УДК. 004

КИБЕРБЕЗОПАСНОСТЬ

Бирюлина С.С. Ф-МИ221 1 курс

Гулидова О.П. ст. преподаватель

Алтайский государственный гуманитарно-педагогический университет им. В. М. Шукшина

Алтайский край г. Бийск

Аннотация: в 21-м веке вместе с новыми технологиями, компьютеризацией к нам пришли и IT – проблемы. В современное время наблюдается рост числа киберугроз. Практически каждый день мы слышим из новостей о новых утечках какой-либо информации и хакерских взломах. Как же избежать, защитить себя и своих родных от данных угроз? Как безопасно находиться в интернете и хранить личные данные на персональном компьютере? Умный дом – безопасно или нет? На все эти вопросы мы постараемся дать ответ в данной статье.

Ключевые слова: технологии, хакеры, преступники, правила, политика, безопасность, кибератака, IT, программы, защита, умный дом, система, сети, чёрный рынок.

Abstract: In the 21st century together with new technologies, computerization came to us and IT - problems. In modern times, there is an increase in the number of cyber threats. Almost every day we hear from the news about new leaks of some information and hacking. So how to avoid, to protect yourself and your relatives from these threats? How to be safe on the Internet and keep personal data on your personal computer? Smart home - is it safe or not? We will try to answer all these questions in this article.

Прежде чем начать описывать правила безопасности, поймем от чего же нам нужно защищаться. Киберугрозы делятся на 3 типа – это киберпреступление, кибератака и кибертероризм, с первого взгляда может показаться, что данные слова синонимы, но это не совсем так.

Киберпреступление – это злоумышленные действия одного или нескольких лиц с целью нарушения работы какой-либо системы или же извлечения финансовой выгоды.

Кибератака – данное действие нацелено на сбор информации, в основном политического характера.

Кибертероризм – действия такого типа направлены на дестабилизацию электронных систем с целью вызвать страх и панику.

Нарушителям удается заполучить контроль над компьютерными системами используя различные инструменты, программы и приемы.

Например, вирусы, троянцы, шпионские ПО, программы-вымогатели, рекламное ПО, ботнет и т.д. При таких атаках злоумышленники пытаются обмануть машинный алгоритм, заставляя его выдавать неправильные ответы.

Для чего информация нужна хакерам? Вся информация очень легко продается, либо тому, у кого она была похищена, либо в даркнете. Чаще всего, после взлома компании, злоумышленники действуют по следующему сценарию:

1. выставляют товар на чёрном рынке

2. шантажируют компанию

3. шифруя данные получают от компании выкуп за восстановление.

К сожалению, такие ситуации случаются довольно часто. Только за 2022 год доля массовых атак увеличилась на 33% от общего числа. Больше всего предприятий, подверженных взлому – это компании в которых небольшой финансовый оборот и слабая защита IT- инфраструктуры. Например, промышленные предприятия и объекты ТЭК.

В науке похожий тип взломов был описан как клептографические атаки 20 лет назад. Никто не был уверен, что это возможно.

Не только компании подвержены нападениям хакеров, но и обычные пользователи. Так как мы часто совершаем одни и те же ошибки, а злоумышленники не могут не воспользоваться шансом. Такие частые ошибки, как переход к непроверенным источникам, использование неизвестных флэш-накопителей, скачивание пиратского антивирусного ПО, постоянно включенная веб-камера, создание ненадежных паролей др.

Хакеры и спецслужбы могут даже перехватить SMS с помощью уязвимости в SS7 — системе служебных протоколов, с помощью которых телеком-операторы управляют телефонными сетями. Получив доступ к SMS пользователя, можно войти в его почту, сбросив пароль.

Что же нужно делать, чтобы персональный компьютер и все ваши данные всегда оставались в безопасности?

1. Обновляйте ПО и ОС

2. Используйте проверенные антивирусные программы

3. Придумывайте надежные пароли и не передавайте их кому-либо

4. Не переходите по ссылкам, которые получены от неизвестных отправителей

5. Избегайте незащищенных сетей Wi-Fi

6. Каждые полгода чистите свой ПК

Соблюдая всего несколько простых правил, вы никогда не столкнётесь с атакой хакеров.

Но только ли наш компьютер может быть подвержен кибератакой? А вот и нет, каждый из нас желает обставить свой дом инновационной техникой, робот-пылесос, умный-замок, климат-контроль и другая домовая инфраструктура. Но всё это тоже может быть далеко не безопасно.

Был случай, когда анализ исходящего трафика от гаджетов в квартире раскрыл привычки ее обитателей: когда дети ложатся спать и что они смотрят по телевизору, когда родители на работе. Этот эксперимент провела журналистка издания Gizmodo. На два месяца она превратила свою квартиру в умный дом. Все устройства — кофеварки, зубные щетки, пылесосы и так далее — передавали данные компаниям-производителям несколько раз в день, а, например, телевизор передавал данные о привычках семьи сторонним компаниям.

Некий мужчина купил чайник, а хакеры с его помощью накручивали лайки в социальной сети. Канадцы столкнулись с нетипичным ботнетом, который состоит из зараженных устройств интернета вещей и используется для накруток лайков и фолловеров в соцсетях. Подобные ботнеты используются для DDoS-атак, рассылки спама или открутки баннеров. А в данном случае злоумышленники зарабатывали на раскрутке социальных-аккаунтов.

Случалось, и такое, молодая семья купила домашнюю камеру наблюдения. В следующие несколько месяцев за их жизнью наблюдали тысячи из интернета. Пользователи российского развлекательного форума перебором находили китайские камеры наблюдения со стандартным паролем и делились на сайтах информацией.

И даже политические выборы не полностью безопасны, после выборов в США протестировали на уязвимость к кибератакам машины, использующиеся для голосования. Эксперты заявили, что все машины надёжны. Но это не так. Всего 1,5 часа понадобилось группе хакеров на конференции DEFCON, чтобы найти первые уязвимости в одной из машин, использующихся для голосования.

Еще один вопрос, на который мы должны дать ответ – это вопрос о том, как безопасно хранить свои данные в сети Интернет?

Каждый из нас пользуется смартфонами, планшетами, компьютерами и все они собирают информацию о пользовании. А в интернет-сети всё также существуют проблемы с приватностью данных. Как мы поняли, информация – это деньги. Что нужно делать, чтобы защитить свою личную информацию?

Опишем несколько способов:

1. Почаще меняйте пароли и не делайте их очень простыми

2. Заведите запасной почтовый ящик

3. Обращайте внимание на политику конфиденциальности

4. Включите двухфакторную аутентификацию

5. Не используйте Wi-Fi в общественных местах

Подведем небольшой итог всему вышесказанному. Мы, как современные люди, должны не только хорошо разбираться в IT-технологиях, но и уметь правильно хранить и защищать свои данные. Чтобы наши данные всегда оставались личными не пренебрегайте правилами безопасности, внимательно читайте документы в которых ставите согласие «на обработку данных», сохраняйте бдительность. Ведь безопасность - это не состояние, а процесс.

Список литературы:

1. Киберпреступность и киберконфликты: Россия - https://www.tadviser.ru/index.php/Статья:Киберпреступность_и_киберконфликты_:_Россия

2. Как защитить личные данные в интернете - https://www.raiffeisen-media.ru/zhizn/kak-zashhitit-lichnye-dannye-v-internete-10-sposobov/

3. Интернет приватность - https://www.kaspersky.ru/resource-center/threats/internet-and-individual-privacy-protection