ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ И НАУКИ ГОРОДА МОСКВЫ
Государственное бюджетное образовательное учреждение
города Москвы дополнительного профессионального образования
(повышения квалификации) специалистов
Городской методический центр
Департамента образования и науки города Москвы

УТВЕРЖДАЮ
Директор ГБОУ ГМЦ ДОНМ

_____ А.С. Зинин

«30» октября 2020 г.

Дополнительная профессиональная программа
(повышение квалификации)

Обеспечение комплексной защиты информационного пространства подростка в современных условиях с применением инструментов Лаборатории Касперского

Авторы и составители курса:
Четверов А.В.,
эксперт Лаборатории Касперского
по детской онлайн безопасности,
учитель информатики ГБОУ Школа № 1409

Сиденко А.Г.,
ведущий аналитик
Лаборатории Касперского

ГБОУ ГМЦ ДОНМ

Москва – 2020

Раздел 1. *«Характеристика программы»*

1.1. Цель реализации программы

Совершенствование профессиональных компетенций обучающихся в области обеспечения комплексной защиты информационного пространства подростка с применением инструментов Лаборатории Касперского

Совершенствуемые компетенции

№	Компетенция	Направление подготовки 44.03.01 Педагогическое образование
		Код компетенции
1.	Способен осуществлять педагогическую деятельность на основе специальных научных знаний	ОПК – 8

1.2. Планируемые результаты обучения

№	Уметь – знать	Направление подготовки 44.03.01 Педагогическое образование
		Код компетенции
1.	**Уметь:** Различать атаки, угрозы, исходящие из сети интернет, социальных сетей, с применением инструментов Лаборатории Касперского (решение кейсов). **Знать:** 1. Типы атак, угроз в сети интернет, социальных сетей их классификации и признаки. 2. Методы социальной инженерии как механизм создания основы для информационной угрозы. 3. Особенности тренинговых систем. 4. Стратегию различения атак и угроз, исходящих из сети интернет, социальных сетей, с применением инструментов Лаборатории Касперского.	ОПК – 8
	Уметь: Разрабатывать стратегию обеспечения информационной безопасности с применением инструментов Лаборатории Касперского (решение кейсов). **Знать:** 1. Классификацию каналов утечки информации. 2. Особенности защиты персональных данных. 3. Способы блокировки трекинговых систем. 4. Способы защиты информации: стенография, шифрование.	

	5. Математические основы криптологии и алгоритмов шифрования данных. 6. Способы поиска информации в открытых источниках с соблюдением мер безопасности, в том числе с использованием инструментов Лаборатории Касперского. 7. Алгоритм разработки стратегии обеспечения информационной безопасности.	
3.	**Уметь:** Разрабатывать систему заданий для учащихся, направленных на обеспечение информационной безопасности (CTF (Capture the Flag), алгоритмы шифрования данных и т.д.) **Знать:** Стратегию разработки системы заданий для учащихся, направленных на обеспечение информационной безопасности (CTF (Capture the Flag), алгоритмы шифрования данных и т.д.)	

1.3. Категория обучающихся: уровень образования – ВО, область профессиональной деятельности – обучение информатике в общеобразовательной организации.

1.4. Программа реализуется с применением дистанционных образовательных технологий.

1.5. Режим занятий: доступ к образовательной платформе организации круглосуточно при соблюдении установленных сроков обучения.

1.6. Трудоемкость программы: 18 час.

Раздел 2. *«Содержание программы»*

2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Внеаудиторные занятия			Формы контроля
		Трудоемкость	Лекции	Практические занятия	
1.	Современный интернет и современные угрозы	**4**	2	2	**Решение кейсов№1**
2.	Информационная безопасность: методы обеспечения	**8**	4	4	**Решение кейсов№2**
3.	Обеспечение информационной безопасности учащихся	**6**	2	4	**Проект**
	Итоговая аттестация				Зачет на основании совокупности выполненных работ
	Итого:	**18**	**8**	**10**	

2.2. Учебная программа

№ п/п	Виды учебных занятий, учебных работ	Содержание
Тема 1. Современный интернет и современные угрозы	*Интерактивная лекция-вебинар, 2 часа*	Особенности и возможности современного интернета. Современные типы атак, угроз в сети интернет и социальных сетях, их классификация и признаки. Основы компьютерной вирусологии. Классификация вирусов. Понятие «фишинговый сайт» и его признаки. Опасности фишинговых сайтов и алгоритмы их распознавания. Методы социальной инженерии как механизм создания основы для информационной угрозы. Особенности тренинговых систем. Стратегия различения атак и угроз, исходящих из сети интернет, социальных сетей, в том числе с использованием инструментов Лаборатории Касперского.
	Практическое занятие, 2 часа	**Решение кейсов № 1** На основании содержания кейсов различить атаку, угрозу, исходящую из сети интернет, социальных сетей (с использованием инструментов Лаборатории Касперского).
Тема 2 Информационная безопасность: методы обеспечения	*Интерактивная лекция-вебинар, 4 часа*	Законодательная и нормативная база по информационной безопасности. Каналы утечки информации их классификация. Персональные данные в сети интернет и особенности их защиты. Трекинговые системы и способы блокировки. Методы стеганографии, шифрования как способы защиты информации. Математические основы криптологии и алгоритмов шифрования данных. Возможности их использования для защиты информации. Способы поиска информации в открытых источниках с соблюдением мер безопасности с применением инструментов Лаборатории Касперского. Алгоритм разработки стратегии обеспечения информационной безопасности.
	Практическое занятие, 4 часа	**Решение кейсов №2** На основании содержания кейсов разработать стратегию обеспечения информационной безопасности (с использованием инструментов Лаборатории Касперского).

Тема 3 Обеспечение информационной безопасности учащихся	*Лекция-вебинар, 2 часа*	Особенности, структура учебных заданий, ориентированных на выработку у обучающихся безопасного поведения в сети интернет и социальных сетях. Стратегия разработки системы заданий для учащихся, направленных на обеспечение информационной безопасности (CTF (Capture the Flag), алгоритмы шифрования данных и т.д.)
	Практическое занятие, 4 часа	**Проект** Разработать систему заданий для учащихся, направленную на обеспечение информационной безопасности (тема по выбору слушателя).
Итоговая аттестация	Зачет	Зачет на основании совокупности выполненных работ.

Раздел 3. *«Формы аттестации и оценочные материалы»*

3.1. Текущий контроль:

Кейс № 1

На основании содержания кейсов различить атаку, угрозу, исходящую из сети интернет, социальных сетей (с использованием инструментов Лаборатории Касперского).

Требования к решению кейсов: решение осуществляется на основании стратегии различения атак и угроз, исходящих из сети интернет, социальных сетей (с использованием инструментов Лаборатории Касперского).

Критерии оценивания:

1. Все шаги стратегии выполнены правильно.

2. Все угрозы определены верно**.**

Оценивание: зачет/незачет.

Пример кейса № 1

На почту слушателям направляются разного рода письма:

- рассылки;
- спам;
- содержащие ссылку на фишинговый сайт;
- содержащие полезную информацию.

Необходимо рассортировать письма по типу содержимого.

Слушателям даются:

- ссылки на профили учащихся, необходимо определить угрозы, которым подвержены данные профили.

- сообщения, полученные учащимися через социальные сети, необходимо среди этих сообщений выделить те, которые потенциально могут принести вред.

Кейс № 2

На основании содержания кейсов разработать стратегию обеспечения информационной безопасности с применением инструментов Лаборатории Касперского.

Требования к решению кейсов: решение осуществляется на основании алгоритма разработки стратегии обеспечения информационной безопасности с применением инструментов Лаборатории Касперского.

Критерии оценивания:

1. Все шаги алгоритма выполнены правильно.

2. Все угрозы определены верно**.**

Оценивание: зачет/незачет

Пример кейса № 2

Слушателю выдается доступ к виртуальной машине, необходимо указать все возможные недостатки в информационной безопасности системы.

Слушателю выдается схема передачи секретного сообщения, необходимо определить пути возможной утечки информации в указанной схеме.

Проект

Разработать систему заданий для учащихся, направленную на обеспечение информационной безопасности (тема по выбору слушателя).

Требования к проекту: проект осуществляется на основании стратегии разработки системы заданий для учащихся, направленных на обеспечение информационной безопасности.

Критерии оценивания:

1. Все шаги стратегии выполнены правильно.

2. Система заданий, учитывает особенности, рассматриваемых угроз, атак и все варианты обеспечения безопасности учащихся в рамках данной тематики.

Оценивание: зачет/незачет.

3.2. Итоговая аттестация: зачет на основании совокупности выполненных на положительную оценку работ.

Раздел 4. ***«Организационно-педагогические условия реализации программы»***

4.1. Учебно-методическое обеспечение и информационное обеспечение программы

Основная литература:

Наместникова М.С. Информационная безопасность, или На расстоянии одного вируса. 7-9 классы. Учебное пособие. ФГОС. Москва. Просвещение. 2019

Информационные источники и ресурсы:

1. Инструменты с открытым исходным кодом https://www.rsaconference.com/rsac-programs/open-source-tools (1.10.2020)
2. CyberSafety:Kids https://www.rsaconference.com/rsac-programs/cybersafety (1.10.2020)
3. Kids Safe Media https://kids.kaspersky.ru/ (1.10.2020)
4. Блог «Касперского» https://www.kaspersky.ru/blog/ (1.10.2020)
5. Статистика киберугроз https://statistics.securelist.com/ru (1.10.2020)
6. ИТ-энциклопедия «Касперского» https://encyclopedia.kaspersky.ru/ (1.10.2020)
7. Академия по кибербезопасности https://academy.kaspersky.ru/ (1.10.2020)
8. Математика в Кибербезопасности https://stepik.org/course/62247 (1.10.2020)
9. Описания киберугроз https://threats.kaspersky.com/ru/ (1.10.2020)
10. Исследования и описания вредоносного ПО https://securelist.ru/all/ (1.10.2020)

4.2. Материально-технические условия реализации программы

Для реализации программы необходимо следующее материально-техническое обеспечение:

- компьютерное и мультимедийное оборудование для использования видео- и аудиовизуальных средств обучения с подключением к сети интернет;
- программное обеспечение (ОС Microsoft Windows, браузеры Internet Explorer, Mozilla Firefox, Google Chrome и др., пакет офисных приложений Microsoft Office).