



Принято  
Решением Педагогического совета  
АНО ДПО «СИБИНДО»  
Протокол № 01-01/1 от 21.01.2025

Утверждено  
Ректор АНО ДПО «СИБИНДО»



В.И. Гам

## РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

### **«Информационная безопасность»**

для реализации дополнительной профессиональной программы  
профессиональной переподготовки  
«Педагогическое образование. Преподавание предмета "Информатика" в  
условиях реализации ФГОС»

## СОДЕРЖАНИЕ

1. Паспорт рабочей программы учебной дисциплины
2. Требования к уровню освоения содержания учебной дисциплины
3. Структура и содержание дисциплины (модуля)
4. Методические указания для организации самостоятельной работы
5. Условия реализации программы
6. Контроль и оценка результатов освоения учебной дисциплины
7. Приложения

# 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

## 1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины является частью дополнительной профессиональной программы профессиональной переподготовки «Педагогическое образование. Преподавание предмета "Информатика" в условиях реализации ФГОС»

## 1.2. Место учебной дисциплины в структуре профессиональной образовательной программы

Данная учебная дисциплина относится к блоку профессиональных и специальных дисциплин.

## 1.3. Цели и задачи учебной дисциплины

Цель дисциплины: изучение основных понятий информационной безопасности и рассмотрение законодательной базы по защите информации в РФ.

Задачи дисциплины:

- освоить основные понятия информационной безопасности;
- изучить нормативно-правовую базу по защите информации в РФ;

## 1.4. Рекомендуемое количество часов на освоение примерной программы учебной дисциплины

Количество часов на освоение программы дисциплины: максимальной учебной нагрузки обучающегося – 38 часов, включая: обязательной аудиторной учебной нагрузки обучающегося – 28 часов, самостоятельной работы обучающегося – 10 часов.

## 2. ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

В результате изучения дисциплины обучающийся должен

**знать:**

- информационные угрозы;
- нормативно-правовую базу по защите информации в РФ;

**уметь:**

- проводить оценку риска информационной безопасности;
- защищать ПК от вредоносных программ;
- выявлять правонарушение в сфере информационной безопасности;

**владеть:**

- информацией об основных законах по защите информации.

### 3. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

#### УЧЕБНЫЙ ПЛАН

Объем часов (по наличию видов занятий)									Форма итогового контроля	
Общая трудоемкость	Аудиторные занятия					Самостоятельная работа				
	Всего	Лекции	Семинарские (практические занятия)	Консультации	Другие виды занятий	Всего	Курсовая работа	Реферат	Другие виды самостоятель	
<b>38</b>	<b>28</b>	<b>18</b>	<b>10</b>			<b>10</b>			<b>10</b>	<b>зачёт</b>

#### ТЕМАТИЧЕСКИЙ ПЛАН

Раздел дисциплины, содержание	Всего	Аудиторные			Самостоятельная работа слушателей	Формы межсессионного контроля
		Лекции	Семинарские (практические занятия)	Лабораторный практикум		
<b>Тема 1.</b> Информационная безопасность и информационные угрозы	<b>12</b>	<b>6</b>	<b>2</b>		<b>4</b>	
<b>Тема 2.</b> Методы защиты информации. Законодательный уровень информационной безопасности	<b>14</b>	<b>6</b>	<b>4</b>		<b>4</b>	
<b>Тема 3.</b> Риски информационной безопасности	<b>12</b>	<b>6</b>	<b>4</b>		<b>2</b>	
<b>Всего по дисциплине</b>	<b>38</b>	<b>18</b>	<b>10</b>		<b>10</b>	<b>зачёт</b>

#### Основное содержание дисциплины:

##### *Тема 1. Информационная безопасность и информационные угрозы*

Понятие информационной безопасности. Понятие информационной угрозы. Качество и ценность как один из показателей информационной безопасности. Угроза безопасности информации в компьютерных сетях.

##### *Тема 2. Методы защиты информации. Законодательный уровень информационной безопасности*

Основные методы защиты информации. Профилактика заражения вирусами компьютерных систем. Порядок и действие пользователя при обнаружении заражения вирусами компьютерных систем. Авторское право. Ответственность за правонарушение в сфере информационной безопасности.

### ***Тема 3. Риски информационной безопасности***

Понятие риска информационной безопасности Оценка риска информационной безопасности.

## **4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ**

Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся. Ознакомиться с рабочей программой дисциплины можно на вводной лекции из её представления преподавателем или самостоятельно на официальном Интернет-сайте Академии. Следует обратить внимание на список основной и дополнительной литературы, которая имеется в электронной библиотечной системе на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения. Подготовка к учебному занятию лекционного типа.

Обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса:

- 1) знакомит с новым учебным материалом;
- 2) разъясняет учебные элементы, трудные для понимания;
- 3) систематизирует учебный материал;
- 4) ориентирует в учебном процессе.

С этой целью:

- внимательно прочитайте материал лекции;
- ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;
- внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;
- запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;
- постарайтесь уяснить место изучаемой темы в своей подготовке;
- узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу. Подготовка к занятию семинарского типа.

При подготовке и работе во время проведения занятий семинарского типа следует обратить внимание на следующие моменты: процесс предварительной подготовки, работа во время занятия, обработка полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач практического занятия, техники безопасности при работе в аудитории.

Для более углубленного изучения темы предлагаются задания для самостоятельной работы, их рекомендуется выполнять параллельно с

изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала.

## **5. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ**

### **5.1. Организационно-педагогические требования, обеспечивающие реализацию Программы**

Условия реализации Программы в АНО ДПО «СИБИНДО» обеспечивают реализацию ППО в полном объеме, соответствие качества подготовки слушателей установленным требованиям.

Продолжительность учебного часа теоретических и практических занятий составляет один академический час (45 минут).

### **5.2. Кадровые требования, обеспечивающие реализацию Программы**

Реализация Программы обеспечивается высококвалифицированными педагогическими и научно-педагогическими кадрами, имеющими достаточный опыт работы в области профессиональной деятельности, соответствующей преподаваемому учебному предмету, курсу, дисциплине (модулю), состоящими в штате АНО ДПО «СИБИНДО» или привлекаемыми.

### **5.3. Материально-технические условия реализации Программы**

Программа реализуется в заочной (без отрыва от производства)/очно-заочной форме с использованием в соответствии с частью 2 статьи 13 Федерального закона от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации» электронного обучения, а также дистанционных образовательных технологий.

Под дистанционными образовательными технологиями понимаются образовательные технологии, реализуемые с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) взаимодействии слушателей и педагогических работников.

Для реализации учебной дисциплины с применением электронного обучения, дистанционных образовательных технологий созданы условия для функционирования электронной информационно-образовательной среды, включающей в себя электронные информационные ресурсы, электронные образовательные ресурсы, совокупность информационных технологий, телекоммуникационных технологий, соответствующих технологических средств, которые обеспечивают освоение слушателями ППО в полном объеме, независимо от места нахождения.

Дистанционный курс проходит на виртуальной образовательной платформе CMS (LMS) Moodle (по лицензии GNU GPL). Система расположена на сервере организации под управлением ОС Linux Debian 9 с СУБД MYSQL.

Идентификация пользователей осуществляется с помощью уникального логина и пароля. Работа организована на широкополосных высокочастотных каналах передачи данных. Предусматривается организация дистанционной поддержки преподавателям и обучающимся.

При реализации Программы с применением электронного обучения и дистанционных технологий местом осуществления образовательной деятельности является место нахождения АНО ДПО «СИБИНДО» независимо от места нахождения слушателя.

Для организации самостоятельного продвижения слушателей в программе: лекционные материалы, дополнительные материалы, методические рекомендации по организации индивидуальной работы слушателей, задания для самопроверки, требования к оформлению итоговых работ, задания для итоговой аттестации. Сопровождение самостоятельной работы слушателей предполагает согласование индивидуальных планов работы (виды и темы заданий, сроки представления результатов); проведение индивидуальных и групповых консультаций; промежуточный контроль хода выполнения заданий; оценка результатов выполнения заданий.

Эффективное использование электронных образовательных ресурсов возможно при условии наличия качественного доступа слушателей к информационно-телекоммуникационной сети Интернет. Слушатели, выполняя задания, предусмотренные программой при необходимости, имеют возможность обратиться к педагогическим работникам за помощью.

#### **5.4. Информационно-методическое обеспечение реализации Программы**

Образовательный процесс в АНО ДПО «СИБИНДО» в полном объеме обеспечен электронными учебниками, учебно-методической литературой и материалами по всем учебным дисциплинам Программы, имеется доступ к печатным и электронным образовательным ресурсам (ЭОР), в том числе к электронным образовательным ресурсам, размещенным в федеральных и региональных базах данных ЭОР. Подключение библиотеки к Интернету обеспечивает удаленный доступ к электронным каталогам и полнотекстовым базам. Перечень используемых источников, учебных изданий, Интернет-ресурсов, дополнительной литературы предоставляется слушателям.

Используются следующие информационные технологии и информационные справочные системы:

- проведение онлайн занятий через ПО BigBlueButton с использованием слайд-презентаций, демонстрации видео и графических материалов;
- проведение занятий и проверка знаний с использованием СДО Moodle;
- офисные программы Windows; Linux, Microsoft Office; LibreOffice, Adobe Reader, Mozilla Firefox;

По всем темам дисциплины разработаны:

- электронные презентации для проведения лекционных и практических занятий;
- используется составленная фильмотека по отдельным темам учебного курса;
- имеется комплект видеороликов для наглядного представления вопросов при изучении ряда тем учебной дисциплины.

#### **5.5. Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы**

### **Основные источники:**

1. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: учебное пособие. – СПб: СПбГУ ИТМО, 2009. – 84 с.
2. Нестеров С. А. Информационная безопасность и защита информации: Учеб. пособие. – СПб.: Изд-во Политехн. ун-та, 2009. – 126 с.

### **Дополнительные источники:**

1. Семакин И.Г., Хеннер Е.К. Энциклопедия учителя информатики: Вып.9 «Социальная информатика и информационная безопасность»// Информатика. 2007 №19.
2. В. П. Мельников, С. А. Клейменов, А. М. Петраков. Информационная безопасность и защита информации: учеб. пособие для студ.высш.учеб.заведений / - М.: Академия, 2006. - 336 с.
3. Расторгуев С. П. Основы информационной безопасности: Учебное пособие. - М.: Академия, 2007. - 186 с.

## **6. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ**

Освоение программы, в том числе отдельной части (модуля) или всего объема темы, сопровождается текущим контролем успеваемости, промежуточной и итоговой аттестацией слушателей. Формы и порядок текущего контроля, промежуточной и итоговой аттестации определяются при разработке программы целесообразно ее целевым установкам и доводятся до сведения слушателей в начале обучения.

Текущий контроль - процесс определения степени владения и/или усвоения слушателями изучаемого учебного материала в ходе семинарских (практических) занятий в соответствии с содержанием программы. Цель текущего контроля - обеспечение обратной связи между актуальными знаниями и умениями обучающихся и планируемыми результатами обучения в рамках изучения определенной темы, модуля программы для реализации преподавателем контрольно-корректировочной деятельности.

Система текущего контроля включает: контроль знаний, умений, навыков, усвоенных в данном курсе в форме контрольной работы, индивидуального собеседования; выполнения заданий в ходе практических работ; исследовательского, творческого проекта; решения кейсов. Показатели и шкала оценивания формы контроля – устное сообщение, собеседование, решение кейса, тестирование в Приложении. Формы, виды, средства осуществления текущего контроля ориентированы на реализацию компетентностного подхода, определяются посредством учета планируемых результатов обучения, структуры и логики программы.

Промежуточная аттестация - процесс определения уровня достижения слушателями планируемых результатов обучения в завершении освоения структурно-логического компонента. Цель промежуточной аттестации - обеспечение обратной связи между образовательными результатами, достигнутыми слушателями, и планируемыми результатами обучения по отдельной части курса (модуля) для установления фактического уровня ее



освоения слушателями. Система промежуточной аттестации предполагает: зачет, зачет с оценкой или экзамен. Показатели и шкала оценивания форм контроля в Приложении.

Формы, виды, средства осуществления промежуточной аттестации ориентированы на реализацию компетентностного подхода, определяются посредством учета планируемых результатов обучения, структуры и логики программы.

Итоговая аттестация - форма оценки степени и уровня освоения слушателями образовательной программы. Итоговая аттестация для слушателей, завершающих обучение по программе, является обязательной. Итоговая аттестация проводится с использованием ДОТ. Итоговая аттестация слушателей осуществляется аттестационной комиссией. Итоговая аттестация планируется с учетом организационной целесообразности и возможности наиболее эффективно оценить и проанализировать качество освоения (соответствие результатов освоения слушателями заявленным целям и планируемым результатам обучения). Формы, виды, средства осуществления промежуточной аттестации ориентированы на реализацию компетентностного подхода, определяются посредством учета планируемых результатов обучения, структуры и логики программы. Итоговая аттестация проводится в форме зачета. Выполняется итоговая работа в соответствии с Требованиями к итоговой аттестационной работе. Конкретную тему итоговой работы слушатель формулирует самостоятельно в пределах содержания программы.

Приложение 1

### **Примерные задания для промежуточной аттестации (тесты)**

**1) К правовым методам, обеспечивающим информационную безопасность, относятся:**

- а) Разработка аппаратных средств обеспечения правовых данных

- b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

**2) Основными источниками угроз информационной безопасности являются все указанное в списке:**

- a) Хищение жестких дисков, подключение к сети, инсайдерство
- b) Перехват данных, хищение данных, изменение архитектуры системы
- c) Хищение данных, подкуп системных администраторов, нарушение регламента работы

**3) Виды информационной безопасности:**

- a) Персональная, корпоративная, государственная
- b) Клиентская, серверная, сетевая
- c) Локальная, глобальная, смешанная

**4) Цели информационной безопасности – своевременное обнаружение, предупреждение:**

- a) несанкционированного доступа, воздействия в сети
- b) инсайдерства в организации
- c) чрезвычайных ситуаций

**5) Основные объекты информационной безопасности:**

- a) Компьютерные сети, базы данных
- b) Информационные системы, психологическое состояние пользователей
- c) Бизнес-ориентированные, коммерческие системы

**6) Основными рисками информационной безопасности являются:**

- a) Искажение, уменьшение объема, перекодировка информации
- b) Техническое вмешательство, выведение из строя оборудования сети
- c) Потеря, искажение, утечка информации

**7) К основным принципам обеспечения информационной безопасности относится:**

- a) Экономической эффективности системы безопасности
- b) Многоплатформенной реализации системы
- c) Усиления защищенности всех звеньев системы

**8) Основными субъектами информационной безопасности являются:**

- a) руководители, менеджеры, администраторы компаний
- b) органы права, государства, бизнеса
- c) сетевые базы данных, фаерволлы

**9) К основным функциям системы безопасности можно отнести все перечисленное:**

- a) Установление регламента, аудит системы, выявление рисков

- b) Установка новых офисных приложений, смена хостинг-компаний
- c) Внедрение аутентификации, проверки контактных данных пользователей

**10) Принципом информационной безопасности является принцип недопущения:**

- a) Неоправданных ограничений при работе в сети (системе)
- b) Рисков безопасности сети, системы
- c) Презумпции секретности

Приложение 2

**Примерные задания для итоговой аттестации  
(реферат)**

Напишите реферат на предложенную тему:

1. Понятие информационной безопасности.
2. Угрозы безопасности информации в компьютерных системах.
3. Методы защиты информации.
4. Профилактика заражения вирусами компьютерных систем.
5. Порядок и действие пользователя при обнаружении заражения вирусами компьютерных систем.
6. Законодательная база РФ в сфере информационной безопасности.
7. Ответственность за нарушение в сфере информационной безопасности.

Приложение 3

**Показатели и шкала оценивания формы контроля –тестирование.**

Шкала оценивания	Критерии для контрольной работы, кейса, теста
5 «отлично»	Правильный ответ не менее чем на 84% заданий

4 «хорошо»	Правильный ответ не менее чем на 67% заданий
3 удовлетворительно	Правильный ответ не менее чем на 50% заданий
2 неудовлетворительно	Правильный ответ менее чем на 50% заданий.

### Шкала оценивания в зависимости от уровня сформированности компетенций

Результаты освоения	1. Недостаточный: компетенции не сформированы	2. Пороговый: компетенции сформированы	3. Продвинутой: компетенции сформированы	4. Высокий: компетенции сформированы
<b>Знать:</b>	Знания отсутствуют.	Сформированы базовые структуры знаний.	Знания обширные, системные.	Знания твердые, аргументированные, всесторонние.
<b>Уметь:</b>	Умения не сформированы	Умения фрагментарны и носят репродуктивный характер.	Умения носят репродуктивный характер применяются к решению типовых заданий.	Умения успешно применяются к решению как типовых, так и нестандартных творческих заданий.
<b>Владеть:</b>	Навыки не сформированы	Демонстрируется низкий уровень самостоятельности практического навыка.	Демонстрируется достаточный уровень самостоятельности устойчивого практического навыка.	Демонстрируется высокий уровень самостоятельности, высокая адаптивность практического навыка.

### Требования, предъявляемые к реферату и его оформлению

Требования к содержанию	<ol style="list-style-type: none"> <li>1. содержание реферата должно четко соответствовать теме и цели конкретного занятия, программы, методики и т. д.;</li> <li>2. содержание реферата должно быть понятным и применимым на практике в любых условиях;</li> <li>3. содержание реферата не должно повторять содержание учебников, учебных программ и иных методических разработок других авторов;</li> <li>4. материал должен быть систематизирован, изложен максимально просто и четко;</li> <li>5. язык реферата должен быть лаконичным, грамотным, убедительным. Применяемая терминология должна соответствовать общепринятой;</li> <li>6. рекомендуемые методы, методические приемы, формы и средства обучения должны подкрепляться примерами практического опыта;</li> <li>7. реферат должен содержать конкретные материалы, которые можно использовать в работе (карточки задания, планы, инструкции, карточки схемы, тесты и т.д.).</li> </ol>
Требования к структуре	<ol style="list-style-type: none"> <li>1. Вводная часть <ul style="list-style-type: none"> <li>- автор реферата, должность, место работы;</li> <li>- название реферата;</li> </ul> </li> </ol>

	<ul style="list-style-type: none"> <li>- пояснительная записка;</li> <li>- цели и задачи проводимого практического мероприятия;</li> <li>- целевая категория (возраст детей, группа детей, группа педагогов и пр.);</li> <li>- условия для проведения;</li> <li>- оборудование и оформление;</li> </ul> <p>2. Основная часть</p> <p>--сценарный план, ход проведения мероприятия.</p> <p>3. Список использованной литературы;</p> <p>4. Приложения (ссылки на источники дополнительного материала, подбор сопровождающих материалов, таблиц, схем).</p>
Требования к оформлению	<ol style="list-style-type: none"> <li>1. объем – не более 10 страниц машинописного текста;</li> <li>2. размеры полей левое –2 см, правое –1см, нижнее - 2 см, верхнее – 2 см.</li> <li>3. шрифт Times New Roman (14), интервал полуторный;</li> <li>4. страницы необходимо нумеровать арабскими цифрами, соблюдая сквозную нумерацию по всему тексту. Номер страницы проставляется посередине верхнего поля без точки в конце;</li> <li>5. на первой странице размещается титульный лист;</li> <li>6. список использованных источников в алфавитном порядке в соответствии с требованиями, предъявляемыми к оформлению литературы.</li> </ol>
Критерии оценки	<ol style="list-style-type: none"> <li>1. Соответствие предложенной структуре</li> <li>2. Четкая постановка целей и задач</li> <li>3. Раскрытие темы (полнота, ясность)</li> <li>4. Отражение в работе своего опыта;</li> <li>5. Грамотность изложения и оформления .....</li> </ol> <p>Каждый критерий оценивается в баллах от 1 до 10. Слушатель получает отметки по системе:  0 – 29 баллов – не зачтено;  30 – 50 баллов – зачтено.</p>