Семеновская средняя школа

учитель информатики Колесова Елена Анатольевна

**Разработка урока**
**«Основы информационной безопасности и защиты информации»**
(в рамках проведения Единого урока безопасного Интернета)

**Цель**: изучить опасные угрозы сети Интернет и методы борьбы с ними

З**адачи:**

**Образовательная***:* обучить детей личной и информационной безопасности в Интернете, сформировать навыки поведения в информационном обществе с целью обеспечения информационной безопасности, а также разработать нормы и правила безопасного поведения в сети Интернет

**Развивающая**: развивать навыки самостоятельной работы, формировать сознательность и внимание к информационной безопасности; развивать интерес к предмету; формировать приёмы логического мышления; развивать способность анализировать и обобщать, делать выводы

**Воспитательная:** прививать навыки безопасного использования сети Интернет, воспитывать информационную культуру, прививать навыки самостоятельной работы, сотрудничества.

**Ход урока:**

**Эпиграф:** «Интернет несет читателю тонны мусора и крупинки золотого песка, и умение выбрать самое интересное и полезное становится весьма востребованным талантом»

**I. Организационный момент**.

1.Вступительное слово учителя.

Проблема информационной безопасности стала особенно острой при бурном развитии сети Интернет. К концу сентября 2020 года ожидалось, что закончатся 4,3 миллиарда адресов базового протокола передачи данных IPv4. Так что же такое информационная безопасность?

**II. Знакомство с новым материалом.**

Блиц – выступления учащихся с сообщениями, подготовленными дома (с выводом на экран).

*1 ученик*. Информационная безопасность – процесс соблюдения (сохранения) трёх аспектов (атрибутов) безопасности: доступности, целостности и конфиденциальности информации.

Доступность информации заключается в том, что информация в безопасном состоянии должная быть доступна для пользователя, т.е. должна быть сохранена возможность всех операций по её обработке. Это означает, что необходимо работающее оборудование, неповреждённые носители информации, правильно настроенные работающие программы.

Целостность информации – это соответствие логической структуры информации определённым правилам, логически корректное её состояние. Процедуры обработки и изменения информации должны преобразовывать одно целостное состояние в другое.

Конфиденциальность информации – это выполнение тех или иных операций с информацией, в соответствии с некоторыми правилами политики безопасности.

Нарушение конфиденциальности – возможность выполнения операций (например, чтения или записи) теми, кто не должен этого делать.

*2 ученик.* Всё перечисленное – это стороны одного и того же процесса, они тесно связаны между собой. Нарушение одного из них может привести к нарушению другого. Возможность нарушения или нежелательного изменения одного из аспектов безопасности называется угрозой.

Наиболее часто возникающими угрозами являются:

1. угроза отказа аппаратуры;

2. угроза утечки (несанкционированного доступа);

3. угроза некорректной работы программных средств.

Атака – действие или (или последовательность действий), которое приводит к реализации угрозы.

Для обеспечения информационной безопасности нужно минимизировать вероятность наступления одной из возможных угроз.

Наиболее распространёнными атаками являются:

1. Перехват данных. Особенно чувствителен перехват таких данных, как имена пользователей и пароли.
2. Отказ в обслуживании. Например, при большом количестве запросов на установку сетевого соединения.
3. Подбор пароля. При отсутствии средств защиты или создании простых паролей возможен несанкционированный доступ к информации.
4. Внедрение исполняемых фрагментов.
5. Социальная инженерия (фишинг).

*3 ученик.* Вредоносная программа – программа, целью работы которой является выполнение действий, затрудняющих работу или ущемляющих права пользователя, а также приводящих к нарушению безопасности.

Рассмотрим классификацию вредоносных программ от Лаборатории Касперского. К вредоносному программному обеспечению (ПО) относятся: вирусы, черви, трояны, подозрительные упаковщики и вредоносные утилиты.

Одна из наиболее опасных и серьёзных опасных угроз для безопасности информации на личном компьютере – это компьютерные вирусы.

История компьютерных вирусов начинается в 1983 г., когда американский ученый Фред Коэн (FredCohen) впервые ввел термин «компьютерный вирус».

Компьютерные вирусы – это программы, которые распространяются по доступным носителям без ведомапользователя и наносят тот или иной ущерб данным пользователя.

Brain (1986 год) – первый вирус для IBM-совместимых компьютеров, вызвавший глобальную эпидемию. Он был написан двумя братьями-программистами – БаситомФаруком и АмжадомАлви (BasitFarooqAlvi и AmjadAlvi) из Пакистана.

Сетевые «черви» – вредоносные программы, использующие уязвимости в сетевых программах. Они распространяются по сети, а не с помощью передачи файлов.

Червь Морриса (ноябрь, 1988 год) – первый сетевой червь, вызвавший эпидемию. Он написан 23-летним студентом Корнельского университета (США) Робертом Моррисом, использовавшим ошибки в системе безопасности операционной системы Unix (Юникс) для платформ VAX (Вакс) и SunMicrosystems (Сан Микросистемс).

Троянские кони (Трояны) – вредоносные программы, которые не начинают действие сразу после внедрения, а ждут получения команды извне или наступления какого-либо события.

Злоумышленники используют целые сети поражённых машин и используют их для своей деятельности: рассылки нежелательной почты, сбора паролей, организации распределённых атак на отказ в обслуживании.

Широкое распространение сетевых средств обмена информацией привело к возникновению явления массовой несанкционированной рассылки сообщений рекламного или вредоносного характера. Явление получило название спам. Каналы распространения спама различны, но чаще всего это:

• письма по электронной почте;

• сообщения в форумах, конференциях;

• сообщения в средствах мгновенного обмена сообщениями.

Наиболее популярной защитой информации являются антивирусы.

*4 ученик*. Антивирусы– специализированные программы для выявления и устранения вирусов. Чаще всего они используют поиск заданных участков кода – сигнатур.

В качестве примеров антивирусных программ можно назвать: антивирус Касперского, Dr. Web, NOD32, свободно распространяемые антивирусы: Avast и Clamwin.

Для полноценной защиты от появления на личном компьютере вредоносных программ рекомендуется:

1) установить и своевременно обновлять систему антивирусной защиты;

2) проверять все носители (карты памяти, флэшки и т. д.), которые находились за пределами Вашей системы перед использованием;

3) не открывать вложений, полученных от неизвестных адресатов с неизвестными целями;

4) регулярно проводить полную проверку системы.

Для защиты компьютерных сетей или отдельных компьютеров от несанкционированного доступа используют межсетевые экраны.

Современные брандмауэры (межсетевые экраны) – сложные и многофункциональные комплексы программ, задача которых – обеспечение безопасного взаимодействия сетей.

Регламентация доступа к данным. Общий подход, применяемый для разграничения доступа к данным, состоит в том, что операции выполняются только после проверки наличия прав на их осуществление. Наиболее часто используется пароль доступа или доступ на основе учётной записи.

Логин – это сочетание различных символов, которые сервис ассоциирует с пользователем; иначе говоря, это имя пользователя, под которым его будут «видеть» другие пользователи.

Пароль – это сочетание различных символов, подтверждающих, что логином намеревается воспользоваться именно владелец логина.

Существенным условием сохранения информации является создание устойчивого пароля, а также нераспространение пароля. К мерам защиты пароля относятся:

1. Не разглашать пароль (не записывать их в тетради, не оставлять записанные пароли в доступных местах).
2. Не использовать простые пароли. Простыми считаются короткие пароли (до четырёх символов), пароли, состоящие только из букв или только из цифр, предсказуемые сочетания типа qwerty (кверти).
3. Не использовать легко отгадываемые пароли – год рождения, своё имя, имена родственников и т. д.
4. Нежелательно использовать осмысленные слова.
5. Время от времени пароли нужно менять (например, раз в два месяца).

Соблюдение этих простых правил существенно затруднит атаки на Ваш пароль.

Все рассмотренные средства обеспечения информационной безопасности направлены, в первую очередь, на уменьшение вероятности сбоев в процессе обработки данных. Ни одно из них не позволяет исключить такие печальные события полностью. Наиболее эффективным и надёжным способом защиты данных является резервное копирование.

## II. Систематизация и обобщение имеющихся знаний

Мы рассмотрели теоретические основы информационной безопасности и защиты информации, а теперь давайте вспомним основные правила, которых должен придерживаться каждый, чтобы обезопасить себя при работе в сети.

У детей на партах лежат карточки с правилами безопасной работы в Интернете. Дети рассматривают правила и на листах стараются проиллюстрировать их и отгадать, какое правило было изображено. Потом дети сами рассказывают о правилах, которые они проиллюстрировали.

1. **Никогда не разглашайте личную информацию.** Никогда не указывайте свою личную информацию, например полное имя или город проживания во время общения с

помощью мгновенных сообщений или в чатах, если вы полностью не уверены в личности человека, с которым вы общаетесь, лучше придумать псевдоним.

2. **Любой человек в интернете может с легкостью выдавать себя за другую личность**. И это несет в себе огромную опасность. Ни в коем случае нельзя встречаться с лично незнакомыми друзьями по переписке, даже если вы давно общаетесь.

3. **Не спеши отправлять sms.** Если хочешь скачать картинку или мелодию, но тебя просят отправить смс - не спеши! Стоимость отправки sms на разные порталы очень отличается, поэтому, прежде всего, стоит посоветоваться с родителями.

4. **Установите антивирус.** Антивирусные программы помогут уберечь ваш компьютер от сомнительных файлов, а специальные почтовые фильтры предотвратят попадание спама на электронную почту. Такие программы останавливают вредоносные атаки.

5. **Не открывайте приложенные файлы.** Научитесь не открывать вложения, присланные с неизвестных адресов электронной почты: они нередко бывают вирусами.

6. **Интернет-мошенничество**. Не кликайте по подозрительным рекламным баннерам, предлагающим мгновенное обогащение или другие нереально выгодные услуги и сервисы. Скорее всего, вас пытаются обмануть.

7. **Интернет-хулиганство**. Если на ресурсе (в чате или игре) встретятся хулиганы, которые пишут грубые и неприличные вещи, необходимо сразу отключиться и вернуться позже либо перейти на другой ресурс. Вступать в диалог с ними нельзя.

8. **Интернет-зависимость. Нужно контролировать время провождения за компьютером, ведь он не может заменить реальный мир. Интернет-зависимость схожа с зависимостью от азартных игр. Она также характеризуется потерей ощущения времени, неумением вовремя остановиться, отрывом от реальности, раздражительностью и отчаянием по причине отсутствия возможности выхода в интернет.**

1. **Защитите свой компьютер:**
   - регулярно обновляйте операционную систему;
   - используйте антивирусную программу;
   - применяйте брандмауэр;
   - создавайте резервные копии важных файлов;
   - будьте осторожны при загрузке содержимого.
2. **Защитите себя в Интернет:**
   - с осторожностью разглашайте личную информацию;
   - думайте о том, с кем разговариваете;
   - помните, что в Интернет не вся информация надежна и не все пользователи откровенны.

**Правила относительно электронной почты:**

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого сразу удалите их, выбрав команду в меню сообщений.

2. Никогда не отвечайте на спам.

3. Применяйте фильтр спама поставщика услуг Интернета или программы работы с электронной почтой (при наличии подключения к Интернету).

4. Никогда не пересылайте «письма счастья». Вместо этого сразу удаляйте их.

**Учитель.** Сегодня на уроке вы познакомитесь с некоторыми терминами, которые вы, возможно, слышали, но не до конца знали, что они означают.

На столах у вас лежат термины, слова в них спутаны, ваша задача поставить слова в правильном порядке и сложить термин. После этого ребята читают и обсуждают термины, написанные у них на листочках.

ФИШИНГ — это особый вид мошенничества, цель которого — получить какую-либо секретную информацию, например авторизационные данные для выхода в Интернет, информацию о банковских счетах и кредитных картах.

Прежде всего важно понимать, что банки, системы денежных расчетов, почтовые и прочие сервисы и организации никогда не просят коды и пароли, которые они выдали клиентам. Банковские системы и технологии надежны, в них используется система резервирования важной информации, поэтому клиенты не должны верить утверждениям вроде «что-то пропало» или «необходимо что-то проверить». Любая информация о том, что у банка что-то случилось, может повредить его репутации, поэтому банк скроет проблему, а не будет рассказывать о ней. Проблема будет решаться тихо по мере обращения в службу поддержки.

КИБЕРБУЛЛИНГ — подростковый виртуальный террор, анонимное преследование, которое нередко приводит к реальным физическим столкновениям.

Как защитить себя от подобных атак?

Немаловажно научиться не делиться информацией личного характера в сети, не публиковать конфиденциальные данные. Излишняя откровенность в Интернете чревата. При этом важно помнить, что персональные сведения могут стать доступными ненамеренно: используя функции автозаполнения, разрешая приложениям отслеживать местоположение, заполняя графы с указанием адреса и телефона, вы подвергаете себя дополнительной опасности.

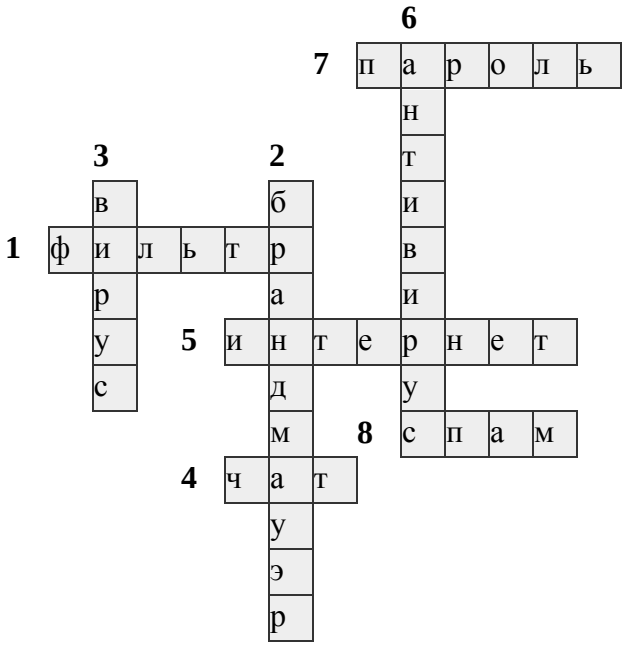
ФАРМИНГ - это перенаправление автоматически злоумышленниками пользователя Интернета на ложный сайт – правильную копию настоящего банка или сервисного торгового предприятия.

СПАМ-БОТ — это компьютерная программа или группа (пакет) компьютерных программ основной или единственной целью которой является автоматизированная рассылка рекламных сообщений — спама.

ДРО́ППЕРЫ — семейство вредоносных программ, предназначенных для несанкционированной и скрытой от пользователя установки на компьютер жертвы других вредоносных программ, содержащихся в самом теле дроппера или загружаемых по сети.

## III. Закрепление нового материала

**А для того что бы проверить, как вы запомнили**



**Вопросы к Кроссворду:**

1. Фильтр — компьютерная программа, выделяющая из данных только те, которые нужны пользователю.
2. Брандмауэр — это защитный экран между глобальным интернетом и локальной компьютерной сетью организации.
3. Ви́рус — вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по разнообразным каналам связи.
4. Чат — средство обмена сообщениями по компьютерной сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение.
5. Интернет –Всемирная информационная компьютерная сеть, связывающая между собой как пользователей компьютерных сетей, так и пользователей индивидуальных компьютеров для обмена информацией.
6. Антивирус - программа, которая находит и уничтожает компьютерные вирусы.
7. Пароль –секретная строка символов, предъявляемая пользователем компьютерной системе для получения доступа к данным и программам.
8. Спам – незапрашиваемые сообщения электронной почты, содержание которых может быть вредоносным и (или) мошенническим.

Итак, все угрозы в сети можно условно разделить на три группы.

**Первая** объединяет угрозы, связанные с общением в Интернете, — это виртуальный террор, пропаганда жестокости, экстремизма и нетерпимости, сетевая педофилия, контакты с сетевыми мошенниками, «киберсуицид» или согласованные самоубийства и прочее.

**Вторая** — нежелательный контент. К сожалению, он так многообразен, а порой чудовищен, что ограничение доступа к информации подобного рода принесло бы взрослым не меньшую пользу.

**Третья** — вредоносные программы, а именно вирусы, фишинговые атаки, спам-боты, дропперы и т.д.

И хотя Интернет это безграничное море возможностей, нужно не забывать, что он таит и много опасностей, поэтому нужно соблюдать все правила безопасной роботы в сети.

## IV. Итог урока

Учащиеся высказывают свое мнение, оправдались ли их ожидания от проделанной работы.
Оценка учащимися занятия

**Список используемой литературы**

1. Блинков И.А.: Безопасность детей и молодежи в сети Интернет.

2. Брошюра «Безопасность детей в Интернете» изд. Microsoft.

**Используемые материалы и Интернет-ресурсы**

1. https://my.mail.ru/mail/illari.sochi/video/_myvideo/1.html

2. http://www.youtube.com/watch?v=5YhdS7rrxt8

3. https://vseosvita.ua/library/deti-v-internete-bezopasnyj-internet-dla-detej-108171.html