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:* Привести классификацию злоумышленников. Для выбранного объекта защиты информации разработать и описать круг злоумышленников.

*Объект*: планшет.

*Классификация злоумышленников:*  
1. Работник информационно-вычислительной системы.  
Работник ИВС владеет наиболее полной информацией о программных и аппаратных средствах ИВС и имеет возможность внедрения "закладок" на этапах создания и модернизации систем, но не получает доступа на эксплуатируемые объекты ИВС.  
2. Сотрудник из числа обслуживающего персонала.  
Наиболее опасный класс – работники службы безопасности информации, далее идут системные и прикладные программисты, затем – инженерно-технический персонал.  
3. Пользователь.  
Пользователь имеет общее представление о структуре ИВС и механизмах её защиты, но может осуществлять сбор информации методами традиционного шпионажа и попытками несанкционированного доступа к информации.  
4. Постороннее лицо.  
Постороннее лицо может осуществлять дистанционные методы шпионажа и диверсионную деятельность.  
  
*Описание круга злоумышленников:*  
Для выбранного нами объекта информации (планшета) наиболее опасными злоумышленниками являются пользователь и постороннее лицо.  
- 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.  
- 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.  
- Работник ИВС или сотрудник из числа обслуживающего персонала не являются актуальными для нашего объекта защиты информации, поскольку он не относится к какой-либо организации.  
  
*Вывод:* Мы привели классификацию злоумышленников и можем сделать вывод о том, что пользователь и постороннее лицо – возможные взломщик и нашего объекта информации.