**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**



**МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**ВЫСШАЯ ШКОЛА ПЕЧАТИ И МЕДИАИНДУСТРИИ**

***Институт Принтмедиа и информационных технологий***

***Кафедра Информатики и информационных технологий***

**направление подготовки**

**09.03.02 «Информационные системы и технологии»**

**ЛАБОРАТОРНАЯ РАБОТА № 1**

**Дисциплина:** пппппПроектирование и разработка интерактивных приложений кие методы обрабо….h \_hhh \_hhh \_hhh\_hhh\_hhh\_hhh\_hhh\_hhh\_h

**Тема: р**вjjjjjjjjjjjБезопасность интерактивных приложенийоооооооооооо рррррррррррррррррррррррррррррррррррррррррррррhhhhhhhhhрррррррррррв

**Выполнил(а): студент(ка) группы:** ДЦисБ-3-3

\_hhh Кортошкина Екатерина\_hhh\_hhh\_hhh\_hhh

(Фамилия И.О.)

**Дата, подпись** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ***\_\_\_\_\_\_\_\_\_\_\_***

(Дата) (Подпись)

**Проверил:** ррр доц. Иванько М.А.оааао ***\_\_\_\_\_\_\_\_\_***

(Фамилия И.О., степень, звание) **(Оценка)**

**Дата, подпись** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  ***\_\_\_\_\_\_\_\_\_\_\_***

(Дата) (Подпись)

**Замечания: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Москва**

**2017**

Технические угрозы

Основными техническими угрозами для пользователей являются вредоносные программы, ботнеты и и DoS и DDoS-атаки.

Вредоносные программы

Цель вредоносных программ – причинить ущерб компьютеру, серверу или компьютерной сети. Они могут, например, испортить, украсть или стереть данные, хранящиеся на компьютере, замедлить или полностью остановить работу устройства.

Чаще всего вредоносные программы распространяются через электронную почту или скачанные из Интернета файлы. Файлы или ссылки, присланные по электронной почте, могут подвергать устройство заражению.

Злоумышленники могут заражать компьютер, чтобы сделать его частью   **ботнета**– сети из зараженных устройств, расположенных по всему миру. Крупные ботнеты могут включать в себя десятки и сотни тысяч компьютеров. Пользователи часто даже не догадываются, что их компьютеры заражены вредоносными программами и используются злоумышленниками. Ботнеты создаются путем рассылки разными способами вредоносных программ, а зараженные машины в дальнейшем регулярно получают команды от администратора ботнета, так что оказывается возможным организовать согласованные действия компьютеров-ботов по атаке других устройств и ресурсов.

DoS и DDoS атаки

Суть DoS-атаки заключается в том, что злоумышленник пытается сделать временно недоступным конкретный сервер, перегрузить сеть, процессор или переполнить диск. Цель атаки – просто вывести компьютер из строя, а не получить информацию, захватить все ресурсы компьютера-жертвы, чтобы другие пользователи не имели к ним доступа. К ресурсам относятся: память, процессорное время, дисковое пространство, сетевые ресурсы и т. д.

Для организации DDoS-атак злоумышленники используют **ботнет** – специальную сеть компьютеров, зараженных особым видом вирусов. Каждым таким компьютером злоумышленник может управлять удаленно, без ведома владельца. При помощи вируса или программы, искусно маскирующейся под легальную, на компьютер-жертву устанавливается вредоносный программный код, который не распознается антивирусом и работает в фоновом режиме. В нужный момент по команде владельца ботнета такая программа активизируется и начинает отправлять запросы на атакуемый сервер, в результате чего заполняется канал связи между сервисом, на который проводится атака, и Интернет-провайдером и сервер перестает работать.

Социальная инженерия

Большинство злоумышленников полагается не только на технологии, но и на человеческие слабости, используя при этом **социальную инженерию**. Этот термин обозначает способ получать нужную информацию не с помощью технических возможностей, а путем обыкновенного обмана, хитрости. Такие люди применяют психологические методы воздействия на людей через электронную почту, социальные сети и чаты. В результате их умелой работы пользователи добровольно выдают свои данные, не всегда понимая, что их обманули.

Мошеннические сообщения чаще всего содержат угрозы, например, закрытия пользовательских банковских счетов, обещания огромного выигрыша с минимальными усилиями или вовсе без них, запросы о добровольных пожертвованиях от лица благотворительных организаций.

Фишинг

Фишинг является наиболее популярным способом атаки на пользователей и одним из методов социальной инженерии. Он представляет собой особый вид Интернет-мошенничества. Цель фишинга – получение доступа к конфиденциальным данным, таким как адрес, телефон, номера кредитных карт, логины и пароли, путем использования поддельных веб-страниц. Часто фишинговая атака происходит следующим образом: на электронную почту приходит письмо с просьбой войти в систему Интернет-банкинга от имени якобы сотрудника банка. Письмо содержит ссылку на ложный сайт, который трудно отличить от настоящего. Пользователь вводит личные данные на поддельном сайте, а злоумышленник перехватывает их. Завладев персональными данными, он может, например, получить кредит на имя пользователя, вывести деньги с его счета и расплатиться его кредитными картами, снять деньги с его счетов или создать копию пластиковой карты и с ее помощью снять деньги в любом месте мира.

Раздражающая и потенциально опасная реклама

Назойливая реклама преследует нас повсюду. Каждый сталкивался с ситуацией, когда перед видео на YouTube необходимо просматривать 30-секундный рекламный ролик. Это не только отвлекает от работы, мешает просматривать сайты, вести переписку: загрузка рекламного сообщения на вашем экране (будь то преролл или баннер) съедает часть вашего интернет-трафика. Получается, что за эту рекламу вы еще и платите. Часто из-за большого веса рекламных сообщений, сайты грузятся дольше. От этого у смартфонов значительно сокращается заряд батареи. Кроме того, реклама может содержать вредоносный код или вести на сайты с таким кодом.

Способы защиты от угроз в Интернете

Существует много видов и способов атак, но также есть и достаточное количество способов защиты от них. При работе в Интернете рекомендуется выполнять следующие требования:

Настроенный спам в почте.

Не скачивать файлы с непроверенных сайтов.

Не вводить пароли на незащищенных сайтах.

Не говорить никому пароли

Пользуйтесь паролями

Используйте шифрование данных

Регулярно выполняйте обновления программного обеспечения

Используйте и регулярно обновляйте антивирусные программы