История возникновения Интернета.

Понятия Интернет-угроз. Изменения границ допустимого в контексте цифрового образа жизни

Интернет – всемирная сеть, состоящая из большого количества локальных сетей.

Днем рождения **Интернета** считается 29 октября 1969 года, однако в массовом пользовании он появился гораздо позже, в начале 90-х.

История создания интернета берет свое начало в 60-х годах прошлого века в США. Страна обладала огромными возможностями, в научных центрах работало много талантливых ученых. Первый прототип интернета был разработан для использования в военное время. Например, для связи во время ядерной войны.

В 1971 году была разработана первая электронная почта, а спустя всего два года, интернет распространился и за океаном. Однако пользоваться им могли по-прежнему лишь узкий круг людей.

Таким образом, в США был дан первый толчок развитию интернета, однако основателем интернета является Тим Бернесрс-Ли, который трудился в европейской организации ЦЕРН. Потратив два года на разработки, именно этот ученый сделал интернет таким, каким сейчас его знают миллионы пользователей.

**Угрозы в сети Интернет**

Интернет – это безграничный мир информации, который дает широкие возможности для общения, обучения, организации работы и отдыха и в то же время представляет собой огромную, ежедневно пополняющуюся базу данных, которая содержит интересную для злоумышленников информацию о пользователях. Существует два основных вида угроз, которым могут подвергаться пользователи: технические и социальная инженерия.

**Технические угрозы**

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

**Угроза** – это потенциально возможное событие, действие, которое посредством воздействия на объект защиты может привести к нанесению ущерба.

**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. Вредоносные программы часто «прячутся» в письмах и сообщениях с заманчивыми предложениями от неизвестных лиц и компаний, в страницах новостных сайтов или других популярных ресурсах, которые содержат уязвимости. Пользователи заходят на эти сайты, и вредоносные программы незаметно проникают на компьютер.

Также вредоносные программы распространяются через электронную почту, съемные носители информации или скачанные из Интернета файлы. Файлы или ссылки, присланные по электронной почте, могут подвергать устройство заражению.

Вредоносные программы могут скрываться и под видом звуковых или графических сообщений. Например, красивая экранная заставка, которой с удовольствием любуется пользователь, может оказаться троянской программой (что это такое, читайте ниже). Ссылки, которые появляются во всплывающих окнах и в рекламных объявлениях на различных сайтах, также могут содержать вирусы.

**К вредоносным программам относятся вирусы, черви, троянские программы.**

**Вирус** – разновидность компьютерной программы, отличительной особенностью которой является способность к размножению (саморепликации) и незаметному для пользователя внедрению в файлы, загрузочные секторы дисков и документы. Название «вирус» по отношению к компьютерным программам пришло из биологии именно по признаку способности к саморазмножению. Лежащий в виде зараженного файла на диске вирус не опасен до тех пор, пока его не открыть или не запустить. Он начинает действовать только тогда, когда пользователь его активирует. Вирусы разработаны, чтобы копировать себя, заражая компьютеры, при этом обычно они уничтожают файлы.

**Черви** – это разновидность вирусов. Они полностью оправдывают свое название, поскольку распространяются путем «переползания» из устройства в устройство. Так же, как и вирусы, они представляют собой саморазмножающиеся программы, но в отличие от вирусов, червю не нужна помощь пользователя, чтобы распространиться. Он сам находит лазейку.

**Троянские программы** – вредоносные программы, которые целенаправленно внедряются злоумышленниками для сбора информации, ее разрушения или модификации, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях. Внешне троянские программы выглядят как легальные программные продукты и не вызывают подозрений. В отличие от вирусов, они полностью готовы к выполнению своих функций. На это и делается расчет злоумышленников: их задача – сделать такую программу, которую пользователи не побоятся запускать и использовать.

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**

DoS-атака (отказ в обслуживании) – это атака, приводящая к парализации работы сервера или персонального компьютера вследствие огромного количества запросов, с высокой скоростью поступающих на атакуемый ресурс.

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.

**Социальная инженерия**

Большинство злоумышленников полагается не только на технологии, но и на человеческие слабости, используя при этом **социальную инженерию**. Этот сложный термин обозначает способ получать нужную информацию не с помощью технических возможностей, а путем обыкновенного обмана, хитрости. Социальные инженеры применяют психологические методы воздействия на людей через электронную почту, социальные сети и службы мгновенного обмена сообщениями. 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. Например, сообщение от злоумышленника может выглядеть так: «Ваш аккаунт заблокирован. Чтобы восстановить доступ к нему, необходимо подтвердить следующие данные: номер телефона, электронную почту и пароль. Присылайте их по такому-то электронному адресу». Чаще всего злоумышленники не оставляют пользователю времени для размышлений, например, просят заплатить в день получения письма.

**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.

**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:

Пользуйтесь паролями

Работайте на компьютере под учетной записью с ограниченными правами

Используйте шифрование данных

Регулярно выполняйте обновления программного обеспечения

Используйте и регулярно обновляйте антивирусные программы

Используйте межсетевой экран