Философские проблемы в информатике

Киберпреступность

В настоящее время развитее информационных технологий происходит постоянно, ведь современное общество является информационным. Множество различной информации находится в общем доступе, но есть и та информация, которую каждый из людей бы хотел сохранить. Такой информацией являются личные пароли, переписки и многое другое, в частности и та информация, которая может стать неким компроматом на самого человека. Вследствие развития ИТ, люди всё чаще сталкиваются с таким понятием как киберпреступность, ведь данный вид деятельности широко распространился в связи с развитием сети интернет. Что же такое киберпреступность? Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства[1].

Кто же такие киберпреступники и для чего они ведут свою деятельность? Основной задачей киберпреступников является незаконное получение информации, для получения собственной прибыли от этого. Основной проблемой ИТ в современном обществе является защита информации от рук злоумышленников, путём её кодирования, хранения на безопасных носителях и многими другими методами, которые позволяет использовать современный ПК и сеть интернет[2]. Как же происходят утечки информации и похищение, несмотря на её хорошую “защищённость”. Несмотря на так называемое шифрование и использование защищённых каналов связи, киберпреступники, так называемые хакеры, находят различные способы, для выполнения тех или иных планов. Множество народа попадаются на очень простые уловки, связанные с изменением ссылок, переходом на не безопасные источники или фишинговые сайты, а также самая распространённая ошибка обычных пользователей, а именно использование простых паролей или использование одинаковых паролей для различных сервисов[3].

Однако если вдаваться в эту тему подробнее, то можно понять, что те хакеры, которые занимаются кражей паролей от аккаунтов или некоторой другой личной информации, на самом деле являются только верхушкой айсберга. Настоящая проблема современного общества, это те хакеры, которые остаются в тени, совершая кражу той информации, которая может стать оружием в политике различных стран и даже стать причиной возникновения вооружённого конфликта[4]. Как же происходит борьба с

такими киберпреступниками на государственном уровне, во избежание утечек закрытой политической информации? В наше время помимо стандартных, всем привычных правоохранительных органов, существуют также и специальные отделы, которые занимаются расследованиями в данной сфере, основной задачей которых является расследование и предотвращение киберпреступлений[5]. Несмотря на то, что данные преступления являются малоизвестными, а обычному обывателю не всегда известно о самых громких из них, их серьёзность очень весомы. И в связи с тем, что данные преступления чаще всего происходят из-за слабой защищённости сетей различных предприятий и компаний, а подготовленность преступников имеет высокий уровень, они чаще всего остаются в тени, что значительно усложняет их поиск и задержание[6]. Однако задержание таких преступников это лишь вопрос времени, ведь несмотря на то, что они работают только удалённо и пользуются специальными утилитами, чтобы как можно лучше замести следы, их информационный след всё же остаётся в сети, что позволяет задержать их.

Однако существуют и те, чей след до сих пор не был найден, кого знает практически каждый, кто когда-либо сталкивался или изучал тему киберпреступности, а именно группировка Legion или известное всем их название Anonymous. Они получили известность, вследствие своих преступлений. На их счету большое количество громких событий, которые в своё время сильно потрепали нервы и бюджеты некоторых стран. Однако их особенностью является не только это. Anonymous это единственная группа хакеров, которая не боится появляться в сети, это можно понять из того, что они много раз на прямую обращались к народу и правительству со своими заявлениями, однако умело стирали все следы своего появления после этого[7].

Подводя некий итог, можно сказать, что киберпреступность в наше время является огромной проблемой в сфере ИТ и бороться с ней будет только сложнее. Ведь с развитием и внедрением новых технологий, данный вид преступной деятельности также будет расти и развиваться.

Список литературы:

1.Клаверов В.Б.Современная киберпреступность: Характеристика и подробный анализ / В.Б. Клаверов // LAP Lambert Academic Publishing, 2012. – С. 92.

2.Краковский Ю.М. Защита информации / Ю.М. Краковский // Феникс, 2017. – С. 348.

3.Камский В.А. Защита личной информации: в Интернете, смартфоне и компьютере / В.А. Камский // Наука и техника, 2017. – С. 272.

4.Овчинский В.С. Основы борьбы с киберпреступностью и кибертерроризмом / В.С. Овчинский // НОРМА, 2017. – С. 528.

5.Жданов Ю.Н. Киберполиция XXI века. Международный опыт / Ю.Н. Жданов, В.С. Овчинский // Международные отношения, 2020. – С. 288.

6.Шелупанов А.А. Форензика. Теория и практика расследования кибепреступлений / А.А. Шелупанов, А.Р. Смолина // 2019. – С. 104.

7.Кушнер Дэвид А значит Anonymous / Кушнер Дэвид, Шадми Корен, М.А. Райтман // Бомбора, 2021. – С. 120.