МИНЕСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧЕРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«Брестский государственный технический университет»

Кафедра «Интеллектуальные информационные технологии»

Практическая работа №1

По дисциплине «Основы защиты информации»

За 3 семестр

Тема: «Введение в защиту информации»

Выполнили:

студентки 2 курса

группы АС-56

Казак А.А.

Карпенко М.В.

Проверил:

Безобразов С.В.

Брест 2020

*Задание:* Выбрать объект для защиты информации. Описать его. Ответить на вопрос: Почему применятся защита информации? Предложить меры по защите информации.

*Объект*: планшет.

*Описание*  
Электронный планшет — электронное устройство с сенсорным экраном, позволяющее управлять компьютерными программами, через прикосновение пальцами к объектам программы на экране. Существует несколько видов планшетов:  
1. Планшетные ноутбуки  
Свое название получили благодаря возможности трансформироваться из ноутбука в планшетный компьютер. В сущности, трансформер отличается от обычного ноутбука лишь поворотным экраном и «планшетными» расширениями операционной системы.  
2. Интернет-планшет  
Тип планшетных компьютеров с диагональю экрана от 4 до 11 дюймов, совмещающих в себе качества ноутбука и смартфона. Интернет-планшеты, как правило, имеют возможность быть постоянно подключёнными к сети интернет — через Wi-Fi или 3G/4G-соединение.  
3. Электронная книга  
Общее название группы узкоспециализированных компактных планшетных компьютерных устройств, предназначенных для отображения текстовой информации, представленной в электронном виде. Основным отличием данной группы компьютерных устройств от планшетных ПК является ограниченная функциональность при существенно большем времени автономной работы.  
  
*Почему применяется защита информации?*  
На современных устройствах хранится много информации о пользователе,которую нужно защищать по нескольким причинам :  
1. От вредоносных программ.  
2. От сетевых атак.  
3. От фишинга.  
По нашему мнению, фишинг является одной из самых опасных причин кражи конфединциальных данных персонального пользователя. Часто он может не обратить внимание на массовые рассылки, например, от популярных брендов, под видами которых скрываются мошенники. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.  
Вредоносные программы также могут причинить вред владельцу информации, путём копирования, искажения, удаления или подмены информации. Может производится блокировка компьютера, шифрование файлов пользователя с целью шантажа и вымогательства денежных средств.  
Удалённый взлом (сетевые атаки) относительно персонального пользователя менее распространён в связи с тем, что он [удалённый взлом] является основным инструментом в политической войне и не добросовестной конкуренции.  
  
*Предлагаемые нами меры защиты информации*  
1. Сохранение паролей.  
При вводе своих логинов и паролей на страницах интернета , не нужно сохранять их в памяти браузера, поскольку они могут использоваться мошенникам и для доступа к другим конфединциальных данным.  
2. Использование безопасного Wi-Fi.  
Хотя переход на зараженный веб-сайт это не предотвратит, использование защищенных паролем Wi-Fi-соединений не позволяет нежелательным третьим сторонам следить за вами или совершать атаки между вашим устройством и нужным вам адресатом.  
3. Следить за своей электронной почтой.  
Многие злоумышленники все еще используют вредоносные вложения электронной почты, чтобы заразить планшет. Не нужно нажимать на ссылки в письмах и других сообщениях, так как они могут направить вас на фишинговые или вредоносные сайты.  
4. Быть последовательным.  
Скачивать приложения только из надежных источников. Это гарантия того, что приложения являются легитимными (находящимися в соответствии с законом) и не содержат вредоносных мобильных программ.  
5. Установка антивирусной защиты.  
Теперь антивирусные решения есть и для мобильных устройств. Установить антивирусное решение из надежного источника, запускать его регулярно, чтобы обеспечить чистоту вашего устройства. Также следить за тем, чтобы вредоносное ПО не маскировалось под защиту от вирусов: скачивать только легитимные приложения из надежных источников.