УДК:004.735

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИ РАБОТЕ В ГЛОБАЛЬНОЙ СЕТИ ИНТЕРНЕТ

САХНО Виталий Викторович
студент
ПИЩАЕВА Александра Сергеевна
студент
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

Немалую роль занимает и Интернет, он уже является частью информационного общества, в нем сохранены наша информация и даже персональные данные. Одна из распространенных угроз в сети Интернет представляет собой, потерю персональных данных и их использование злоумышленниками в корыстных целях. В данной статье будут рассмотрены основные методы и способы, которые злоумышленники применяют к своим жертвам в сети Интернет.

Ключевые слова: сеть Интернет, технические угрозы, социальная инженерия, фигинг, вредоносная программа.

Рассмотрим, для начала, что представляет собой сама сеть. Интернет – это глобальная компьютерная сеть, в которой локальные, региональные и корпоративные сети соединены между собой многочисленными каналами передачи информации с высокой пропускной способностью [4].

В информационном сообществе все чаще происходят открытие в сфере IT, на данном этапе развитее уже давно появился мобильный интернет, что позволяет практически везде воспользоваться сетью. Так же помимо телефонов, войти в интернет возможно уже и с наручных часов. Интернет используется дома, на работе и в образовательных учреждениях это позволяетсэкономить время и облегчить умственную нагрузку, а так же получать свежие новости в интересующей области. Но так же он таит в себе скрытые угрозы.

Существуют два основных вида угроз в сети Интернет:

– технические угрозы;

– социальная инженерия.

Технические угрозы. Основными угрозами для пользователя сети Интернет является вредоносные программы, Dos и DDos-атаки. Основная цель вредоносных программ – причинение ущерба пользователю посредствам модификации, удаление или раскрытия личной для него информации путем воздействия на ПЭВМ, сервер либо ЛВС. Вредоносные программы могут скрываться в файлах, скаченных через Интернет, или распространиться через электронную почту. Суть DoS и DDos-атак заключается в том, что злоумышленник пытается сделать временно недоступным определенный сервер, перегрузить сеть, процессор [2].

Социальная инженерия. Основная идея заключается в получении несанкционированного доступа к информационным ресурсам пользователя, основанная на психологии человека. Целью социальных инженеров является получение доступа к защищенным информационным ресурсам с целью личных данных пользователя. Основным отличием от технических угроз является то, что в роли объекта атаки выбирается не машина, а ее пользователь. Все способы и методы социальных инженеров основываются на использовании человеческих слабостей [5].

Одна из популярных и действующих схем социальной инженерии является фишинг. Основная цель заключается в получении доступа к персональным данным пользователя, а именно логина и пароля. Одним из ярких примеров фишинговых атак может быть сообщение, отправленное жертве по электронной почте, подделанное под офици-

альное письмо – от банка или платёжной системы – требующее проверки определённой информации или совершения определённых действий [1]. Причины могут быть очень разнообразные и самые различные.

Так же можно выделить как отдельный вид угроз, это контент сайта, ведь в сети Интернет могут попасть и несовершеннолетние. Можно выделить следующие виды контента [3]:

1. *Незаконный контент.* В зависимости от законодательства страны разные материалы могут считаться нелегальными. В большинстве стран запрещены: материалы сексуального характера с участием детей и подростков, порнографический контент.

2. *Контентные риски*. Контентные риски связаны с информацией, которая публикуется в интернете и включает в себя незаконный и непредназначенный для несовершеннолетних контент.

3. *Неподобающий контент.* В зависимости от культуры, законодательства, менталитета и узаконенного возраста согласия в стране определяется группа материалов, считающихся неподобающими.

Рассмотренные угрозы приносят как материальный, так и духовный ущерб при использовании сети Интернет. Для предотвращения данных угроз используют специализирующие программные обеспечения (межсетевой экран, антивирусное ПО и др.), но еще важно не поддаваться на провокации мошенников, быть всегда спокойным и обдумывать свои действия.

СПИСОК ЛИТЕРАТУРЫ

1. *Безмалый В.* Фишинг-атаки. – URL:https://www.osp.ru/winitpro/2008/02/4887833/(дата обращения: 13.11.2019).

2. Безопасность пользователей в сети интернет. – URL:https://safe-surf.ru/users-of/article/212/ (дата обращения 14.11.2019).

3. Безопасность работы в сети интернет // Старт в науку: сб. статей. – Абдулино, 2018. – URL: https://multiurok.ru/files/issledovatelskaia-rabota-bezopasnost-v-seti-intern.html (дата обращения: 13.11.2019).

4. Информатика на пять. Теоретический материал. – URL:http://www.5byte.ru/9/ (дата обращения 14.11.2019).

5. *Мазаев Д.В., Ермолаева В.В., Мурзагалиев А.Г.* Интернет-угрозы и способы защиты от них // Молодой ученый. – 2015. – № 11. – С. 193-197. – URL https://moluch.ru/archive/91/19771/ (дата обращения: 13.11.2019).

ACTUAL PROBLEMS WHEN WORKING ON THE GLOBAL INTERNET NETWORK

SAKHNO Vitaliy Viktorovich
student
PISHCHAEVA Alexandra Sergeevna
student
Don State Technical University
Rostov-on-Don, Russia

The Internet also plays a significant role, it is already part of the information society, it stores our information and even personal data. One of the common threats on the Internet is the loss of personal data and their use by malefactors for personal gain. This article will discuss the main methods and methods that cybercriminals apply to their victims on the Internet.

Key words: Internet, technical threats, social engineering, figing, malware.