МИНЕСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

УЧЕРЕЖДЕНИЕ ОБРАЗОВАНИЯ

«Брестский государственный технический университет»

Кафедра «Интеллектуальные информационные технологии»

Практическая работа №5

По дисциплине «Основы защиты информации»

За 3 семестр

Тема: «Программа повышения осведомленности»

Выполнили:

студентки 2 курса

группы АС-56

Казак А.А.

Карпенко М.В.

Проверил:

Безобразов С.В.

Брест 2020

*Задание:* для пользователей выбранного объекта разработать программу повышения осведомленности в области защиты информации. Программа должна содержать перечень тем и порядок действий пользователя (необязательно) для повышения их уровня знаний.

*Объект*: планшет.

Программа повышения осведомленности в области защиты информации – это один из важнейших этапов внедрения систем защиты информации, который направлен на поддержание знаний пользователя в актуальном состоянии.

Тема 1. Вирусы.

Вирусы – это зловредные программы, которые незаметно проникают на планшет благодаря уязвимости системы. Они самостоятельно заражают другие файлы в системе. Вирус может проникать на планшет после просмотра рекламы, посещения сайтов, а также чтения писем в социальных сетях. При неосторожном скачивании файлов с интернета пользователь может совершенно случайно либо скачать на планшет вирус, либо разрешить доступ к своим конфиденциальным данным. В случае неосторожной загрузки вируса последствия могут быть самыми непредсказуемыми. Мошенники маскируют вирусы под безобидные приложения и файлы: браузеры, плееры, игры, навигаторы, книги, антивирусы. Затем они распространяют их: например, ищете в интернете какую-нибудь игру или программу, и попадаете на форум. Кто-то оставил нужную ссылку и все дружно его благодарят. На самом деле форум и комментаторы не настоящие. Или, заходя на сайт с пиратскими фильмами и сериалами, появляется сообщение. В нем написано, что планшет заражен вирусами или какая-то программа сильно устарела. Бывает даже так, что устройство начинает вибрировать или издавать странные звуки. На самом деле это не так и с устройством все в порядке. Или второй вариант, по SMS или электронной почте. Как правило, это SMS с сайтов бесплатных объявлений, письма от «нотариусов из Германии», сообщения о выигрыше в лотерею. Нужно быть осторожным, в большинстве случаев это мошенники. У всех подобных сообщений общая цель – заставить нажать на ссылку, чтобы вирус скачался на устройство.

Тема 2. Проблема электропитания.

Суть данной проблемы кроится в повышенной мобильности выбранного нами объекта защиты информации, а именно – планшета. Благодаря наличию аккумуляторной батареи работа на данном устройстве не предполагает подключение к сети. Это в разы увеличивает возможности использования и способы применения устройства, но порождает рассматриваемую проблему. В следствие всего вышеперечисленного появляется вероятность непредвиденного снижения заряда аккумуляторной батареи вплоть до её резкого выключения, что может повлечь за собой потерю важной информации или прекращение работы приложения, активного в момент разряда аккумулятора. Также следует учитывать, что в момент выключения объекта защиты информации пользователь может оказаться в неблагоприятных условиях, а именно – без возможности подключить планшет к электропитанию либо без подходящего к нему провода (шнура от зарядного устройства). По этой причине следует помнить о том, что при использовании планшета нужно следить за процентом заряда аккумулятора или всегда иметь при себе зарядное устройство и помнить о возможности резкой разрядки планшета.

Тема 3. Внешние нападения.

3.1. Пользователь.

Опасность пользователя заключается в том, что он имеет доступ, который позволяет выполнять самые разнообразные вредоносные действия - от неправильного использования данных до полного разрушения системы. Они могут украсть любую конфиденциальную и финансовую информацию – продать ее или просто выложить в Интернет.

3.2. Постороннее лицо.

Посторонние лица придумали уникальные способы мониторинга планшетов. Часто они используют уязвимости в операционной системе планшета, чтобы взломать его. Тем не менее, весьма часто они используют социальную инженерию, чтобы обмануть ничего не подозревающих людей при загрузке вредоносного программного обеспечения на свои планшеты. Вот три популярных способа взломать ваш планшет без вашего ведома:

1. Через тексты. Метод является популярным, поскольку может казаться, что сообщение отправлено банком или другой известной организацией так, что пользователь рассматривает это как обычную ситуацию, следовательно метод – хорошее прикрытие.

2. Через общедоступный Wi-Fi. Взломщик может использовать общедоступный Wi-Fi для выполнения следующих действий:

1)Атака «человек посередине»: взломщик вставляет себя между сервером и клиентом, разрывает связь между клиентом и сервером и отслеживает взаимодействие.   
 2) Обнаружение пакетов: программное обеспечение взломщика, отслеживает пакеты данных, передаваемых между мобильным устройством и сервером. Таким образом, если пользователь вводит имена других пользователей и пароли при подключении к общедоступной сети Wi-Fi, взломщик может просмотреть ее.

3. С помощью программы шпиона. Популярная шпионская программа Xnspy используется для кражи информации с планшетов. Можно установить приложение и осуществлять удаленный мониторинг планшета. Несмотря на то, что приложение предназначено для родительского и сотруднического мониторинга, взломщик может установить приложение, чтобы шпионить за вашим планшетом.

Вывод: Для пользователей планшета разработали программу повышения осведомленности в области защиты информации. Программа содержит перечень тем, причины появления определенных угроз и проблем и порядок действий пользователя для повышения их уровня знаний.