ФГБОУ ВО «Югор. гос. ун-т», Гуманитар. ин-т североведения, Высшая психолого-педагогическая школа. – Ханты-Мансийск: Сектор редакционно-издательской работы Научной библиотеки ЮГУ, 2019. – С. 399-403.

Казимирчик В.В., Дождикова Р.Н. **Кибербезопасность: угрозы безопасности**

Кибербезопасность – это совокупность методов и практик, направленных на защиту электронных систем, серверов, компьютеров, сетей и данных от цифровых атак. «Целью таких кибератак обычно является получение доступа к конфиденциальной информации, ее изменение или уничтожение, вымогательство денег у пользователей или нарушение нормального бизнес-процесса» [1]. В настоящее время внедрение эффективных методов для обеспечения кибербезопасности особенно трудно, поскольку электронных устройств становится больше, и киберпреступники разрабатывают и применяют все более новые методы атак. Угрозами безопасности являются фишинг, вредоносное программное обеспечение, программа-вымогатель, социальная инженерия.

Сегодня фишинг является наиболее развитой формой интернет-мошенничества, целью которого является кража конфиденциальных данных. Наиболее распространенным типом кибератаки является проведение массовых рассылок электронных писем от имени известных брендов, а также создание фишинговых сайтов [2]. Для защиты от фишинга используют технические методы, которые блокируют вредоносные электронные письма и предупреждают о подозрительных сайтах.

Под вредоносным программным обеспечением подразумевается любая программа, созданная для получения несанкционированного доступа и, как правило, выполнения любого вредоносного действия на устройстве пользователя [3]. Для надежной защиты от данного программного

обеспечения применяются программные средства защиты, а также требуется соблюдение правил «техники безопасности» в Интернете.

Программа-вымогатель, программа-шантажист – вид вредоносного программного обеспечения, предназначенного для вымогательства денежных средств за отмену изменений, которые были произведены программой в компьютере. Социальную инженерию киберпреступники используют для несанкционированного доступа к конфиденциальной информации без использования технических средств. Используя психологические приёмы, злоумышленники заставляют человека раскрыть конфиденциальную информацию или предоставить доступ к сетям.

«Социальная инженерия может сочетаться с любым из перечисленных выше типов угроз, чтобы вы с большей вероятностью переходили по ссылкам, загружали вредоносное программное обеспечение или доверяли вредоносному источнику» [1]. Передовыми программами для обеспечения кибербезопасности в современном сетевом мире пользуется каждый. Однако кибератакам подвергаются не только персональные компьютеры, но и объекты инфраструктуры: больницы, различные финансовые учреждения и другие критически важные объекты. «Защита этих и других организаций имеет принципиальное значение для нормального функционирования нашего общества» [4].

Литература

1. Что такое кибербезопасность [Электронный ресурс]. – Режим доступа: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html

2. Фишинг [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Фишинг

3. Вредоносное ПО, вирусы и другие угрозы в Интернете [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/preemptive-safety/faq

4. Что такое кибербезопасность [Электронный ресурс]. – Режим доступа: https://safeness.xyz/computer-security/51-chto-takoe-kiberbezopasnost.html

Бойко Е.П. **Способы заработка в интернете**

Мы живем во времена, когда можно работать, не выходя из дома. Это помогает совмещать работу с учебой или же находить дополнительный заработок для того, чтобы иметь финансовую незавсподушку безопасности. Один из способов заработка – транскрибация. Суть этого способа заключается в воспроизведении информации с аудио или видео в текстовом формате. Потребность в такой помощи часто возникает у редакторов блогов, журналистов, предпринимателей, работников телевидения и других специалистов. Это позволяет им значительно сэкономить время на рутине и подобную подработку можно найти на фриланс-биржах или в социальных сетях.

Продажа фото и видео – отличный вариант дополнительного дохода для дизайнеров, фотографов, видеографов, иллюстраторов. Суть в том, что вы размещаете свои работы, обязательно в хорошем качестве, на фото и видео площадках, с возможностью их неограниченной покупки.

Вы получаете бонус-гонорар, который будет составлять около 30 процентов от стоимости фото и видео. Чем больше раз вашу работу скачали, тем больше доход. Для этого типа заработка достаточно иметь уникальные фото и видео, потому как нельзя одни и те же работы продавать на разных площадках.