно удалить самому

в) Никто не может проследить, какие веб-страницы Вы просматривали

г) Вы оставляете электронные следы, которые хранятся только на Вашем компьютере

**11.** Укажите устройство для подключения компьютера к сети:

а) Модем

б) Мышь

в) Сканер

г) Монитор

**12.** Авторские посты, размещаемые пользователями в социальных сетях и блогах:

а) Показывают уникальность человека и всегда позитивно влияют на его репутацию

б) Никогда не содержат персональной информации, поэтому их публикация не несет серьезных последствий

в) Оцениваются читателями по-разному, поэтому невозможно предсказать, как публикация поста отразится на репутации его автора

г) Всегда содержат излишнюю персональную информацию о человеке, что может навредить не только его репутации, но и личной безопасности

д) Не содержат ничего хорошего, поскольку свидетельствуют исключительно о желании похвастаться и продемонстрировать то, чего на самом деле нет

***Ответы к тесту***: 1. а; 2. г; 3. в; 4. г; 5. б; 6. в; 7. а; 8. а; 9. а; 10. а; 11. а; 12. в

**7. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № п/п | Наименование | Авторы | Место издания | Год издания | Наличие |
| печатные издания | ЭБС (адрес в сети Интернет) |
| 1. | Web-технологии в профессиональной деятельности учителя: учебное пособие | Белоконова С. С. | Москва; Берлин: Директ-Медиа | 2020 |  | <http://biblioclub.ru>  |
| 2. | Риски интернет-коммуникации детей и молодежи: учебное пособие | Лесконог Н.Ю., Жилавской И.В., Бродовской Е.В. | Москва: МПГУ | 2019 |  | <http://biblioclub.ru> |
| 3. | Основы эксплуатации компьютерных сетей: учебник для бакалавров | Демидов Л.Н. | Москва: Прометей | 2019 |  | <http://biblioclub.ru> |
| 4.  | Международные стандарты правовой защиты информации и информационных технологий: учебное пособие | Арзуманян А. Б. | Ростов-на-Дону; Таганрог: Южный федеральный университет | 2020 |  | <http://biblioclub.ru> |

**8. Ресурсы информационно-телекоммуникационной сети «Интернет»:**

1. «НЭБ». Национальная электронная библиотека. – Режим доступа: [http://нэб.рф/](http://www.biblioclub.ru/)

2. «eLibrary». Научная электронная библиотека. – Режим доступа: [https://elibrary.ru](https://elibrary.ru/)

3. «КиберЛенинка». Научная электронная библиотека. – Режим доступа: <https://cyberleninka.ru/>

4. ЭБС «Университетская библиотека онлайн». – Режим доступа: [http://www.biblioclub.ru/](http://www.knigafund.ru/)

5. Российская государственная библиотека. – Режим доступа: <http://www.rsl.ru/>

**9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ИСПОЛЬЗУЕМЫЕ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ:**

В ходе осуществления образовательного процесса используются следующие информационные технологии:

- средства визуального отображения и представления информации (LibreOffice) для создания визуальных презентаций как преподавателем (при проведении занятий) так и обучаемым при подготовке докладов для семинарского занятия.

- средства телекоммуникационного общения (электронная почта и т.п.) преподавателя и обучаемого.

- использование обучаемым возможностей информационно-телекоммуникационной сети «Интернет» при осуществлении самостоятельной работы.

**9.1. Требования к программному обеспечению учебного процесса**

Для успешного освоения дисциплины, обучающийся использует следующие программные средства:

* Windows 10 x64
* MicrosoftOffice 2016
* LibreOffice
* Firefox
* GIMP

**9.2. Информационно-справочные системы (при необходимости):**

Не используются

**10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Для проведения занятий лекционного типа предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий.

Для изучения дисциплины используется следующее оборудование: аудитория, укомплектованная мебелью для обучающихся и преподавателя, доской, ПК с выходом в интернет, мультимедийным проектором и экраном.

Для самостоятельной работы обучающихся используется аудитория, укомплектованная специализированной мебелью и техническими средствами (ПК с выходом в интернет и обеспечением доступа в электронно-информационно-образовательную среду организации).