Муниципальное общеобразовательное административное учреждение

«Средняя общеобразовательная школа №86»

**Пояснительная записка**

к проекту по элективному курсу "Компьютерная графика"

**«Знакомство с основами безопасности в интернете»**

Работу выполнил ученик 11Т класса: Шарков Марк

Руководитель проекта: Спивак Татьяна Юрьевна

Оренбург

2024

**Содержание:**

Оглавление

[Введение 3](#_Toc133606206)

[Глава 1. Теоретическая часть 7](#_Toc133606207)

[Глава 2. Разработка сайта 14](#_Toc133606208)

[Заключение 17](#_Toc133606209)

[Список использованной литературы 18](#_Toc133606210)

[Приложение А 19](#_Toc133606211)

[Приложение Б 20](#_Toc133606212)

[Приложение В 21](#_Toc133606213)

# Введение

 Мы пользуемся смартфонами, компьютерами, планшетами – все они собирают информацию об использовании. Мы оплачиваем покупки в онлайн-банках, бронируем билеты и общаемся с друзьями онлайн. Дети делают домашнее задание онлайн. В интернете мы работаем, общаемся и даже ищем вторую половинку.

 Интернет-пространство меняется с бешеной скоростью, а проблемы с приватностью данных усугубляются.

 Информация – это деньги. Это главная причина, по которой вашим личным данным угрожает опасность.

 В целом, проект по безопасности в интернете помогает пользователям стать более осведомленными о возможных угрозах, предоставляет им необходимые знания и инструменты для защиты себя в онлайн-среде и, следовательно, повышает безопасность в интернете.

Актуальность проекта

 Проект по теме "Интернет безопасность и интернет угрозы, безопасная работа в интернете" в настоящее время является крайне актуальным. Постоянно растущее число пользователей Интернета на всем мире, необходимость постоянной работы в онлайн-среде в связи с расширением списка доступных на аудитории услуг онлайн, всё это делает Интернет одним из главных источников информации и коммуникации в современном обществе.

 В наше время кибератаки, вирусы, хакерские атаки и другие интернет-угрозы стали повседневной реальностью жизни в интернете. Эти угрозы могут нанести серьезный ущерб как физической, так и финансовой безопасности пользователей интернета.

 Проект по безопасности в интернете позволяет обучить пользователей Интернета основам безопасной работы в онлайн-среде и как уберечь себя от возможных угроз.

Проблема

 Отсутствие знаний у пользователей в интернет безопасности. Недопонимаем важности основ безопасности в интернете таких как: защита паролей, безопасный выбор программного обеспечения, антивирусы и многое другое.

Объект

 Безопасность в интернете.

Предмет

 Исследование угроз и способов их решения для безопасности в интернете.

Цель исследования

 Рассмотреть часто-встречающиеся угрозы в интернет пространстве, создать рекомендации для обеспечение безопасности.

Задачи

* Рассмотреть возможные угрозы в интернете
* Узнать разнообразие и классификацию интернет угроз
* Разработать рекомендации для безопасного пользования
* Создать сайт с информацией по теме проекта

Степень разработанности проблемы

 Данная тема с каждым днем становится все более актуальной, поэтому в Интернете можно найти целое множество проектов.

Методы

* Классификация
* Поиск
* Анализ

Методики моего проекта

* Теоретическая часть
* Практическая часть

Практическая значимость проекта

 Продукт, предоставленный в этом проекте, содержит информацию о том, как обезопасить себя в интернете.

Предполагаемы результаты

 В ходе моего проекта я планирую создать сайт на котором расскажу о распространенных угрозах в наше время и методах их решения.

Проектный продукт

 Проектным продуктом моего исследования является сайт с рекомендациями.

Портрет целевой аудитории

 Целевой аудиторией моего проекта являются родители и дети в возрасте от 8 и более лет.

Конкуренты (аналоги). Конкурентное преимущество

 В интернет пространстве присутствует довольно больше количество сайтов по данной теме, но в них достаточно лишний информации несвязанной с темой.

Ресурсная карта



Смета расходов



# Глава 1. Теоретическая часть

1.1 Что такое интернет безопасность?

 Интернет безопасность - это совокупность мер, направленных на защиту пользователей в сети Интернет от различных видов киберугроз. Это тема одновременно и проста и сложна, ведь в чем заключается сложность просто установить антивирус на свой ПК, но на самом деле все не так легко как кажется по началу. Проще говоря, интернет безопасность – это процесс соблюдения определенных правил и мер, с целью обеспечить свою безопасность в сети. [6]

1.2 История развития интернет безопасности

 В начале 90-х годов компания Netscape Communications Corporation создала SSL/TLS протоколы для обеспечения безопасной передачи данных в Интернете. Протокол Secure Sockets Layer (SSL) был разработан корпорацией Netscape Communications для обеспечения аутентификации, целостности и секретности трафика на сеансовом уровне модели OSI.  В январе 1999 года на смену SSL v3.0 пришел протокол TLS vl.O (Transport Layer Security) последняя версия TLS v.1.2 описывается в RFC 5246. С точки зрения выполняемых действий, различия между этими протоколами SSL и TLS весьма невелики, в то же время, они несовместимы друг с другом.

 SSL обеспечивает защищенное соединение, которое могут использовать протоколы более высокого уровня — HTTP, FTP, SMTP и т. д. Наиболее широко он используется для защиты данных, передаваемых по HTTP (режим HTTPS). Для этого должны использоваться SSL-совместимыс web-ссрвср и браузер.

 Протокол предусмагривает два этапа взаимодействия клиента и сервера:

1) установление SSL-ссссии (процедура «рукопожатия», от англ, «handshake»), на этом этапе может производиться аутентификация сторон соединения, распределение ключей сессии, определяются настраиваемые параметры соединения;

2) защищенное взаимодействие.

 Затем появились первые антивирусы, которые защищали пользователей от заражения вирусами, троянами и другими злонамеренными программами.

 В 2002 году правительство США начало разработку стандарта безопасности данных в Интернете - HIPAA, который был создан для защиты медицинской информации. В 2004 году был создан стандарт PCI DSS(1), который регулирует обработку данных, связанных с платежными картами.

(1) PCI DSS (Payment Card Industry Data Security Standard) — стандарт безопасности данных индустрии платежных карт.

1.3 Какими были первые антивирусы?

 Несмотря на то, что еще в 1961 году была создана игрушка Darwin для компьютеров IBM 7010, которую многие называют прообразом первого вируса, история создания вирусных и антивирусных программ началась еще в начале 70-х годов XX века.
 Именно тогда мало кому известный, но очень талантливый программист Боб Томас сумел создать прототип первого электронного вируса. Он назвал его The Creaper, а сама идея программы возникла у него на фоне интереса к вопросу касаемо возможности существования самовоспроизводящихся программ, которые способны перемещаться с одного компьютерного устройства на другое.
 А если ты создаешь прототип вируса, то должен создать и первый прототип антивируса, который должен справляться с ним, выявлять такой софт и прекращать его работу.
 **Именно поэтому Томасом была придумана еще одна разработка – антивирус Reaper. Его ключевыми функциями были:**

* Поиск вируса The Creaper.
* Нейтрализация этой программы, прекращение работы этого софта.

 Но несмотря на то, что Боб Томас внес невероятный вклад в развитие программ, предшествовавших возникновению первых полноценных антивирусов, он был всего лишь разработчиком первых прототипов вирусного и антивирусного ПО.
 Уже в 80-е годы появились первые полноценные антивирусные программы, которые были придуманы такими людьми как Энди Хопкинс (две разработки под названием BOMBSQAD и еще CHK4BOMB). А спустя всего лишь год специалист по имени Джи Вонг сумел придумать программу DRPROTECT, появившуюся в 1985 году и блокировавшую все операции, осуществляемые сторонними приложениями и софтом через BIOS.
 К тому времени вирусные угрозы были уже вполне реальными, а не возникающими по воле программистом в специализированных лабораториях и научно-исследовательских комплексах.

1.4 Виды угроз в интернете

 В современном цифровом мире угрозы в интернете стали огромной проблемой для миллионов пользователей по всему миру. Угрозы в интернете могут быть множественными и разнообразными, и благодаря технологическому прогрессу они постоянно обновляются и усложняются. Однако можно выделить несколько основных типов угроз в интернете:

* Вирусы и вредоносные программы - это программы, которые могут повредить компьютеру и украсть личные данные пользователя. Они могут распространяться через электронную почту, сайты и другие устройства
* Фишинг – это одна из наиболее распространенных угроз в интернете, которая включает атаки на выходы пользователей в Интернет с целью получения их личных данных, таких как пароли, номера карты и другие конфиденциальные данные. Криминальные элементы умело маскируют свои сайты.
* Программные вымогатели — это злонамеренные программы, которые блокируют доступ к файлам на вашем компьютере и требуют оплату для их восстановления. В большинстве случаев, когда программа была успешно запущена на вашем компьютере, вы увидите сообщение, указывающее, что ваши данные были зашифрованы.
* Вредоносная реклама - это способ распространения вредоносных программ через контекстную рекламу, которая используется на сайтах и в приложениях. Когда пользователь посещает веб-страницу или использует приложение, вредоносная реклама может перенаправлять пользователя на нежелательные сайты или устанавливать вредоносное ПО на компьютер пользователя.

Принимая во внимание эти и другие варианты угроз в интернете, пользователи должны уделять большое внимание своей безопасности, соблюдать предосторожность, использовать антивирусное ПО, никогда не делиться личными данными, если не уверены в безопасности соединения, и действовать аккуратно в сети. [6]

1.5 Методы защиты в интернете

 Антивирус – это специальное программное обеспечение, которое защищает компьютер от вирусов, троянов, червей и других вредоносных программ. Его задача заключается в обнаружении и нейтрализации угроз на компьютере. Несмотря на то, что антивирус не гарантирует 100% защиту, он является ключевым инструментом в поддержании безопасности в интернете и на других площадках.

 Влияние антивируса на безопасность в интернете заключается в следующем:

1. Обнаружение вредоносных программ: Антивирус сканирует файлы, скачиваемые из интернета на предмет наличия вредоносных элементов. Он способен обнаружить и блокировать многие виды вирусов и троянов.
2. Предотвращение фишинговых атак: Антивирус может также предотвращать фишинговые атаки. Они могут прийти в виде электронных писем или на фиктивных сайтах, которые могут запрашивать вашу личную информацию. Антивирус может идентифицировать и блокировать вредоносный контент и помочь избежать опасности.
3. Обновление базы данных: Антивирусное ПО должно регулярно обновлять свою базу данных, чтобы знать о наиболее новых и опасных вирусах. Эти обновления содержат информацию о новых угрозах, которые могут угрожать вашей безопасности. Этим образом, антивирус помогает контролировать и предотвращать новые угрозы, удерживая вашу систему в безопасности.

 При использовании сайтов с постоянным шифрованием данных (HTTPS) обеспечивается безопасность передачи информации между вашим устройством и сервером сайта.

 HTTPS - это протокол, который обеспечивает безопасность передачи данных с помощью шифрования. Когда вы вводите личную информацию на сайте, например, логин и пароль, ваш браузер шифрует эту информацию, что делает её недоступной для посторонних. [5]

Но не только это делает HTTPS наиболее безопасным протоколом для передачи данных в интернете. Включение SSL-шифрования обеспечивает дополнительные преимущества:

1. Защита от межсетевых атак: внедрение SSL-шифрования может помочь защитить ваш сайт от атак типа Man-in-the-middle, при которых злоумышленник пытается перехватить данные, передаваемые между браузером и сервером. [1,5]

2. Верификация сервера: SSL-сертификат связывает определенный домен с конкретным сервером, подтверждая тем самым, что посетитель находится на том сайте, где ему полагается находиться. [1,5]

3. Усиление доверия к сайту: наличие SSL-сертификата и отображение зеленого замка в адресной строке браузера, обозначающего защищенное соединение, поднимает уровень доверия пользователей к сайту. [1,5]

 Двухфакторная аутентификация является одним из наиболее эффективных способов защиты аккаунтов и данных пользователей в интернете. Этот процесс требует от пользователя ввода двух подтверждающих факторов для доступа к конкретной учетной записи или веб-ресурсу. Это могут быть пароль и код, отправляемый на мобильный телефон пользователю в режиме реального времени, отпечаток пальца и пароль, или ответ на контрольный вопрос и отпечаток пальца. [7]

 Вот несколько причин, почему важно использовать двухфакторную аутентификацию для безопасности в интернете:

1. Безопасность: сразу после появления в интернете личных данных ваши аккаунты могут быть скомпрометированы. Двухфакторная аутентификация обеспечивает более высокий уровень безопасности, чем обычная аутентификация паролем.

2. Защита от взлома пароля: Даже если злоумышленник поймает ваш пароль, а также другую конфиденциальную информацию, ему все равно будет трудно получить доступ к учетной записи, если вы используете двухфакторную аутентификацию.

 Когда дело касается защиты от программ-вымогателей, профилактика лучше лечения. Для этого очень важна **внимательность** и использование [**надлежащих программ обеспечения безопасности**](https://www.kaspersky.ru/total-security). Поиск уязвимостей также помогает обнаружить злоумышленников в вашей системе. Во-первых, важно убедиться, что ваш компьютер не является целью для программ-вымогателей. Программное обеспечение устройства необходимо регулярно обновлять, чтобы пользоваться **последними исправлениями безопасности**. Кроме того, очень важно соблюдать осторожность, особенно в отношении мошеннических веб-сайтов и вложений в сообщения электронной почты. Но даже самые лучшие превентивные меры могут потерпеть неудачу, поэтому очень важно иметь план действий на случай непредвиденных обстоятельств. В случае с программами-вымогателями план действий для непредвиденных обстоятельств заключается в **создании резервной копии данных**. [1]

# Глава 2. Разработка сайта

1.1 Выбор платформы для создания сайта

 Был произведен выбор платформы, на которой будет создаваться сайт. Выбор происходил между двумя конструкторами: AdvantShop и uKit. [4]

 AdvantShop — это конструктор для создания различных типов сайтов: интернет-магазинов, лендингов, корпоративных сайтов, мини-каталогов, квизов, страниц с возможностью бронирования.

 В AdvantShop все настроено для онлайн-продаж и привлечения посетителей: интеграции с маркетплейсами, социальными сетями, сервисами доставки и оплаты, SEO-оптимизация, бонусная программа и многое другое. Также внутри AdvantShop можно запустить собственное мобильное приложение компании.

**Редактор**: Выбирайте подходящий дизайн для вашего типа сайта и редактируйте цвета, фото и тексты по своему усмотрению.

**Специализация**: интернет-магазины, лендинги, воронки, опросники.

**Шаблоны**: внутри платформы есть 74 готовых шаблона для разных типов сайтов и ниш.

**Плюсы**:

* отличная техническая поддержка, которая поможет как настроить сайт с нуля, так и в дальнейшем решить возникающие вопросы;
* конструктор развивается, постоянно появляются новые функции и модули;
* подходит для новичков: для создания полноценного сайта не нужны навыки программирования;

**Минусы**:

* нужно время на изучение;
* часть шаблонов и модулей оплачиваются отдельно;

**Цена**: есть пробный период — 14 дней. Далее тариф зависит от того, как вы оплачиваете сайт – ежемесячно или за 1 год.

 uKit - конструктор сайтов для малого бизнеса. Он позволяет быстро создавать привлекательные и функциональные веб-страницы, используя профессиональные шаблоны и готовые блоки с разными элементами интерфейса. Для работы с его визуальным редактором не требуются специальные навыки — только время на то, чтобы наполнить страницы уникальным контентом. [2,3]

 Простота — одно из основных преимущество конструктора uKit. Он предлагает несколько встроенных инструментов, помогающих начинающему вебмастеру создать, который понравится и посетителям, и поисковикам. [2,3]

 Для решения первой задачи используется жёсткая вёрстка и автоматическое исправление ошибок. В редакторе физически невозможно сделать так, чтобы элементы интерфейса наезжали друг на друга или как-то иначе мешали взаимодействовать с ними пользователю. Для поисковой оптимизации конструктор предлагает систему проверки готовности сайта к публикации с выдачей рекомендаций по оптимизации.

 uKit — один из лучших конструкторов для быстрого старта. Он поможет в короткий срок создать сайт, который внешне не будет отличаться от проекта, разработанного профессионалом. За счёт чего сервису удаётся добиться такого результата — разбираемся в обзоре.

**Плюсы:**

* Большая база шаблонов, выполненных профессионалами.
* Система подсказок для подготовки сайта к публикации и поисковому продвижению.
* Автоматическая адаптация страниц под разные экраны и возможность вручную настроить разные версии сайта: мобильную, планшетную, десктопную.
* Бесплатный SSL.
* Высокая скорость загрузки страниц благодаря отличной технической оптимизации движка.

**Минусы:**

* Некоторые шаблоны выглядят однотипными и устаревшими.
* Доступ к вставке своего HTML-кода появляется только на максимальном тарифе.

 После сравнения была выбрана платформа uKit, так как она показалась наиболее подходящей и бюджетной для создания сайта. [3]

1.2 Создание сайта

 В рамках изучения темы «Интернет безопасность» был создан сайт. В нем была размещена самая главная информация по выбранной теме.

 На основе изученного материала была собрана основная информация, которая занесена в продукт моего проекта.

 https://secure56.ukit.me данный сайт был размещен на различных площадках.

# Заключение

 В заключение проекта можно отметить, что тема "интернет безопасности" остаётся актуальной и открытой на сегодняшний день по нескольким причинам:

1. Развитие технологий. Современные технологии не стоят на месте. Каждое новое программное обновление приносит с собой новые угрозы в интернете, что делает безопасность в сети главной проблемой.
2. Каждый день происходят множество атак на компьютеры и серверы.
3. Недостаток осведомленности пользователей. Некоторые пользователи не понимают, какие действия могут привести к различным угрозам в интернете.
4. В рамках решения первой задачи были рассмотрены возможные
5. В рамках второй задачи были выявлены разнообразные и наиболее часто встречаемые угрозы в интернете
6. В рамках третьей задачи были разработаны рекомендации
7. В рамках решения четвертой задачи был создан сайт

 Таким образом, безопасность в сети остается важной проблемой в нашем мире, так как личная информация и финансы остаются на волоске и могут быть украдены в любой момент.

# Список использованной литературы

https://studme.org/179783/informatika/protokoly [1]

https://vc.ru/u/1255405-igor-gundyrev/469644-obzor-konstruktora-saytov-ukit-vozmozhnosti-plyusy-i-minusy-integracii [2]

https://ukit.com/sites/url/secure56/dashBoard [3]

https://postium.ru/konstruktory-sajtov/ [4]

https://habr.com/ru/articles/188042/ [5]

https://www.cactusvpn.com/ru/beginners-guide-online-security/what-is-online-security/ [6]

https://www.kaspersky.ru/blog/what\_is\_two\_factor\_authenticatio/4272/ [7]

https://www.securitylab.ru/analytics/537030.php [8]

https://habr.com/ru/articles/218319/ [9]

https://blog.avast.com/ru/history-of-cybersecurity-avast [10]

https://www.securitylab.ru/analytics/534347.php [11]

https://vc.ru/flood/31740-fishing-smishing-kak-zashchititsya-ot-tehnologicheskogo-moshennichestva [12]

https://www.websiterating.com/ru/online-security/what-is-ransomware-protection/ [13]

https://www.securitylab.ru/blog/personal/bezmaly/350242.php [14]

https://ib-bank.ru/bisjournal/news/16504 [15]

# Приложение А

Паспорт индивидуального проекта

|  |  |
| --- | --- |
| **Автор проекта** | Шарков Марк Евгеньевич |
| **Тема индивидуального проекта** | Интернет безопасность |
| **Вид проекта** | Социальный |
| **Наименование предмета (предметов), в рамках которой выполняется индивидуальный проект**  | Информатика |
| **Место реализации проекта** | Школа 86 |
| **Сроки реализации проекта** | Ноябрь 2022 – май 2024 |
| **Руководитель проекта** | Спивак Татьяна Юрьевна |
| **Заказчик проекта** |  |
| **Участники проекта** (**заинтересованные стороны проекта)** | Шарков Марк Евгеньевич |

# Приложение Б

Дорожная карта



# Приложение В

Описание проекта

|  |  |
| --- | --- |
| Краткое описание (аннотация) проекта | Создать сайт , в котором будут рассказаны основные угрозы в интернете и способы сохранить вашу конфиденциальность |
| Актуальность проекта | Интернет-пространство меняется с бешеной скоростью, а проблемы с приватностью данных усугубляются.Информация – это деньги. Это главная причина, по которой вашим личным данным угрожает опасность. |
| Социальная значимость проекта | Проинформировать пользователей о компьютерной безопасности при использовании Интернет ресурсов. |
| Цель проекта | Изучение правил пользования интернет ресурсами, предоставить сайт, содержащий нормы безопасной и надежной работы за компьютером. |
| Задачи проекта | Рассмотреть возможные угрозы в интернетеУзнать разнообразие и классификацию интернет угрозРазработать способы безопасного пользования |
| Целевая аудитория | Подойдет для тех, кто только начинает знакомиться с интернетом и его возможностями. |
| Новизна проекта (новаторство, что делает проект особенным, уникальным, идущим на шаг впереди остальных, востребованным) | Тема безопасности в интернете будет актуальна всегда, именно поэтому я создаю сайт, в котором расскажу о безопасном использовании Интернет ресурсов. |
| Продукт проекта | Сайт |
| Результат (результаты) проекта | Повышение знаний пользователей о интернет угрозах |
| Риски реализации проекта | Ограниченный ресурс времени |
| Критерии успеха проекта | Достигнут результат, информация о проекта широко распространяется |
| География проекта и его масштабируемость | Регионы России |
| Перспективы дальнейшей работы над проектом | Продолжить совершенствовать свой проект  |