

Документ подписан простой электронной подписью  
Информация о владельце:  
ФИО: Жуйкова Татьяна Валерьевна  
Должность: Директор  
Дата подписания: 02.09.2026 16:02:05  
Уникальный программный ключ:  
d3b13764ec715c944271e8630f1e6d3513421163

Министерство просвещения Российской Федерации  
Нижнетагильский государственный социально-педагогический институт (филиал)  
федерального государственного автономного образовательного учреждения  
высшего образования  
«Российский государственный профессионально-педагогический университет»

Факультет естествознания, математики и информатики  
Кафедра информационных технологий и физико-математического образования

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**  
**Б1.О.08.14 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ**

|                        |                                                                    |
|------------------------|--------------------------------------------------------------------|
| Направление подготовки | 44.03.05 Педагогическое образование (с двумя профилями подготовки) |
| Профиль программы      | Все профили                                                        |
| Автор:                 | Доцент кафедры ИТФМ Васева Е. С.                                   |

Одобрена на заседании кафедры информационных технологий и физико-математического образования. Протокол от 12 января 2023 г. № 6.

Рекомендована к использованию в образовательной деятельности научно-методической комиссией ФЕМИ НТГСПИ (ф) РГППУ. Протокол от 22 января 2023 г. № 5.

## СОДЕРЖАНИЕ

|                                                                       |   |
|-----------------------------------------------------------------------|---|
| 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....                             | 3 |
| 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ.....        | 3 |
| 3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....                                | 3 |
| 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ.....                             | 4 |
| 4.1. Объем дисциплины и виды контактной и самостоятельной работы..... | 4 |
| 4.2. Содержание и тематическое планирование дисциплины.....           | 5 |
| 4.3. Содержание разделов (тем) дисциплин.....                         | 5 |
| 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.....                                    | 7 |
| 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ.....              | 8 |
| 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....                | 9 |

## **1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

Цель дисциплины – формирование компетенций будущих учителей в области обеспечения информационной безопасности участников образовательных отношений и защиты информации в условиях современной информационной образовательной среды.

### **Задачи дисциплины:**

- познакомить студентов с правовыми основами и нормами профессиональной этики в сфере обеспечения информационной безопасности;
- сформировать навыки взаимодействия с участниками образовательных отношений при соблюдении норм профессиональной этики и требований соблюдения конфиденциальности информации;
- сформировать умения обоснованного выбора и использования современных информационных технологий и программных средств, в том числе отечественного производства, для решения задач обеспечения информационной безопасности участников образовательных отношений;
- сформировать способности использовать теоретические знания и практические умения в области информационной безопасности и защиты информации при разработке учебных программ, отборе содержания учебных предметов, разработке различных форм учебных занятий, формировании развивающей образовательной среды.

## **2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ**

Дисциплина «Информационная безопасность и защита информации» является частью основных образовательных программ подготовки бакалавров по направлению 44.03.05 Педагогическое образование (с двумя профилями подготовки). Дисциплина входит в обязательную часть образовательной программы, включена в Блок Б.1 «Дисциплины (модули)» и является составной частью предметно-методического модуля по профилю «Информатика». Реализуется кафедрой информационных технологий и физико-математического образования в 10 семестре.

Дисциплина «Информационная безопасность и защита информации» базируется на компетенциях, полученных при изучении дисциплин «Технологии цифрового образования», «Информационные системы и управление данными», «Сети и телекоммуникации», «Теория и методика обучения информатике».

## **3. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ**

Процесс изучения дисциплины направлен на формирование и развитие следующих компетенций:

ОПК-1. Способен осуществлять профессиональную деятельность в соответствии с нормативными правовыми актами в сфере образования и нормами профессиональной этики.

ОПК-4. Способен осуществлять духовно-нравственное воспитание обучающихся на основе базовых национальных ценностей.

ОПК-7. Способен взаимодействовать с участниками образовательных отношений в рамках реализации образовательных программ.

ОПК-9. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности.

ПК-1. Способен осуществлять обучение учебному предмету на основе использования предметных методик и современных образовательных технологий.

ПК-2. Способен осуществлять целенаправленную воспитательную деятельность.

ПК-3. Способен применять предметные знания при реализации образовательного процесса.

В результате освоения дисциплины (модуля) обучающийся должен знать:

31. Нормативно-правовую базу, регламентирующую отношения в сфере информационной безопасности, позволяющую организовать защиту жизни и здоровья обучающихся;

32. Основные понятия курса (информационная безопасность, угроза, защита информации, персональные данные, интеллектуальная собственность, конфиденциальность, авторские права и др.);

33. административные и процедурные принципы обеспечения защиты информации при организации информационно-образовательной среды;

34. основные сервисы современных информационных систем обеспечения информационной безопасности;

Уметь:

У1. Определять структуру и содержание образовательных программ по учебному предмету в соответствии с образовательными стандартами с учетом требований информационной безопасности;

У2. Применять предметные знания в области информационной безопасности при реализации образовательного процесса;

У3. Создавать условия для формирования у обучающихся конкретных знаний, умений и навыков в области информационной безопасности;

У4. Организовывать ограничение доступа к контенту, далекого от дидактических задач,

У5. Использовать программно-технические сервисы защиты информации;

Владеть:

В1. Навыками анализа деятельности организации на соответствие нормативно-правовым документам в области информационной безопасности;

В2. Навыками планирования образовательных программ по учебному предмету согласно требованиям образовательных стандартов и информационной безопасности;

В3. Способностью установки и настройки программно-технических сервисов защиты информации при проектировании, разработке и сопровождении информационно-образовательной среды.

## 4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

### 4.1. Объем дисциплины и виды контактной и самостоятельной работы

Общая трудоемкость дисциплины составляет 3 зач. ед. (108 час.), семестр изучения – 10, распределение по видам работ представлено в табл.№1.

Таблица 1. Распределение трудоемкости дисциплин по видам

| Вид работы                                             | Форма обучения   |
|--------------------------------------------------------|------------------|
|                                                        | очная            |
|                                                        | Семестр изучения |
|                                                        | 10 семестр       |
|                                                        | Кол-во часов     |
| <b>Общая трудоемкость</b> дисциплины по учебному плану | <b>108</b>       |
| <b>Контактная работа, в том числе:</b>                 | <b>42</b>        |
| Лекции                                                 | 14               |

|                                        |            |
|----------------------------------------|------------|
| Лабораторные работы                    | 28         |
| Самостоятельная работа                 | 66         |
| Промежуточная аттестация, в том числе: |            |
| Экзамен                                | 10 семестр |

#### 4.2. Содержание и тематическое планирование дисциплины

Таблица 2. Тематический план дисциплины

| Наименование разделов и тем дисциплины (модуля)                                               | Сем. | Всего часов | Контактная работа |             |               | Сам. работа |
|-----------------------------------------------------------------------------------------------|------|-------------|-------------------|-------------|---------------|-------------|
|                                                                                               |      |             | Лекции            | Лаб. работы | Практ. работы |             |
| Введение в проблему информационной безопасности. Основные понятия информационной безопасности | 10   | 6           | 2                 |             |               | 4           |
| Угрозы информационной безопасности и методы их реализации                                     | 10   | 8           | 2                 | 2           |               | 4           |
| Правовые основы информационной безопасности и защиты персональных данных                      | 10   | 15          | 2                 | 6           |               | 7           |
| Программные средства защиты информации                                                        | 10   | 12          | 2                 | 6           |               | 4           |
| Технические средства защиты и комплексное обеспечение информационной безопасности             | 10   | 14          | 2                 | 4           |               | 8           |
| Элементы криптографии                                                                         | 10   | 12          | 2                 | 4           |               | 6           |
| Общие меры по созданию безопасной ИС в образовательном учреждении                             | 10   | 14          | 2                 | 6           |               | 6           |
| Экзамен                                                                                       | 10   | 27          | -                 |             | -             | 27          |
| <b>Итого</b>                                                                                  |      | 108         | 14                | 28          | 0             | 66          |

#### 4.3. Содержание разделов (тем) дисциплин

**Тема 1. Введение в проблему информационной безопасности. Основные понятия информационной безопасности.**

Персональные данные как вид защищаемой информации. Определение и эволюция понятия «информационная безопасность». Цели, задачи, направления информационной безопасности. Базовые принципы обеспечения информационной безопасности.

Программа информационной безопасности России и пути ее реализации. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности РФ. Концепция информационной безопасности.

## **Тема 2. Угрозы информационной безопасности и методы их реализации.**

Виды возможных нарушений информационной системы. Понятие угрозы. Анализ угроз безопасности информации. Причины, виды, каналы утечки и искажения информации. Основные методы реализации угроз информационной безопасности: методы нарушения секретности, целостности и доступности информации. Информационная безопасность в условиях функционирования в России глобальных сетей.

## **Тема 3. Правовые основы информационной безопасности и защиты персональных данных.**

Современное состояние правового регулирования в информационной сфере. Правовое обеспечение информационной безопасности.

Основные нормативные руководящие документы, касающиеся государственной тайны, защиты персональных данных, интеллектуальной собственности, авторского права, нормативно-справочные документы.

## **Тема 4. Программные средства защиты информации.**

Компьютерные вирусы и антивирусная защита.

Парольная защита. Идентификация и аутентификация. Разграничение доступа. Межсетевые экраны как средство защиты от несанкционированного доступа. Средства родительского контроля.

## **Тема 5. Технические средства защиты и комплексное обеспечение информационной безопасности.**

Средства контроля доступа в информационных системах. Технические средства защиты информации. Механические системы защиты информации. Электронные ключи и замки. Биометрические системы идентификации.

Основные этапы обеспечения защиты информации: определение политики и составляющих информационной безопасности, управление рисками, аудит информационной безопасности. Меры и методы по защите информации в образовательных организациях.

Анализ и оценивание угроз информационной безопасности личности в цифровой образовательной среде. Интернет-зависимость. Влияние социальных сетей на адаптацию молодежи.

## **Тема 6. Элементы криптографии.**

Понятие шифра. Симметричное и асимметричное шифрование. Односторонние функции. Метод RSA. Электронная подпись.

## **Тема 7. Общие меры по созданию безопасной ИС в образовательном учреждении.**

Изучение и реализация основных направлений законодательства РФ по вопросам информационной безопасности образовательного учреждения. ФЗ «О персональных данных». ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию». Разработка методических рекомендаций. Использование контентной фильтрации Интернета, для фильтрации сайтов с одержимым, далёким от задач образования. Обучение детей основам информационной безопасности, воспитание информационной культуры.

### **Лабораторные работы для очной формы обучения**

| <b>№ п.п.</b> | <b>Тема занятия</b>                                                          | <b>Количество часов</b> |
|---------------|------------------------------------------------------------------------------|-------------------------|
| 1.            | Анализ угроз информационной безопасности                                     | 2                       |
| 2.            | Анализ основных нормативных документов в области информационной безопасности | 2                       |

|     |                                                                                                                                |    |
|-----|--------------------------------------------------------------------------------------------------------------------------------|----|
| 3.  | Политика информационной безопасности организации. Частная модель угроз                                                         | 2  |
| 4.  | Обеспечение безопасности при работе с документами                                                                              | 2  |
| 5.  | Возможности защиты информации в операционной системе                                                                           | 2  |
| 6.  | Работа с командной строкой. Сетевая активность                                                                                 | 2  |
| 7.  | Защита от несанкционированного доступа и сетевых хакерских атак                                                                | 2  |
| 8.  | Основные признаки присутствия на компьютере вредоносных программ. Установка и предварительная настройка антивирусной программы | 2  |
| 9.  | Использование контентной фильтрации Интернета, для фильтрации сайтов с одержимым, далёким от задач образования                 | 2  |
| 10. | Методы криптографии                                                                                                            | 4  |
| 11. | Обучение детей основам информационной безопасности, воспитание информационной культуры                                         | 6  |
|     | Итого                                                                                                                          | 28 |

## 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Обучение по дисциплине «Информационная безопасность и защита информации» целесообразно построить с использованием компетентностного подхода, в рамках которого образовательный процесс строится с учетом специфики будущей профессиональной деятельности студентов.

Лекционные занятия должны стимулировать познавательную активность студентов, поэтому в ходе лекций необходимо обращение к примерам, взятым из практики, включение проблемных вопросов и ситуаций.

Основными методами, используемыми на практических занятиях, будут: практикум с использованием практико-ориентированных задач, метод проектов, метод проблемных ситуаций.

При реализации образовательной программы с применением дистанционных образовательных технологий и электронного обучения:

- состав видов контактной работы по дисциплине (модулю), при необходимости, может быть откорректирован в направлении снижения доли занятий лекционного типа и соответствующего увеличения доли консультаций (групповых или индивидуальных) или иных видов контактной работы;

- информационной основой проведения учебных занятий, а также организации самостоятельной работы обучающихся по дисциплине (модулю) являются представленные в электронном виде методические, оценочные и иные материалы, размещенные в электронной информационно-образовательной среде (ЭИОС) филиала, в электронных библиотечных системах и открытых Интернет-ресурсах;

- взаимодействие обучающихся и педагогических работников осуществляется с применением ЭИОС филиала и других информационно-коммуникационных технологий (видеоконференцсвязь, облачные технологии и сервисы, др.);

- соотношение контактной и самостоятельной работы по дисциплине (модулю) может быть изменено в сторону увеличения последней, в том числе самостоятельного изучения теоретического материала.

## 6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

### 6.1. Основная литература

1. Кисляков, П. А. Безопасность образовательной среды. Социальная безопасность : учебное пособие для вузов / П. А. Кисляков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2023. — 156 с. — (Высшее образование). — ISBN 978-5-534-11818-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/518183>. (дата обращения: 2024 г.).

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2024. — 325 с. — (Высшее образование). — ISBN 978-5-534-03600-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/536225> (дата обращения: 2024 г.).

3. Чернова, Е. В. Информационная безопасность человека : учебное пособие для вузов / Е. В. Чернова. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2020. — 243 с. — (Высшее образование). — ISBN 978-5-534-12774-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/449350> (дата обращения: 2022 г.).

## **6.2. Дополнительная литература**

1. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2020. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451108> (дата обращения: 2024 г.).

2. Информационное право : учебник для вузов / Н. Н. Ковалева [и др.] ; под редакцией Н. Н. Ковалевой. — Москва : Издательство Юрайт, 2020. — 353 с. — (Высшее образование). — ISBN 978-5-534-13786-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/466887> (дата обращения: 2024 г.).

3. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/454453> (дата обращения: 2024 г.).

4. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2020. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/448295> (дата обращения: 2024 г.).

5. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: <https://urait.ru/bcode/451486> (дата обращения: 2024 г.).

## **6.3. Программное обеспечение и Интернет-ресурсы**

Интернет-ресурсы:

1. eLIBRARY.RU : научная электронная библиотека : сайт. — Москва, 2000. — URL: <https://elibrary.ru> (дата обращения: 2024 г.). — Режим доступа: для зарегистрир. пользователей. — Текст: электронный.

2. INTUIT.ru : Учебный курс — Защита детей от вредной информации : сайт. URL: <https://intuit.ru/studies/courses/3452/694/info>. (дата обращения: 2024 г.). — Режим доступа: для зарегистрир. пользователей. — Текст: электронный.

3. STEPik : Учебный курс — Введение в кибербезопасность : сайт. URL: <https://stepik.org/course/61595/syllabus>. (дата обращения: 2024 г.). — Режим доступа: для зарегистрир. пользователей. — Текст: электронный.

4. Единое окно доступа к образовательным ресурсам : Федеральный портал. — URL: <http://window.edu.ru/window/library>. (дата обращения: 2024 г.). — Режим доступа: свободный — Текст: электронный.

Программное обеспечение:

1. Среда электронного обучения «Русский Moodle» (<https://do.ntspi.ru/>).
2. Интернет-платформа онлайн-курсов со свободным кодом «Open edX» (<https://www.edx.org/>).
3. Интернет-платформа онлайн-курсов «Открытое образование» (<https://openedu.ru/>).
4. Электронная информационно-образовательная среда РГППУ (<https://eios.rsvpu.ru/>).
5. Платформа для организации и проведения вебинаров «Mirapolis Virtual Room».
6. Microsoft Office /LibreOffice /Р-Офис.
7. Kaspersky Endpoint Security.
8. Adobe Reader.
9. Браузеры Firefox, Google Chrome, Яндекс.Браузер.

## **7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Перечень материально-технического обеспечения для реализации образовательного процесса по дисциплине:

1. Учебная аудитория для проведения занятий лекционного типа с проекционным оборудованием.
2. Компьютерный класс, содержащий не менее 11 посадочных мест для студентов, рабочее место преподавателя, компьютеры – 12 шт., маркерная доска, проекционное оборудование.
3. Помещения для самостоятельной работы, оснащенные персональными компьютерами с доступом в интернет, доступом в электронную информационно-образовательную среду, программное обеспечение общего и профессионального назначения.