Кибербезопастность.

Защита компьютера и информации.

Задача.

- Познакомить читателя с кибербезопаснотью. Объяснить простые правила для безопасности компьютера.

Введение: Информационное общество.

- В настоящее время человек живет в информационном обществе и активно участвует в информационных процессах. Вся жизнь человеческого общества зависит от информации. И нет ничего удивительного, что на безопасность информации может кто-то покушаться. Таким образом, перед обществом встает задача обеспечения информационной безопасности.

Введение: преступность

- Сегодня техническими возможностями компьютеров, их программным обеспечением, сетью Интернет, сотовой связью стремятся воспользоваться криминальные элементы, количество которых с каждым днем возрастает. По мнению специалистов, темпы роста преступности в глобальной сети Интернет являются самыми быстрыми на планете.

Что такое кибербезопасность?

- Начнем со знакомства понятия «кибербезопастность». Это совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействий с нежелательными последствиями. Другими словами, целью кибербезопастности является защита компьютерных устройств, информации, пользователя.

Интернет.

Со временем сеть становится все сложнее, в ней хранится все больше информации. компьютер может стать жертвой. Существуют две основные возможности:
Первое – вы сами, странствуя по различным сайтам или устанавливая программное обеспечение с непроверенных источников, а иногда и с проверенных, заражаете свой компьютер.

Неосторожное поведение пользователя - неосторожность пользователя – это серьезная проблема, которая ставит под удар даже самую защищенную систему, даже данные, которые расположены на отключенном от Интернета компьютере. Например, задавая слишком простой пароль для почтового ящика, вы делаете его взлом сравнительно легким, неприятны последствия случайного удаления важных данных.

Интернет: социальная сеть.

- Например, регистрируясь в какой либо социальной сети, где просят указывать верные личные данные- фамилия и имя. Просят заполнить личные данные о себе, просят поставить фотографию. Затем попросят указать номер телефона, вроде бы на случай если забудете пароль сайта. Вам будет выслан код для смены пароля. А некоторые просят ввести паспортные данные и находятся такие, кто вводит. Не нужно заполнять такие данные. Помните об этом.

Интернет:

Вирусы

- Второе – возможна также ситуация, когда злоумышленники преднамеренно, с помощью, например, троянских программ или вирусов, делают ваше устройство источником опасности.

- Компьютерные вирусы, сетевые и почтовые черви могут распространяться самостоятельно. Например, если вам приходит подозрительное электронное письмо с вложением – весьма высока вероятность того, что оно содержит компьютерный вирус, который может заразить некоторые файлы на вашем компьютере, испортить или украсть какие-нибудь данные. Троянские программы самостоятельно не распространяются, хотя они могут распространяться с помощью компьютерных вирусов. Их основные цели – красть и уничтожать Трояны и вирусы могут быть спрятаны в различных бесплатных, доступных для скачивания из интернета программах, которых огромное множество или на пиратских дисках, имеющихся в свободной продаже.

Интернет: хакеры.

- Хакеры стараются получить доступ к вашим электронным почтам, кошелькам, аккаунтам в социальных сетях, форумах. Или могут заблокировать работу операционной системы и потребовать деньги за устранение проблемы.

Статистика: общие сведения.

- Несмотря на то, что официальная статистика ведется по всем преступлениям (в том числе и не Интернет-преступлениям) в сфере компьютерной информации, среди них преобладают преступления, совершенные посредством Интернет. Это подтверждают некоторые региональные и общероссийские исследования. Например, в Республике Дагестан самым частым преступлением является неправомерный доступ к сети Интернет посредством чужих реквизитов (в 2003 г. – 100% от всех преступлений в сфере компьютерной информации)99. Следовательно, статистика по преступлениям в сфере компьютерной информации может быть использована для оценки характеристик Интернет- преступности

Статистика: преступления.

- Перед Вами Сведения о росте преступности в Интернете. Из донной таблицы следует сделать вывод: Получается, что число зарегистрированных преступлений данной категории выросло в 309 раз с 1997 по 2005 гг.

Сведения по России о количестве зарегистрированных преступлений в сфере компьютерной информации (Глава 28 УК РФ) за период 1997–2007 гг.

Год / Показатель	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Количество зарегистрир. преступлений	33	67	285	800	2072	4050	7549	8739	10214	8889	7236
Прирост в % по сравнению с предыдущим годом	-	103	325,4	180,7	159	95,5	86,2	15,9	16,9	-13	-18,6
Доля в % в зарегистрир. преступлениях	0,0013	0,003	0,01	0,027	0,07	0,07	0,27	0,3	0,29	0,23	0,2

Простые правила.

- Люди стали забывать о простых правилах, которые нужны для безопасности:
  Удаляйте сразу же все письма подозрительного содержания, не вздумайте открывать файлы из неизвестных источников. Игнорируйте все предложения легкого заработка, никому не высылайте свои пароли, не переходите по подозрительным ссылкам. Предпочитайте работать с платежными системами через их собственные приложения, а не через сайт. Это намного безопаснее.

Дети и Интернет.

- Все больше становиться количество детей, которые имеют выход в Интернет. И добавляется еще одна задача: обеспечить безопасность детей в сети Интернет. В ней есть очень много информации, доступа к которой у детей быть не должно. Они легко могут попасться на удочку опытного мошенника или злоумышленника. У многих есть меньшие братья или сестренки. Расскажите им несколько правил, которые следует соблюдать. Объясните, что в виртуальном пространстве не нужно никому называть свою фамилию, домашний адрес, номер школы. Посоветуйте не встречаться с друзьями из сети, так как ожидания могут быть обмануты, не верить всему тому, что им говорят/пишут. Расскажите, как соблюдать конфиденциальность. Установите программное обеспечение, блокирующее нежелательные сайты, не разрешайте без согласования с вами устанавливать любые программы. И не забывайте следить за тем, чтобы они не стали зависимыми от Интернета.

Интернет цензор.

- **Интернет цензор** — бесплатное программное обеспечение, которое блокирует доступ к плохим сайтам. Вам нужно установить программу и поставить пароль на вход в панель администрирования. Интернет цензор довольно серьезно относится к безопасности ребенка. Она полностью отключает доступ к социальным сетям, фото хостингам, файлообменнникам

Меры безопасности.

- Установите антивирусное и антишпионское программное обеспечение. Антивирусные программы должны быть свежими и регулярно скачивать базы с обновлениями через интернет. Антивирусное ПО должно запускаться автоматически при загрузке Windows и работать постоянно, проверяя запускаемые вами программы, в фоновом режиме. Обязательно проверяйте на вирусы перед первым запуском любые программы, которые вы где-либо скачиваете или покупаете. . Следует помнить, что любой антивирус замедляет работу компьютера, но для безопасности с этим стоит смириться. Производители антивирусов совершенствуют свою продукцию и сейчас это уже не так заметно, как это было раньше. Помимо того, что антивирус производит защиту компьютера в реальном времени, необходимо, не реже раз в месяц, проводить полную проверку компьютера и всех дисков. Нельзя устанавливать одновременно на компьютер два антивируса от разных производителей, они будут конфликтовать друг с другом.

Антивирус.

- Проверить файлы на компьютере можно и в Интернете, через онлайн-сканеры антивирусных компаний. Например, сервис VirusTotal проверяет файл с помощью 43 (на сегодняшний день) онлайновых программ.
- Следует помнить, что в Интернете существует множество фальшивых антивирусов. Вы наверняка встречали в Интернете такие всплывающие объявления, в которых написано, что ваш компьютер заражен. Фальшивые антивирусы находят на вашем компьютере множество вирусов и предлагают загрузить программу для лечения вашего компьютера. Эта программа сама затем станет источником вирусов

Я богат?

- Если вам сообщают, что вы стали миллионным посетителем сайта, предлагают планшетный ПК или другой приз в обмен на заполнение анкеты, а также рассказывают о быстром и легком способе заработать деньги или получить работу ("Узнайте, как быстро разбогатеть, работая у себя дома всего по два часа в день!"), будьте осторожны. Получив письмо о том, что вы что-то выиграли, а для получения приза вам достаточно указать личную информацию в анкете, не поддавайтесь соблазну и не заполняйте ее. Зачастую мошенникам достаточно того, что пользователь набрал данные в полях на сайте, не нажимая кнопку "Отправить". Помните: «бесплатный сыр только в мышеловке ».

Удаляем информацию.

- **Правильно удаляйте информацию**
- Представьте, что Вам прислали отчет. Вы его прочитали, сделали необходимые выводы и удалили его. А как Вы его удалили? Если Вы удалили отчет и оправили его в корзину, то его можно достать из корзины и изучить. Получается, что Вы удалили данные, но на самом деле они все еще есть на компьютере. Злоумышленники первым делом лезут в корзину, что бы найти там якобы удаленные данные. Всегда **удаляйте информацию, минуя корзину**. Для этого выберите нужные файлы и папки и нажмите “Shift” + “Delete”. Так данные не будут перемещены в корзину, а сразу удалятся. Восстановить их можно только с помощью специальных программ, но это займет много времени и не факт что их удастся восстановить.

Пароль.

- Используйте надежный пароль
- Первое и главное правило сохранности Ваших данных, учетных записей, почтовой пересылки это **надежный пароль**! Много раз хакеры взламывали страницы в социальных сетях или почтовые адреса из-за того, что пользователь ставил простой пароль. Вы ведь не хотите, что бы Ваши личную переписку узнал кто-то чужой?

Скачивание программ.

- Скачивайте программы либо с официальных сайтов разработчиков, либо с крупных торрент трекеров. Не скачивайте программы с подозрительных сайтов или с файлообменников. Так Вы уменьшите риск скачать вирус вместо программы. Не нажимайте на красивые баннеры или рекламные блоки на сайтах, какими бы привлекательными и заманчивыми они не были. В лучшем случае, Вы поможете автору сайта получить деньги, а в худшем — получите вирус. Не нажимайте на вплывающие окна, в которых написано, что Ваша учетная запись в социальной сети заблокирована. Это проделки злоумышленников! Если Вас вдруг заблокируют, Вы узнаете об этом, зайдя в эту социальную сеть, или администрация отправит Вам электронное письмо.

Заключение.

- Вот несколько простых правил, которые помогут Вам для защиты компьютера. Но запомните: никогда не становитесь зависимыми от Интернета и компьютера.