Секция «Компьютерное право и информационная безопасность»

Как защитить себя, свои данные и получать достоверную информацию в интернет пространстве

Научный руководитель – Гориленко Татьяна Васильевна

Леонов В.Е.[1], *Пидько Л.В.*[2]

1 - Передовая инженерная школа МГУ, Москва, Россия, *E-mail: LeonovVEvgenevich070809HiTiop@yandex.ru*; 2 - Передовая инженерная школа МГУ, Москва, Россия, *E-mail: lolita.pi1219@yandex.ru*

Департамент образования и науки города Москвы**Государственное бюджетное общеобразовательное учреждение города Москвы «Школа №2010 имени Героя Советского Союза М. П. Судакова»**

Кибербезопасность — сфера деятельности, занимающаяся защитой компьютерных систем, сетей, программ и данных от киберугроз, включая хакерские атаки, вирусы, вредоносное программное обеспечение и другие цифровые угрозы.

Взлом аккаунта в соцсетях — это получение злоумышленниками доступа к учётной записи пользователя с различными целями.

Фишинг — это разновидность онлайн-мошенничества или кибератаки, при которой злоумышленники пытаются украсть личную информацию пользователей.

Режим инкогнито — это режим безопасного просмотра в браузере, который позволяет держать в секрете поисковые запросы и посещения сайтов.

Нормативно – правовые акты:

Федеральный закон 152 «О персональных данных» данных» . **Федеральный закон Российской Федерации «О персональных данных»** .**Дата принятия**:8 июля 2006 года (принят Государственной Думой), 14 июля 2006 года (одобрен Советом Федерации) . **Был опубликован** на разных источника , таких как: **«Российская газета»**, №165, 29 июля 2006 года; **«Парламентская газета»**, №126–127, 3 августа 2006 года; **«Собрание законодательства Российской Федерации»**, №31 (часть I), 31 июля 2006 года, статья 3451. :

• Перед сбором и обработкой персональных данных нужно спрашивать согласие их владельца.

• Для защиты информации закон обязывает собирать персональные данные только с конкретной целью.

• Если вы собираете персональные данные, то обязаны держать их в секрете и защищать от посторонних.

• Если владелец персональных данных потребует их удалить, вы обязаны сразу же это сделать.

Федеральный закон 149 «Об информации, информационных технологиях и о защите информации» . **Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации»**. **Дата принятия**: Государственная Дума приняла закон 8 июля 2006 года, Совет Федерации одобрил 14 июля 2006 года. **Место публикации**: текст закона был опубликован в **«Российской газете»** под номером 165 29 июля 2006 года, а также в **«Парламентской газете»** под номерами 126–127 3 августа 2006 года и в **«Собрании законодательства Российской Федерации»** под номером 31 (часть I) 31 июля 2006 года. :

• Нельзя собирать и распространять информацию о жизни человека без его согласия.

• Все информационные технологии равнозначны — нельзя обязать компанию использовать какие-то конкретные технологии для создания информационной системы.

• Есть информация, к которой нельзя ограничивать доступ, например сведения о состоянии окружающей среды.

• Тот, кто хранит информацию, обязан ее защищать, например, предотвращать доступ к ней третьих лиц.

• Некоторую информацию распространять запрещено, например ту, которая пропагандирует насилие или нетерпимость.

• У государства есть реестр запрещенных сайтов. Роскомнадзор может вносить туда сайты, на которых хранится информация, запрещенная к распространению на территории РФ.

Актуальность: Рост числа киберугроз и утечек информации создают серьезные угрозы для пользователей интернета. Масса людей подвергаются проблеме утечки личной информации из-за невнимательности или неопытности. Знание способов защиты личной информации позволит обезопасить себя от хакерских атак и защитить свою конфиденциальность. В России был проведён «Цифровой диктант», определяющий уровень цифровой грамотности населения. В этом мероприятии приняли участие 2,1 миллиона человек. Средний балл цифровой грамотности составил 6,65/10, что является неплохим результатом, но указывает на наличие пробелов в знании и понимании цифровых технологий. Этот диктант стал важным стимулом для проведения исследовательской работы в области цифровой грамотности.

Объект исследования: интернет как средство получения информации.

Предмет исследования: защита от киберугроз, безопасность данных, а также конфиденциальность пользователей интернет пространства.

Гипотеза: Современные подростки не осведомлены о возможных способах защиты в интернет пространстве.

Цель: повысить осведомленность пользователей интернета, обучить техническим методам защиты от угроз и использованию интернета для поиска достоверной информации.

Задачи:

1. Составить и провести социальный опрос
2. Изучение информации, включая нормативно-правовые акты
3. Провести квиз по цифровой грамотности среди учеников школы 2010
4. Определить уровень цифровой грамотности учеников
5. Составить рекомендации по использованию интернет ресурсов

Методы исследования: Поиск, изучение и анализ информации, проведение опроса, выявление и разрешение способов решения поставленной проблемы.

Практический выход: Результаты данной работы можно использовать на уроках, в соцсетях, на различных сайтах.

2.Результаты социального опроса

По итогам социального опроса: Большинство опрошенных (48%) используют мобильные устройства более 5 часов в день, что указывает на высокую степень зависимости от технологий, особенно среди молодежи в возрасте от 16 до 18 лет.

Некоторые упомянутые сайты(а именно: www.liveinternet.ru, https://my.mail.ru, https://www.youtube.com) находятся в реестре запрещенных ресурсов, что может говорить о рисках, связанных с их использованием. Одним из вариантов ответов была неверная ссылка(https://ru.wikipedia.org).

Большинство пользователей считают, что найти нужную информацию в интернете легко или скорее легко (76%). Это говорит о высоком уровне уверенности в своих навыках поиска.

Половина опрошенных сообщила о том, что их аккаунты в соцсетях когда-либо взламывались. Это подчеркивает важность повышения осведомленности о безопасности.

Подростки в возрасте 16-18 лет более осведомлены о возможных угрозах и методах защиты от них, по сравнению с опрошенными до 15 лет. Это связано с их большим опытом использования цифровых технологий и интернета.

3. Практический выход

В рамках проектной деятельности был проведен квиз среди учеников школы 2010 (Раздавались задания на листах). В квизе по цифровой грамотности приняли участие учащиеся 7, 8, 10 и 11 классов. Результаты показали разный уровень знаний и понимания темы среди классов.

- Большая часть учащихся 7 класса продемонстрировала хорошее знание цифровой грамотности. Однако некоторые из них столкнулись с трудностями в восприятии текста и понимании смысла предложений. В тестовой части была зафиксирована всего одна ошибка
- В 8 классе ситуация оказалась более сложной. Большинство учеников не знают основ цифровой грамотности. Это связано с неправильными ответами и плохим пониманием ситуации. В данной группе было допущено 7 ошибок в тестовой части.
- В 10 классе большинство учащихся показали хорошие знания по теме. Некоторые ошибки были связаны с отсутствием ответов. Зафиксирована всего одна ошибка в тестовой части.
- Результаты 11 класса не так однозначны. Половина учащихся продемонстрировала хорошее владение материалом, в то время как другая половина допустила значительное количество ошибок. В этом классе также было зафиксировано 7 ошибок в тестовой части.

Задания квиза

1. Выберите наиболее правильное утверждение:

а) Достаточно установить антивирус, чтобы быть уверенным в безопасности своих данных.

б) Хранить пароли в браузере безопасно, если не использовать общедоступные компьютеры.

в) Фишинговые письма - это письма от знакомых, которые просят о помощи.

г) Проверять достоверность информации, особенно с новостных сайтов, важно для формирования собственного мнения.

2. Какое из действий НЕ является правильным для защиты личных данных в интернете?

а) Использовать сильные и уникальные пароли для разных аккаунтов.

б) Отключать геолокацию на устройствах, если она не нужна.

в) Открывать вложения в письмах от неизвестных отправителей.

г) Избегать публикацию личной информации в социальных сетях.

3. Вы сидите в социальных сетях и в ленте вам попадается реклама, предлагающая бесплатный подарок, скидку или другую интересную возможность. Реклама ведёт вас на сайт, который выглядит так же, как и сайт известной компании. На сайте вам нужно ввести свои персональные данные для получения желаемого подарка. Что вы будете делать в данной ситуации?

4. Вы пришли работать/учиться в кофейню, сделали заказ и заметили, что ваш интернет работает плохо. Вы решили подключиться к незащищенной сети с привлекательным

названием "Free Wi-fi". Вскоре вам приходит уведомление о списании средств с вашего счета. Как такое возможно? Как можно было избежать данной ситуации?

5. В интернете вы нашли онлайн-магазинкоторый продает брендовую одежду со скидками до 50%. Вы увидели шикарную рубашку и, решив не терять времени, купили её. При оформлении заказа вы указали свои ФИО, номер телефона, реквизиты вашей банковской карты и адрес доставки. Правильно ли вы поступили? Есть ли опасность в ваших действиях?

Результаты квиза получились следующими:

7 класс

- 75% Верно ; 25% Неверно

8 класс

- 50% Верно ; 50% Неверно

10 класс

- 78% Верно ; 22% Неверно

11 класс

- 65% Верно ; 35% Неверно

Наибольшее количество ошибок допустил 8 класс, поэтому в нем была проведена работа (урок по цифровой грамотности) по анализу и исправлению ошибок. После её проведения средний балл учащихся составил 9,2/10

План урока по «Цифровой грамотности»:

1) Введение (с указанием целей и объяснением важности работы)
2) Основные понятия
3) Обсуждение возможных интернет-угроз
4) Рекомендации по теме
5) Практическое задание

Средний балл по результатам квиза учеников школы 2010 составил 6,7/10. Данные показывают, что школа демонстрирует хорошие результаты, но тем не менее стоит обратить внимание на возможности для дальнейшего улучшения осведомленности всех учеников.

4. Рекомендации

Некоторые способы повысить цифровую грамотность:

Прочитать книги по цифровой грамотности«Компьютер без напряга. Энциклопедия», «1001 совет по обустройству компьютера»

Пройти бесплатные курсы «Белый хакер» от SkillFactory и «Профессия "Специалист по кибербезопасности» от Skillbox

Пройти платные курсы «Специалист по информационной безопасности: старт карьеры» от «Нетологии» и «Курс по анонимности и безопасности в сети» от Cyber Yozh Academy

Почитать познавательные сайты

От сайта Dropbox

https://experience.dropbox.com/ru-ru/resources/protecting-personal-info-online

От сайта Kaspersky

https://www.kaspersky.ru/resource-center/threats/internet-and-individual-privacy-protection

Для эффективной защиты себя и своих данных необходимо соблюдать несколько ключевых рекомендаций:

1. Используйте сложные пароли: Создавайте уникальные пароли для разных аккаунтов, состоящие из комбинации букв, цифр и символов. Используйте менеджеры паролей для их хранения.

2. Двухфакторная аутентификация (2FA): Включите 2FA на всех доступных платформах. Это добавит дополнительный уровень защиты к вашим аккаунтам.

3. Ограничьте личную информацию: Не делитесь излишней личной информацией в социальных сетях. Настройте параметры конфиденциальности, чтобы контролировать, кто видит ваши данные.

4. Будьте осторожны с публичными Wi-Ficетями: Избегайте входа в важные аккаунты (например, банковские) через общедоступные сети.

5. Осторожно с подозрительными ссылками: не переходите по ссылкам из неизвестных источников и не загружайте файлы от ненадежных отправителей

6. Проверяйте адреса сайтов: убедитесь, что вы находитесь на официальном сайте, особенно при вводе личной информации или финансовых данных. Обратите внимание на «https://» в адресной строке.

7. Обновляйте программное обеспечение: регулярно обновляйте операционную систему, антивирусные программы и приложения, чтобы защититься от уязвимостей.

8. Проверяйте источники: Используйте надежные и авторитетные источники информации. Обращайте внимание на репутацию сайта и его авторов.

9. Обращайте внимание на дату публикации: убедитесь, что информация актуальна и не устарела.

10. Развивайте критическое мышление: не принимайте информацию на веру только потому, что она популярна или распространена.

Заключение

В условиях современного цифрового мира защита личных данных и получение достоверной информации становятся крайне важными аспектами для пользователей. Подростки, большая часть жизни которых проходит в цифровом мире должны уделять внимание своей безопасности в нем.

Гипотеза была подтверждена частично.

Большинство прошедших опрос знают основные методы защиты от интернет-угроз, но тем не менее многих из них взламывали в соцсетях. Это может свидетельствовать о том, что базовых знаний по кибербезопасностинедостаточно для защиты от современных угроз.

Цифровые технологии развиваются стремительно, и злоумышленники постоянно совершенствуют свои методы, обходя стандартные меры безопасности. Простой набор базовых знаний, быстро устаревает и становится неэффективным. Необходимо постоянно совершенствовать свои знания и навыки, чтобы оставаться защищенным.

Источники и литература

1) Статьи на сайте Kaspersky (https://www.kaspersky.ru/resource-center/threats/internet-and-individual-privacy-protection)
2) Сайт Цифровой Ликбез (https://digital-likbez.datalesson.ru)
3) Сайт SecurityLab (https://www.securitylab.ru)