C=RU, O="МБУ ""
Лицей №19""", CN="
Кизилов Денис
Сергеевич, директор",
E=school19@edu.tgl.ru
00 a3 60 7a 9d 2f 91
a4 16
2022.09.26
08:21:01+04'00'

Муниципальное бюджетное общеобразовательное учреждение

городского округа Тольятти

«Лицей №19 имени Героя Советского Союза Евгения Александровича Никонова»

Принята на заседании
Педагогического совета
Протокол № 1
от «26» августа 2022 г

Утверждаю
Директор МБУ «Лицей №19»
_____ /Кизилов Д.С./
Приказ № 294/1
от «26» августа 2022г

РАБОЧАЯ ПРОГРАММА
внеурочной деятельности

Курс Информационная безопасность «Цифровая гигиена» **Класс 8**

Направление: общекультурное

Срок реализации 1 год

Общее количество часов по учебному плану 34 часа.

I. Пояснительнаязаписка

Программаповнеурочномукурсу«Цифроваягигиена» составленав соответствии нормативно-правовымидокументами:

- ✓ Федеральнымзаконом«ОбобразованиивРФ»№273-ФЗот29.12.12г.;
- ✓ ПриказомМинобрнаукиРоссииот17.12.2010г.№1897«Об утверждении федеральногогосударственногообразовательного стандарта основного общего образования» (в редакции от 29.12.2014 №1644, от 31 декабря 2015 г. N 1577);
- ✓ Примерной основной образовательной программойосновного общего образования (одобрена решением федерального учебно-методическогообъединенияпообщемуобразованию(протоколот8апреля2015г.№ 1/15,входитв специальныйгосударственный реестр примерных основных образовательных программ, размещена на официальном сайте http:edu.crowdexpert.ru/results-noo).
- ✓ Основнаяобразовательнаяпрограммаосновногообщегообразования

Основнымицелямиизучениякурса«Цифроваягигиена»являются:

Обеспечение условий для профилактики негативныхтенденцийв информационной культуре учащихся, повышения защищенности детей от информационных рисков и угроз;

Формирование навыков своевременного распознавания онлайнрисков (технического, контентного, коммуникационного, потребительского характера и риска интернетзависимости).

Задачипрограммы:

- ✓ сформировать общекультурные навыки работы с информацией (умения, связанные с поиском, пониманием, организацией, архивированием цифровой информации и ее критическим осмыслением, а также с созданием информационных объектов с использованием цифровых ресурсов (текстовых, изобрази- тельных, аудио и видео);
- ✓ создать условия для формирования умений, необходимых для различных форм коммуникации (электронная почта, чаты, блоги, форумы, социальные сети и др.) сразличными целями иответственного отношения к взаимодействию в современной информационно- телекоммуникационной среде;
- ✓ сформироватьзнания,позволяющиеэффективноибезопасноиспользоватьтехническиеипрограммныесредствадлярешения

различныхзадач,втомчислеиспользованиякомпьютерныхсетей,облачныхсервисовит.п.;

- ✓ сформировать знания, умения, мотивацию и ответственность, позволяющие решать с помощью цифровых устройств и интернета различные повседневные задачи, связанные с конкретными жизненными ситуациями, предполагающими удовлетворение различных потребностей;
- ✓ сформироватьнавыкипопрофилактикеикоррекциизависимого поведенияшкольников, связанного скомпьютерными технологиями и Интернетом.

Общаяхарактеристикаучебногокурса

Курс «Цифровая гигиена»являетсяважнойсоставляющей работы собучающимися, активно использующими различные сетевые формы общения (социальные сети, игры, пр.) с целью мотивации ответственного отношения к обеспечению своей личной безопасности, безопасности своей семьи и своихдрузей. Кроме того, реализациякурса создаст условиядлясокращения цифрового разрыва между поколениями и позволит родителям выступать вкачестве экспертов, передающих опыт.

Описаниеместакурса«Цифроваягигиена»в учебном плане

В соответствиисучебным планом внеурочный курс«Цифроваягигиена» реализуется в 8 классе в объеме 34 часа, из расчета 1 час в неделю. Продолжительность занятий 40 минут.

Формытекущегоконтроляипромежуточной аттестации

Форма текущего контроля: устный опрос; наблюдение за самостоятельной работой обучающегося, за его умением работать в группе сверстников; практическая работа; рефлексия в форме вербального проговаривания или письменного выражения своего отношения к теме, собственному участию в совместной работе

Годоваяпромежуточная аттестацияпроводитсявформетестирования.

II. Содержаниевнеурочногокурса

Раздел1.«Безопасностьобщения»

Тема1.Общениевсоциальныхсетяхи мессенджерах.1час.
Социальнаясеть.Историясоциальныхсетей.Мессенджеры. Назначениесоциальныхсетейимессенджеров.Пользовательскийконтент.

Тема2.Скембезопаснообщатьсявинтернете.1час.
Персональныеданныекакосновнойкапиталличного пространствавцифровоммире.Правиладобавлениядрузейв социальныхсетях. Профиль пользователя. Анонимные социальные сети.

Тема3.Паролидляаккаунтов социальныхсетей.1час.
Сложныепароли.Онлайнгенераторыпаролей.Правилахраненияпаролей.Использованиефункциибраузерапозапоминаниюпаролей.

Тема4.Безопасныйвходваккаунты.1 час.
Видыаутентификации. Настройкибезопасностиаккаунта.Работаначужомкомпьютересточкизрениябезопасностиличного аккаунта.

Тема5.Настройкиконфиденциальностивсоциальныхсетях. 1час.
Настройкиприватностиконфиденциальностивразныхсоциальныхсетях. Приватностьиконфиденциальностьвмессенджерах.

Тема6.Публикацияинформациивсоциальныхсетях.2час. Персональные
данные. Публикация личной информации.

Тема7.Кибербуллинг.1час.
Определениекибербуллинга. Возможныепричинькибербуллингаикакегоизбежать?Какнестатьжертвойкибербуллинга. Какпомочь жертве кибербуллинга.

Тема8.Публичныеаккаунты. 1час.
Настройкиприватностипубличныхстраниц.Правилаведенияпубличныхстраниц.Овершеринг.

Тема9.Фишинг.2 час.
Фишингкакмошенническийприем.Популярныевариантыраспространенияфишинга. Отличиенастоящихифишинговыхсайтов. Как защититься от фишеров в социальных сетях и мессенджерах.

Раздел2.«Безопасность устройств»

Тема1.Чтотакоевредоносный код.1час.
Видывредоносныхкодов.Возможностиидеструктивныефункциивредоносныхкодов.

Тема2.Распространениевредоносногокода.1час.
Способыдоставкивредоносныхкодов.Исполняемыефайлыирасширениявредоносныхкодов.Вредоноснаярассылка.Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.

Тема3.Методызащитыотвредоносныхпрограмм.2час.
Способызащиты устройствотвредоносного кода. Антивирусныепрограммыииххарактеристики. Правилазащитыотвредоносных кодов.

Тема 4.Распространение вредоносного кода для мобильныхустройств.1 час.
Расширениевредоносныхкодовдлямобильныхустройств. Правилабезопасностиприустановкеприложенийнамобильныеустройства. Раздел 3

«Безопасность информации»

Тема1.Социальнаяинженерия:распознатьиизбежать.1час.
Приемысоциальнойинженерии.Правилабезопасностипривиртуальныхконтактах.

Тема2.ЛожнаяинформациявИнтернете.1час.
Цифровоепространствокакплощадкасамопрезентации,экспериментированияиосвоенияразличныхсоциальныхролей.Фейковые новости. Поддельные страницы.

Тема3.Безопасностьприиспользованииплатежныхкартв Интернете.1 час.
Транзакцииисвязанныеснимириски.Правиласовершенияонлайнпокупок.Безопасностьбанковскихсервисов. Тема 3.

Беспроводная технология связи. 1 час.

УязвимостьWi-Fi-соединений.Публичныеинепубличныесети.Правилаработывпубличныхсетях.

Тема4.Резервноекопирование данных.2час.
Безопасностьличнойинформации.Созданиерезервныхкопийнаразличныхустройствах.

Тема6.Основыгосударственнойполитикивобластиформированиякультурыинформационнойбезопасности.3часа.

III. Планируемыерезультатыосвоениякурсавнеурочнойдеятельности

Предметные:

- ✓ анализироватьдоменныеименакомпьютеровиадресадокументовв интернете;
- ✓ безопасноиспользоватьсредствакоммуникации,
- ✓ безопасновестииприменятьспособысамозащитыприпопыткемошенничества,
- ✓ безопасноиспользоватьресурсыинтернета.

Выпускниковладеет:

- ✓ приемамибезопаснойорганизациисвоего личногопространстваданныхсиспользованиеминдивидуальныхнакопителей данных, интернетсервисов и т.п.

Выпускникполучитвозможностьовладеть:

- ✓ основамисоблюдениянорминформационнойэтикииправа;
- ✓ основамисамоконтроля,самооценки,принятиярешенийиосуществленияосознанноговыборавучебнойи познавательной
- ✓ деятельностиприформированиисовременнойкультурыбезопасностижизнедеятельности;
- ✓ использоватьдлярешениякоммуникативныхзадачвобластибезопасностижизнедеятельностиразличныеисточники информации, включая Интернет- ресурсы и другие базы данных.

Метапредметные.

Регулятивныеуниверсальныеучебныедействия

Врезультатеосвоенияучебногокурса обучающийся сможет:

- ✓ идентифицироватьсобственныепроблемыиопределятьглавнуюпроблему;
- ✓ выдвигатьверсиирешенияпроблемы,формулироватьгипотезы,предвосхищать конечный
- ✓ выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достиженияцели;составлятьпланрешенияпроблемы(выполненияпроекта,проведения исследования);
- ✓ описыватьсвойопыт,оформляяегодляпередачи другим людямввидетехнологиирешенияпрактическихзадач определенного класса;
- ✓ оцениватьсвоюдеятельность,аргументируяпричиныдостиженияилиотсутствияпланируемогорезультата;
- ✓ приниматьрешениевучебнойситуацииинестизанегоответственность.

Познавательныеуниверсальныеучебныедействия.

Врезультатеосвоенияучебногокурсаобучающийсясможет:

- ✓ выделятьявлениеизобщегорядадругихявлений;
- ✓ определятьобстоятельства,которыепредшествоваливозникновениюсвязимеждуявлениями,из этихобстоятельств выделять
- ✓ строитьрассуждениеотобщихзакономерностей кчастным явлениямиотчастныхявленийк общим закономерностям; излагать полученную информацию, интерпретируя ее в контексте

решаемойзадачи;

- ✓ самостоятельноуказыватьнаинформацию,нуждающуюсявпроверке,предлагатьиприменятьспособпроверки достоверности информации;
- ✓ критическиоцениватьсодержаниеиформутекста;
- ✓ определятьнеобходимыеключевыепоисковыесловаизапросы.

Коммуникативныеуниверсальныеучебныедействия.

Врезультатеосвоенияучебногокурсаобучающийсясможет:

- ✓ строитьпозитивныеотношениявпроцессеучебнойипознавательнойдеятельности;
- ✓ договариватьсяо правилахи вопросахдляобсуждения всоответствии сопоставленнойпередгруппойзадачей;
- ✓ целенаправленно искатьииспользоватьинформационныересурсы,необходимыедлярешения учебныхи практических задач с помощью средств ИКТ;
- ✓ использовать компьютерные технологии (включая выбор адекватных задаче инструментальных программно-аппаратных средств и сервисов) для решения информационных и коммуникационных учебных задач, в том числе: вычисление, написание писем, сочинений, докладов, рефератов, создание презентаций и др.;
- ✓ использоватьинформациюсучетом этическихи правовыхнорм;
- ✓ создаватьинформационныересурсыразноготипаидляразныхаудиторий,соблюдатьинформационнуюгигиенуи правила информационной безопастности.

Личностные.

- ✓ осознанное, уважительное идоброжелательноеотношениекокружающим людям вреальномивиртуальном мире, ихпозициям, взглядам,готовность вестидиалог сдругими людьми, обоснованноосуществлять выбор виртуальных собеседников;
- ✓ готовностьиспособностькосознанномувыборуи построениюдальнейшейиндивидуальнойтраекторииобразования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- ✓ освоенностьсоциальныхнорм,правилповедения,ролейиформсоциальнойжизнивгруппахи сообществах;
- ✓ сформированностьпониманияценностибезопасногообразажизни;интериоризацияправилиндивидуальногои коллективного безопасного поведения в информационно-телекоммуникационной среде

Тематическоепланирование

№п/п	Тема	Количествочасов	Основноесодержание	Характеристикаосновныхвидовучебной деятельности обучающихся
Тема1.«Безопасностьобщения»				
1	Общение в социальныхсетяхи мессенджерах	1	Социальнаясеть.Историясоциальныхсетей. Мессенджеры.Назначениесоциальныхсетей и мессенджеров. Пользовательскийконтент.	Выполняет базовые операции при использованиимессенджеровисоциальных сетей. Создает свой образ в сети Интернет. Изучает историюи социальнуюзначимостьличныхаккаунтовв сети Интернет.
2	Скембезопасно общаться в интернете	1	Персональныеданныекакосновнойкапитал личного пространства в цифровом мире. Правиладобавлениядрузейвсоциальных сетях.Профильпользователя.Анонимные социальные сети.	Руководствуется в общении социальными ценностями и установками коллектива и обществавцелом.Изучаетправиласетевогообще ния.
3	Пароли для аккаунтов социальныхсетей	1	Сложныепароли.Онлайнгенераторыпаролей. Правила хранения паролей. Использование функции браузерапозапоминаниюпаролей.	Изучаетосновныепонятиярегистрационной информации и шифрования. Умеетихприменить.
4	Безопасныйвходв Аккаунты	1	Видыаутентификации. Настройки безопасностиаккаунта.Работаначужом компьютересточкизрениябезопасности личного аккаунта.	Объясняетпричиныиспользованиябезопасного входапри работе на чужом устройстве. Демонстрируетустойчивыйнавыкбезопасного входа.
5	Настройки Конфиденциальност и в социальных сетях	1	Настройки приватности и конфиденциальности в разных социальных сетях.Приватностьиконфиденциальностьв мессенджерах.	Раскрываетпричиныустановкизакрытого профиля. Меняет основные настройки приватности в личном профиле.

6	Публикация информации в социальныхсетях	1	Персональныеданные. Публикацияличнойинформации.	Осуществляетпоискииспользуетинформацию, необходимую для выполнения поставленных задач.
7	Кибербуллинг	1	Определение кибербуллинга. Возможные причинькибербуллингаикакегоизбежать? Какнестатьжертвойкибербуллинга. Какпомочьжертвекибербуллинга.	Реагируетнаопасныеситуации,распознает провокации и попытки манипуляции со стороны виртуальных собеседников.
8	Публичные аккаунты	1	Настройки приватностипубличныхстраниц. Правилаведенияпубличныхстраниц. Овершеринг.	Решает экспериментальные задачи. Самостоятельно создает источники информацииразноготипаидляразных аудиторий,соблюдаяправилаинформационной безопасности.
9	Фишинг	2	Фишинг какмошеннический прием. Популярныеварианты распространения фишинга. Отличиенастоящихфишинговыхсайтов. Как защититься от фишеровв социальных сетях и мессенджерах.	Анализ проблемных ситуаций. Разработка кейсов с примерами из личной жизни/жизни знакомых. Разработка и распространениечек-листа(памятки)попротиводействиюфишингу.
Тема2.«Безопасностьустройств»				
1	Чтотакоевредонос ныйкод	1	Виды вредоносных кодов. Возможности и деструктивные функции вредоносныхкодов.	Соблюдает техникубезопасностипри эксплуатации компьютерных систем. Используетинструментальныепрограммные средства и сервисы адекватно задаче.

2	Распространение вредоносногокода	1	Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносныхкодов.Вредоноснаярассылка. Вредоносные скрипты. Способы выявления наличиявредоносныхкодовнаустройствах. Действияприобнаружениивредоносныхкодовна устройствах.	Выявляет и анализирует (при помощи чек-листа) возможные угрозы информационной безопасности объектов.
3	Методызащитыот вредоносных программ	2	Способызащитыустройствот вредоносногокода.Антивирусныепрограммы и их характеристики. Правила защиты от вредоносных кодов	Изучает виды антивирусных Программиправилаихустановки.
4	Распространение вредоносногокода для мобильных устройств	1	Расширение вредоносных кодов для мобильныхустройств.Правилабезопасности при установке приложений на мобильные устройства.	Разрабатываетпрезентацию,инструкциюпо обнаружению, алгоритм установки приложений на мобильные устройствадля учащихся более младшего возраста.
5.	Выполнение и защита индивидуальных и групповыхпроектов	3		Умеет работать индивидуально и в группе. Принимает позицию собеседника, понимая позициюдругого,различаетвего речи:мнение (точку зрения), доказательство(аргументы), факты; гипотезы, аксиомы, теории.
Тема 3 «Безопасностьинформации»				
1	Социальная инженерия: распознатьи избежать	2	Приемысоциальнойинженерии.Правила безопасностипри виртуальных контактах.	Находитнужнуюинформациювбазахданных, составляя запросы на поиск. Систематизируетполучаемуюинформацию в процессепоиска.

2	Ложнаяинформация вИнтернете	2	Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковыеновости.Поддельныестраницы.	Определяет возможные источники необходимыхсведений, осуществляет поиск информации. Отбираетисравниваетматериал по нескольким источникам.
3	Безопасностьпри использовании платежныхкартв Интернете	1	Транзакцииисвязанныеснимириски. Правила совершенияонлайн покупок. Безопасность банковских сервисов.	Приводитпримерырисков,связанныхс совершением онлайн покупок (умеет определить источник риска). Разрабатываетвозможные варианты решения ситуаций,связанныхсрискамииспользования платежных карт в Интернете.
4	Беспроводнаятехнологиясвязи	1	Уязвимость Wi-Fi-соединений.Публичныеи непубличные сети. Правила работы в публичных сетях.	Используяразличнуюинформацию,определяет понятия. Изучает особенности и стиль ведения личных и публичных аккаунтов.
5	Резервноекопированиеданных	2	Безопасность личной информации.Созданиерезервныхкопийна различных устройствах.	Создаетрезервныекопии.
6	Основы государственной политикивобласти формирования культуры информационной Безопасности	2	Доктрина национальной информационной безопасности. Обеспечение свободы и равенствадоступакинформациииизнаниям. Основныенаправлениягосударственнойполитики в области	Умеетпривестивыдержкииззаконодательства РФ: - обеспечивающего конституционное правонапоиск,получениеираспространение информации;

			Формированиякультурыинформационнойбезопасности.	- отражающегоправовыеаспектызащитыкиберпространства.
7	Выполнениеи защита индивидуальныхи групповыхпроектов	3	Темы проектов Безопасность общения Безопасностьустройств Безопасностьобщения	Уметьвыполнятьпроекты Защитапроектов
8	Годоваяпромежуточнаяаттестация	1	Тест Безопасностьработывинтернете	Выполнениетеста
9	Разбортипичных ошибок аттестационной работы	1	Анализтеста	Разборошибок
10	Итоговоезанятие	1	Повторение	Повторение
	Итого	34		