Автономная некоммерческая организация общеобразовательная организация «АКАДЕМИЯ»

Рассмотрено
на заседании МО
Протокол №
от 29.08. 2022 г.
Руководитель МО
_____

Согласовано
Педагогическим Советом
АНО ОО «Академия»
Протокол № 1
от «29» 08 2022 г.

Утверждено
Директор
АНО ОО «Академия»
_____ И.В. Зимарева
Приказ № 1
от «29» 08 2022 г.

Рабочая программа
курса внеурочной деятельности
для обучающихся 7 класса
«Информационная безопасность»

1. Характеристика личностных, метапредметных и предметных результатов освоения учебного курса

Личностные.

- осознанное, уважительное и доброжелательное отношение к окружающим людям в реальном и виртуальном мире, их позициям, взглядам, готовность вести диалог с другими людьми, обоснованно осуществлять выбор виртуальных собеседников;
- готовность и способность к осознанному выбору и построению дальнейшей индивидуальной траектории образования на базе ориентировки в мире профессий и профессиональных предпочтений, с учетом устойчивых познавательных интересов;
- освоенность социальных норм, правил поведения, ролей и форм социальной жизни в группах и сообществах;
- сформированность понимания ценности безопасного образа жизни; интериоризация правил индивидуального и коллективного безопасного поведения в информационно-телекоммуникационной среде.

Метапредметные.

Регулятивные универсальные учебные действия.

В результате освоения учебного курса обучающийся сможет:

- идентифицировать собственные проблемы и определять главную проблему;
- выдвигать версии решения проблемы, формулировать гипотезы, предвосхищать конечный результат;
- ставить цель деятельности на основе определенной проблемы и существующих возможностей;
- выбирать из предложенных вариантов и самостоятельно искать средства/ресурсы для решения задачи/достижения цели;
- составлять план решения проблемы (выполнения проекта, проведения исследования);
- описывать свой опыт, оформляя его для передачи другим людям в виде технологии решения практических задач определенного класса;
- оценивать свою деятельность, аргументируя причины достижения или отсутствия планируемого результата;
- находить достаточные средства для выполнения учебных действий в изменяющейся ситуации и/или при отсутствии планируемого результата;
- работая по своему плану, вносить коррективы в текущую деятельность на основе анализа изменений ситуации для получения запланированных характеристик продукта/результата;
- принимать решение в учебной ситуации и нести за него ответственность.

Познавательные универсальные учебные действия.

- В результате освоения учебного курса обучающийся сможет:
- выделять явление из общего ряда других явлений;
- определять обстоятельства, которые предшествовали возникновению связи между явлениями, из этих обстоятельств выделять определяющие,

способные быть причиной данного явления, выявлять причины и следствия явлений;

- строить рассуждение от общих закономерностей к частным явлениям и от частных явлений к общим закономерностям;
- излагать полученную информацию, интерпретируя ее в контексте решаемой задачи;
- самостоятельно указывать на информацию, нуждающуюся в проверке, предлагать и применять способ проверки достоверности информации;
- критически оценивать содержание и форму текста;
- определять необходимые ключевые поисковые слова и запросы.

Коммуникативные универсальные учебные действия.

- В результате освоения учебного курса обучающийся сможет:
- строить позитивные отношения в процессе учебной и познавательной деятельности;
- критически относиться к собственному мнению, с достоинством признавать ошибочность своего мнения (если оно таково) и корректировать его;
- договариваться о правилах и вопросах для обсуждения в соответствии с поставленной перед группой задачей;
- делать оценочный вывод о достижении цели коммуникации непосредственно после завершения коммуникативного контакта и обосновывать его.
- целенаправленно искать и использовать информационные ресурсы, необходимые для решения учебных и практических задач с помощью средств ИКТ;
- выбирать, строить и использовать адекватную информационную модель для передачи своих мыслей средствами естественных и формальных языков в соответствии с условиями коммуникации;
- 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.;
- использовать информацию с учетом этических и правовых норм;
- создавать информационные ресурсы разного типа и для разных аудиторий, соблюдать информационную гигиену и правила информационной безопасности.

Предметные:

Выпускник научится:

- анализировать доменные имена компьютеров и адреса документов в интернете;
- безопасно использовать средства коммуникации,

- безопасно вести и применять способы самозащиты при попытке мошенничества,
- безопасно использовать ресурсы интернета.

Выпускник овладеет:

- приемами безопасной организации своего личного пространства данных с использованием индивидуальных накопителей данных, интернет-сервисов и т.п.

Выпускник получит возможность овладеть:

- основами соблюдения норм информационной этики и права;
- основами самоконтроля, самооценки, принятия решений и осуществления осознанного выбора в учебной и познавательной деятельности при формировании современной культуры безопасности жизнедеятельности;
- использовать для решения коммуникативных задач в области безопасности жизнедеятельности различные источники информации, включая Интернет-ресурсы и другие базы данных.

Воспитательные результаты

Первый уровень результатов – приобретение школьником социальных знаний (об общественных нормах, устройстве общества, о социально одобряемых и неодобряемых формах поведения в обществе и т. п.), первичного понимания социальной реальности и повседневной жизни.

Второй уровень результатов – получение школьником опыта переживания и позитивного отношения к базовым ценностям общества (человек, семья, Отечество, природа, мир, знания, труд, культура), ценностного отношения к социальной реальности в целом.

Третий уровень результатов – получение школьником опыта самостоятельного общественного действия. Только в самостоятельном общественном действии, за пределами дружественной среды школы, юный человек действительно становится (а не просто узнаёт о том, как стать) социальным деятелем, гражданином, свободным человеком.

2. Содержание курса внеурочной деятельности

7 и 9 классах

Раздел 1. «Безопасность общения»

Тема 1. Общение в социальных сетях и мессенджерах. 1 час.

Социальная сеть. История социальных сетей. Мессенджеры. Назначение социальных сетей и мессенджеров. Пользовательский контент.

Формы организации занятий: презентация

Виды деятельности: познавательный

Тема 2. С кем безопасно общаться в интернете. 1 час.

Персональные данные как основной капитал личного пространства в цифровом мире. Правила добавления друзей в социальных сетях. Профиль пользователя. Анонимные социальные сети.

Формы организации занятий: просмотр видео

Виды деятельности: коммуникативная

Тема 3. Пароли для аккаунтов социальных сетей. 1 час.
Сложные пароли. Онлайн генераторы паролей. Правила хранения паролей. Использование функции браузера по запоминанию паролей.
Формы организации занятий: практикум
Виды деятельности: совместная

Тема 4. Безопасный вход в аккаунты. 1 час.
Виды аутентификации. Настройки безопасности аккаунта. Работа на чужом компьютере с точки зрения безопасности личного аккаунта.
Формы организации занятий: практическая работа
Виды деятельности: групповая

Тема 5. Настройки конфиденциальности в социальных сетях. 1 час.
Настройки приватности и конфиденциальности в разных социальных сетях. Приватность и конфиденциальность в мессенджерах.
Формы организации занятий: семинар
Виды деятельности: групповая

Тема 6. Публикация информации в социальных сетях. 1 час.
Персональные данные. Публикация личной информации.
Формы организации занятий: практикум
Виды деятельности: совместная

Тема 7. Кибербуллинг. 1 час.
Определение кибербуллинга. Возможные причины кибербуллинга и как его избежать? Как не стать жертвой кибербуллинга. Как помочь жертве кибербуллинга.
Формы организации занятий: лекция
Виды деятельности: предметная

Тема 8. Публичные аккаунты. 1 час.
Настройки приватности публичных страниц. Правила ведения публичных страниц. Овершеринг.
Формы организации занятий: презентация
Виды деятельности: предметная

Тема 9-10. Фишинг. 2 часа.
Фишинг как мошеннический прием. Популярные варианты распространения фишинга. Отличие настоящих и фишинговых сайтов. Как защититься от фишеров в социальных сетях и мессенджерах.
Формы организации занятий: практикум
Виды деятельности: групповая

Тема 11-13. Выполнение и защита индивидуальных и групповых проектов. 3 часа.
Формы организации занятий: проектирование
Виды деятельности: групповая

Раздел 2. «Безопасность устройств»
Тема 14. Что такое вредоносный код. 1 час.
Виды вредоносных кодов. Возможности и деструктивные функции вредоносных кодов.
Формы организации занятий: беседа
Виды деятельности: коммуникативная

Тема 15. Распространение вредоносного кода. 1 час.
Способы доставки вредоносных кодов. Исполняемые файлы и расширения вредоносных кодов. Вредоносная рассылка. Вредоносные скрипты. Способы выявления наличия вредоносных кодов на устройствах. Действия при обнаружении вредоносных кодов на устройствах.
Формы организации занятий: презентация
Виды деятельности: предметная

Тема 16-17. Методы защиты от вредоносных программ. 2 час.
Способы защиты устройств от вредоносного кода. Антивирусные программы и их характеристики. Правила защиты от вредоносных кодов.
Формы организации занятий: практикум
Виды деятельности: познавательная

Тема 18. Распространение вредоносного кода для мобильных устройств. 1 час.
Расширение вредоносных кодов для мобильных устройств. Правила безопасности при установке приложений на мобильные устройства.
Формы организации занятий: семинар
Виды деятельности: групповая

Тема 19-21. Выполнение и защита индивидуальных и групповых проектов. 3 часа.
Формы организации занятий: проектирование
Виды деятельности: совместная

Раздел 3 «Безопасность информации»
Тема 22. Социальная инженерия: распознать и избежать. 1 час.
Приемы социальной инженерии. Правила безопасности при виртуальных контактах.
Формы организации занятий: лекция
Виды деятельности: предметная

Тема 23. Ложная информация в Интернете. 1 час.
Цифровое пространство как площадка самопрезентации, экспериментирования и освоения различных социальных ролей. Фейковые новости. Поддельные страницы.
Формы организации занятий: беседа
Виды деятельности: коммуникативная

Тема 24. Безопасность при использовании платежных карт в Интернете. 1 час.
Транзакции и связанные с ними риски. Правила совершения онлайн покупок. Безопасность банковских сервисов.
Формы организации занятий: семинар
Виды деятельности: групповая

Тема 25. Беспроводная технология связи. 1 час.
Уязвимость Wi-Fi-соединений. Публичные и непубличные сети. Правила работы в публичных сетях.
Формы организации занятий: практикум
Виды деятельности: познавательная

Тема 26. Резервное копирование данных. 1 час.
Безопасность личной информации. Создание резервных копий на различных устройствах.
Формы организации занятий: практическая работа
Виды деятельности: групповая

Тема 27-28. Основы государственной политики в области формирования культуры информационной безопасности. 2 час.
Доктрина национальной информационной безопасности. Обеспечение свободы и равенства доступа к информации и знаниям. Основные направления государственной политики в области формирования культуры информационной безопасности.
Формы организации занятий: лекция
Виды деятельности: предметная

Тема 29-31. Выполнение и защита индивидуальных и групповых проектов. 3 часа.
Формы организации занятий: проектирование
Виды деятельности: коммуникативная

Тема 32-34. Повторение. 3 часа.

Формы организации занятий: практикум
Виды деятельности: груааовая

3. Тематическое планирование
7 класс

№ п/п	Тема	Общее количество часов	Теорет. занятия	Практ. занятия	Примерные сроки проведения
Тема 1. «Безопасность общения»					
1	Общение в социальных сетях и мессенджерах	1	0.5	0.5	5.09
2	С кем безопасно общаться в интернете	1	0.5	0.5	12.09
3	Пароли для аккаунтов социальных сетей	1	0.5	0.5	19.09
4	Безопасный вход в аккаунты	1	0.5	0.5	26.09
5	Настройки конфиденциальности в социальных сетях	1	0.5	0.5	3.10
6	Публикация информации в социальных сетях	1	0.5	0.5	10.10
7	Кибербуллинг	1	0.5	0.5	24.10
8	Публичные аккаунты	1	0.5	0.5	31.10
9-10	Фишинг	2	0.5	1.5	7.11 14.11
11-13	Выполнение и защита индивидуальных и групповых проектов	3	0	3	21.11 28.11 5.12
Тема 2. «Безопасность устройств»					
14	Что такое вредоносный код	1	0.5	0.5	12.12
15	Распространение вредоносного кода Распространение вредоносного кода	1	0.5	0.5	19.12
16-17	Методы защиты от вредоносных программ	2	0.5	1.5	26.12 9.01
18	Распространение вредоносного кода для мобильных устройств	1	0.5	0.5	16.01
19-21	Выполнение и защита индивидуальных и групповых проектов	3	0	3	23.01 30.01 6.02
Тема 3 «Безопасность информации»					
22	Социальная инженерия: распознать и избежать	1	0.5	0.5	13.02
23	Ложная информация в Интернете	1	0.5	0.5	20.02
24	Безопасность при использовании платежных карт в Интернете	1	0.5	0.5	5.03
25	Беспроводная технология	1	0.5	0.5	12.03

	связи				
26	Резервное копирование данных	1	0.5	0.5	19.03
27-28	Основы государственной политики в области формирования культуры информационной безопасности	2	0.5	1.5	26.03 9.04
29-31	Выполнение и защита индивидуальных и групповых проектов	3	0	3	16.04 23.04 30.04
32-34	Повторение	3	0	3	14.05 21.05 28.05
	Итого:	**34**	**9.5**	**24.5**	

9А класс

№ п/п	Тема	Общее количество часов	Теорет. занятия	Практ. занятия	Примерные сроки проведения
Тема 1. «Безопасность общения»					
1	Общение в социальных сетях и мессенджерах	1	0.5	0.5	3.09
2	С кем безопасно общаться в интернете	1	0.5	0.5	10.09
3	Пароли для аккаунтов социальных сетей	1	0.5	0.5	17.09
4	Безопасный вход в аккаунты	1	0.5	0.5	24.09
5	Настройки конфиденциальности в социальных сетях	1	0.5	0.5	1.10
6	Публикация информации в социальных сетях	1	0.5	0.5	8.10
7	Кибербуллинг	1	0.5	0.5	15.10
8	Публичные аккаунты	1	0.5	0.5	22.10
9-10	Фишинг	2	0.5	1.5	29.10 12.11
11-13	Выполнение и защита индивидуальных и групповых проектов	3	0	3	19.11 26.11 3.12
Тема 2. «Безопасность устройств»					
14	Что такое вредоносный код	1	0.5	0.5	10.12
15	Распространение вредоносного кода Распространение вредоносного кода	1	0.5	0.5	17.12
16-17	Методы защиты от вредоносных программ	2	0.5	1.5	24.12 31.12

18	Распространение вредоносного кода для мобильных устройств	1	0.5	0.5	14.01
19-21	Выполнение и защита индивидуальных и групповых проектов	3	0	3	21.01 28.01 4.02
Тема 3 «Безопасность информации»					
22	Социальная инженерия: распознать и избежать	1	0.5	0.5	11.02
23	Ложная информация в Интернете	1	0.5	0.5	18.02
24	Безопасность при использовании платежных карт в Интернете	1	0.5	0.5	3.03
25	Беспроводная технология связи	1	0.5	0.5	10.03
26	Резервное копирование данных	1	0.5	0.5	17.03
27-28	Основы государственной политики в области формирования культуры информационной безопасности	2	0.5	1.5	24.03 31.03
29-31	Выполнение и защита индивидуальных и групповых проектов	3	0	3	14.04 21.04 28.04
32-34	Повторение	3	0	3	12.05 19.05 26.05
	Итого:	**34**	**9.5**	**24.5**	

9Б класс

№ п/п	Тема	Общее количество часов	Теорет. занятия	Практ. занятия	Примерные сроки проведения
Тема 1. «Безопасность общения»					
1	Общение в социальных сетях и мессенджерах	1	0.5	0.5	7.09
2	С кем безопасно общаться в интернете	1	0.5	0.5	14.09
3	Пароли для аккаунтов социальных сетей	1	0.5	0.5	21.09
4	Безопасный вход в аккаунты	1	0.5	0.5	28.09
5	Настройки конфиденциальности в социальных сетях	1	0.5	0.5	5.10
6	Публикация информации в социальных сетях	1	0.5	0.5	12.10
7	Кибербуллинг	1	0.5	0.5	19.12

8	Публичные аккаунты	1	0.5	0.5	26.10
9-10	Фишинг	2	0.5	1.5	2.11 16.11
11-13	Выполнение и защита индивидуальных и групповых проектов	3	0	3	23.11 30.11 7.12
Тема 2. «Безопасность устройств»					
14	Что такое вредоносный код	1	0.5	0.5	14.12
15	Распространение вредоносного кода Распространение вредоносного кода	1	0.5	0.5	21.12
16-17	Методы защиты от вредоносных программ	2	0.5	1.5	28.12 11.01
18	Распространение вредоносного кода для мобильных устройств	1	0.5	0.5	18.01
19-21	Выполнение и защита индивидуальных и групповых проектов	3	0	3	25.01 1.02
Тема 3 «Безопасность информации»					
22	Социальная инженерия: распознать и избежать	1	0.5	0.5	8.02
23	Ложная информация в Интернете	1	0.5	0.5	15.02
24	Безопасность при использовании платежных карт в Интернете	1	0.5	0.5	22.02
25	Беспроводная технология связи	1	0.5	0.5	7.03
26	Резервное копирование данных	1	0.5	0.5	14.03
27-28	Основы государственной политики в области формирования культуры информационной безопасности	2	0.5	1.5	21.03 28.03
29-31	Выполнение и защита индивидуальных и групповых проектов	3	0	3	11.04 18.04 25.04
32-34	Повторение	3	0	3	12.05 16.05 23.05
	Итого:	**34**	**9.5**	**24.5**	