

Презентация по теме: Киберпреступность

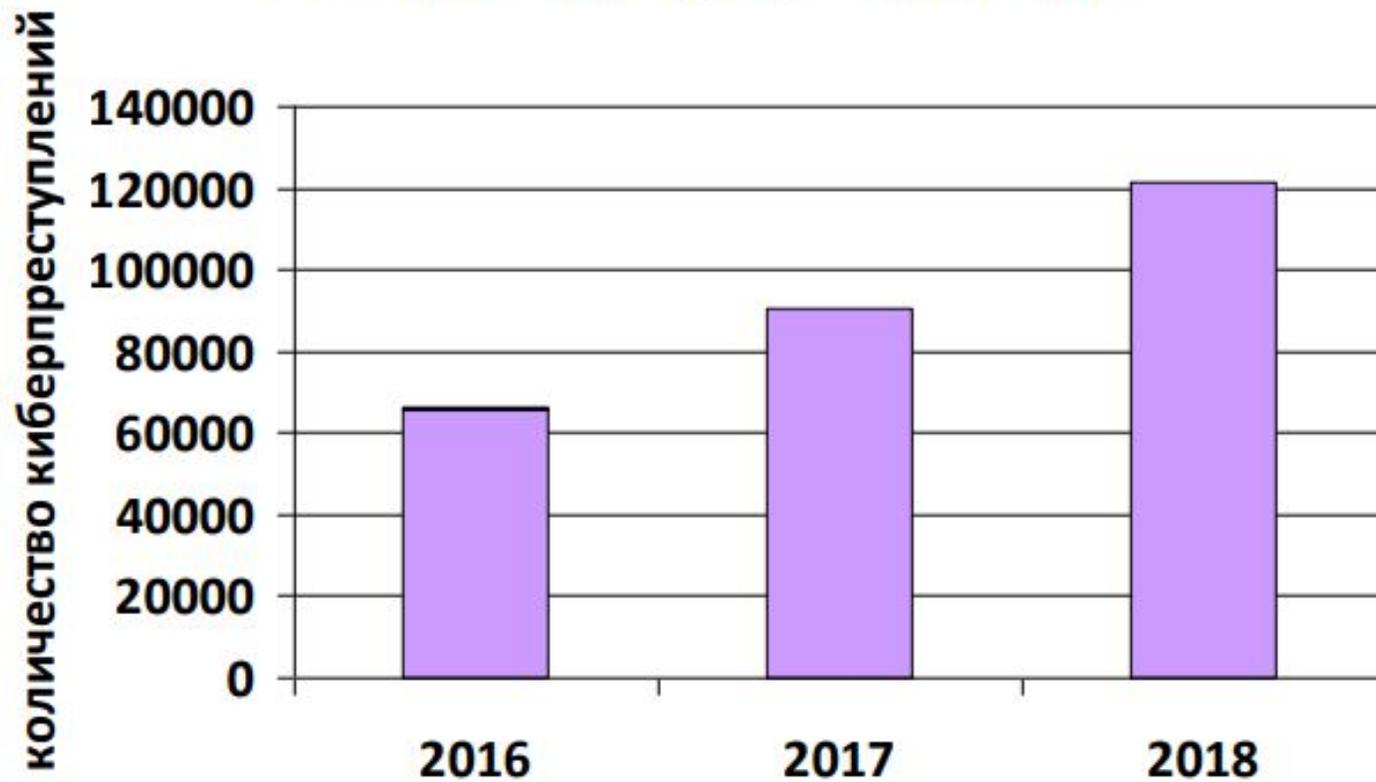
Выполнил: Голиков Илья Иванович

Руководитель: Елена Васильченко

Учебное заведение: ОГАПОУ "Валуйский колледж"

Актуальность

Рост числа киберпреступлений



Проблема

Как защитить себя от мошенничества в сети?

Гипотеза

Суть моей гипотезы в том что: все мошеннические действия производятся не по причине плохого антивируса или браузера на компьютере пользователя, а по причине глупости самого пользователя

Методы исследования

Изучение информации в интернете

Практическая значимость

Практическая значимость заключается в том что, почти у каждого человека есть доступ в интернет, и каждый человек может стать жертвой киберпреступности

Как возникает киберпреступление?

Киберпреступление, как и любое иное преступление, является плодом труда одного или нескольких злоумышленников, в данном случае с обширными знаниями в области Интернета и цифровых технологий, используемыми для достижения корыстных целей. Киберпреступники используют целый арсенал узкоспециальных знаний и навыков в целях получения несанкционированного доступа к банковским счетам, совершения краж личности, вымогательства финансовых средств, мошенничества, преследования и запугивания или использования зараженного компьютера в разветвленной сети ботнетов с целью совершения DDoS-атак на крупные организации.

Как распознать киберпреступление?

Признаки киберпреступления зависят от рода совершенного преступления. Вредоносное ПО, скрыто установленное на компьютер, может замедлять скорость его работы и служить причиной отображения большого количества сообщений об ошибках. Фишинговые атаки подразумевают получение пользователем эл. писем от неизвестных отправителей, пытающихся выманить у него пароли или личные данные. Кейлоггеры тоже обладают характерными признаками, к которым относятся появление странных иконок, дублирование введенных пользователем сообщений и т. п. С другой стороны, пользователь почти не имеет шансов распознать принадлежность своего компьютера к ботнету.

Некоторые советы по предупреждению киберпреступлений

Не загружайте файлы из непроверенных источников

Не переходите по ссылкам, содержащимся в эл. письмах отправителей, которых вы не знаете

Не сообщайте никому свои пароли и личные данные

ИСТОЧНИКИ

- <https://www.avast.ru/c-cybercrime>
- https://urgi.urfu.ru/fileadmin/user_upload/site_15503/000_subpages_projects/M_konvent/prezentacii_2020

