VI Городской конкурс методических разработок
«Вернисаж педагогических идей»

Номинация «Лучшая методическая разработка урока математики, информатики с применением технологий искусственного интеллекта»

Название методической разработки «Методическая разработка урока по теме «Вредоносное программное обеспечение и способы защиты от него»»

Автор:
Зиятдинова Татьяна Леонидовна,
учитель информатики
муниципального бюджетного
общеобразовательного учреждения
Сургутского естественно – научного лицея

Сургут, 2026

ВВЕДЕНИЕ

Актуальность темы обусловлена стремительным развитием цифровых технологий и ростом киберугроз в современном мире. Вредоносное программное обеспечение становится всё более изощрённым, а методы его распространения — всё более совершенными. В этих условиях критически важным становится не только понимание природы угроз, но и освоение современных инструментов защиты, включая технологии искусственного интеллекта.

Современный этап развития информационных технологий характеризуется активным внедрением искусственного интеллекта в сферу кибербезопасности. ИИ-системы способны анализировать огромные массивы данных, выявлять аномалии в поведении программ и предсказывать потенциальные угрозы, что делает их незаменимым инструментом в борьбе с цифровыми угрозами.

Значимость темы определяется тем, что каждый пользователь цифровых технологий должен обладать базовыми знаниями о методах защиты от вредоносного ПО и уметь применять современные инструменты безопасности.

Тема: «Вредоносное программное обеспечение и способы защиты от него»

Рабочая программа: Информатика. Углублённый уровень (для 7-9 классов образовательных организаций)

Класс: 7

Время: 45 мин

Форма урока: деловая игра

Форма организации обучения: групповая работа.

Методические приёмы, педагогические методы, технологии обучения:

- технология развития критического мышления:
- приемы: эмоциональный вход в урок, «корзина идей», «подводящий диалог», текстовая реконструкция, схематизация, ребус, кластер, «светофор», «привлекательная цель», «выделение опорных пунктов».

Содержательная цель урока: формирование у учащихся представления о вредоносном программном обеспечении, признаках заражения и способах защиты компьютера от вредоносных программ.

Деятельностная цель учителя: формирование у учащихся умения реализации новых способов действия.

Задачи:

Образовательные:

- познакомить с видами вредоносного программного обеспечения и их ключевыми особенностями;
- познакомить со способами распространения вредоносных программ;
- научить распознавать признаки заражения ПК;
- познакомить с методами защиты от вредоносных программ;
- составить алгоритмы защиты компьютеров.

Развивающая:

- способствовать:

- умению распознавать опасные ситуации при работе на компьютере;

- развитию критического мышления при работе с информацией через анализ и решение ситуационных задач;

- формированию навыков работы с ИИ-инструментами и анализа ответов ИИ-ассистентов;

- развитию умения взаимодействовать в группе.

Воспитательная:

- воспитывать ответственное отношение к информационной защищённости;
- формирование навыков безопасного использования цифровых устройств;
- воспитывать терпеливость, уважение к мнению товарища.

Универсальные учебные действия (УУД)

- Личностные УУД: формирование ответственного отношения к собственной информационной защите
- Познавательные УУД:

- освоение способов защиты от вредоносного программного обеспечения;

- формирование навыков безопасного использования цифровых устройств

- Коммуникативные УУД: развитие умения взаимодействовать в группе при решении учебных задач
- Регулятивные УУД: развитие умения планировать свои действия в цифровой среде

Ожидаемые результаты:

- Личностные: формирование ответственного отношения к защищённости в цифровой среде
- Метапредметные:

- развитие умения анализировать информацию и принимать решения в нестандартных ситуациях;

- формирование навыков работы с ИИ-инструментами;

- Предметные: знание основных видов вредоносных программ и способов защиты от них.

Используемое оборудование:

- мультимедийный проектор;
- интерактивная доска;
- компьютеры с доступом в Интернет;
- ИИ-сервисы: ChatGPT/GigaChat;
- флипчарты по количеству групп;
- фломастеры, магниты для крепления.

Программное обеспечение:

- платформа для интерактивных заданий Wordwall

https://wordwall.net/resource/63180508/кибербезопасность/признаки;

- презентация, созданная средствами Microsoft Office PowerPoint;

Роль учителя: руководитель Центра борьбы с киберпреступностью (ЦБК).

Роль учащихся: сотрудники отделов ЦБК (работа в группах).

Описание организации деятельности учащихся:

Учащиеся разделены на «отделы» до проведения урока, ознакомлены со своими ролями и направлением деятельности каждого отдела. Рассадка учащихся организована по группам. Возле парты каждой группы размещен флипчарт для размещения материалов по результатам работы группы.

На партах размещены таблички с названиями отделов и направлением их деятельности:

Отдел анализа угроз - изучает виды вредоносных программ и принципы их работы.

Отдел мониторинга — выявляет признаки и симптомы заражения компьютера.

Отдел киберзащиты — разрабатывает меры профилактики.

Технологическая карта урока

Виды работы, формы, методы, приемы	**Содержание педагогического взаимодействия**		**Формируемые УУД**	**Примечание (оборудование, презентация, раздаточный материал)**
	Деятельность учителя	**Деятельность учащихся**		
I этап. Мотивация к учебной деятельности **Цель этапа:** Создание благоприятного психологического настроя на работу				
Эмоциональный вход в урок	«Коллеги, рад приветствовать вас на нашем оперативном совещании! Прошу внимания! Наш Центр получил срочное предупреждение: обнаружена новая версия вредоносного программного обеспечения *(ролик).*	Просматривают ролик	Коммуникативные УУД	Презентация, слайд № 1, слайд 2
Проблемная ситуация	Информация ограниченная, известно лишь название - «Химерус86». Эксперты утверждают, что угроза серьезная, способна быстро распространяться. Согласно данным на сегодняшний день, эта программа угрожает стабильной работе компьютеров, установленных в учреждениях и на предприятиях Ханты – Мансийского автономного округа - Югры.			
	Как вы думаете, почему я вас пригласил? Какой основной вопрос нашего совещания?	Отвечают на вопросы		
Постановка темы урока	Верно. Наше совещание посвящено вопросам обеспечения защиты компьютеров нашего города от вредоносного программного обеспечения.			Презентация, слайд № 3
	Коллеги, напоминаю правила корпоративной работы в нашем Центре: ➢ работайте сообща – вы один отдел; ➢ принимайте активное участие в работе; ➢ уважайте мнение других сотрудников отдела; ➢ следите за временем выполнения задач;	Повторяют правила работы.	Коммуникативные УУД	Презентация, слайд № 4

<table>
<tr><td></td><td>➢ после выполнения каждой задачи – ретроспектива (обратная связь, обсуждение);
Напоминаю о том, что:
Руководитель группы — координирует работу, следит за временем.
Эксперт-аналитик — изучает материалы, формулирует выводы.
Менеджер проектов — представляет результаты отдела.
Секретарь – референт - фиксирует решения в рабочем «отчете».</td><td></td><td></td><td>Презентация, слайд № 5

Карточки с указанием ролей</td></tr>
<tr><td colspan="5">II этап. Актуализация знаний и фиксирование индивидуальных учебных затруднений.
Цель этапа: Создание условий для возникновения у учеников внутренней потребности включения в учебную деятельность.</td></tr>
<tr><td>Прием «Корзина идей» (позволяет выяснить все, что учащиеся знают/не знают по данной теме)</td><td>Коллеги, начнем с экспресс – опроса. на ваших столах - стикеры. Напишите на них:
1.Один факт, который вы точно знаете о вредоносных программах.
2.Один вопрос, ответа на который вы еще не знаете, но именно этот ответ позволит обеспечить защиту компьютеров от вредоносного ПО.
3.Прикрепите стикеры на доску в соответствующие колонки: «Знаем» и «Хотим узнать».</td><td>Пишут на стикерах, прикрепляют в табличку на доске</td><td>Познавательные УУД
Регулятивные УУД</td><td>Схема доски:<table><tr><td>Знаем</td><td>Хотим узнать</td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td>Прием «Подводящий диалог»</td><td>Теперь давайте обобщим. Что у нас в колонке «Знаем»? (Выбирает стикеры с описанием актуальной для темы урока информацией)
А какие вопросы самые актуальные в колонке «Хотим узнать»? (Выбирает 2–3 стикеры с ключевыми вопросами, которые могут подвести к формулированию цели урока)</td><td>Отвечают на вопросы</td><td>Познавательные УУД
Регулятивные УУД
Коммуникативные УУД</td><td></td></tr>
<tr><td>Формулирование цели урока.</td><td>Согласна. Для того, чтобы обеспечить защиту компьютеров, необходимо познакомиться с</td><td></td><td></td><td></td></tr>
</table>

	типами вредоносных программ, способами распространения и признаками заражения.			
III этап. Построение проекта выхода из создавшейся ситуации. Постановка учебной задачи **Цель этапа:** Активизация знаний учащихся.				
Прием «Привлекательная цель»	В рамках нашего совещания нам необходимо оперативно проанализировать существующие угрозы, выявить механизмы заражения и разработать комплекс защитных мер. Каждый отдел получит своё оперативное задание. В конце совещания мы сформируем **единый протокол защиты**, который будет внедрён во всех учреждениях города. Готовы приступить к работе? Тогда за дело!» Руководители отделов, прошу получить кейсы для работы.	Определяют и «принимают» цель урока		Кейсы с материалами, справочные материалы, бумага для флипчарта для оформления результатов.
IV. Реализация построенного проекта («открытие» нового знания) **Цель этапа:** Организация учащихся по исследованию проблемной ситуации. Установление осознанности восприятия.				
Прием «Ребус»	**Задача 1. «Виды вредоносного программного обеспечения» (3 мин)** Для того, чтобы познакомиться с основными видами вредоносных программ предлагаю разгадать ребусы.	Разгадывают ребус	Познавательные УУД Регулятивные УУД Коммуникативные УУД	Карточки - ребусы
	Давайте проверим. Отделы, озвучьте ваши ответы.	Озвучивают ответы	Коммуникативные УУД	Презентация, слайд № 6
Прием «Светофор»	Руководитель отдела, организуйте обсуждение работы отдела над задачей, оцените. Если все понятно, работали совместно – зеленый стикер, возникли затруднения в процессе работа – желтый стикер, ничего не понятно, остались вопросы – красный стикер. Выйдите к доске, наклейте	Обсуждают, оценивают, выбирают цвет стикера. Руководитель клеит стикер на доску задач	Регулятивные УУД	Доска задач
Прием «Выделение опорных пунктов»	**Задача 2. «Ключевые характеристики вредоносного программного обеспечения» (7 мин.)**	Работают с текстом, отбирают карточки (3 мин.)	Познавательные УУД Регулятивные УУД	Карточки с описаниями видов вредоносного ПО;

	Каждый отдел получил описание какого – либо программы из названных выше. Ваша задача - познакомится с текстом, в котором описаны вид вредоносной программы, выделить его ключевые основные характеристики, наклеить на флипчарт в соответствии со схемой. Схема флипчарта: Характеристика 1 Вид ПО → Характеристика 2 ……. **Давайте обсудим:** 1. Чем троян принципиально отличается от вируса? 2. Почему черви особенно опасны для локальных сетей? 3. Какая главная цель вируса?	Каждый отдел выступает с отчетом (2 мин). Отвечают на вопросы	Коммуникативные УУД	текст для каждого учащегося **Возможные ответы:** 1. Вирус способен к саморазмножению, троянская программа маскируется под полезные приложения. 2. Черви (вирусы-черви) опасны для локальных сетей, потому что способны самостоятельно распространяться по компьютерным сетям, не требуя действий пользователя. В отличие от обычных вирусов, червь живёт «сам по себе» и использует сеть для размножения.

				3. Создание и распространение своих копий
	Коллеги, хочу отметить, что это только основные типы вредоносных программ. Есть еще и другие – программы – шпионы, блокировщики, шифровальщики. Я думаю, что вы догадались, какой вред наносят эти программы, исходя из названия.		Познавательные УУД	Презентация, слайд № 7
Прием «Светофор»	Руководитель отдела, организуйте обсуждение работы отдела над задачей, оцените.	Обсуждают, оценивают, выбирают цвет стикера. Руководитель клеит стикер на доску задач	Регулятивные УУД Коммуникативные УУД	Доска задач Презентация, слайд № 8
Прием «Кластер»	**Задача 3. «Сценарий атаки» (5 мин)** Ознакомиться с текстом и составить кластер «Способы распространения вредоносных программ»	Заполняют кластер	Познавательные УУД Регулятивные УУД Коммуникативные УУД	Текст Кластер
	Коллеги, я тоже вместе с вами работал над решением этой задачи, давайте сравним, что у нас получилось.		Познавательные УУД	Презентация, слайд № 9
Прием «Светофор»	Руководитель отдела, организуйте обсуждение работы отдела над задачей, оцените.	Обсуждают, оценивают, выбирают цвет стикера.	Регулятивные УУД Коммуникативные УУД	Доска задач
	Физкультминутка (3 мин) «Сотрудники ЦБК, время производственной гимнастики! Чтобы сохранить остроту ума, выполним **кибер-зарядку**: 1. *«Сканируем угрозы»*: повороты головы влево-вправо (3 раза).	Выполняют зарядку	Регулятивные УУД Коммуникативные УУД	Презентация, слайд № 10

	2. *«Блокируем вирус»*: руки в стороны, сжимаем пальцы в кулак (4 раза). 3. *«Устанавливаем надежный пароль»*: сжимаем и разжимаем кулаки (5 раз). 4. *«Производим резервное копирование»*: плавно наклоняемся вперёд, руки к полу (3 раза). 5. *«Обновляем систему»*: потянулись вверх на носочках, опустились (3 раза). Отлично! Теперь мы готовы к дальнейшей работе»			
Прием «Установи соответствие»	**Задача 4. «Диагностика угрозы и методы защиты» (3 мин.)** Коллеги, для того, чтобы познакомиться с признаками заражения компьютерными вирусами и способами защиты, предлагаю выполнить следующее задание.		Познавательные УУД Регулятивные УУД Коммуникативные УУД	Интерактивная викторина https://wordwall.net/resource/63180508/кибербезопасность/признаки Презентация, слайд № 11
Прием «Светофор»	Руководитель отдела, организуйте обсуждение работы отдела над задачей, оцените.	Руководитель организует обсуждение, клеит стикер на доску задач	Регулятивные УУД Коммуникативные УУД	Доска задач
V. Этап первичного закрепления с проговариванием во внешней речи **Цель этапа:** Проверка алгоритма восприятия				
Прием «Текстовая реконструкция»	Теперь объединим ваши наработки в **единый протокол защиты** компьютеров. **Задача 5. Составление единого протокола защиты (5 мин)** Задание: Заполнить пропуски.	Руководитель организует обсуждение	Познавательные УУД Регулятивные УУД Коммуникативные УУД	Единый протокол защиты 1.Установить надёжный антивирус и регулярно его обновлять. 2.Включать автоматическое обновление ОС и программ.

				3.Не открывать письма и вложения от незнакомых отправителей. 4.Регулярно делать резервные копии важных данных. Презентация, слайд № 12
VI. Этап самостоятельной работы с проверкой по эталону **Цель этапа:** Организация деятельности с применением новых знаний (с помощью искусственного интеллекта).				
Прием «Ситуационная задача»	Коллеги, пока шло совещание, нам поступила информация об различных инцидентах, которые произошли с компьютерами в разных учреждениях города. Наша задача – помочь. **Задача 6: «Реагирование на инцидент» (5 мин).** Проанализировать **реальный кейс кибератаки** и выработать рекомендации по предотвращению подобных инцидентов.	Работают над заданием	Познавательные УУД Регулятивные УУД Коммуникативные УУД	Ситуационные задачи Презентация, слайд № 13
VII. Этап рефлексии учебной деятельности на уроке Цель: Рефлексия деятельности на уроке				
Прием «Три М» (позволяет провести самооценку групповой работы)	Коллеги, мы с вами хорошо поработали сегодня. Прошу руководителей групп организовать оценку работы группы в целом. Сформулируйте два момента, которые сегодня у вас получились очень хорошо, и предложите одно действие, которое улучшит вашу работу в дальнейшем.	Обсуждают, принимают решение, озвучивают результаты	Регулятивные УУД Коммуникативные УУД	Презентация, слайд № 14
Прием «Светофор» (позволяет провести самооценку	На ваших рабочих местах лежат стикеры. Прошу оценить вклад каждого сотрудника ЦБК в работу. Если у вас все получилось в процессе	Выбирают стикер, клеят на доску в раздел «ИТОГ»	Регулятивные УУД	Презентация, слайд № 15

индивидуальной работы учащегося на уроке)	работы – наклейте зеленый стикер, нужно доработать – желтый, ничего не понятно – красный.			Доска задач
VIII. Постановка домашнего задания				
	Коллеги, в конце совещания хочу дать каждому из вас индивидуальное задание, которое необходимо выполнить до следующего совещания. **Обязательное:** создать памятку «Защита от вредоносных программ: 10 правил» с использованием ИИ (ChatGPT/GigaChat для генерации идей). **Дополнительное:** исследовать новости о последних кибератаках и проанализировать, как искусственный интеллект мог бы помочь в их предотвращении.			
	Спасибо за плодотворную работу, коллеги! В конце нашего совещания хочу каждому из вас подарить буклет, в котором собрана вся информация о вредоносном программном обеспечении и способах защиты от него.			Буклет

ЗАКЛЮЧЕНИЕ

На уроке рассмотрены основные аспекты темы «Вредоносные программы и способы защиты от них» с применением технологий искусственного интеллекта.

Практическая значимость урока заключается в том, что с помощью полученных знаний и умений учащиеся смогут:

- распознавать потенциальные угрозы в цифровой среде;
- эффективно использовать инструменты защиты;
- формировать правильные запросы к искусственному интеллекту и анализировать ответы ИИ-ассистента.

Перспективы развития темы связаны с постоянным совершенствованием технологий искусственного интеллекта и появлением новых методов защиты от цифровых угроз. Важно понимать, что обеспечение информационной безопасности - это очень важный процесс, требующий постоянного обновления знаний и навыков.

Рекомендации по дальнейшему изучению темы:

- отслеживание актуальных новостей в сфере кибербезопасности
- изучение новых методов защиты и анализа угроз с помощью искусственного интеллекта. Например, на на этапе актуализации знаний на следующем уроке можно предложить выполнить практическую работу по теме «Анализ угроз с помощью ИИ»
- ученики получают набор файлов и ссылок (часть - безопасные, часть - подозрительные).
- через VirusTotal и Google Safe Browsing проверить их.
- занести результаты в таблицу:

Файл/ссылка	Результат проверки	Тип угрозы	Рекомендации по защите

Преимущества использования искусственного интеллекта на уроке

- наглядность: демонстрация реальных инструментов киберзащиты.
- интерактивность: вовлечение учеников в практику работы с ИИ.
- актуальность: изучение современных методов борьбы с угрозами.
- практико-ориентированность: навыки, применимые в реальной жизни.

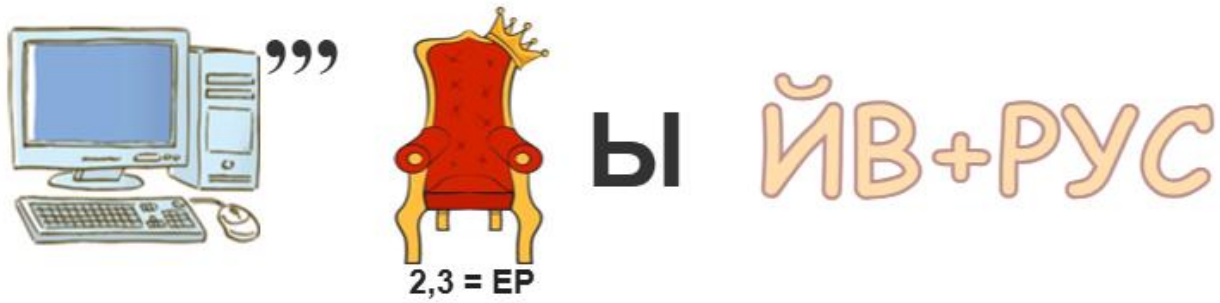
ПРИЛОЖЕНИЯ

Доска задач

Задача	**Отдел анализа угроз**	**Отдел мониторинга**	**Отдел киберзащиты**
Задача 1			
Задача 2			
Задача 3			
Задача 4			
Задача 5			
Задача 6			
ИТОГ			

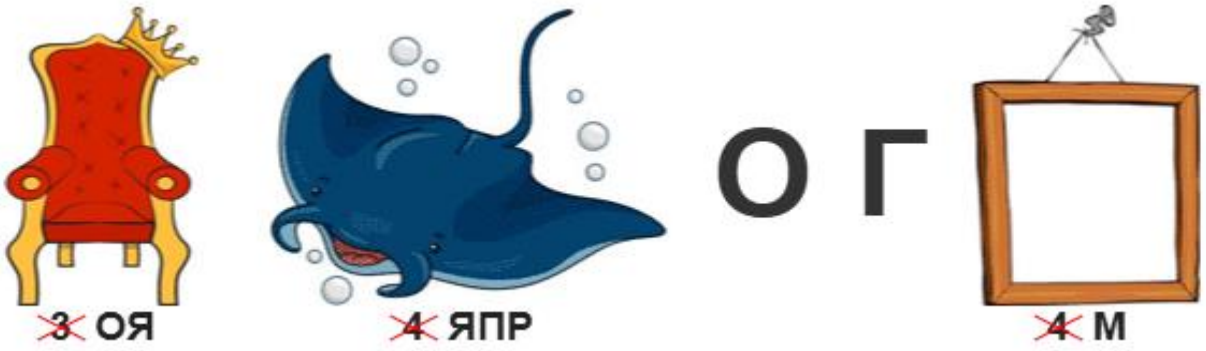
Задача 1. Ребусы.

Отдел анализа угроз (КОМПЬЮТЕРНЫЙ ВИРУС):



Отдел мониторинга (СЕТЕВЫЕ ЧЕРВИ):

Отдел киберзащиты (ТРОЯНСКИЕ ПРОГРАММЫ):



Технологическая карта урока

Задача 2.

Отдел анализа угроз	**Отдел мониторинга**	**Отдел киберзащиты**
Текст		
Компьютерные вирусы прикрепляются к файлам и приложениям, активируются при их запуске и могут саморазмножаться. Вирусы способны уничтожать файлы, изменять данные и нарушать работу системы.	Сетевые черви - вредоносные утилиты, которые распространяются через сети и заражают другие устройства, используя уязвимости операционной системы.	Троянские программы (трояны) - маскируются под полезные приложения, но при установке выполняют вирусные действия, например, открывают доступ к устройству для злоумышленников или воруют данные. Он не распространяется сам по себе: его нужно запустить (открыть вложение, запустить файл и т. д.).
Карточки с характеристиками		
Прикрепляются к файлам	Прикрепляются к файлам	Прикрепляются к файлам
Маскируются под полезные программы	Маскируются под полезные программы	Маскируются под полезные программы
Воруют данные	Воруют данные	Воруют данные
Распространяются через сети	Распространяются через сети	Распространяются через сети
Могут саморазмножаться	Могут саморазмножаться	Могут саморазмножаться

Задача 3.

Текст

Способы распространения вредоносных программ

Распространение вредоносных программ осуществляется различными способами.

Распространение с помощью физических носителей

Физические носители (флеш-накопители, CD/DVD-диски, жесткие диски и другие устройства хранения данных) могут служить источником заражения компьютеров вирусами, червями и троянскими программами. Пользователи часто обмениваются такими устройствами, вставляют их в разные компьютеры, тем самым способствуя быстрому распространению угроз.

Обмен файлами посредством внешних устройств также представляет собой угрозу. Если файлы были скачаны из ненадежных источников или получены от незнакомых пользователей, они могут содержать скрытые угрозы.

Некоторые вирусы маскируются под обновления ОС или известных программ, предлагая загрузить обновление операционной системы и приложений вручную. Это особенно актуально для пользователей, отключивших автоматическое обновление или предпочитающих сторонние источники обновлений.

В некоторых случаях заражение происходит через исполняемый файл, который запускает извлечение и выполнение компонентов вредоносной программы.

Распространение по сетям

Небезопасные загрузки или скачивание файлов с зараженных сайтов может быть сопряжено с риском. Внешне легитимные программы могут содержать встроенные вредоносные элементы, которые начинают действовать после установки.

Электронная почта остается одним из наиболее распространенных способов доставки вредоносных программ. К письмам прикрепляются заражённые вложения или ссылки на инфицированные веб-сайты. Пользователям рекомендуется проявлять осторожность при открытии писем от неизвестных отправителей и проверять безопасность вложений перед открытием.

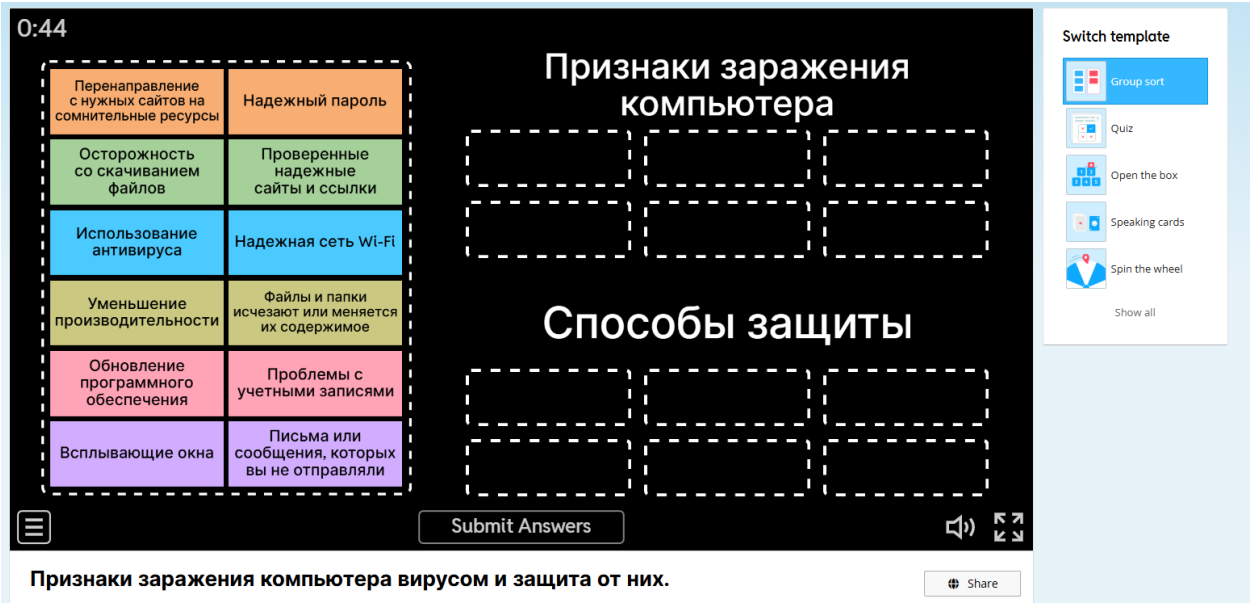
Социальные сети и мессенджеры для мгновенного обмена сообщениями активно используются злоумышленниками для распространения вредоносного ПО. Например, ссылка, присланная знакомым человеком (его аккаунт мог быть взломан), может привести к загрузке вируса на устройство жертвы.

Рекламные баннеры и всплывающие окна в Интернете иногда используется для скрытого размещения вредоносных элементов. Такие элементы автоматически запускают программы загрузки нежелательного программного обеспечения.

Некоторые сайты маскируются под легитимные сервисы (например, социальные сети, онлайн-магазины или банки). Когда пользователь вводит свои личные данные (логин, пароль), эта информация попадает злоумышленникам. Такие сайты называются фишинговые.

Кластер

Задача 4. Установи соответствие:



Задача 5. Заполни пропуски:

1. Установить надёжный _____и регулярно его _____.
2. Включать автоматическое _____и программного обеспечения.
3. _____и вложения от незнакомых отправителей.
4. Регулярно делать _____важных данных.
5. Скачивать файлы с _____сайтов.

обновление ОС не открывать письма проверенных
обновлять антивирус резервные копии

Задача 6. Даны ситуации. Группам необходимо выполнить следующее задание:

1. сформулировать 2-3 запроса для ИИ-ассистента (GigaChat, ChatGPT) для решения задачи: определить тип вредоносного ПО; указать 2–3 признака заражения; предложить 1–2 первоочередных действия;
2. проанализировать ответы нейросети;
3. опираясь на ответы ИИ, подготовить ответ на решение задачи.

Отдел анализа угроз:

Ситуационная задача «Атака файлового вируса»

Ситуационная задача	**Ответы к ситуационным задачам по видам вредоносного ПО**

Ситуация: В корпоративной сети участились случаи «зависания» рабочих станций, появляются неожиданные сообщения об ошибках, происходят изменения в дате/времени модификации файлов. При анализе обнаружено, что исполняемые файлы с расширением `.exe` на компьютерах имеют увеличенный размер - к ним дописан дополнительный код. Антивирусные решения не срабатывают. **Вопросы:** 1. Определить тип вредоносного ПО; 2. Указать 2–3 признака заражения; 3. Предложить 1–2 первоочередных действия по защите.	**Ответ:** 1.Вирус 2. Признаки заражения файловым вирусом: ✓ увеличение размера исполняемых файлов; ✓ замедление работы системы; ✓ неожиданные сообщения об ошибках; ✓ изменения в дате/времени модификации файлов. 3. Действия: ✓ запустить полное сканирование антивирусом в безопасном режиме. ✓ удалить заражённые файлы; ✓ изолировать заражённые компьютеры от сети

Отдел мониторинга

Ситуационная задача «Эпидемия сетевого червя»

Ситуационная задача	**Ответы к ситуационным задачам по видам вредоносного ПО**
Ситуация: После подключения флешки к компьютеру начальника отдела маркетинга, который подключен к корпоративной локальной сети, система начала «тормозить», а в сетевом окружении появились неизвестные общие папки. Антивирус выдал предупреждение о попытке запуска autorun.inf. **Вопросы:** 1. Какие признаки указывают на заражение ПК вредоносным ПО? 2. Определите вид ПО. 3. Какие меры защиты от этого ПО?	**Ответ:** 1. Система начала «тормозить», а в сетевом окружении появились неизвестные общие папки. Антивирус выдал предупреждение о попытке запуска autorun.inf. 2. Это сетевой червь. 3. Надо проверить антивирусом все компьютеры в сети. Изолировать зараженные компьютеры от сети.

Отдел киберзащиты

Ситуационная задача: «Подозрительная программа — где троян?»

Ситуационная задача	**Ответы к ситуационным задачам по видам вредоносного ПО**
Ситуация Вы — начинающий специалист отдела кибербезопасности. К вам обратился сотрудник отдела продаж, Иван Сергеевич. Он рассказал следующее: «Вчера мне на почту пришло письмо от «Партнёра компании» с темой «Обновлённый прайс-лист Q3». В письме была ссылка и приписка: «Открой файл в Excel, макросы включи — там интерактивные фильтры». Я скачал файл `Прайс_Q3_обновлённый.xlsm`, открыл, включил макросы, как просили. Сначала всё было нормально, но сегодня утром компьютер стал тормозить. В антивирусе выскочило предупреждение: «Обнаружена подозрительная активность». Ещё я заметил, что из моей почты сами собой отправляются письма с каким-то вложением. Что делать?» **Задание** Какие признаки указывают на заражение компьютера? Определите тип вредоносного ПО, которое попало на компьютер Ивана Сергеевича. Как помочь Ивану Сергеевичу?	**Ответ:** 1. Признаки: ✓ заражение произошло после открытия файла из письма (трояны маскируются под полезные документы). ✓ требование включить макросы — явный маркер атаки: вредоносный код прячется в макросах Excel. ✓ самостоятельная отправка писем с компьютера ✓ торможение системы 2. Это троянская программа 3. План действий: ✓ *изолировать компьютер:* отключить от сети (интернет, локальная сеть), чтобы остановить рассылку писем и утечку данных. ✓ *удалить заражённый файл:* найти и удалить `Прайс_Q3_обновлённый.xlsm` и другие подозрительные вложения. ✓ *запустить полное сканирование антивирусом:* проверить систему и вылечить/удалить заражённые объекты.

Буклет


Вредоносные программы (вирусы)
Типы вредоносных программ:
Компьютерные вирусы
Это программы, которые заражают другие полезные программы, добавляя в них свой вредоносный код, выполняют нежелательные действия на ПК.
Сетевые черви
Вредоносные программы, которые тайком от пользователя проникают и быстро распространяются по компьютерной сети.
Троянские программы
Безобидные на вид программы, которые незаметно для пользователя несут разрушение информации и нарушают работу компьютера.
Программы-шпионы (spyware)
Программы, которые скрытным образом устанавливаются на компьютер, перехватывают вашу личную информацию (пароли, номера кредитных карт, адреса электронной почты и т.д.), и передают полученные данные своему автору.
Программы показа рекламы (adware)
Такие программы, предназначены для показа рекламы на вашем компьютере, перенаправления запросов поиска на рекламные веб-сайты и сбора маркетинговой информации о вас.
Вредоносные (хакерские) утилиты
Это программы, разработанные для автоматизированного создания вирусов, червей или троянских программ и т. п.
Вредоносные программы-вирусы
Классификация:
По среде обитания
Загрузочные
Файловые
Макровирусы
Сетевые
По степени воздействия
Безвредные
Неопасные
Опасные
Разрушительные
По способам заражения
Резидентные
Нерезидентные
По алгоритмической особенности
Троянский конь
Логическая бомба
Мутанты
Невидимки (стелс)
Каналы распространения компьютерных вирусов:
Флеш-накопители (флешки)
Большое количество вирусов распространяется через съемные накопители USB: флеш-карты, флеш-диски, цифровые фотоаппараты / видеокамеры, MP3 плееры, сотовые телефоны.
Электронная почта
Основной канал распространения вирусов. Обычно вирусы маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.
Система обмена сообщениями
Здесь также распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся путями к распространению вредоносных программ.
Веб-страницы (сети Интернет)
Возможно также заражение через страницы сети Интернет ввиду наличия на страницах всемирной паутины "активного" содержимого: скриптов, ActiveX - компоненты, Java-апплетов.
Интернет и локальные сети (черви)
Черви - вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые "дыры" (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.
Признаки заражения компьютера:
Программы неожиданно перестают работать или работают с ошибками.
Происходит произвольный, без участия пользователя, запуск на компьютере каких-либо программ.
На экран выводятся посторонние символы и сообщения, появляются странные видео и звуковые эффекты.
Работа компьютера замедляется, некоторые компьютерные диски оказываются испорченными.
Пароли для доступа к программе (например, к почте) не подходят.
Компьютер при включении не загружается.
Антивирусная программа
Компьютерная программа, целью которой является обнаружить, предотвратить размножение и удалить компьютерные вирусы и другие вредоносные программы, а также препятствуют несанкционированному проникновению вредоносных программ в компьютер.
Классы антивирусных программ
Антивирусный сканер
CRC сканер (ревизор)
Вирусный блокировщик
Вирусный иммунизатор