

Муниципальное казенное общеобразовательное учреждение
средняя общеобразовательная школа с. Кулыги
Вятскополянского района Кировской области

УТВЕРЖДЕНО

Директор МКОУ СОШ
с.Кулыги

Санникова А.С.
№83 от «27» 08 2024 г

**РАБОЧАЯ ПРОГРАММА
УЧЕБНОГО КУРСА
«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
для 10 – 11 классов**

Автор - составитель
Лопаткина Любовь Леонидовна,
учитель русского языка и литературы.

Стаж работы 42 года

Высшая квалификационная категория
(2023 год)

Кулыги, 2024

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели изучения учебного курса «Информационная безопасность»

Безопасность в сети Интернет в свете быстрого развития информационных технологий, их глобализации, использования облачных технологий и повсеместного массового распространения среди детей мобильных персональных цифровых устройств доступа к сети Интернет, появления большого количества сетевых сервисов и интернет-коммуникаций, в том числе закрытых сетевых сообществ неизвестного толка, а также общедоступных и зачастую навязчивых интернет-ресурсов (СМИ, реклама, спам), содержащих негативный и агрессивный контент, расширения угроз новых сетевых средств вмешательства в личное информационное пространство на персональных устройствах, работающих в Интернете, в также в связи с массовым использованием детьми электронных социальных/банковских карт, имеющих персональные настройки доступа к ним, резко повышает потребность в воспитании у обучающихся культуры информационной безопасности в целях предотвращения негативных последствий массового использования Интернета молодежью и их защиты от агрессивной и противоправной информации.

Программа учебного курса информационной безопасности имеет высокую актуальность и отражает важные вопросы безопасной работы с новыми формами коммуникаций и услуг цифрового мира: потребность в защите персональной информации, угрозы, распространяемые глобальными средствами коммуникаций Интернет и мобильной связи, использующими рассылки сообщений, электронную почту, информационно-коммуникативные ресурсы взаимодействия в сети Интернет через массово доступные услуги электронной коммерции, социальные сервисы, сетевые объединения и сообщества, ресурсы для досуга (компьютерные игры, видео и цифровое телевидение, цифровые средства массовой информации и новостные сервисы), а также повсеместное встраивание дистанционных ресурсов и технологий в учебную деятельность, использующую поиск познавательной и учебной информации, общение в социальных сетях, получение и передачу файлов, размещение личной информации в коллективных сервисах. Помимо профилактики информационных угроз и противоправных действий через ресурсы в сети Интернет и мобильные сети, крайне актуально использовать коммуникации для привлечения обучающихся к информационно-учебной и познавательно-творческой активности по использованию позитивных интернет-ресурсов: учебных, культурных, научно-популярных, интеллектуальных, читательских, медийных, правовых, познавательных ресурсов и специализированных социальных сообществ и сервисов для детских объединений и творческих мероприятий для детей и молодежи.

При реализации требований безопасности в сети Интернет для любого пользователя, будь то школьник или учитель, образовательное учреждение должно обеспечивать защиту конфиденциальных сведений, представляющих собой в том числе персональные данные школьника, и предотвращать доступ к противоправной негативной информации. Но включение подростков в интернет-взаимодействие наиболее активно осуществляется вне школы самостоятельно, уже без надлежащего надзора со стороны взрослых.

В связи с этим в настоящее время необходимо особое внимание уделять воспитанию у старшеклассников правовой культуры информационной безопасности при работе в сети Интернет вне школы с привлечением их родителей. Для этого необходимо проводить непрерывную образовательно-просветительскую работу не только с обучающимися, но и с семьей, формировать у обучающихся ответственное и критическое отношение к источникам информации, правовую культуру в сфере защиты от негативной информации и противоправных действий средствами коммуникаций, в том числе

внимательно относиться к использованию личных устройств мобильной связи, домашнего компьютера с Интернетом, телевизора, подключенного к Интернету, знать виды ответственности несовершеннолетних при противоправных действиях в сфере защиты информации, использовать программные средства защиты от доступа к негативной информации или информации по возрастным признакам (возраст+). Научить школьника правильно ориентироваться в большом количестве ресурсов в сети Интернет — важная задача для вовлечения в современную цифровую образовательную среду, профориентации в условиях цифровизации профессий, отвлечения от бесполезного контента и игромании, бесцельной траты времени в социальных сетях и сервисах мобильной связи.

Главная цель курса — обеспечить социальные аспекты информационной безопасности в воспитании культуры информационной безопасности у старшеклассников в условиях цифрового мира, включение на регулярной основе цифровой гигиены в контекст воспитания и обучения, формирование у выпускника школы правовой грамотности по вопросам информационной безопасности, которые влияют на социализацию подростков в информационном обществе, формирование личностных и метапредметных результатов воспитания и обучения старшеклассников:

— формировать понимание сущности и воспитывать необходимость принятия обучающимися таких ценностей, как ценность человеческой жизни, свободы, равноправия и достоинства людей, здоровья, опыта гуманных, уважительных отношений с окружающими;

— создавать педагогические условия для формирования правовой и информационной культуры обучающихся, развития у них критического отношения к информации, ответственности за поведение в сети Интернет и последствия деструктивных действий, формирования мотивации к познавательной, а не игровой деятельности, воспитания отказа от пустого времяпрепровождения в социальных сетях, осознания ценности живого человеческого общения;

— формировать отрицательное отношение ко всем проявлениям жестокости, насилия, нарушения прав личности, экстремизма во всех его формах в сети Интернет;

— мотивировать обучающихся к осознанному поведению на основе понимания и принятия ими морально-правовых регуляторов жизни общества и государства в условиях цифрового мира;

— научить молодых людей осознавать важность проектирования своей жизни и будущего своей страны — России в условиях развития цифрового мира, ценность ИКТ для достижения высоких требований к обучению профессиям будущего в мире, принимать средства в Интернете как среду созидания, а не разрушения человека и общества.

Место учебного курса «Информационная безопасность» в учебном плане

Изучение курса предусматривается в течение двух лет, в 10-11 классах по 1 часу в неделю. Всего на изучение курса «Информационная безопасность» отводится 68 часов, из них по 34 часа в каждом классе.

Общая характеристика учебного курса «Информационная безопасность»

Программа курса для старших школьников включает изучение правовой грамоты в сфере информационной безопасности, в том числе основных видов юридической ответственности (уголовной, административной и гражданско-правовой) за преступления и проступки в области информационной безопасности (защиты информации). Полученные знания помогут избежать ошибок и правонарушений в информационном мире, а также ответственно работать в информационном пространстве, соблюдая нормы права. Важную часть программы составляет изучение правовой информации об основных

законодательных актах в сфере информационной безопасности, а также материалов, размещенных на сайте Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций. В программе для старшеклассников предусмотрена практика применения культуры информационной безопасности в электронном обучении, которое уже повсеместно встроено в профессиональную подготовку и дальнейшую активность в труде.

Отражение потребностей цифрового мира в современной цифровой грамотности и новых профессиональных качествах современного человека востребовано в жизни и учебе и несет в себе актуальные запросы для выпускника основного общего образования в его дальнейшей жизни и профессиональном выборе с обязательным использованием требований информационной безопасности:

- профориентация в мире профессий будущего, знакомство с профессиями в сфере информационной безопасности;
- популяризация электронных средств и ресурсов обучения;
- развитие кругозора о полезных интернет-ресурсах;
- получение представлений о цифровых технологиях для соблюдения правовых норм защиты информации;
- навыки обдуманного поведения при поиске информации в сети Интернет, критический анализ полученной информации, умение работать с информацией избирательно и ответственно.

СОДЕРЖАНИЕ УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ» ДЛЯ СРЕДНЕГО ОБЩЕГО ОБРАЗОВАНИЯ

Содержание учебного курса «Информационная безопасность» программы складывается из двух линий:

- 1) Информационное общество и информационная культура.
- 2) Информационное пространство и правила информационной безопасности.

Линия «Информационное общество и информационная культура»

Модуль 1. Правовые основы информационной безопасности.

1.1. Понятия юридической ответственности за правонарушения в области информационной безопасности.

1.2. Нормативное обеспечение информационной безопасности в Российской Федерации.

Модуль 2. Профилактика правонарушений в сфере информационной безопасности. 2.1. Понятие гражданско-правовой ответственности. Законодательство Российской Федерации о гражданско-правовой ответственности в сфере информационной безопасности.

2.2. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации).

2.3. Понятие административной ответственности. Законодательство Российской Федерации об административной ответственности в сфере информационной безопасности.

2.4. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).

2.5. Понятие уголовной ответственности. Законодательство Российской Федерации об уголовной ответственности в сфере информационной безопасности.

2.6. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации).

Линия «Информационное пространство и правила информационной безопасности»

Модуль 3. Практика применения правил и норм информационной безопасности.

3.1. Проектная работа. Нормативные основы лицензионных соглашений.

3.2. Проектная работа. Практика соблюдения норм информационной безопасности в личном информационном пространстве.

3.3. Практика электронного обучения и культура информационной безопасности при самостоятельной работе с коммуникациями, сервисами и ресурсами сети Интернет. Электронное обучение по информационной безопасности.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ПРОГРАММЕ

Программа учебного курса «Информационная безопасность» отражает в содержании цели поддержки и сопровождения безопасной работы с информацией в учебно-познавательной, творческой и досуговой деятельности (планируемые личностные, метапредметные и предметные результаты освоения курса).

В соответствии с федеральным государственным образовательным стандартом общего образования необходимо сформировать у обучающихся с учетом возрастных особенностей такие *личностные результаты*, которые позволят им грамотно ориентироваться в информационном мире с учетом имеющихся в нем угроз:

— принимать ценности человеческой жизни, семьи, гражданского общества, многонационального российского народа, человечества;

— быть социально активными, уважающими закон и правопорядок, соизмеряющими свои поступки с нравственными ценностями, осознающими свои обязанности перед семьей, обществом, Отечеством;

— уважать других людей, уметь вести конструктивный диалог, достигать взаимопонимания, сотрудничать для достижения общих результатов;

— осознанно выполнять правила здорового и экологически целесообразного образа жизни, безопасного для человека и окружающей его среды.

В результате освоения программы курса информационной безопасности акцентируется внимание на *метапредметных результатах* освоения основной образовательной программы:

— готовность и способность к самостоятельной информационно-познавательной деятельности, включая умение ориентироваться в различных источниках информации, критически оценивать и интерпретировать информацию, получаемую из различных источников;

— освоение социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах, включая взрослые и социальные сообщества; участие в школьном самоуправлении и общественной жизни в пределах возрастных компетенций с учетом региональных, этнокультурных, социальных и экономических особенностей;

— формирование коммуникативной компетентности в общении и сотрудничестве со сверстниками, детьми старшего и младшего возраста, взрослыми в процессе образовательной, общественно полезной, учебно-исследовательской, творческой и других видов деятельности;

— умение использовать средства информационно-коммуникационных технологий (ИКТ) в решении когнитивных, коммуникативных и организационных задач с соблюдением требований эргономики, техники безопасности, гигиены, ресурсосбережения, правовых и этических норм, норм информационной безопасности.

Планируется достижение *предметных результатов*, актуальных для данного курса в интеграции с предметами «Обществознание» и (или) «Информатика» (раздел «Социальная информатика») для 10—11 классов.

Линия «Информационное общество и информационная культура»:

— освоение приемов работы с социально значимой информацией, ее осмысление; развитие способностей обучающихся делать необходимые выводы и давать обоснованные оценки социальным событиям и процессам;

— формирование основ правосознания для соотнесения собственного поведения и поступков других людей с нравственными ценностями и нормами поведения, установленными законодательством Российской Федерации;

— принятие этических аспектов информационных технологий; осознание ответственности людей, вовлеченных в создание и использование информационных систем, распространение информации.

Линия «Информационное пространство и правила информационной безопасности»:

— понимание основ правовых аспектов использования компьютерных программ и работы в Интернете;

— формирование навыков и умений безопасного и целесообразного поведения при работе с компьютерными программами и в Интернете, умения соблюдать нормы информационной этики и права.

В результате освоения программы курса с учетом возрастных групп выпускник освоит жизненно важные практические компетенции.

Выпускник научится понимать:

— источники информационных угроз, вредоносные программы и нежелательные рассылки, поступающие на мобильный телефон, планшет, компьютер;

— роль близких людей, семьи, правоохранительных органов для устранения проблем и угроз в сети Интернет и мобильной телефонной связи, телефоны экстренных служб;

— виды информационных угроз, правила поведения для защиты от угроз, виды правовой ответственности за проступки и преступления в сфере информационной безопасности;

— проблемные ситуации и опасности в сетевом взаимодействии и правила поведения в проблемных ситуациях, ситуациях профилактики и предотвращения опасности;

— этикет сетевого взаимодействия, правовые нормы и законодательство в сфере информационной безопасности;

— правила защиты персональных данных;

— назначение различных позитивных ресурсов в сети Интернет для образования и в профессиях будущего.

Выпускник научится применять на практике:

— правила цифровой гигиены для использования средств защиты персональных данных (формировать и использовать пароль, использовать код защиты персонального устройства, регистрироваться на сайтах без распространения личных данных);

— информационно-коммуникативные компетенции по соблюдению этических и правовых норм взаимодействия в социальной сети или в мессенджере, умение правильно вести себя в проблемной ситуации (оскорбления, угрозы, предложения, агрессия, вымогательство, ложная информация и др.), отключаться от нежелательных контактов, действовать согласно правовым нормам в сфере информационной безопасности (защиты информации).

Выпускник освоит нормы культуры информационной безопасности в системе универсальных учебных действий для самостоятельного использования в учебно-познавательной и досуговой деятельности позитивного Интернета и средств электронного обучения с соблюдением правил информационной безопасности.

**ТЕМАТИЧЕСКОЕ ПЛАНИРОВАНИЕ
УЧЕБНОГО КУРСА ДЛЯ 10—11 КЛАССОВ**

Модуль/тема	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
<i>Линия «Информационное общество и информационная культура»</i>	34	19	15
Модуль 1. Правовые основы информационной безопасности	5	3	2
1.1. Понятия юридической ответственности за правонарушения в области информационной безопасности	3	3	
1.2. Нормативное обеспечение информационной безопасности в Российской Федерации	2		2
Модуль 2. Профилактика правонарушений в сфере информационной безопасности	29	16	13
2.1. Законодательство Российской Федерации о гражданско-правовой ответственности. Понятие гражданско-правовой ответственности	1	1	
2.2. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации)	4	2	2
2.3. Законодательство Российской Федерации об административной ответственности в сфере информационной безопасности. Понятие административной ответственности	1	1	
2.4. Административная ответственность несовершеннолетних	10	5	5

граждан за проступки в области информационной безопасности (защиты информации)			
2.5. Законодательство Российской Федерации об уголовной ответственности в сфере информационной безопасности. Понятие уголовной ответственности	1	1	
2.6. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации)	12	6	6
<i>Линия «Информационное пространство и правила информационной безопасности»</i>	34	2	32
Модуль 3. Практика применения правил и норм информационной безопасности	34	2	32
3.1. Проектная работа. Нормативные основы лицензионных соглашений	2	1	1
3.2. Проектная работа. Практика соблюдения норм информационной безопасности в личном информационном пространстве	11	1	10
3.3. Практика электронного обучения и культура информационной безопасности при самостоятельной работе с коммуникациями, сервисами и ресурсами сети Интернет. Электронное обучение по информационной безопасности	21		21
Всего:	68	21	47

ПОУРОЧНОЕ ПЛАНИРОВАНИЕ

10 к

№	Тема урока	Количество часов	Электронные (цифровые) образовательные ресурсы
Глава 1. Понятия юридической ответственности за правонарушения в области информационной безопасности			
1	Техника безопасности и организация рабочего места. Основные документы в области информационной безопасности Российской Федерации	<i>1</i>	https://lbz.ru/metodist/authors/ib/10-11.php
2	Информация как объект правовых отношений. Функции, принципы и виды юридической ответственности	<i>1</i>	
3	Субъективная и объективная стороны юридической ответственности	<i>1</i>	https://lbz.ru/metodist/authors/ib/10-11.php
4	Подготовка презентации по теме в группах учащихся	<i>1</i>	
5	Подготовка презентации по теме в группах учащихся	<i>1</i>	
Глава 2. Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)			
6	Общие положения законодательства Российской Федерации о гражданско-правовой ответственности.	1	
7	Порядок привлечения несовершеннолетних к Гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации)	1	https://lbz.ru/metodist/authors/ib/10-11.php
8	Ответственность за проступок в области присвоение авторства (плагиат)	1	https://lbz.ru/metodist/authors/ib/10-11.php
9	Ответственность за проступок за оскорбления, в том числе в социальных сетях	1	
10	Индивидуальный зачет	1	
Глава 3. Административная ответственность за проступки в области информационной безопасности (защиты информации)			
11	Административное правонарушение. Основные понятия административного правонарушения.	1	
12	Особенности административной ответственности несовершеннолетних.	1	https://lbz.ru/metodist/authors/ib/10-11.php

13	Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение	1	https://lbz.ru/metodist/authors/ib/10-11.php
14	Ответственность за проступок — за оскорбления, в том числе в социальных сетях. Ответственность за проступок — ложный вызов экстренных служб	1	https://lbz.ru/metodist/authors/ib/10-11.php
15	Ответственность за проступок — пропаганду в Интернете наркотических и психотропных веществ	1	
16	Ответственность за проступок — нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные)	1	https://lbz.ru/metodist/authors/ib/10-11.php
17	Ответственность за проступок — нарушение правил защиты информации	1	https://lbz.ru/metodist/authors/ib/10-11.php
18	Ответственность за проступок — представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство	1	
19	Ответственность за проступок — за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт	1	https://lbz.ru/metodist/authors/ib/10-11.php
20	Ответственность за проступок — нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации	1	
21	Индивидуальный зачет	1	
Глава 4. Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации)			
22	Уголовный кодекс Российской Федерации. Виды наказаний в области уголовной ответственности.	1	https://lbz.ru/metodist/authors/ib/10-11.php
23	Ответственность за преступления в области компьютерной информации и применения компьютеров	1	
24	Ответственность за преступления в области присвоения авторства (плагиат)	1	https://lbz.ru/metodist/authors/ib/10-11.php

25	Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение	1	
26	Ответственность за преступления в области мошенничества (обмана)	1	https://lbz.ru/metodist/authors/ib/10-11.php
27	Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений	1	
28	Ответственность за преступления — за проведение скрытой (негласной) аудиозаписи	1	https://lbz.ru/metodist/authors/ib/10-11.php
29	Ответственность за преступления — за заведомо ложное сообщение о теракте	1	
30	Ответственность за преступления — за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг)	1	
31	Ответственность за преступления — за мошенничество в сфере компьютерной информации	1	
32	Ответственность за преступления — за незаконное распространение порнографических материалов.	1	https://lbz.ru/metodist/authors/ib/10-11.php
33	Ответственность за преступления — за заведомо ложный донос	1	
34	Индивидуальный зачет	1	

11 класс

№	Тема урока	Количество часов	Электронные (цифровые) образовательные ресурсы
Глава 5. Проектные задания			
1	Техника безопасности и организация рабочего места. Лицензионное соглашение свободного ПО Линукс	1	
2	Как купить лицензию на платную антивирусную программу	1	https://lbz.ru/metodist/authors/ib/10-11.php
3	Что такое СС лицензия.	1	
4	Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию	1	https://lbz.ru/metodist/authors/ib/10-11.php
5	Индивидуальный зачет	1	
6	Индивидуальный зачет	1	

7	Защита проекта	1	https://lbz.ru/metodist/authors/ib/10-11.php
8	Как задавать безопасный пароль.	1	
9	Настройки телефона, планшета для защиты от несанкционированного доступа.	1	
10	Защита персональных данных. Обзор.	1	
11	Личный контент в облаке и система его защиты.	1	
12	Индивидуальный зачет.	1	
13	Защита проекта	1	
Онлайн - курс «Основы информационной безопасности»			
14	Понятие информационной безопасности. Основные составляющие. Важность проблемы.	1	https://intuit.ru/studies/courses?page=1
15	Распространение объектно-ориентированного подхода на информационную безопасность.	1	https://intuit.ru/studies/courses?page=1
16	Наиболее распространенные угрозы.	1	https://intuit.ru/studies/courses?page=1
17	Наиболее распространенные угрозы.	1	https://intuit.ru/studies/courses?page=1
18	Законодательный уровень информационной безопасности.	1	https://intuit.ru/studies/courses?page=1
19	Законодательный уровень информационной безопасности.	1	https://intuit.ru/studies/courses?page=1
20	Стандарт и спецификации в области информационной безопасности.	1	https://intuit.ru/studies/courses?page=1
21	Стандарт и спецификации в области информационной безопасности.	1	https://intuit.ru/studies/courses?page=1
22	Административный уровень информационной безопасности.	1	https://intuit.ru/studies/courses?page=1
23	Управление рисками	1	https://intuit.ru/studies/courses?page=1
24	Процедурный уровень информационной безопасности.	1	https://intuit.ru/studies/courses?page=1
25	Основные программно-технические меры.	1	https://intuit.ru/studies/courses?page=

			1
26	Идентификация и аутентификация, управление доступом.	1	https://intuit.ru/studies/courses?page=1
27	Идентификация и аутентификация, управление доступом.	1	https://intuit.ru/studies/courses?page=1
28	Протоколирование и аудит, шифрование, контроль целостности.	1	https://intuit.ru/studies/courses?page=1
29	Экранирование, анализ защищенности.	1	https://intuit.ru/studies/courses?page=1
30	Обеспечение высокой доступности.	1	https://intuit.ru/studies/courses?page=1
31	Туннелирование и управление.	1	https://intuit.ru/studies/courses?page=1
32	Подведение итогов курса «Информационная безопасность»	1	https://intuit.ru/studies/courses?page=1
33-34	Хакер Джеймс Хендли Чейз	2	https://intuit.ru/studies/courses?page=1