жет быть замечено членом семьи, или критические замечания о вашем рабочем месте могут быть замечены вашим боссом.

8. После размещения информации в соцсетях ее удаление или извлечение может быть затруднено или невозможно.

9. Чрезмерное использование социальных сетей может привести к стрессу в отношениях в офлайн с семьей, друзьями и.

10. Издевательства, преследования и притеснения не редкость в социальных сетях. Сообщения с угрозами могут быть отправлены анонимно. Преследователи часто могут получить личную информацию или определить местонахождение и перемещения пользователя.

11. Несанкционированный обмен может отнимать доходы у художников и музыкантов, поскольку законы об авторском праве часто попираются.

12. Агрессивная реклама может негативно повлиять на восприятие пользователем.

13. Информационная перегрузка вызывает стресс и чувство перегруженности у некоторых пользователей.

14. Значительная часть информации в социальных сетях поступает из плохих источников или просто не соответствует действительности. Часть информации рассчитана на то, чтобы ввести в заблуждение в политических или иных целях.

15. Некоторые психологи выразили озабоченность по поводу социальной разобщенности, которая возникает, когда люди заменяют реальные жизненные отношения на виртуальные.

Романькова П.А., Дождикова Р.Н. **Киберпреступления**

Несмотря на огромное количество предостережений, мы не привыкли ждать от интернета чего-то плохого, ведь всемирная паутина пред-

лагает легкий доступ к информации и быстрое общение с людьми из разных частей света. Однако помимо множества преимуществ, которые предоставляет интернет, он породил людей, нацеленных на обман и использование в своих интересах других людей при помощи непонятных большинству простых пользователей способов [1].

Так что же такое киберпреступление? Киберпреступления – незаконные, противоправные действия, которые осуществляются людьми, использующими информационно телекоммуникационные технологии, компьютеры и компьютерные сети для преступных целей.

Большинство киберпреступлений совершаются хакерами, которые зарабатывают на этом деньги. Киберпреступная деятельность осуществляется отдельными лицами или организациями [2].

С другой стороны, необходимо понимать, что далеко не все хакеры имеют злые намерения. Их можно поделить на три основные группы:

- белые хакеры: работают над повышением безопасности компьютеров;
- серые хакеры: запускают компьютерные атаки ради забавы;
- черные хакеры: действуют с единственной целью – навредить.

Последняя группа является наиболее опасной и, как показала история, люди многократно становились жертвами черных хакеров, при этом последние умеют очень хорошо заметать следы[1].

Типы киберпреступлений:

- Мошенничество с электронной почтой и интернет-мошенничество;
- Мошенничество с использованием личных данных (кража и злонамеренное использование личной информации);
- Кража финансовых данных или данных банковских карт;
- Кража и продажа корпоративных данных;

- Кибершантаж (требование денег для предотвращения кибератаки);
- Атаки программ-вымогателей (тип кибершантажа);
- Криптоджекинг (майнинг криптовалюты с использованием чужих ресурсов без ведома их владельцев);
- Кибершпионаж (несанкционированное получение доступа к данным государственных или коммерческих организаций);

Большинство киберпреступлений относится к одной из двух категорий:

- Криминальная деятельность, целью которой являются сами компьютеры;
- Криминальная деятельность, в которой компьютеры используются для совершения других преступлений.

В первом случае преступники используют вирусы и другие типы вредоносных программ, чтобы заразить компьютеры и таким образом повредить их или остановить их работу. Также с помощью вредоносных программ можно удалять или похищать данные.

Киберпреступления второй категории используют компьютеры или сети для распространения вредоносных программ, нелегальной информации или неразрешенных изображений. Иногда злоумышленники могут совмещать обе категории киберпреступлений. Сначала они заражают компьютеры с вирусами, а затем используют их для распространения вредоносного ПО на другие машины или по всей сети [2].

Самые громкие киберпреступления последних лет:

- 15 февраля 2015 года «Лаборатория Касперского», Европол и Интерпол раскрыли киберпреступную операцию, в ходе которой хакеры похитили $1 млрд. Ограбление продолжалось два года и затронуло около 100 финансовых организаций по всему миру. В преступлении подозревают

международную преступную группировку из России, Украины, Китая и ряда стран Европы.

- 5 февраля 2016 года хакеры украли $101 млн Центробанка Бангладеш со счета в ФРС США. Сумма одной из крупнейших единовременных краж могла быть еще больше (более $950 млн), но хакеры допустили опечатку, когда осуществляли перевод, что вскрыло преступную схему.
- 14 февраля 2016 года хакеры получили контроль над компьютерами Пресвитерианского медицинского центра в Голливуде. Для возврата доступа к информационным системам преступники потребовали выкуп в размере 17 тыс. биткоинов ($3,6 млн). Спустя четыре дня клиника заплатила эту сумму.
- 23 февраля 2016 года руководство Yahoo! заявило о том, что в 2014 году хакеры похитили 500 млн аккаунтов пользователей. В результате крупнейшей в истории утечки персональных данных в сети оказались имена, адреса электронной почты, номера телефонов, даты рождения и пароли к аккаунтам.
- 14 ноября 2016 года журнал PCWorld сообщил о взломе 412 млн аккаунтов пользователей сайтов американской компании FriendFinder Network. Большая часть информации была похищена с сайта знакомств. Хакеры похитили адреса электронной почты и пароли.
- В декабре 2016 года Центробанк РФ сообщил, что за год киберпреступники похитили 2 млрд руб. со счетов российских банков. Одной из крупнейших стала кража 200 млн руб. у столичного Металлинвестбанка. В результате действий хакеров терминалы, с которых управляется корреспондентский счет учреждения в ЦБ, начали отправлять с него деньги на сторонние счета частных лиц [3].

Литература

1. https://www.computerra.ru/243121/10-samyh-izvestnyh-v-mire-hakerov-i-chto-s-nimi-stalo/

2. Советы по защите от киберпреступников [Электронный ресурс]https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime

3. Громкие киберпреступления последних лет [Электронный ресурс] https://www.kommersant.ru/doc/3270122

Стриевич И.И., Дождикова Р.Н. **Развитие Интернета и его будущее**

Интернет, изначально созданный как средство хранения и передачи информации, быстро стал самым массовым источником просвещения, коммуникации и развлечения. В наше время среднестатистический пользователь проводит онлайн почти семь часов в день – больше трети времени бодрствования. Сеть без преувеличения стала необходимым продолжением реальности на уровне базовой потребности.

Сложно сказать, когда точно появился Интернет. Первый прототип был создан для военных США в 1969 году. Эта компьютерная сеть позволяла безопасно передавать сообщения и файлы между военными в случае войны. Однако же отсчетом развития Интернета считается 29 октября 1969 года, когда двое исследователей, находящихся на расстоянии 640 километров – в Калифорнийском университете и в Стэнфордском исследовательском институте, отправили друг другу сообщение. Успешную передачу они подтвердили по телефону. И все же это не было похоже на современную сеть в том виде, к которому мы привыкли. Она появилась в 1991 году и сразу начала набирать популярность.

Интернет XXI века представляет собой огромное поле для творчества, бизнеса, самореализации. С каждым днем пользователей становится