

Научно-исследовательская работа

предмет: Информатика

**БЕЗОПАСНОСТЬ В СЕТИ ИНТЕРНЕТ:
КАК ЗАЩИТИТЬ СВОИ ЛИЧНЫЕ ДАННЫЕ**

Выполнил:

Слепцов Данил Михайлович

учащийся 5 класса

МБНОУ "Октемский научно-образовательный центр им. М.Е. Николаева"

Руководитель:

Абрамов Евгений Семенович

заместитель директора по дополнительному образованию

МБНОУ "Октемский научно-образовательный центр им. М.Е. Николаева"

Введение

Актуальность моего исследования заключается в том, что на сегодняшний день вопрос о безопасности стоит на первом месте. Безопасность использования интернета, информационных и коммуникационных технологий является одной из самых актуальных и важных тем современности.

Объект исследования: личные данные

Предмет исследования: приложения для защиты личных данных

Цель исследования: Определить, как защититься от вирусов, нежелательного контента в интернете и научиться как правильно защитить свои данные.

Задачи:

- найти приложения для безопасности
- сравнить приложения для безопасности
- выявить плюсы и минусы найденных приложений
- сделать опрос населения по выявлению грамотности в сфере информационной безопасности
- сделать анализ опроса
- собрать группу для апробирования найденных приложений
- собрать обратную связь
- по итогам анализа обратной связи написать рекомендации по информационной безопасности для детей
- для большого охвата сделать видео в youtube shorts
- разработать тренажер создания паролей разных сложностей
- сделать выводы

Основная часть

Количество онлайн пользователей с каждым годом растёт, и использование различных онлайн услуг и сервисов становится обычной практикой. Но также и увеличивается количество мошенников, которые желают завладеть вашими средствами и данными. Я нашел 4 приложения, которые помогают защитить личные данные:

1. Phone Guardian
2. AppLock
3. Cleaner AI
4. McAfee Security

И сделал сравнительный анализ приложений.

	Phone Guardian	AppLock	Cleaner AI	McAfee Security
Плюсы	Быстрый запуск Не требует аккаунт Защищает от мошенников подключение к интернету	можно спрятать и защитить фотографии	блокировка звонков по номеру, защита файлов, секретная папка, батарея.	проверка обновления, проверка утечки почты, защита от угроз
Минусы	нужно включить VPN только один функционал	есть реклама	просит купить много раз,	просить купить, больше функционала в платном

Для того, чтобы определить, что население знает о приложениях защиты личных данных, я провел опрос в социальной сети. Всего приняло участие 86 респондентов.

При обработке результатов выяснилось следующее:

1. более 70% опрошенных забывают данные авторизации (логины, пароли)
2. около 80% респондентов звонили мошенники
3. 12% опрошенных были подвергнуты атакам кибер-мошенников (взлом аккаунтов)
4. очень мало людей хранят свои личные данные в конфиденциальности и знают приложения по безопасности.

Это говорит о том, что нам нужно более серьезно отнестись к информационной безопасности. Поэтому я собрал группу для апробирования найденных приложений. Они скачали приложения и должны в течении недели пользоваться этими приложениями.

Проведенное исследование обратной связи от респондентов и апробаторов привело меня к мысли создать рекомендации по защите в интернете для детей. Из сайта учителя информатики [1] я выявил некоторые советы:

Договоритесь с ребенком о подходе

Зачастую бывает полезным договориться с ребенком о принципах предоставления личной информации в Интернете. Если ребенку разрешается предоставление подобной информации, необходимо знать о надежности сайтов, на которых предоставлялись сведения.

Ознакомьтесь с политикой защиты конфиденциальной информации

Мы советуем каждый раз проверять, прилагается ли к используемой службе соответствующая политика защиты конфиденциальной информации, в которой должен объясняться способ использования личной информации, время и цели ее использования.

Предоставляйте только обязательную информацию

Как правило, требуется указывать только небольшой объем обязательной информации. При подписке на новую услугу ее поставщик обычно запрашивает разрешение на осуществление прямого маркетинга. В самом начале от этого можно отказаться, но в случае непреднамеренного согласия его можно отменить, обратившись к поставщику услуг. Если планируется предоставление личных сведений в Интернете, рекомендуется создать семейный адрес электронной почты для использования взрослыми и детьми.

Не сохраняйте личную информацию в обозревателе

Личную информацию или пароли не рекомендуется сохранять в обозревателе Интернета или других программах, которые подключены к Интернету.

Публикация фотографий и личной информации детей

Публикация в Интернете фотографий, снятых на камерофон или цифровую фотокамеру, осуществляется просто и быстро. При публикации в Интернете фотографии очень сложно предотвратить ее распространение, изменение и использование в различных контекстах. Копии фотографий могут легко оказаться в нескольких местах, и их полное удаление может оказаться очень трудным делом. Дважды подумайте, прежде чем публиковать личную информацию вместе с фотографией.

Публикация чьей-либо фотографии или другой личной информации, например, на веб-сайте школы, подразумевает разглашение личной информации, что всегда требует согласия данного человека. Любой разглашающие личную информацию также имеет право на ее проверку и, при необходимости, исправление. Детей необходимо предостеречь от публикации личной информации на собственных веб-сайтах или в интерактивных дневниках (блогах).

Чтобы донести эти советы с привлечением большой аудитории я решил сделать короткое видео в youtube shorts. Готовое видео можете посмотреть по ссылке <https://youtube.com/shorts/0VqJUZ3qXHw?si=IeK4kAzrVJoYvXH7>, в данное время посмотрело более 700 человек и собрано 103 лайка.

Разработка тренажера создания паролей

По итогам опроса, среди вопросов было: "Где вы храните свои пароли?", ответы на который примерно такие: в голове, в заметках, в блокноте, в уме. Что показывает, что мы небезопасно храним свои пароли.

На большинстве современных сайтов требуются не простые пароли. Пароль должен содержать цифры, буквы и специальные символы. Чтобы создавать такие пароли нам нужно знать какие пароли сайты считают "простыми", а какие "сложными". Чтобы решить эту задачу мы с моим учителем решили создать тренажер создания паролей разной сложности с использованием языков программирования HTML, CSS, Java Script.

Тренажер выполнен в игровой форме. Чтобы спасти главного героя - смайлика - вам нужно придумать определенной сложности пароль. Готовую игру можете найти по адресу: <https://oktemsec.ru/password-trainer> .

Заключение

Опрос населения вывел, что грамотность в сфере информационной безопасности, мягко говоря, низкая. В ходе исследовательской работы я нашел приложения для повышения безопасности телефонов. Сделал сравнение этих приложений и выявил плюсы, минусы с помощью группы апробирования. В итоге создал видео о рекомендациях по защите в интернете для детей.

Список литературы

1. Сайт учителя информатики Гончара Михаила Васильевича
<http://inf.kalga.edusite.ru/p9aa1.html>
- 2.