

Приложение
к основной образовательной программе
среднего общего образования
МАОУ СОШ № 18

РАБОЧАЯ ПРОГРАММА
учебного предмета
«Информационная безопасность»
уровень среднего общего образования

ФГОС (10-11 класс)

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

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.

В результате изучения курса информационной безопасности ученик должен знать/понимать:

- 1) Основы ИБ
- 2) Основные направления ИБ
- 3) Базовые принципы анализа защищенности
- 4) Основные инструменты для проведения анализа защищенности

Уметь:

- 1) Оценивать безопасность информационных систем
- 2) Оценивать уровень защищенности информационных систем
- 3) Программировать на языке Python для написания базовых скриптов

Использовать приобретенные знания и умения в практической деятельности и повседневной жизни для

- 1) Защиты своей личной информации
- 2) Повышения уровня знаний для обеспечения собственной безопасности в информационном поле.

Для выявления достижения планируемых результатов обучения рекомендуется использовать диагностические тесты и опросы, проектные работы и конкурсы по информационной безопасности в образовательных организациях.

СОДЕРЖАНИЕ

УЧЕБНОГО КУРСА «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»

10 класс

1. Вводный урок. Информационная безопасность: что это такое?
2. Национальные интересы РФ в информационной сфере
3. Системный подход к решению проблемы защиты информации
4. Информация как объект юридической защиты
5. Общедоступная, конфиденциальная и секретная информация.
6. Основные принципы засекречивания информации
7. Государственная система правового обеспечения защиты информации в РФ
8. Основные положения закона «Об информации, информатизации и защите информации»
9. Авторское право, права автора или правообладателя в законе «О правовой охране программ и данных».
10. Основные положения главы «преступления в сфере компьютерной информации» УК РФ
11. Закон «Об электронной цифровой подписи».
12. Методы обеспечения санкционированного доступа.
13. Средства и методы идентификации и аутентификации пользователя
14. Формирование электронной цифровой подписи и аутентификатора
15. Технология централизованной аутентификации
16. Управление доступом к данным
17. Методы управления доступом к сети связи
18. Методы защиты передачи данных в сети связи
19. Целостность данных в ИС
20. Ограничения целостности
21. Семантическая целостность
22. Ссылочная целостность.
23. Особенности защиты данных в ИС, основанной на криптографии
24. Методы криптографического преобразования информации
25. Сравнение симметричных и асимметричных алгоритмов шифрования
26. Основные технологии обеспечения защиты информации в сети Интернет. Функции и средства защиты информации в сети Интернет
27. Методы криптографического преобразования информации. Сравнение симметричных и асимметричных алгоритмов шифрования.

11 класс

1. Основные документы в области информационной безопасности Российской Федерации
2. Информация как объект правовых отношений
3. Функции, принципы и виды юридической ответственности.
4. Субъективная и объективная стороны юридической ответственности
5. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности
6. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации)
7. Ответственность за проступок в области присвоение авторства (плагиат)
8. Ответственность за проступок за оскорбления, в том числе в социальных сетях
9. Административное правонарушение. Основные понятия административного правонарушения
10. Особенности административной ответственности несовершеннолетних.
11. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение
12. Ответственность за проступок – за оскорбления, в том числе в социальных сетях
13. Ответственность за проступок - ложный вызов экстренных служб
14. Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ
15. Ответственность за проступок –нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные)
16. Ответственность за проступок – нарушение правил защиты информации
17. Ответственность за проступок – представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство
18. Ответственность за проступок – за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт
19. Ответственность за проступок –нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации

20. Уголовный кодекс Российской Федерации
21. Виды наказаний в области уголовной ответственности
22. Ответственность за преступления в области компьютерной информации и применения компьютеров
23. Ответственность за преступления в области присвоения авторства (плагиат)
24. Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение
25. Ответственность за преступления в области мошенничества (обмана)
26. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений
27. Ответственность за преступления – за проведение скрытой (негласной) аудиозаписи
28. Ответственность за преступления – за заведомо ложное сообщение о теракте
29. Ответственность за преступления – за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг)
30. Ответственность за преступления – за мошенничество в сфере компьютерной информации
31. Ответственность за преступления – за незаконное распространение порнографических материалов
32. Ответственность за преступления – за заведомо ложный донос
33. Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве

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

Программа учебного курса для 10 классов среднего общего образования рассчитана на объем 34 часов, а 11 класс – 33 часа.

10 класс:

Модуль/тема	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
1. Вводный урок. Информационная безопасность: что это такое?	1	1	
2. Национальные интересы РФ в информационной сфере	1	1	
3. Системный подход к решению проблемы защиты информации	1	1	
4. Информация как объект юридической защиты	1	1	
5. Общедоступная, конфиденциальная и секретная информация.	1	1	
6. Основные принципы засекречивания информации	2	1	1
7. Государственная система правового обеспечения защиты информации в РФ	1	1	
8. Основные положения закона «Об информации, информатизации и защите информации»	2	2	

9. Авторское право, права автора или правообладателя в законе «О правовой охране программ и данных».	1	1	
10. Основные положения главы «преступления в сфере компьютерной информации» УК РФ	1	1	
11. Закон «Об электронной цифровой подписи».	1	1	
12. Методы обеспечения санкционированного доступа.	2	1	1
13. Средства и методы идентификации и аутентификации пользователя	2	1	1
14. Формирование электронной цифровой подписи и аутентификатора	1	1	
15. Технология централизованной аутентификации	1	1	
16. Управление доступом к данным	1		1
17. Методы управления доступом к сети связи	1		1
18. Методы защиты передачи данных в сети связи	1		1
19. Целостность данных в ИС	1	1	
20. Ограничения целостности	1	1	
21. Семантическая целостность	1	1	
22. Ссылочная целостность.	1	1	

23. Особенности защиты данных в ИС, основанной на криптографии	3	1	2
24. Методы криптографического преобразования информации	2	1	1
25. Сравнение симметричных и асимметричных алгоритмов шифрования	1		1
26. Основные технологии обеспечения защиты информации в сети Интернет. Функции и средства защиты информации в сети Интернет	1		1
27. Методы криптографического преобразования информации. Сравнение симметричных и асимметричных алгоритмов шифрования.	1	1	0
Всего:	34	23	11

11 класс:

Модуль/тема	Всего часов	Теоретические занятия	Практическая работа с ресурсами и программами на компьютере
1. Основные документы в области информационной безопасности Российской Федерации	1	1	
2. Информация как объект правовых отношений	1	1	
3. Функции, принципы и виды юридической ответственности.	1	1	
4. Субъективная и объективная стороны юридической	1	1	

ответственности			
5. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности	1	1	
6. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации)	1		1
7. Ответственность за проступок в области присвоение авторства (плагиат)	1	1	
8. Ответственность за проступок за оскорбления, в том числе в социальных сетях	1	1	
9. Административное правонарушение. Основные понятия административного правонарушения	1	1	
10. Особенности административной ответственности несовершеннолетних.	1	1	
11. Ответственность за проступок в области нарушения авторских прав	1	1	

на лицензионное программное обеспечение			
12. Ответственность за проступок – за оскорбления, в том числе в социальных сетях	1	1	
13. Ответственность за проступок - ложный вызов экстренных служб	1	1	
14. Ответственность за проступок - пропаганду в Интернете наркотических и психотропных веществ	1	1	
15. Ответственность за проступок –нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные)	1	1	
16. Ответственность за проступок – нарушение правил защиты информации	1		1
17. Ответственность за проступок – представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство	1		1

18. Ответственность за проступок – за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт	1		1
19. Ответственность за проступок – нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации	1	1	
20. Уголовный кодекс Российской Федерации	1	1	
21. Виды наказаний в области уголовной ответственности	1	1	
22. Ответственность за преступления в области компьютерной информации и применения компьютеров	1	1	
23. Ответственность за преступления в области присвоения авторства (плагиат)	1	1	
24. Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение	1		1

25. Ответственность за преступления в области мошенничества (обмана)	1		1
26. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений	1		1
27. Ответственность за преступления – за проведение скрытой (негласной) аудиозаписи	1	1	
28. Ответственность за преступления – за заведомо ложное сообщение о теракте	1	1	
29. Ответственность за преступления – за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг)	1	1	
30. Ответственность за преступления – за мошенничество в сфере компьютерной информации	1	1	
31. Ответственность за преступления – за незаконное распространение порнографических материалов	1	1	

32. Ответственность за преступления – за заведомо ложный донос	1	1	
33. Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве	1		1
Всего:	33	25	8