

Министерство образования Пензенской области  
Государственное автономное профессиональное образовательное учреждение  
Пензенской области  
«Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»  
(ГАПОУ ПО ПКИПТ)



УТВЕРЖДАЮ

Директор ГАПОУ ПО ПКИПТ

 А.Н. Фетисов

«11» \_\_\_\_\_ 2019г.

**ДОПОЛНИТЕЛЬНАЯ ОБЩЕРАЗВИВАЮЩАЯ ПРОГРАММА**

**«Безопасность сети Интернет»**

Пенза – 2019

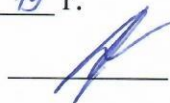
Организация – разработчик: ГАПОУ ПО «Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»

Разработчики: Д.А. Ручкин, преподаватель первой категории

Дополнительная общеразвивающая программа рассмотрена на заседании МЦК профессиональных дисциплин по укрупненной группе специальности 10.00.00 «Информационная безопасность»

Протокол № 3 от 05.11.19 г.

Председатель МЦК



А.Ю. Сазонова

## I. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

Исследование проблемы безопасности детей и подростков в сети Интернет последние годы является особенно актуальным, в связи с бурным развитием IT-технологий и со свободным использованием детьми и подростками современных информационно - коммуникационных технологий (Интернет, сотовая (мобильная) связь).

Дополнительная общеобразовательная программа «Безопасность в сети Интернет» разработана в связи с возросшей потребностью обеспечения информационной безопасности детей и подростков при организации урочной и внеурочной деятельности. Программа разработана для следующих уровней общего образования: начального общего образования, основного общего и среднего общего образования.

Направленность дополнительной общеобразовательной программы - естественнонаучная.

Программа разработана с учетом требований законов Российской Федерации: «Об образовании в Российской Федерации», «О защите детей от информации, причиняющей вред их здоровью и развитию» и «Санитарно-эпидемиологических требований к условиям и организации обучения в общеобразовательных учреждениях» и "Санитарно-эпидемиологических требований к устройству, содержанию и организации режима работы образовательных организаций дополнительного образования детей".

В требованиях ФГОС к предметным результатам освоения курса информатики для уровней начального, основного общего и среднего общего образования отсутствует предметная область «Основы безопасности в Интернете», но в рамках метапредметных результатов и предметных умений дисциплины «Информатика» вопросы информационной безопасности обозначены. Новизна дополнительной общеобразовательной программы «Безопасность в сети Интернет» заключается в достижении метапредметных результатов и предметных умений дисциплины «Информатика» по формированию навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в сети интернет, умений соблюдать нормы информационной этики и права.

**1.1. Цель программы:** освоение обучающимися базовых принципов безопасного поведения в сети интернет и безопасности личного информационного пространства

### **1.2. Образовательные результаты программы**

В результате освоения программы слушатель должен **уметь:**

- соблюдать нормы информационной этики;
- безопасно работать с информацией, анализировать и обобщать полученную информацию;

В результате освоения программы слушатель должен **знать**:

- о безопасном поведении при работе с компьютерными программами, информацией в сети Интернет
- развивать компьютерную грамотность информационную культуру личности в использовании информационных и коммуникационных технологий;
- развивать умение анализировать и систематизировать имеющуюся информацию;
- развивать познавательную и творческую активность в безопасном использовании информационных и коммуникационных технологий

**1.3. Трудоемкость обучения: 36 часов**

## II. СОДЕРЖАНИЕ ПРОГРАММЫ

### 2.1. Рабочий учебный план

Министерство образования Пензенской области  
Государственное автономное профессиональное образовательное учреждение  
Пензенской области  
«Пензенский колледж информационных и промышленных технологий (ИТ-колледж)»  
(ГАПОУ ПО ПКИПТ (ИТ-колледж))



УТВЕРЖДАЮ

Директор ГАПОУ ПО ПКИПТ

А.Н. Фетисов

11 2019 г.

### РАБОЧИЙ УЧЕБНЫЙ ПЛАН дополнительной общеразвивающей программы

#### «Безопасность сети интернет»

#### Категория слушателей

- программа рассчитана для обучающихся, уровень образования - начальное общее образование.

Трудоемкость обучения 36 часов  
Срок обучения 1 неделя  
Форма обучения очно-заочная

№	Наименование модулей	Всего, ак. час	В том числе			Форма контроля
			лекции	практ. занятия	промеж. и итог. контроль	
1	2	3	4	5	6	7
1	Информация, компьютер и Интернет.	10	7	3		
2	Техника безопасности и экология	8	5	3		
3	Мир виртуальный и реальный. Интернет зависимость.	5	3	2		
4	Методы безопасной работы в Интернете	5	3	2		
5	Потребительские опасности в Интернете	4	3	1		
6	Основные правила поведения сетевого взаимодействия	2	1	1		
7	Государственная политика в области защиты информации	2	1	1		
ИТОГО:		36	23	13		

Согласовано

Заместитель директора по работе с социальными партнерами Чистякова Н.В.

Председатель методической цикловой комиссии А.Ю. Сазонова

## 2.2. Содержание программы

### 2.2.1. Тематический план дополнительной общеразвивающей программы «Безопасность сети интернет»

№	Наименование модулей	Всего, ак. час	В том числе			Форма контроля
			лекции	практ. занятия	промеж. и итог. контроль	
1	2	3	4	5	1	2
<b>1</b>	<b>Информация, компьютер и Интернет.</b>	<b>10</b>	<b>7</b>	<b>3</b>	<b>0</b>	<b>-</b>
1.1	Как защитить себя от информационной перегрузки. Что такое файл. Как обращаться со своими и чужими файлами, чтобы их не потерять. Какие файлы можно скачивать, а какие нельзя. Полезные и вредные страницы Интернета. Как отличать полезную и правдивую информацию.	2	2			
1.2	Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты. К чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Возьми с собой электронного помощника. Мобильные устройства. Польза и опасности мобильной связи, Общение в Интернете - переписка, форумы, социальные сети.	2	2			
1.3	Совместные игры в Интернете. Обмен данными при совместной работе - скайп, IP-телефония, ICQ. Безопасный обмен данными. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.). Как работать в группе.	3	3			
1.4	Поиск информации в сети Интернет. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.). Общение с использованием видеосвязи на примере Skype. Создание электронной почты	3		3		
<b>2</b>	<b>Техника безопасности и экология</b>	<b>8</b>	<b>5</b>	<b>3</b>	<b>0</b>	<b>-</b>
2.1	Гигиена при работе с компьютером. Правила работы с ПК, электронными книгами и мобильными устройствами.	2	2			
2.2	Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером. Как защитить компьютер от повреждений, Компьютеру тоже нужна забота, Компьютер и среда обитания	2	2			

	(растения, животные, другие члены семьи). Везде ли есть Интернет?					
2.3	Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности.	1	1			
2.4	Использование мобильного приложения Компас Создание буклетов по различным темам	3		3		
<b>3</b>	<b>Мир виртуальный и реальный. Интернет зависимость.</b>	<b>5</b>	<b>3</b>	<b>2</b>	<b>0</b>	<b>-</b>
3.1	Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную?	2	2			
3.2	Социальные сети. Детские социальные сети.	1	1			
3.3	Создание сообщества класса в детских социальных сетях	2		2		
<b>4</b>	<b>Методы безопасной работы в Интернете</b>	<b>5</b>	<b>3</b>	<b>2</b>	<b>0</b>	
4.1	Как защититься от вредного контента. Что такое контент-фильтры, движение в Интернете (серфинг).	2	2			
4.2	Знаки Интернета, рассказывающие об опасной информации.	1	1			
4.3	Исследовательская работа «Колобанга в поисках вируса» (выявление признаков заражения вирусом).	2		2		
<b>5</b>	<b>Потребительские опасности в Интернете</b>	<b>4</b>	<b>3</b>	<b>1</b>	<b>0</b>	
5.1	Интернет и экономика - польза и опасность.	2	2			
5.2	Что такое личная информация.	1	1			
5.3	Прохождение интерактивного курса. «Мошеннические действия в Интернете. Киберпреступления». Квест «Покупка в интернет-магазине».	1		1		
<b>6</b>	<b>Основные правила поведения сетевого взаимодействия</b>	<b>2</b>	<b>1</b>	<b>1</b>	<b>0</b>	
6.1	Что такое интернет-этикет. Как вести себя в гостях у «сетевых» друзей	1	1			
6.2	Пишу письмо другу	1		1		
<b>7</b>	<b>Государственная политика в области защиты информации</b>	<b>2</b>	<b>1</b>	<b>1</b>	<b>0</b>	
7.1	Как государство защищает киберпространство. Войны нашего времени. Что такое кибервойна.	1	1			
7.2	Квест «Война миров»	1		1		
<b>ИТОГО:</b>		<b>36</b>	<b>23</b>	<b>13</b>	<b>0</b>	

## 2.2.1.1. Содержание дополнительной общеразвивающей программы «Безопасность сети интернет»

### **Тема 1 Информация, компьютер и Интернет.**

Основные вопросы: Компьютер - как он появился, как появился Интернет. Почему компьютер нужно беречь. Где и как искать информацию для урока. Интернет средство для поиска полезной информации. Как защитить себя от информационной перегрузки. Что такое файл. Как обращаться со своими и чужими файлами, чтобы их не потерять. Какие файлы можно скачивать, а какие нельзя. Полезные и вредные страницы Интернета. Как отличать полезную и правдивую информацию. Ненужные ссылки, ложные ссылки, реклама. Что такое вредоносные сайты. К чему ведет переход по вредоносным ссылкам. Опасная информация в сети. Возьми с собой электронного помощника. Мобильные устройства. Польза и опасности мобильной связи, Общение в Интернете - переписка, форумы, социальные сети. Совместные игры в Интернете. Обмен данными при совместной работе - скайп, IP-телефония, ICQ. Безопасный обмен данными. На каких устройствах можно сохранить информацию и как с ними правильно обращаться (диски, флэш, карты и пр.). Как работать в группе. Как передать товарищам результаты работы и не повредить их компьютерам. Что такое электронная почта.

#### Требования к знаниям и умениям:

Обучающиеся должны знать об истории появления компьютера и Интернета. Правила работы с компьютером. Научиться соблюдать правила работы с файлами. Уметь отличать безопасные сайты и ссылки от вредоносных. Знать технические и программные возможности мобильных устройств. Преимущества мобильной связи и их опасность. Понимать пользу и опасности виртуального общения, социальных сетей.

Обучающиеся должны уметь правильно работать за компьютером. Пользоваться браузером для поиска полезной информации. Внимательно прочитывать сообщения о нежелательных страницах, отказываться от их просмотра. выполнять основные действия с файлами. Копировать файлы, проверять файлы на вирусы. Уметь работать с информацией и электронной почтой. Владеть основными приемами поиска информации в сети Интернет.

Практическая работа Поиск информации в сети Интернет. Работа с мобильными устройствами (2 ГИС, Госуслуги, Википедия, эл.книги, фотоколлаж, Компас, диктофон, Калькулятор и пр.).

Практическая работа Общение с использованием видеосвязи на примере Skype.

Практическая работа Создание электронной почты

### **Тема 2 Техника безопасности и экология**

Основные вопросы: Гигиена при работе с компьютером. Правила работы с ПК, электронными книгами и мобильными устройствами. Сколько времени можно проводить за компьютером. Как правильно сидеть за компьютером. Как защитить компьютер от повреждений, Компьютеру тоже нужна забота, Компьютер и среда обитания (растения, животные, другие члены семьи). Везде ли есть Интернет? Может ли компьютер заменить компас. Как мобильные устройства помогают ориентироваться на местности. Воздействие компьютера на зрение и др. органы. Физическое и психическое здоровье. Польза и вред компьютерных игр. Компьютер и недостаток движения. Что делать с компьютером в чрезвычайных ситуациях. Улица и мобильные устройства. Компьютер (мобильные устройства) в грозу.

#### Требования к знаниям и умениям:

Обучающиеся должны знать основные правила работы с ПК, электронными книгами и мобильными устройствами в условиях окружающей среды, основные навыки ухода за ПК, опасности при работе с электрическими приборами.

Обучающиеся должны уметь соблюдать технику безопасности и гигиену при работе за ПК. Владеть основными приемами навигации в файловой системе.



Практическая работа. Использование мобильного приложения Компас

Практическая работа. Создание буклетов по темам:

«Как может помочь компьютер в сложных чрезвычайных ситуациях»

«Правила поведения на улице с мобильными устройствами»

«Компьютеру тоже нужна забота» (как ухаживать за ПК и мобильными устройствами)

### **Тема 3 Мир виртуальный и реальный. Интернет зависимость.**

Основные вопросы: Что такое Интернет-сообщество. Как не превратить свою жизнь в виртуальную? Социальные сети. Детские социальные сети. Какую информацию о себе следует выкладывать в сеть? Какая информация принадлежит вам? Не слишком ли много у вас друзей в социальной сети? Если слишком долго находиться в Интернете: что такое интернет-зависимость? Виртуальная личность - что это такое. Сайты знакомств. Незнакомцы в Интернете. Превращение виртуальных знакомых в реальных. Развлечения в Интернете. Игры полезные и вредные. Признаки игровой зависимости.

Требования к знаниям и умениям:

Обучающиеся должны знать виды общения в Интернете. Правила безопасной работы при интернет - общении.

Обучающиеся должны уметь пользоваться основными видами программ для общения в сети. Чего не следует делать при сетевом общении.

Уметь применять программу Skype для общения, создание контактов.

Отличать вредные игры от полезных.

Практическая работа Создание сообщества класса в детских социальных сетях

Практическая работа Тест «Есть у меня игровая зависимость».

Квест «Я умею говорить «Нет» в сети интернет»

### **Тема 4 Методы безопасной работы в Интернете.**

Основные вопросы: Ищите в Интернете только то, что вам требуется. Как защититься от вредного контента. Что такое контент-фильтры, движение в Интернете (серфинг). Знаки Интернета, рассказывающие об опасной информации. Правильно ли работает компьютер? Признаки работы вирусов. Вирусы и антивирусы. Обновление баз. Что такое электронные деньги, как с ними правильно обращаться. Почему родители проверяют, что ты делаешь в Интернете?

Требования к знаниям и умениям:

Обучающиеся должны знать основные понятия о компьютерных вирусах и контент-фильтрах.

Обучающиеся должны уметь использовать приемы работы с антивирусными программами, запускать программы-антивируса для сканирования компьютера и внешних носителей информации, устанавливать и сканировать антивирусной программой. Детские контент-фильтры.

Практическая работа Исследовательская работа «Колобанга в поисках вируса» (выявление признаков заражения вирусом).

### **Тема 5 Потребительские опасности в Интернете**

Основные вопросы: Интернет и экономика - польза и опасность. Кто и как может навредить в Интернете. Электронная торговля - ее опасности. Поиск информации: если у вас требуют личную информацию при скачивании данных. Что такое личная информация. Если вам сообщают о выигрыше в лотерею. Если вам предлагают установить новое приложение. Сколько стоят ошибки в интернете.

Требования к знаниям и умениям:

Обучающиеся должны знать принципы работы интернет - магазинов, понятие «электронные деньги». Обучающиеся должны уметь дозированно использовать личную информацию в сети интернет.

Уметь различать (распознавать) мошеннические действия.

Практическая работа Прохождение интерактивного курса.  
«Мошеннические действия в Интернете. Киберпреступления».  
Практическая работа Квест «Покупка в интернет-магазине».

#### **Тема 6 Основные правила поведения сетевого взаимодействия.**

Основные вопросы: Что такое интернет-этикет. Как вести себя в гостях у «сетевых» друзей.

Требования к знаниям и умениям: Обучающиеся должны знать правила сетевого этикета, корректно общаться в сети Интернет.

Практическая работа. «Пишу письмо другу»

#### **Тема 7 Государственная политика в области защиты информации.**

Основные вопросы: Как государство защищает киберпространство. Войны нашего времени. Что такое кибервойна. Почему государство защищает информацию. Защита государства и защита киберпространства.

Требования к знаниям и умениям: Обучающиеся должны знать политику государство в области защиты информации, должны уметь защищать свои информационные данные от внешнего воздействия (интернет и вирусы, вирусы и злоумышленники).

Практическая работа Квест «Война миров»

### III. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

#### 3.1. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по дополнительной общеразвивающей программе: Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по теоретическому обучению: обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю преподаваемой дисциплины.

#### 3.2. Информационно – методические условия реализации программы

Наименование учебной дисциплины	Перечень литератур, Интернет-ресурсов
«Безопасность сети интернет»	<p>– печатные раздаточные материалы для слушателей</p> <p>– электронные ресурсы</p> <p>1) <a href="http://www.kaspersky.ru">http://www.kaspersky.ru</a> - антивирус «Лаборатория Касперского»;</p> <p>2) <a href="http://www.onlandia.org.ua/rus/">http://www.onlandia.org.ua/rus/</a> - безопасная web-зона;</p> <p>3) <a href="http://www.interneshka.net">http://www.interneshka.net</a> - международный онлайн-конкурс по безопасному использованию Интернета;</p> <p>4) Рыжков В.Н. Методика преподавания информатики// <a href="http://nto.immpu.sgu.ru/sites/default/files/3/12697.pdf">http://nto.immpu.sgu.ru/sites/default/files/3/12697.pdf</a>;</p> <p>5) <a href="http://www.saferinternet.ru">http://www.saferinternet.ru</a> - портал Российского Оргкомитета по безопасному использованию Интернета;</p> <p>6) <a href="http://content-filtering.ru">http://content-filtering.ru</a> - Интернет СМИ «Ваш личный Интернет»;</p> <p>7) <a href="http://www.rgdb.ru">http://www.rgdb.ru</a> - Российская государственная детская библиотека</p> <p>8) <a href="http://www.saferinternet.ru/">http://www.saferinternet.ru/</a> - Безопасный Интернет. Портал Российского Оргкомитета по проведению Года Безопасного Интернета. Мероприятия, Интернет и законодательство, проблемы и решения, международные ресурсы;</p> <p>9) <a href="http://www.saferunet.ru/">http://www.saferunet.ru/</a> - Центр Безопасного Интернета в России. Сайт посвящен проблеме безопасной, корректной и комфортной работы в Интернете. Интернет-угрозы и эффективное противодействие им в отношении пользователей;</p> <p>10) <a href="http://www.fid.su/">http://www.fid.su/</a> - Фонд развития Интернет. Информация о проектах, конкурсах, конференциях и др. по компьютерной безопасности и безопасности Интернета;</p> <p>11) <a href="http://www.microsoft.com/Rus/athome/security/kids/etusivu.html">http://www.microsoft.com/Rus/athome/security/kids/etusivu.html</a> - Безопасность в Интернете. "Основы безопасности детей и молодежи в 30 Интернете"</p>

### 3.3. Материально-технические условия реализации программы

Наименование аудиторий	Вид занятий	Наименование оборудования, программного обеспечения
Мастерская «Корпоративная защита от внутренних угроз информационной безопасности»	все занятия	Компьютеры и программное обеспечение по количеству слушателей мультимедийный проектор, экран, доска, флипчарт

#### **IV. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ**

##### **4.1. Контрольно – измерительный материал по дополнительной общеразвивающей программе «Безопасность сети интернет»**

**Способы определения планируемых результатов** - педагогическое наблюдение, тесты, педагогический анализ результатов анкетирования, тестирования, зачётов, взаимозачётов, опросов, выполнения обучающимися диагностических заданий, участия в мероприятиях, защиты проектов, решения задач поискового характера, активности обучающихся на занятиях и т.п.

Для отслеживания результативности можно использовать: педагогический мониторинг, включающий контрольные задания и тесты, диагностику личностного роста и продвижения, анкетирование, педагогические отзывы, ведение журнала учета или педагогического дневника, ведение оценочной системы; мониторинг образовательной деятельности детей, включающий самооценку обучающегося, ведение зачетных книжек, ведение творческого дневника обучающегося, оформление листов индивидуального образовательного маршрута, оформление фотоотчета и т.д.

**Формами подведения итогов** реализации дополнительной общеобразовательной программы «Безопасность в сети Интернет» могут быть выставки буклетов, выполненных обучающимися; проведение квестов; выступления обучающихся по актуальным вопросам информационной безопасности с собственными мультимедийными презентациями на ученических мероприятиях; демонстрация созданных видеороликов и др.

Тест по безопасности в сети Интернет  
(начальное общее образование)

1. Как могут распространяться компьютерные вирусы?
  - a. Посредством электронной почты.
  - b. При просмотре веб-страниц.
  - c. Через клавиатуру.
  - d. Их распространяют только преступники.
2. Зачем нужен брандмауэр?
  - a. Он не дает незнакомцам проникать в компьютер и просматривать файлы.
  - b. Он защищает компьютер от вирусов.
  - c. Он обеспечивает защиту секретных документов.
  - d. Он защищает компьютер от пожара.
3. Всегда ли можно быть уверенным в том, что электронное письмо было получено от указанного отправителя?
  - a. Да
  - b. Да, если вы знаете отправителя
  - c. Нет, поскольку данные отправителя можно легко подделать
  - d. Может быть.
4. На компьютере отображается непонятное сообщение. Какое действие предпринять?
  - a. Продолжить Будто ничего не произошло.
  - b. Нажать кнопку «ОК» или «ДА»
  - c. Обратится за советом к учителю, родителю или опекуну.
  - d. Больше никогда не пользоваться Интернетом
5. Что нужно сделать при получении подозрительного сообщения электронной почтой?
  - a. Удалить его, не открывая.
  - b. Открыть его и выяснить, содержится ли в нем какая-нибудь важная информация.
  - c. Открыть вложение, если такое имеется в сообщении.
  - d. Отправить его родителям
6. В ящик входящей почты пришло «письмо счастья». В письме говорится, чтобы его переслали пяти друзьям. Какое действие предпринять?
  - a. Переслать его пяти друзьям.
  - b. Переслать его не пяти друзьям, а десяти друзьям.
  - c. Не пересылать никакие «письма счастья»
  - d. Ответить отправителю, что вы больше не хотите получать от него/нее письма.
7. В каких случаях можно, не опасаясь последствий, сообщать в Интернете свой номер телефона или домашний адрес?
  - a. Во всех случаях.

- b. Когда кто-то просит об этом.
  - c. когда собеседник в чате просит об этом.
  - d. Такую информацию следует с осторожностью сообщать людям, которым вы доверяете.
8. Вы случайно прочитали пароль, который ваш друг записал на листочке бумаг. Как вы должны поступить?
- a. Запомнить его.
  - b. Постараться забыть пароль.
  - c. Сообщить другу, что вы прочитали пароль, и посоветовать сменить пароль и никогда больше не записывать на листе бумаги.
  - d. Сообщить пароль родителям.
9. Что такое сетевой этикет?
- a. Правила поведения за столом.
  - b. Правила дорожного движения.
  - c. Правила поведения в Интернете.
  - d. Закон, касающийся Интернета.
10. Что запрещено в интернете?
- a. Запугивание других пользователей.
  - b. Поиск информации.
  - c. Игры.
  - d. Общение с друзьями