**Глава 2 «Обеспечение информационной безопасности при работе в интернете.»**

Рассмотрев наиболее часто встречающиеся и опасные виды интернет-вирусов , перейдем к способам защиты личной информации при работе в сети.

**1.1 Антивирусные программы.**

Несомненно ,самым известным способом защиты личных данных является антивирус-программа, которую можно установить на любое устройство. Рассмотрим на примере персонального ноутбука.

Существует несколько основополагающих методов поиска вирусов, которые применяются антивирусными программами для обнаружения удаления и защиты от компьютерных вирусов:

1. программы-детекторы - осуществляют поиск характерного для конкретного вируса содержимого в оперативной памяти и в файлах и при обнаружении выдают соответствующее сообщение. Недостатком таких антивирусных программ является то, что они могут находить только те вирусы, которые известны разработчикам таких программ.

2. программы-доктора или фаги - не только находят зараженные вирусами файлы, но и «лечат» их, то есть удаляют из файла тело программы-вируса, возвращая файлы в исходное состояние

3. программы-ревизоры (инспектора) - относятся к самым надежным средствам защиты от вирусов. Проверяют данные на диске на предмет вирусов-невидимок, изучают, не забрался ли вирус в файлы и жесткий диск.

4. программы-фильтры (мониторы) - небольшие резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вирусов

5. программы-вакцины или иммунизаторы - резидентные программы, предотвращающие заражение файлов

6. сканер - данный вид программы сканирует секторы и системную память, а также ищет в них известные и новые (неизвестных сканеру) вирусы

Существует большой спектр антивирусных программ-как платные, так и бесплатные. Приведу список наиболее известных и проверенных антивирусов:

Платные антивирусы:

1) Kaspersky Total Security

2) Norton Security Premium

3) Avast Premier

Бесплатные :

1) Kaspersky Free

2) Avast Free Antivirus

3) AVG AntiVirus Free

Нужно упомянуть, что в компьютере уже по умолчанию вшит свой антивирус. Так, для Window -это Microsoft Security Essentials (Защитник Windows ).

**1.2 КАК ПРОВЕРИТЬ БЕЗОПАСНОСТЬ САЙТА?**

Сейчас существует огромное количество фишинговых вредоносных сайтов, которые могут заразить ваш компьютер. Начиная всплывающими окнами и заканчивая вредоносными ссылками, содержащими вирусы- все это составляющие непроверенных сайтов. Чтобы проверить безопасность сайта, нужно:

1. Проверьте URL-адрес сайта. Некоторые сайты намеренно создают неотличимые на первый взгляд сайты-двойники, отличие лишь в мелких незначительных деталях. К примеру, URL-адрес оригинального сайта содержит символ «а», в то время как двойник лишь изменил этот символ на «о», и это уже другой сайт, но с почти идентичным адресом!
2. Аббревиатура «https» означает «Secure»- безопасность. Если веб-сайт работает с протоколом https, то канал передачи данных между браузером и сервером, на котором размещается веб-сайт, надежно зашифрован. Если вы не уверены, что сайт или ссылка защищены протоколом https, будьте внимательны и не вводите никакие персональные данные.
3. Антивирусные программы. Они также блокируют всплывающие окна, рекламу и предупреждают о небезопасности сайта.
4. Существует специальный сервис для проверки URL-адреса. Он называется Visualtotal (есть и другие). Вам требуется скопировать адрес сайта для проверки и вставить его в специальное окно проверки в сервисе, далее он определит, безопасен ли сайт.

Список сервисов для проверки URL-адреса сайта:

1. Sucuri SiteCheck
2. IsItWP Security Scanner
3. Google Safe Browsing

**1.3 Соблюдение конфиденциальности. Интернет-платежи.**

Будьте внимательны и не вносите личные данные на непроверенных и подозрительных сайтах. Один из самых распространенных видов интернет-мошенничества- онлайн-оплата картой. Как правило, системы электронных платежей хорошо защищены. Учетные записи в таких системах обычно взламывают потому, что клиенты сами раскрывают свои секретные данные по невнимательности или излишней доверчивости, например записывают пароль на видном месте, по ошибке выкладывают файлы с ключами в открытый доступ, переходят по фишинговой ссылке в письме и т. д. Для совершения безопасных интернет-платежей соблюдайте следующие правила6

1. Проверяйте используется ли защищенное соединение — адрес в строке браузера должен начинаться с https .
2. Используйте одноразовые пароли и почту, для этого существуют специальные сайты, генерирующие данные для одноразового входа.
3. Для интернет-платежей лучше всего использовать отдельную дебетовую карту, привязанную к отдельному счёту. А основную карту, которой вы расплачиваетесь в магазинах и банкоматах, никогда не использовать в интернете.
4. Кроме того, многие банки сейчас предлагают специальные «виртуальные» карты (по сути - набор цифр), которые можно использовать один или несколько раз, а на следующий платёж выпустить новую карту. Это хороший и достаточно безопасный вариант, но у него есть некоторые недостатки, о которых скажем ниже в пункте о регулярных платежах.
5. Если вы используете для интернет-платежей обычную дебетовую карту (не одноразовую), то можно подключить к ней сервис информирования о платежах. Банки сейчас обязаны информировать клиента обо всех платежах, но в данном случае это особенно актуально, поэтому лучше убедиться, что это информирование работает, а вы получаете сообщение о платеже самым быстрым и удобным для вас образом.
6. старайтесь точно понять, за что именно вы платите. Многие продавцы услуг (доступ на сайт, подписка на интернет-издание, платёж за игру и т.п.) берут не разовый платёж, а подписывают вашу карту на регулярные выплаты, например, ежемесячные. Вы сами должны решить, хотите ли вы, чтобы платежи с карты снимались регулярно. Для таких случаев, кстати, надо иметь постоянную обычную карту для интернет-платежей, а не одноразовую или краткосрочную виртуальную.

Заключение

Предметом исследования являлось изучение принципов действия вирусных программ . Необходимо было выяснить, как обеспечить защиту личной информации при работе в интернете. Важно было оценить степень неосведомленности пользователей сети и составить список правил, способных помочь в обеспечении защиты данных. Благодаря проведенной работе, был составлен список действий, соблюдение которых повысит шанс безопасного нахождения в интернете и поможет пользователям узнать больше новой, а главное-полезной информации о способах борьбы с угрозами в сети. Исходя из заключения, хочу подтвердить правильность выдвинутой гипотезы о том, что «пользователи, используя Интернет, помнят об угрозах, которые он содержит». Могу считать, что цель исследования достигнута.

Список литературы :

1. Компьютерные вирусы Москва, 2011. - 132 c.

2. Касперски Крис Компьютерные вирусы изнутри и снаружи; Питер - Москва, 2006. - 526 c.

3. Касперский, Е. Компьютерные вирусы в MS-DOS; М.: Русская редакция - Москва, 1992. - 176 c.

4. Климентьев К. Е. Компьютерные вирусы и антивирусы. Взгляд программиста; ДМК Пресс - Москва, 2013. - 656 c.

5. Михайлов А. В. Компьютерные вирусы и борьба с ними; Диалог-МИФИ - , 2011. - 104 c.

6. Cookie-files[[1]](#footnote-1)

7.Основные виды интернет-мошенничества[[2]](#footnote-2)

8.Виды мошенничества и интернете[[3]](#footnote-3)

9.Как осуществить защиту информации в интернете? [[4]](#footnote-4)

10.ОСНОВНЫЕ СРЕДСТВА И ТЕХНОЛОГИИ[[5]](#footnote-5)

11. Основы информационной безопасности. Часть 1: Виды угроз [[6]](#footnote-6)

1. https://windowstips.ru/chto-takoe-cookie-v-brauzere [↑](#footnote-ref-1)
2. https://yandex.ru/turbo?text=https%3A%2F%2Favisi.ru%2Fosnovnye-vidy-inte... [↑](#footnote-ref-2)
3. https://businessman.ru/new-kakim-byvaet-moshennichestvo-v-internete.html [↑](#footnote-ref-3)
4. https://camafon.ru/informatsionnaya-bezopasnost/zashhita-v-internete [↑](#footnote-ref-4)
5. https://bezopasnostin.ru/informatsionnaya-bezopasnost/zashhita-informats... [↑](#footnote-ref-5)
6. https://habr.com/ru/company/vps\_house/blog/343110/ [↑](#footnote-ref-6)