Областное государственное бюджетное

профессиональное образовательное учреждение

«Томский политехнический техникум»

**портфолио  
ИНДИВИДУАЛЬНОГО ПРОЕКТА**

Тема: «Проблема защиты информации в интернете»

|  |  |
| --- | --- |
|  | Автор: Стрельцов Ростислав Александрович  студент группы 132Э1  Дата «\_\_\_\_» \_\_\_\_\_\_\_\_\_ 2022 г. |
| Консультант–нормоконтролер:  Виниченко Я.А./ \_\_\_\_\_\_\_\_\_  Дата «\_\_\_\_» \_\_\_\_\_\_\_\_ 2022 г. | Руководитель: Самсонова О.В. /\_\_\_\_\_\_\_\_  Должность: преподаватель  Дата «\_\_\_\_\_\_» \_\_\_\_\_\_\_\_ 2022 г. |

Томск 2022

**СОДЕРЖАНИЕ**

Паспорт проекта………………………………………………………………………………….3

План-график реализации проекта………………………...…………………………………….4

1. Проблема защиты информации в интернете………………………………………………...5

2. Вредоносные приложения и программы…………………………………………………….5

3. Список простых правил, которые помогут обезопасить вашу информацию……………..6  
Заключение……………………………………………………………………………….............8

Список источников информации…………………………………………….............................9

Приложение А………………………...………………………………………………………...10

Приложение Б…………………………...……………………………………………………...11

Приложение В……………………………...…………………………………………………...14

Отзыв руководителея о ходе реализации проекта……………………………………………15

Лист нормоконтроля……………………………………………………………………………16

**Паспорт проекта**

|  |  |
| --- | --- |
| Название проекта | Проблема защиты информации в интернете |
| Направление | – Я – ПРОФЕССИОНАЛ |
| Тип проекта по доминирующей деятельности | ,Информационный |
| Актуальность проекта | Данная тема актуальна так, как до сих пор остаются люди, информация которых попадает в руки интернет-мошенникам |
| Проблема | Незнание людей как защитить себя в интернете |
| Цель | Оповестить людей о проблеме защиты информации и предложить способы защиты |
| Задачи | - Рассказать о проблеме защиты информации в интернете  - Предложить способы защиты информации в интернете  - Собрать статистику о знаниях людей в плане защиты информации в интернете |
| Объект | Интернет, мошенники и вирусы |
| Предмет | Способы защиты информации в сети Интернет |
| Гипотеза | Насколько эффективны способы защиты информации в сети Интернет |
| Механизм реализации (формы и методы) | Создание информационного буклета |
| Требуемые ресурсы (материальные, человеческие, финансовые и прочие), смета расходов | Бумага для распечатки проекта и опросников;  Принтер;  ПК; |
| Ожидаемые результаты (количественные, качественные) | Опрос и его результаты; |
| Риски | Отказы от прохождения опроса; |
| Продукт | Опрос и его результаты; Буклет памятка |
| Рекомендации к применению,  целевая аудитория | Ко всем; |

**План-график реализации проекта**

|  |  |  |  |
| --- | --- | --- | --- |
| Этапы | Сроки | Содержание  работы | Планируемый  результат |
| Подготовительный  -проблема  -планирование |  | -выбор темы | Выбрана тема |
|  | -планирование работы | Составлен план работы |
|  | -формирование  паспорта и графика проекта | Оформил паспорт и график проекта |
| Основной  -поиск информации  -продукт |  | - отработка выбранных механизмов реализации проекта | Отработаны выбранные механизмы реализации проекта |
|  | - оформление разделов портфолио проекта | Оформлены разделы портфолио проекта |
|  | -оформление продукта | Оформлен продукт |
| Заключительный  -портфолио  -презентация |  | - подготовка отзыва руководителя | Руководитель подготовил отзыв |
|  | - нормоконтроль портфолио | Нормоконтроль прошёл |
|  | - подготовка и проведение презентации проекта | Презентацию проекта прошёл |

1. **ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕРНЕТЕ** [2]

Сейчас интернетом пользуется каждый из нас совершая покупки,   
ища информацию, общаясь. Также главным фактором почему люди начинают пользоваться интернетом является переход гос. ресурсов в онлайн формат.

С самого появления интернета им заинтересовались мошенники, стремящиеся получить доступ к личной информации пользователей. Интернет мошенничество распространенно из-за того, что преступления, совершенные в интернете труднее отследить чем преступления в реальности [1].

**2. ВРЕДОНОСНЫЕ ПРИЛОЖЕНИЯ И ПРОГРАММЫ**

Главной целью вирусных программ является не нарушение работы компьютера  
или телефона, а незаметный сбор любой информации пользователя.

Виды вредоносных программ [3]:

Компьютерные вирусы - программное обеспечение, которое   
несанкционированно устанавливается в структуры электронного прибора.

Троян - это тип вредоносных программ, маскирующихся под легитимное ПО.   
Он часто используется кибер-преступниками для кражи личных данных, слежения  
за пользователями и получения несанкционированного доступа к системам.

Кейлогер - программа, которая отслеживает нажатие клавиш.

Червь - В отличие от вирусов, червям для распространения не требуются вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев.

**СПОСОБЫ ЗАЩИТЫ ИНФОРМАЦИИ:**

1. Пароли.

Самый простой и распространенный способ — это установка паролей.   
От сложности пароля напрямую зависит степень защиты вашей информации, чем пароль больше, тем сложнее его угадать. Также стоит помнить,   
что не нужно использовать один и тот же пароль везде т.к. если его все   
же угадают, то преступник сможет получить доступ и к другой информации защищенной эти паролем.

1. Антивирусные программы.

Антивирус - программа для обнаружения компьютерных вирусов   
и удаления.

Также она позволяет предотвращать заражение вирусом, заранее   
его просканировав при запуске. У антивирусов есть своя база, с помощью которой   
они обнаруживают вредоносные программы, поэтому не стоит пренебрегать   
его обновлением. Антивирус — это очень полезная программа для обычного пользователя.

Одни из распространенных антивирусов [5]:

* Bitdefender
* Kaspersky
* Norton
* McAfee
* Avast

**3. СПИСОК ПРОСТЫХ ПРАВИЛ, КОТОРЫЕ ПОМОГУТ ОБЕЗОПАСИТЬ ВАШУ ИНФОРМАЦИЮ** [4]

* Вовремя обновляйте операционную систему и антивирусы

Обновления системы кроме исправления ошибок несут в себе обновления безопасности и убирают обнаруженные уязвимости. Антивирусы тоже нуждаются в обновлении   
для обновления своей базы вирусов.

* Не переходите по подозрительным ссылкам

Ссылки могут перебросить вас на вредоносный сайт, который может подстроиться   
под сайт, которым вы часто пользуетесь (например: Вконтакте, Одноклассники, Госуслуги и т.п.) и если вы введете туда свои данные, то сайт сможет украсть их.

* Внимательно читайте всплывающие окна

Всплывающие окна не только могут перебрасывать вас на другие сайты,   
но и устанавливать расширения для браузера, которые могу следить за вашими действиями в интернете.

* Не скачивайте файлы с подозрительных сайтов

Скачанный файл с незнакомого сайта может содержать в себе много вирусов,   
но если другого варианта получить файл нету, то лучше перед его запуском проверить его в антивирусе.

* Разлогиневайтесь на чужих устройствах

Если вы не вышли из своего аккаунта на чужом пк (например, в интернет кафе),  
то другой пользователь получит доступ к вашей информации. Также не стоит использовать функцию «Сохранить пароль» на чужом устройстве.

* Не сообщайте данные аккаунтов даже друзьям

Даже если вы доверяете своим знакомым, то стоит помнить, что возможно   
их устройства могут быть заражены вирусами ворующими данные.

* Читайте лицензионное соглашение

В лицензионном соглашении указываются условия пользования сайтом, сервисом   
или приложением. Например, вы зарегистрировались в «облаке» (сайт хранящий   
ваши файлы) и забыли оплатить подписку, заходите на сайт и видите, что ваших файлов там нет, всё из-за того, что вы не внимательно ознакомились с лицензионным соглашением в котором указано что сайт, имеет право удалить файлы по истечению подписки.

* Не подключайтесь к незнакомым WIFI сетям

Через WIFI сеть к который вы подключены проходит весь ваш интернет трафик  
(от вас на сервер и с сервера к вам) и злоумышленник запустивший такую WIFI сеть может получить доступ к вашим данным.

**ЗАКЛЮЧЕНИЕ**

Я провёл опрос на знание людей основ безопасности в интернете, на основе этого написал простые правила и сделал буклет-памятку.

В нынешнее время, чтобы не попасться на уловки мошенников в интернете,   
не нужно прилагать много усилий. Чтобы быть в безопасности, нужно всего лишь помнить простые правила пользования интернетом (например, написанные мной выше)   
и иметь установленный антивирус.

**СПИСОК ИСТОЧНИКОВ ИНФОРМАЦИИ**

1. SkyDynamics ИТ-аутсорсинг: сайт. – Москва, 2022. – URL: <https://sky-dynamics.ru/stati/metody-i-sredstva-zashhity-informacii-v-internete/> (дата обращения: 10.10.2022). – Текст: электронный.
2. Студенческий научный форум: XV Международная студенческая научная конференция: сайт. – Томск, 2022. - URL:<https://scienceforum.ru/2020/article/2018021652> (дата обращения: 10.10.2022). – Текст: электронный.
3. Kaspersky: сайт. – Москва, 2022. – URL: <https://www.kaspersky.ru/resource-center/definitions/what-is-internet-security> (дата обращения: 10.10.2022). – Текст: электронный.
4. Microsoft: сайт. – США, 2019. – URL: https://news.microsoft.com/ru-ru/features/protect-yourself-online/ (дата обращения: 10.10.2022). - Текст: электронный.
5. Хабр: Сообщество IT-специалистов. – Россия, 2022. –URL: <https://habr.com/ru/company/first/blog/672996/>. (дата обращения: 10.10.2022). – Текст: электронный.

**ПРИЛОЖЕНИЯ**

*Приложение А*

*Опрос:*

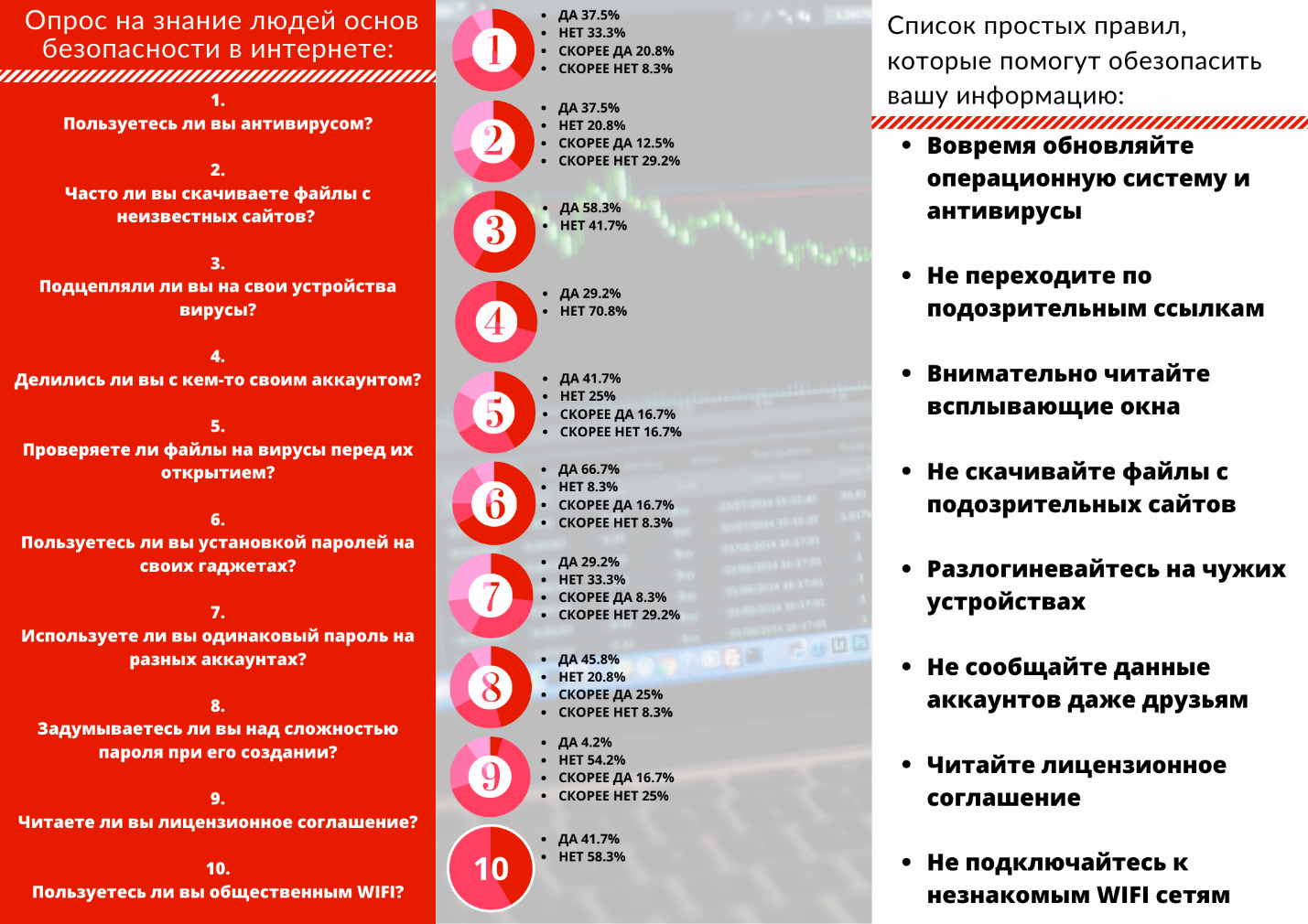
1. Пользуетесь ли вы антивирусом?
2. Часто ли вы скачиваете файлы с неизвестных сайтов?
3. Подцепляли ли вы на свои устройства вирусы?
4. Делились ли вы с кем-то своим аккаунтом?
5. Проверяете ли файлы на вирусы перед их открытием?
6. Пользуетесь ли вы установкой паролей на своих гаджетах?
7. Используете ли вы одинаковый пароль на разных аккаунтах?
8. Задумываетесь ли вы над сложностью пароля при его создании?
9. Читаете ли вы лицензионное соглашение?
10. Пользуетесь ли вы общественным WIFI?

*Приложение Б*

*Результаты опроса:*

*Приложение В*

*Буклет-памятка:*



# **Отзыв руководителя о ходе реализации проекта**

**Заключение о степени соответствия выполненного проекта заданию**  
Данный проект полностью соответствует Положению об   
индивидуальном проекте студента ОГБПОУ «ТПТ».  
  
 **Характеристика выполнения каждого раздела проекта, степень использования последних достижений науки и техники, передовых методов работы, проявленная самостоятельность, дисциплинированность при выполнении проекта, характеристика общих компетенций, проявленных при выполнении проекта** Проект по своему типу является информационно-исследовательским. Данный проект является актуальным поскольку он затрагивает современные проблемы и языковые изменения. Проект был спланирован и реализован под руководством преподавателя.   
При этом студент проявил самостоятельность и реализовывал свои идеи. Также студент показал высокий уровень регулятивных умений, самоорганизацию,  
а также интерес к заявленной теме.

Работа включает в себя все требуемые разделы: паспорт, основную часть, заключение, список источников информации.  
  
 **Перечень положительных качеств проекта**  
Проект освещает интересную тему, творческий продукт.   
   
 **Перечень основных недостатков проекта**Недостатков не выявлено.  
  
 **Отзыв о проекте в целом и предлагаемая оценка проекта**Цели и задачи проекта выполнены в полном объеме, индивидуальный проект заслуживает отметки «отлично».

Руководитель: Самсонова О.В. /\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

Дата «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_2022 г.

**Лист нормоконтроля**

ФИО студента Стрельцов Ростислав Александрович группа 132Э1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | Критерий оценки | Отметка о выполнении | Примечание | Повторная отметка |
| 1 | Оформление портфолио проекта (скоросшиватель) |  |  |  |
| 2 | Титульный лист по образцу |  |  |  |
| 3 | Структура портфолио проекта:  1-титульный лист, 2-содержание, 3-паспорт, 4-план-график проекта, 5-*«разделы по теме проекта»,* 6-заключение, 7-список источников информации, (8-приложения), 9-отзыв руководителя, 10-лист нормоконтроля |  |  |  |
| 4 | Структура паспорта проекта:  1-название проекта, 2-учебная дисциплина, 3-тип проекта по доминирующей деятельности, 4-актуальность, 5-проблема, 6-объект, 7-предмет, 8-цели, 9-задачи, 10-гипотеза, 11-механизм реализации, 12-требуемые ресурсы, 13-ожидаемые результаты, 14-риски, 15-продукт, 16-рекомендации к применению, целевая аудитория |  |  |  |
| 5 | Форматирование:  1-Шрифт, 2-размер шрифта, 3-поля, 4-выравнивание по ширине, 5-номера страниц, 6-оформление абзацев («красных» строк) |  |  |  |
| 6 | Оформление по ГОСТу:  1-рисунки, 2-таблицы, 3-формулы,  4-ссылки на источники информации,  5-список источников информации |  |  |  |

Подпись нормоконтролера: \_\_\_\_\_\_\_\_\_\_\_\_\_\_/ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(инициалы, фамилия)

Дата «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_2022 г.