ПРОБЛЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕРНЕТЕ

Стрельцов Ростислав Александрович
Ольга Викторовна Самсонова, преподаватель
ОГБПОУ «Томский политехнический техникум», г. Томск, Россия

Ключевые слова: защита информации, интернет, вредоносные приложения, программы, антивирус, пароль, опросы.

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].

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.

2. 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

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.

Опрос

Я провёл опрос на знание людей основ безопасности в интернете. В опросе приняли участие около 50 человек, вопросы представлены в Приложении 1. Результаты опроса обработаны в электронной таблице MS Excel и показаны графически в Приложении 2. На основе результатов опроса я написал простые правила и сделал буклет-памятку (см. Приложение 3).

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

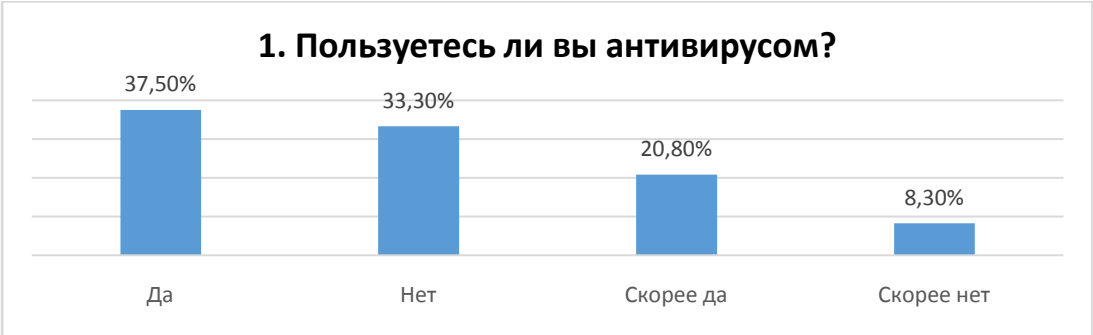
Приложение 1

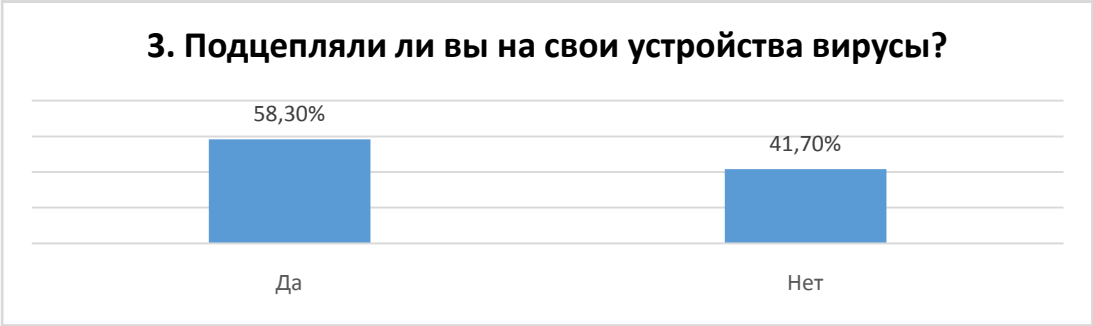
Опрос

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?

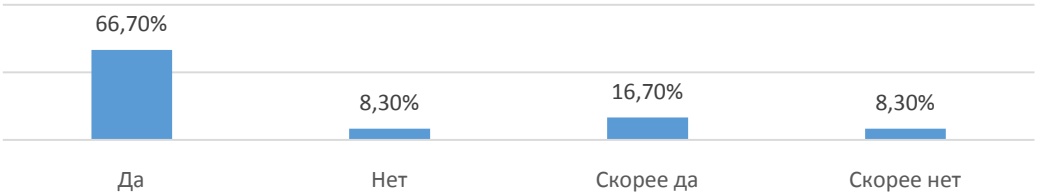
Приложение 2

Результаты опроса

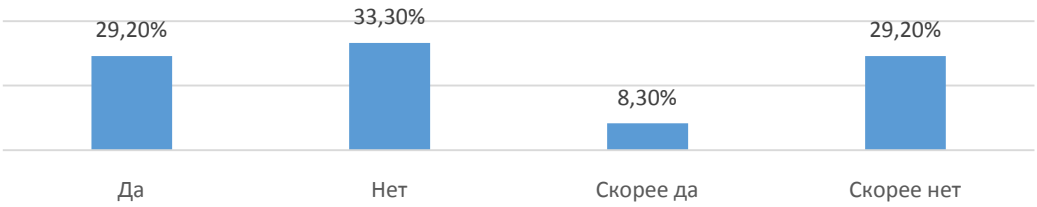




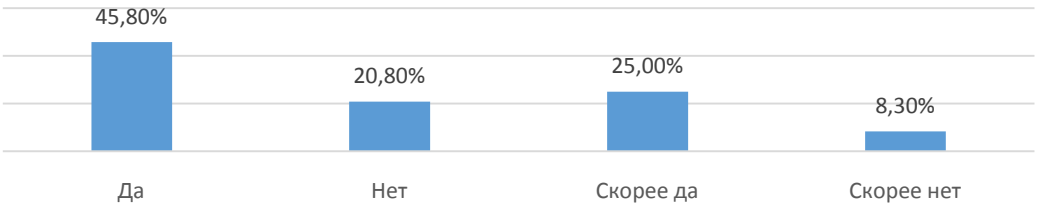
6. Пользуетесь ли вы установкой паролей на своих гаджетах?



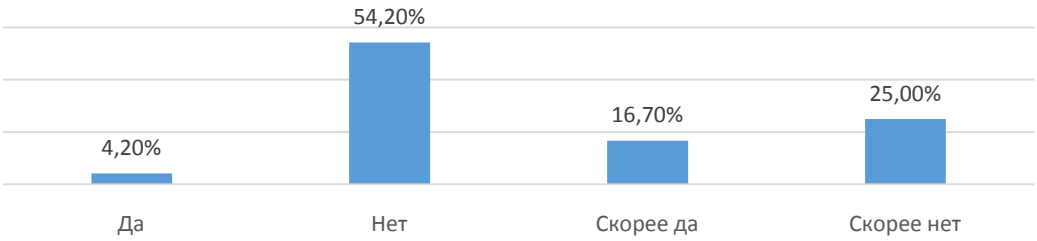
7. Используете ли вы одинаковый пароль на разных аккаунтах?



8. Задумываетесь ли вы над сложностью пароля при его создании?



9. Читаете ли вы лицензионное соглашение?



10. Пользуетесь ли вы общественным WIFI?

Буклет-памятка

Топ 5 антивирусов

- 1 Bitdefender
- 2 kaspersky
- 3 norton
- 4 McAfee
- 5 Avast

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.

Защита информации в интернете

Опрос на знание людей основ безопасности в интернете:

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?

1
- ДА 37.5%
- НЕТ 33.3%
- СКОРЕЕ ДА 20.8%
- СКОРЕЕ НЕТ 8.3%

2
- ДА 37.5%
- НЕТ 20.8%
- СКОРЕЕ ДА 12.5%
- СКОРЕЕ НЕТ 29.2%

3
- ДА 58.3%
- НЕТ 41.7%

4
- ДА 29.2%
- НЕТ 70.8%

5
- ДА 41.7%
- НЕТ 25%
- СКОРЕЕ ДА 16.7%
- СКОРЕЕ НЕТ 16.7%

6
- ДА 66.7%
- НЕТ 8.3%
- СКОРЕЕ ДА 16.7%
- СКОРЕЕ НЕТ 8.3%

7
- ДА 29.2%
- НЕТ 33.3%
- СКОРЕЕ ДА 8.3%
- СКОРЕЕ НЕТ 29.2%

8
- ДА 45.8%
- НЕТ 20.8%
- СКОРЕЕ ДА 25%
- СКОРЕЕ НЕТ 8.3%

9
- ДА 4.2%
- НЕТ 54.2%
- СКОРЕЕ ДА 16.7%
- СКОРЕЕ НЕТ 25%

10
- ДА 41.7%
- НЕТ 58.3%

Список простых правил, которые помогут обезопасить вашу информацию:

- **Вовремя обновляйте операционную систему и антивирусы**
- **Не переходите по подозрительным ссылкам**
- **Внимательно читайте всплывающие окна**
- **Не скачивайте файлы с подозрительных сайтов**
- **Разлогиневайтесь на чужих устройствах**
- **Не сообщайте данные аккаунтов даже друзьям**
- **Читайте лицензионное соглашение**
- **Не подключайтесь к незнакомым WIFI сетям**