Чикишев Александр Анатольевич
Подписано цифровой подписью: Чикишев Александр Анатольевич
Дата: 2024.11.02 12:10:02 +08'00'

Муниципальное бюджетное общеобразовательное учреждение «Средняя общеобразовательная школа №24»
города Ангарска Иркутской области

=Рассмотрено=	=Согласовано=	=Утверждаю=
на заседании МС	Зам. директора по УВР	Директор МБОУ «СОШ №24»
«30 »___08__2024г. Протокол № ___	_____ /О.В.Сарапова /	А.А. Чикишев
Руководитель МС _____/О.А. Воронова/	«_30__»__08___2024 г.	«_02_»__сентября__2024г.

РАБОЧАЯ ПРОГРАММА
по курсу внеурочной деятельности «Информационная безопасность»

.
Учитель: Пантеева К.С.
Год составления: 2024г. на 2024-2025 учебный год
Класс: 10-11
Общее количество часов по плану: 34ч. (10кл. – 17ч., 11 кл. – 17 ч.)
Количество часов в неделю: 0,5ч

«_30_»____08____2024 г. _____
(подпись учителя)

г. Ангарск

Рабочая программа по курсу внеурочной деятельности «Информационная безопасность» разработана на основе требований к результатам основной образовательной программы среднего общего образования с учетом программ, включенных в ее структуру.

Содержание курса внеурочной деятельности «Информационная безопасность»
10 - 11 класс

Модуль 1. Правовые основы информационной безопасности

Понятия юридической ответственности за правонарушения в области информационной безопасности.

Основные документы в области информационной безопасности Российской Федерации. Информация как объект правовых от-Ношений. Функции, принципы и виды юридической ответственности. Субъективная и объективная стороны юридической ответственности.

Модуль 2. Законо дательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности.

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

Общие положения законодательстваРоссийской Федерации о гражданско-правовой ответственности. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации). . Ответственность за проступок в области присвоение авторства (плагиат). Ответственность за проступок за оскорбления, в том числе в социальных сетях.

Модуль 3. Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности.

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

Административное правонарушение. Основные понятия административного правонарушения. Особенности административной ответственности несовершеннолетних.

Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение. Ответственность за проступок — за оскорбления, в том числе в социальных сетях. Ответственность за проступок —ложный вызов экстренных служб. Ответственность за проступок —пропаганду в Интернете наркотических и психотропных веществ. Ответственность за проступок — нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональные данные). Ответственность за проступок —нарушение правил защиты информации. Ответственность за проступок — представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство. Ответственность за проступок — за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт.Ответственность за проступок —нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.

Модуль 4. Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности.

Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации).

Уголовный кодекс Российской Федерации. Виды наказаний в области уголовной ответственности.

Ответственность за преступления в области компьютерной информации и применения компьютеров. Ответственность за преступления в области присвоения авторства (плагиат).

Ответственность за преступления в области нарушения авторских прав на лицензионное программное обеспечение. Ответственность за преступления в области мошенничества (обмана). Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений. Ответственность за преступления — за проведение скрытой (негласной) аудиозаписи. Ответственность за преступления — за заведомо ложное сообщение о теракте. Ответственность за преступления — за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг). Ответственность за преступления — за мошенничество в сфере компьютерной информации. Ответственность за преступления — за незаконное распространение порнографических материалов. Ответственность за преступления — за заведомо ложный донос.

Модуль 5. Практика применения правил и норм информационной безопасности.

Лицензионное соглашение свободного ПО Линукс. Как купить лицензию на платную антивирусную программу. Что такое CC лицензия. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию.

Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного доступа. Защита персональных данных. Обзор. Личный контент в облаке и система его защиты.

Планируемые результаты курса внеурочной деятельности «Информационная безопасность»

Рабочая программа «Информационная безопасность» реализует социальное направление внеурочной деятельности МБОУ «СОШ №24». В результате реализации программы «Информационная безопасность» могут быть достигнуты определённые результаты:

Познавательные УУД

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

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

Регулятивные УУД

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

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

–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;

Коммуникативные УУД

–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;

Тематическое планирование
10-11 класс

Модуль	Название темы	Количество часов		
		Всего	**Теория**	**Практика**
Раздел 1				
Модуль 1 **Правовые основы информационной безопасности**	**Глава 1.** Понятия юридической ответственности за правонарушения в области информационной безопасности.	**3**	**1**	**2**
1.1. Понятия юридической ответственности за правонарушения в области информационной безопасности.	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	2	1	1
1.2. Контрольное занятие	Подготовка презентации по теме в группах учащихся	1		1
Модуль 2 **Законо дательство Российской Федерации о гражданско-правовой ответственности в сфере инфобезопасности**	**Глава 2.** Гражданско-правовая ответственность за проступки в области информационной безопасности (защиты информации)	**4**	**2**	**2**
2.1. Законодательство Российской Федерации о гражданско-правовой ответственности.	1. Общие положения законодательства Российской Федерации о гражданско-правовой ответственности. 2. Порядок привлечения несовершеннолетних к гражданско-правовой ответственности за проступки в области информационной безопасности (защиты информации).	2	1	1
2.2. Гражданско-правовая ответственность несовершеннолетних за проступки в области информационной безопасности (защиты информации)	1. Ответственность за проступок в области присвоения авторства (плагиат). 2. Ответственность за проступок за оскорбления, в том числе в социальных сетях.	1	1	
2.3. Контрольное занятие	Индивидуальный зачет	1		1
Модуль 3	**Глава 3.** Административная ответственность за проступки в области	**6**	**3**	**3**

Законодательство Российской Федерации об административной ответственности в сфере инфобезопасности	информационной безопасности (защиты информации).			
3.1. Понятие административной ответственности	1. Административное правонарушение. Основные понятия административного правонарушения. 2. Особенности административной ответственности несовершеннолетних.	1	1	
3.2. Административная ответственность несовершеннолетних граждан за проступки в области информационной безопасности (защиты информации).	1. Ответственность за проступок в области нарушения авторских прав на лицензионное программное обеспечение. 2. Ответственность за проступок — заоскорбления, в том числе в социальных сетях. 3. Ответственность за проступок —ложный вызов экстренных служб. 4. Ответственность за проступок —пропаганду в Интернете наркотических и психотропных веществ. 5. Ответственность за проступок —нарушение установленного законом порядка сбора, хранения, использованияили распространения информации о гражданах (персональные данные). 6. Ответственность за проступок —нарушение правил защиты информации. 7. Ответственность за проступок —представление ложных сведений для получения документа, удостоверяющего личность гражданина (паспорта), либо других документов, удостоверяющих личность или гражданство. 8. Ответственность за проступок — за подделку документов, штампов, печатей или бланков, их использование, передача, либо сбыт. 9. Ответственность за проступок —нарушение правил производства, хранения, продажи и приобретения специальных технических средств, предназначенных для негласного получения информации.	4	2	2
3.3. Контрольное занятие	Индивидуальный зачет	1		1
Модуль 4. **Законодательство Российской Федерации об уголовной ответственности в сфере инфобезопасности.**	**Глава 4.** Уголовная ответственность за правонарушения в области информационной безопасности (защиты информации).	**7**	**4**	**3**
4.1. Понятие уголовной ответственности	1. Уголовный кодекс Российской Федерации 2. Виды наказаний в области уголовной ответственности	1	1	
4.2. Уголовная ответственность несовершеннолетних за преступления в области информационной безопасности (защиты информации)	1. Ответственность за преступления в области компьютерной информации и применения компьютеров. 2. Ответственность за преступления в области присвоения авторства (плагиат). 3. Ответственность за преступления в области нарушения авторских прав на	5	3	2

	лицензионное программное обеспечение. 4. Ответственность за преступления в области мошенничества (обмана). 5. Ответственность за преступления в области нарушения тайны переписки, телефонных переговоров или иных сообщений. 6. Ответственность за преступления — за проведение скрытой (негласной) аудиозаписи. 7. Ответственность за преступления — за заведомо ложное сообщение о теракте. 8. Ответственность за преступления — за неприкосновенности частной жизни (тайна общения и творчества, дневников, личных бумаг). 9. Ответственность за преступления — за мошенничество в сфере компьютерной информации. 10. Ответственность за преступления — за незаконное распространение порнографических материалов. 11. Ответственность за преступления — за заведомо ложный донос.			
4.3. Контрольное занятие	Индивидуальный зачет	1		1
Всего по разделу 1	***Модули 1–4***	20	10	10
Часы самостоятельной работы	Самостоятельная работа для индивидуальных зачетов и подготовки презентаций (предоставляется в компьютерной форме)	1		1
Итого	***Раздел 1***	***21***	***10***	***11***
Раздел 2				
Модуль 5. **Практика применения правил и норм информационной Безопасности.**	**Глава 5.** Проектные задания	***12***	***2***	***10***
5.1. Проектная работа. Нормативные основы лицензионных соглашений	1. Лицензионное соглашение свободного ПО Линукс. 2. Как купить лицензию на платную антивирусную программу. 3. Что такое СС лицензия. 4. Обзор свободного антивирусного ПО и его возможности по антиспаму и шлюзованию.	2	1	1
5.2. Проектная работа. Практика соблюдения норм инфобезопасности в личном информационном пространстве	1. Как задавать безопасный пароль. Настройки телефона, планшета для защиты от несанкционированного доступа. 2. Защита персональных данных. Обзор. Личный контент в облаке и система его защиты.	2	1	1
5.3. Самостоятельная дистанционная работа	Онлайн-курс «Основы информационной безопасности».	7		7
5.4 Контрольное занятие	Тест по онлайн курсу	1		1

Всего по разделу 2	***Модуль 5***	12	2	10
Резерв к разделу 2		1		1
Итого	***Раздел 2***	**13**	**2**	**11**
Всего часов по курсу (разделы 1 и 2)	За два года обучения (1 час в неделю)	34	12	22

Фомы организации и виды деятельности:

На занятиях по курсу внеурочной деятельности «Информационная безопасность» используются следующие **виды деятельности:**

- игровая деятельность,
- познавательная деятельность,
- проблемно – ценностное общение.

формы организации деятельности:

- практические занятия,
- организация наблюдения, эксперимента,
- викторины, конкурсы, олимпиады,
- диагностические занятия,
- проекты (индивидуальные и групповые).

Приложение

Календарно-тематическое планирование 5 класс

№	Название темы	Количество часов		
		Всего	Теория	Практика
1	Введение	1	1	
Часть 1. Пространство Интернета на планете Земля				
2	Что нужно знать? Пространство интернета на планете Земля.	1	1	
3	История создания сети Интернет	1	1	
4	Практикум. Где находится интернет?	1		1
5	Знакомство с сайтом телеканала «Карусель». Тест 1.	1	1	
6	Что такое Всемирная паутина.	1		1
7	Практикум. Как пользоваться программой-браузером.	1	1	
8	Что такое веб-браузер. Тест 2.	1	1	
9	Путешествие по сети Интернет: Сайты и электронные сервисы.	1	1	
10	Интернет-коммуникации.	1	1	
11	Практикум. Знакомство с социальной сетью «Смешарики»	1		1

12	Что такое поисковая система. Тест 3.	1	1	
13	Практикум. Знакомство с социальной сетью «Культура РФ»	1		1
14	Как стать пользователем интернета.	1	1	
15	Практикум. Правила информационной безопасности.	1		1
16	Способы выхода в интернет. Тест 4.	1	1	
17	Опасности для пользователей интернета.	1	1	
18	Практикум. Знакомство с сайтом Большой Российской энциклопедии.	1		1
19	Как проверить представленную в Интернете информацию. Тест 5.	1	1	
20	Кибератака. Что такое кибератака, направленная на человека.	1	1	
21	Что такое компьютерные вирусы и чем они опасны.	1	1	
22	Практикум. Знакомство с сайтом «Защита детей. Лаборатория Касперского»	1		1
23	Кибербуллинг. Фишинг. Тест 6.	1	1	
24	Что такое информационная безопасность.	1	1	
25	Практикум. Личная памятка безопасности при работе в Интернете.	1		1
26	Обеспечение информационной безопасности. Тест 7.	1	1	
27	Законы о защите личных данных в Интернете. Что такое персональные данные.	1	1	
28	Практикум. Знакомство с общественной организацией «Лига безопасного интернета»	1		1
29	Конфиденциальность. Какие угрозы подстерегают в сетевых играх. Тест 8.	1	1	
30	Сетевой этикет.	1	1	
31	Практикум. Какие правила нужно соблюдать при общении в Интернете, чтобы не навредить себе. Тест 9.	1		1
32	Коллекции сайтов для детей. Что такое позитивный контент.	1	1	
33	Практикум. Специализированный детский интернет-браузер «Гогуль». ВебЛандия.	1		1
34	Электронные музеи. Контрольное задание к части 1.	1		1
		33	21	12

Календарно-тематическое планирование 6 класс

№	Название темы	Количество часов		
		Всего	Теория	Практика
Часть 2. Правила для пользователей сети Интернет				

1	Правила работы с СМС. Рекламные рассылки. СМС-спам.	1	1	
2	Практикум. Правила этикета при работе с СМС.	1		1
3	Приватность аккаунтов. Тест 10.	1	1	
4	Правила работы с электронной почтой.	1	1	
5	Практикум. Настройка почтового ящика в Яндексе.	1		1
6	Практикум. Основные правила использования электронной почты.	1		1
7	Рекламные рассылки. Папка «Спам». Сообщения со взломанных аккаунтов. Тест 11.	1	1	
8	Правила работы с видеосервисами. Пиратские видеоматериалы.	1	1	
9	Практикум. Система помощи по работе с видеозаписями в социальной сети ВКонтакте. Тест 12.	1		1
10	Правила работы в социальных сетях. Троллинг.	1	1	
11	Практикум. Специальные настройки в меню социальных сетей, позволяющие защититься от нежелательных обращений. Кнопка «Пожаловаться».	1		1
12	Как избавиться от неприятных комментариев и сообщений. Тест 13.	1	1	
13	Правила защиты от вирусов, спама, рекламы и рассылок. Антивирусная программа.	1	1	
14	Пути распространения вирусов в Интернете и методы борьбы с ними. Тест 14.	1	1	
15	Правила защиты от негативных сообщений. Виды сетевого мошенничества.	1	1	
16	Практикум. Обманные ссылки (поддельные веб-сайты).	1		1
17	Осторжней в Интернете! – Встроенные покупки! Тест 15.	1	1	
18	Правила общения в социальной сети. Профиль.	1	1	
19	Практикум. Система помощи в социальных сетях ВКонтакте, Facebook, Одноклассники.	1		1
20	Как вести себя в социальных сетях. Тест 16.	1	1	
21	Правила работы с поисковыми системами.	1	1	
22	Пиратские сайты. Фейковые новости. Тест 17.	1	1	
23	Практикум. Ложная информация: как распознать?	1		1
24	Правила ответственности за распространение ложной и негативной информации.	1	1	
25	Правовые акты, связанные с информационной безопасностью в Интернете.	1	1	
26	Правила защиты от нежелательных сообщений и контактов.	1	1	
27	Практикум. Опасность встречи в реале: какие угрозы подстерегают вас при общении с незнакомцами.	1		1

28	Правила вызова экстренной помощи.	1	1	
29	Практикум. Знакомство с сайтом «Пространство безопасности. Школа первой помощи». Основные сведения, которые необходимо сообщить при вызове экстренных служб.	1		1
30	Правила защиты устройств от внешнего вторжения.	1	1	
31	Создание аккаунта. Подборка паролей. Тест 18.	1	1	
32	Правила выбора полезных ресурсов в Интернете.	1	1	
33	Практикум. Медиапортал «Аудиохрестоматия».	1		1
34	Средства работы в Интернете для людей с особыми потребностями. Контрольное задание к части 2.	1	1	
		34	23	11

Календарно-тематическое планирование 7 класс

№	Название темы	Количество часов		
		Всего	Теория	Практика
	Модуль 1 **Раздел 1.Киберпространство**	34	29	5
1	Киберпространство.	1	1	
2	Составляющие киберпространства.	1	1	
3	Технологические аспекты использования ресурсов киберпространства.	1	1	
4	Кибермиры.	1	1	
5	Технологии искусственного интеллекта	1	1	
6	Облачные технологии	1	1	
7	Робототехнические системы	1	1	
8	Киберкостюм, экзоскелет.	1	1	
9	Киберфизическая система.	1	1	
10	Составляющие киберфизической системы. (Большие данные и аналитика, автономные роботы, компьютерное зрение)	1	1	
11	Составляющие киберфизической системы. (Моделирование и симуляторы,	1	1	

	облачные вычисления)			
12	Составляющие киберфизической системы. (Интернет вещей, информационная безопасность)	1	1	
13	Составляющие киберфизической системы. (3D-печать, дополненная реальность)	1	1	
14	Киберобщество.	1	1	
15	Особенности киберобщества.	1	1	
16	Сетевой этикет.	1	1	
17	Клиповое мышление.	1	1	
18	Кибермания.	1	1	
19	Кибераддикция	1	1	
20	Кибергражданe.	1	1	
21	Киберденьги.	1	1	
22	Электронные платежи.	1	1	
23	Электронные деньги.	1	1	
24	Криптовалюта.	1	1	
25	Кибермошенничество	1	1	
26	Виды кибермошенничества. Кардинг.	1	1	
27	Виды кибермошенничества. Скимминг.	1	1	
28	Виды кибермошенничества. Фишинг.	1	1	
29-33	Практическая работа на основе онлайн-курса Академии Яндекс «Безопасность в Интернете» по теме «Безопасные онлайн-платежи»	5		5
34	Контрольное занятие. Тест к разделу 1.	1	1	

Календарно-тематическое планирование 8 класс

№	Название темы	Количество часов		
		Всего	Теория	Практика
	Модуль 2			
	Раздел 2. Киберкультура	34	29	5
1	Киберкультура.	1	1	
2	Составляющие киберкультуры.	1	1	
3	Электронные медиаресурсы.	1	1	
4	Интерактивный исторический парк «Россия. Моя история»	1	1	
5	От книги к гипертексту.	1	1	
6	Использование языка HTML (Hypertext Markup Language)	1	1	

7	Недостатки гипертекста.	1	1	
8	Языки для разметки гипертекста при создании веб-страниц сайтов.	1	1	
9	Протокол передачи гипертекста HTTP (HTTPS)	1	1	
10	Система адресации URI и URL.	1	1	
11	Программы-браузеры.	1	1	
12	Киберкнига.	1	1	
13	Книги с дополненной реальностью (Augmented Reality)	1	1	
14	Виртуальная реальность.	1	1	
15	Архитектурные реконструкции памятников истории с помощью виртуальной реальности.	1	1	
16	Киберискусство.	1	1	
17	Виды компьютерного искусства. Компьютерная графика.	1	1	
18	Виды компьютерного искусства. Компьютерная музыка.	1	1	
19	Виды компьютерного искусства. Компьютерная анимация.	1	1	
20	Виды компьютерного искусства. Интерактивный компьютерный перфоманс.	1	1	
21	Виды компьютерного искусства. Медиаискусство.	1	1	
22	Виды компьютерного искусства. Светомузыкальные композиции.	1	1	
23	Социальная инженерия. Тактики психологической манипуляции.	1	1	
24	Спуфинг.	1	1	
25	Тайпсквоттинг	1	1	
26	Претекстинг.	1	1	
27	Классификация угроз социальной инженерии	1	1	
28	Федеральный закон о персональных данных.	1	1	
29-33	Практическая работа от компаний мобильной связи Билайн, МТС и Мегафон (по выбору учащихся)	5		5
34	Контрольное занятие. Тест к разделу 2	1	1	
	Модуль 3			
	Раздел 3. Киберугрозы	34	29	5
1	Кибервойны. Цели.	1	1	
2	Кибербезопасность.	1	1	
3	Кибершпионаж.	1	1	

Календарно-тематическое планирование 9 класс

№	Название темы	Количество часов		
		Всего	Теория	Практика

4	Кибератаки.	1	1	
5	Виды кибератак. Вандализм, пропаганда, утечка конфиденциальных данных.	1	1	
6	DDoS атаки.	1	1	
7	Кибертерроризм.	1	1	
8	Лаборатория Касперского. «Интерактивная карта киберугроз»/	1	1	
9	Киберпреступность.	1	1	
10	Конвенция о борьбе с киберпреступностью.	1	1	
11	Виды незаконных действий в виртуальном пространстве.	1	1	
12	Примеры киберпреступлений. Хакерская атака.	1	1	
13	Кибersталкинг. Кибертерроризм. Тайпсквоттинг.	1	1	
14	Наказания за кибернарушения. Глава 28 Уголовного кодекса РФ.	1	1	
15	Угрозы современного мира.	1	1	
16	Уязвимости кибербезопасности.	1	1	
17	Бэкдоры. Атаки отказа в обслуживании.	1	1	
18	Атаки прямого доступа. Подслушивание.	1	1	
19	Подделка. Неверные права доступа. Бреши.	1	1	
20	Компьютерный шпионаж. Крэкерская атака.	1	1	
21	Угрозы информационной безопасности.	1	1	
22	Непреднамеренные и преднамеренные угрозы.	1	1	
23	Нежелательный контент. Спам.	1	1	
24	Вредоносные программы. Несанкционированный доступ.	1	1	
25	Фрод. Виды защитного программного обеспечения.	1	1	
26	Запрещенные и нежелательные сайты.	1	1	
27	Новые профессии в киберобществе.	1	1	
28-33	Практическая работа на основе онлайн-курса Академии Яндекса «Безопасность в Интернете» (продолжение), по темам: защита от вредоносных программ; безопасность аккаунтов.	6		6
34	Контрольное занятие. Тест к разделу 3.	1	1	
		34	28	6