Комитет по образованию Мингорисполкома
Учреждение образования «Минский государственный дворец детей и молодежи»
Отдел технического творчества и спорта

СОГЛАСОВАНО _____

УТВЕРЖДАЮ
Приказ директора
от « » 2021г.
№ _____

_____ Н.М.Великая

ПРОГРАММА ОБЪЕДИНЕНИЯ ПО ИНТЕРЕСАМ
«КИБЕРБЕЗОПАСНОСТЬ И ЦИФРОВАЯ ГРАМОТНОСТЬ»
(естественно-математический профиль, базовый уровень изучения образовательной области «Информатика»)

Разработчик:
Пасиков Павел Андреевич,
педагог дополнительного образования
без квалификационной категории
Методическое сопровождение:
Семёнова Екатерина Владимировна,
заведующий сектором

Возраст обучающихся: 9 – 13 лет
Срок реализации программы – 1 год

РЕКОМЕНДОВАНА
на заседании
методического совета
от « » 2021г.
протокол №

Минск 2021

Пояснительная записка

Подключенная электронная информационная сеть стала неотъемлемой частью нашей повседневной жизни. Эта сеть используется в организациях любого типа: медицинских, финансовых, образовательных — без нее в наши дни эффективная работа невозможна. В сети происходят сбор, обработка, хранение и обмен огромным количеством цифровой информации. Чем больше цифровой информации собирается и чем больше ей обмениваются, тем важнее становится защита этой информации для обеспечения национальной безопасности и экономической стабильности.

Занятия в кружке «Кибербезопасность и цифровая грамотность» позволят обучающимся попробовать свои силы и раскрыть способности в области обеспечения безопасности сетей, цифровых носителей информации и прочих электронных устройств, сформировать у обучающихся интерес к данной теме и укрепить положительное отношение к учебному процессу.

Данная программа рассчитана на год обучения, в течение которого обучающиеся изучат основные принципы кибербезопасности и познакомятся с угрозами, которые могут возникать в данной сфере деятельности.

Программа разработана в соответствии с типовой программой дополнительного образования детей и молодежи (естественно-математический профиль), утвержденной Постановлением Министерства образования Республики Беларусь от 06.09.2017 № 123.

Цель программы – обучение основам кибербезопасности на пропедевтическом уровне.

Достижению данной цели будет способствовать решение следующих **задач**:

- сформировать навыки работы на персональном компьютере и с операционной системой Windows;
- ознакомить обучающихся с основными угрозами кибербезопасности и способам их устранения;
- научить понимать и соблюдать базовые принципы защиты информации;
- овладеть навыками работы с сетями;
- развивать логическое и алгоритмическое мышление;
- развивать познавательные, интеллектуальные и творческие способности детей,
- сформировать навыки здоровьесбережения;
- воспитывать самостоятельность, трудолюбие и аккуратность.

Настоящая программа рассчитана на обучающихся в возрасте 9 – 13 лет. Программа курса рассчитана на 1 год обучения. Общее количество часов – 72. Периодичность занятий – 1 раз в неделю по 2 часа.

Материально-техническое обеспечение

- IBM-совместимые компьютеры типа Athlon 2800, 1024 RAM, HDD 500GB;
- программные продукты: OS Windows, MS Office, браузер Opera или Mozilla Firefox.

- мультимедийный проектор;
- экран;
- учебная доска;
- компьютерные учебники.

Учебно-тематический план

№	Название разделов, тем	Количество часов		
		всего	в том числе	
			теорети-ческих	практиче-ских
Вводное занятие		2	2	-
1.	**Введение в кибербезопасность**	**12**	**8**	**4**
1.1.	Потребность в кибербезопасности	4	2	2
1.2.	Атаки, понятия и техники	2	2	-
1.3.	Защита данных и конфиденциальности	4	2	2
1.4.	Защита организации	2	2	-
2.	**Основы кибербезопасности**	**25**	**14**	**11**
2.1.	Кибербезопасность. Мир мастеров, специалистов и преступников	4	2	2
2.2.	Куб кибербезопасности	6	2	4
2.3.	Киберугрозы, уязвимости и атаки	3	2	1
2.4.	Искусство защиты и секретов	3	2	1
2.5.	Искусство обеспечения целостности данных	3	2	1
2.6.	Область применения концепции «пять девяток»	3	2	1
2.7.	Возведение укреплений	3	2	1
3.	**Основы сетей**	**12**	**8**	**4**
3.1.	Модель OSI	3	2	1
3.2.	Сети LAN и WAN	3	2	1
3.3.	Надёжность сети	3	2	1
3.4.	Контроль доступа	3	2	1
4.	**Криптография**	**19**	**12**	**7**
4.1.	Стеганография	6	4	2
4.2.	Что такое хеширование	6	4	2
4.3.	Алгоритмы хеширования	7	4	3
Итоговое занятие		2	-	2
Всего:		**72**	**44**	**28**

Содержание программы

Вводное занятие

Обзор программы обучения.

Беседа о мерах противопожарной безопасности и правилах безопасного поведения на занятиях в компьютерных кабинетах и во Дворце. Экскурсия по Дворцу.

Развитие кибербезопасности.

1. Введение в кибербезопасность

1.1. Потребность в кибербезопасности

Понятия персональных и корпоративных данных. Кто такие злоумышленники и эксперты по кибербезопасности. Кибервойна.

Практические занятия

Исследование нескольких случаев нарушения систем безопасности и определение того, какие данные пропали, какие эксплойты (инструменты эксплуатации уязвимостей) были использованы и что можно сделать для собственной защиты.

1.2. Атаки, понятия и техники

Анализ кибератаки. Ландшафт кибербезопасности.

1.3. Защита данных и конфиденциальности

Как защитить свои данные. Защита персональных данных в сети.

Практические занятия

Создание и сохранение надёжных паролей. Резервное копирование данных во внешнее хранилище. Отдельные способы защиты данных. Как обезопасить себя в сети.

1.4. Защита организации

Межсетевые экраны. Подход к кибербезопасности на основе поведения.

2. Основы кибербезопасности

2.1. Кибербезопасность. Мир мастеров, специалистов и преступников

Мир кибербезопасности. Киберпреступники и специалисты по кибербезопасности. Типовые угрозы. Распространение киберугроз. Как обучают экспертов.

Практические занятия

Идентификация угроз. Задачи профессионалов в сфере кибербезопасности.

2.2. Куб кибербезопасности

Три грани куба кибербезопасности. Триада «КЦД». Состояние данных. Средства противодействия угрозам безопасности. Архитектура управления безопасностью ИТ-среды.

Практические занятия

Знакомство с программой Packet Tracer. Отслеживание перемещения

пакетов данных по сети.

2.3. Киберугрозы, уязвимости и атаки

Вредоносные ПО и вредоносный код. Классификация вредоносных программ Обман. Атаки.

Практические занятия

Поиск примеров вредоносного ПО и вредоносного кода и распределение их по категориям.

2.4. Искусство защиты секретов

Понятие криптографии. Функции управления доступом. Сокрытие данных.

Практические занятия

Знакомство со способами шифрования сообщений. Упражнения на шифрование и расшифровку данных.

2.5. Искусство обеспечения целостности данных

Виды средств контроля целостности данных. Цифровые подписи. Сертификаты. Обеспечение целостности без данных.

Практические занятия

Создание собственных цифровых подписей. Разбор примеров сертификатов.

2.6. Область применения концепции «пять девяток»

Высокая доступность. Меры по повышению доступности. Реагирование на инциденты. Аварийное восстановление.

Практические занятия

Поиск информации и реагировании на инциденты в крупных кампаниях. Как оно устроено и чем отличается от кампании к кампании.

2.7. Возведение укреплений

Защита систем и устройств. Повышение надёжности сервера. Повышение надёжности сетевой инфраструктуры. Физическая безопасность.

Практические занятия

Рассмотрение программного обеспечения для защиты своего устройства. Выбор и установка лучшего.

3. Основы сетей

3.1. Модель OSI

Основные принципы модели. Уровни модели OSI. Плюсы и минусы.

Практические занятия

Разбор примеров. Поиск “своего места” в модели OSI.

3.2 Сети LAN и WAN

Построение сети. Адресация. Понятия LAN и WAN. Различия сетей.

Практические занятия

Как строятся сети и проходит адресация на сайтах крпнейших брендов. Разбор общего и отличий. У кого лучше?

3.3. Надёжность сети

Меры и границы сетевой надёжности. Ориентированные и неориентированные сети. Метод покрытия. Преобразования и сокращения.

Практические занятия

Знакомство со способами улучшения сети. Как улучшить конкретно свою сеть.

3.4. Контроль доступа

Понятия идентификации и аутентификации. Административные политики и процедуры. Дискреционный и императивный подходы.

Практические занятия

Знакомство с различными примерами идентификации и аутентификации на сайтах и в приложениях.

4. Криптография

4.1. Стеганография

Классификация стеганографии. Классическая стеганография. Компьютерная и цифровая стеганографии. Атаки на стегосистемы. Цифровые водные знаки. Применение стеганографии.

Практические занятия

Применение стеганографии. Цифровые подписи.

4.2. Что такое хеширование

Понятие хеширования. Понятие и виды хеш-функций. Методы борьбы с коллизиями. Применение хеш-функций.

Практические занятия

Сравнение данных с помощью хеш-функции.

4.3. Алгоритмы хеширования

Различия и развитие алгоритмов хеширования. Алгоритмы SHA1, SHA2, SHA3, двойное хеширование SHA256. Алгоритмы Ethereum 2.0 и BLAKE. Будущее алгоритмов хеширования.

Практические занятия

Проблемы алгоритмов хеширования. Как обойти такие алгоритмы. Составление своего алгоритма.

Итоговое занятие

Конкурс-викторина.

Ожидаемые результаты

После завершения обучения обучающиеся будут

знать:

– устройства персонального компьютера;

– основные понятия и принципы работы в ОС Windows;

– типы киберугроз и способы им противостоять;

– возможности Cisco Packet Tracer;

– понятия стеганографии и хеширования;

– требования техники безопасности, гигиены, эргономики и ресурсосбережения при работе на ПК;

уметь:

– распознавать киберугрозы и противостоять им;

– соблюдать меры безопасности в сети интернет;

– работать в программе Cisco Packet Tracer;

– разрабатывать меры безопасности для электронных технологий

Формы подведения итогов реализации программы

Диагностика освоения программы осуществляется через наблюдение педагогом за ходом работы, анализ и оценку выполнения практических заданий, тестовых заданий совместно с обучающимися объединения по интересам, участие в профильном конкурсе. Данная программа предусматривает различные виды контроля результатов обучения:

– вводный контроль в начале каждого занятия, направленный на повторение и закрепление изученного материала;

– текущий контроль в процессе проведения занятия, направленный на закрепление технологических правил изучаемой темы.

Итоговое занятие проводится в форме конкурса-викторины.

Формы и методы реализации программы

Основными методами обучения являются:

– объяснительно-иллюстративный – педагог объясняет основные положения новой темы, иллюстрируя их средствами прикладных программ;

– проблемное изложение – перед обучающимися ставится проблема в виде задачи, которую необходимо реализовать на ЭВМ, определив метод и алгоритм ее решения;

– частично-поисковый – ребята находят способ решения поставленных задач и метод его реализации в дополнительной литературе или на страницах Интернета, затем доказывают оптимальность своего выбора.

Для активизации, мотивации к творчеству, организации взаимодействия применяются методы создания ситуации успеха, взаимопроверка, самостоятельная работа, предоставление свободного выбора задания.

Целевое назначение программы предусматривает организацию личностно ориентированного педагогического процесса, который способствует созданию в кружке среды воспитывающего и творческого характера, комфортной для каждого обучающегося. Образовательный процесс строится на основе субъект-субъектных отношений между педагогом и воспитанником.

Работа на ПК обязательно предполагает использование современных здоровьесберегающих технологий, осуществляется смена видов деятельности, систематически проводится профилактическая гимнастика для глаз и комплексы упражнений для снятия усталости.

Для повышения уровня подготовки обучающихся и поддержания их интереса к освоению материала наряду с традиционными формами обучения используются методические и учебные материалы нового типа – компьютерные учебники, задачники, мультимедийные уроки.

Одним из основных направлений повышения эффективности образовательного процесса является проверка и оценка результатов освоения программы обучающимися. При этом ведущая роль принадлежит текущему контролю, который позволяет педагогу следить за уровнем знаний обучающихся, оперативно вносить необходимые коррективы. На теоретических занятиях контроль проводится в устной форме в виде устного фронтального или индивидуального опроса (ответы на контрольные вопросы), беседы.

Также применяется такой метод контроля как поиск информации по сети, обмен информацией с товарищем с применением ПК, практические задания.

Итоговое занятие проводится в форме конкурса.

Литература и информационные ресурсы

1. Бабаш А.В., Баранова Е.К., Ларин Д. А. Информационная безопасность. История защиты информации в России / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин. – Москва: КДУ, 2015. – 736 с.

2. Нестеров С. А. Основы информационной безопасности. Учебное пособие / С. А. Нестеров. – Санкт-Петербург: – Лань, 2016. – 324 с.

3. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.

https://krv.移动/books/kiberbezopasnost-strategiya-atack-i-oborony.pdf

4. Rawat K. Today’s Inventory Management Systems: A Tool in Achieving Best Practices in Indian Business // Anusandhanika. 2015. № 7 (1). C. 128–135. https://search.proquest.com/docview/1914575232?accountid=45049 .

5. Doucek P. The Impact of Information Management // FAIMA Business & Management Journal. 2015. № 3 (3). С. 5–11. https://search.proquest.com/docview/1761642437?accountid=45049.

6. Mascone C. F. Keeping Industrial Control Systems Secure // Chem. Eng. Prog. 2017. № 113 (6). С. 3. https://search.proquest.com/docview/1914869249?account id=45049 .

7. Lindsay T. LANDesk Management Suite / Security Suite 9.5 L... | Ivanti User Community // Community.ivanti.com. 2012. https://community.ivanti.com/docs/DOC26984.

8. I. Latis Networks. “atis Networks // Bloomberg.com. 2017. https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=934296 .

9. The CERT Division // Cert.org. 2017. http://www.cert.org.

10. SecurityFocus // Securityfocus.com. 2017. http://www.securityfocus.com.

11. IT Security Threats // Securityresponse.symantec.com. 2017. http://securityresponse.symantec.com.

12. Manes G. W. et al. NetGlean: A Methodology for Distributed Network Security. Scanning // Journal of Network and Systems Management. 2005. № 13 (3). С. 329–344. https://search.proquest.com/docview/201295573?accountid=45049. DOI: http://dx.doi.org/10.1007/s10922-005-6263-2 .

13. Foundstone Services // Mcafee.com. 2017. https://www.mcafee.com/us/services/foundstone-services/index.aspx.