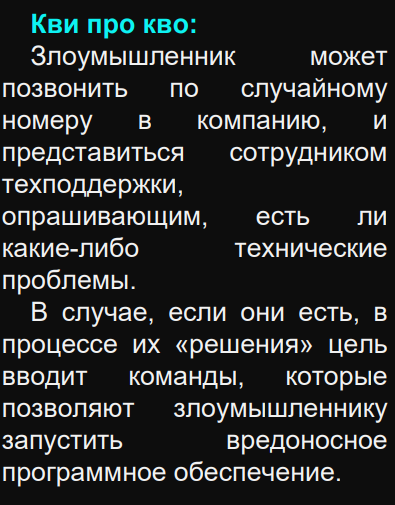
2. Quid pro quo.

фразеологизм, обычно используемый в английском языке в значении «услуга за услугу»[[3]](https://ru.wikipedia.org/wiki/Quid_pro_quo#cite_note-3).

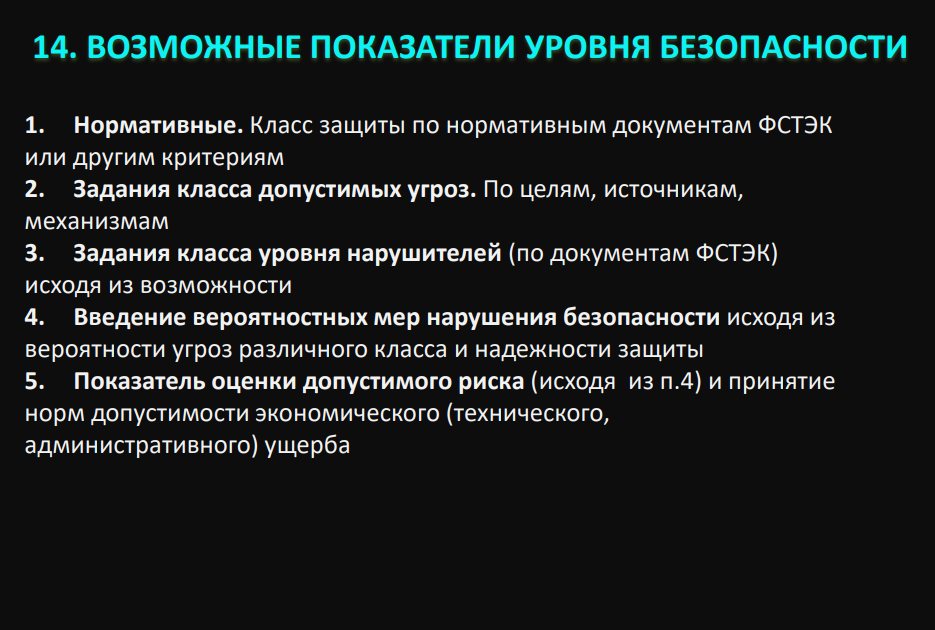


4.Ботнеты. Использование ботнетов.

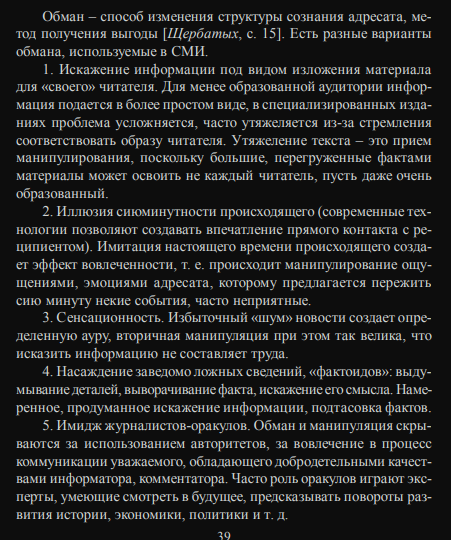
Слово «ботнет» представляет собой сочетание двух слов «робот» и «сеть» Здесь киберпреступник, выполняющий роль ботмастера, использует троянские вирусы, чтобы нарушить безопасность нескольких компьютеров и подключить их к сети в злонамеренных целях. Каждый компьютер в сети действует как «бот» и управляется мошенником для передачи вредоносных программ, спама или вредоносного контента для запуска атаки. Ботнет порой называют «армией зомби», т.к. компьютеры контролируются кем-то иным, кроме их владельца. Рекламное программное обеспечение выглядит как безвредная реклама, но использует шпионское ПО для сбора данных браузера.

Различные виды ботов могут взаимодействовать для совершения крупномасштабной кражи личных данных, что является одним из наиболее быстро растущих преступлений. С помощью ботов можно маскироваться под известный бренд и просить пользователя предоставить личные данные, такие как пароль банковского счета, данные кредитной карты, данные о налогообложении. Рекламное программное обеспечение используется для привлечения пользователей за счет рекламы на веб-страницах или в приложениях.

8. Возможные показатели уровня безопасности.



1. Дезинформация как средство манипуляции в СМИ.



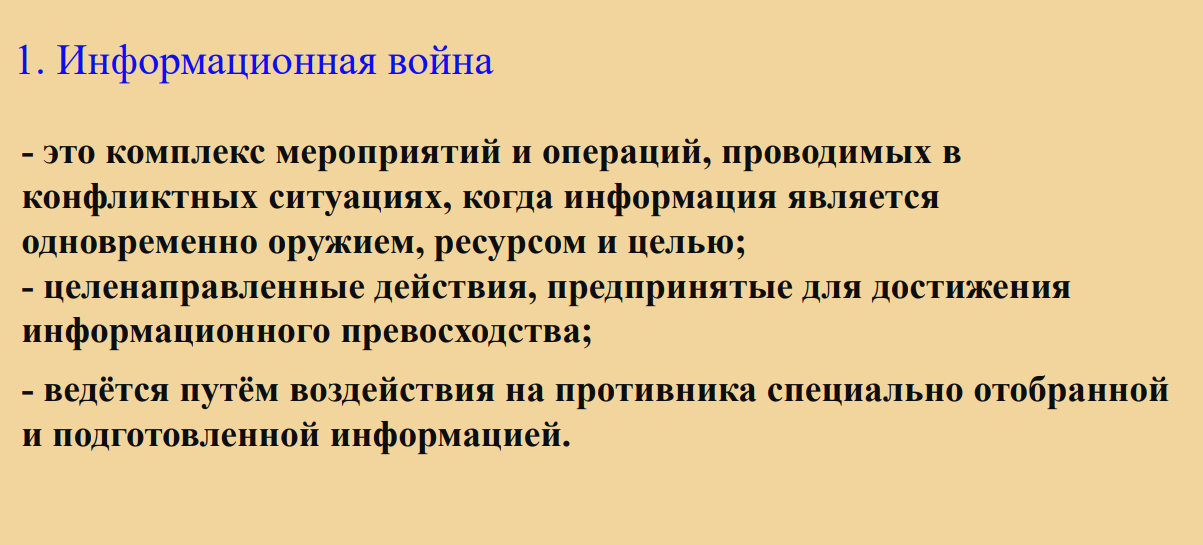
12. Интернет-мемы. Примеры.

Интернет-мем— информация в той или иной форме, как правило, остроумная и ироническая, спонтанно приобретающая популярность, распространяясь в Интернете разнообразными способами (посредством социальных сетей, форумов, блогов, мессенджеров и пр.). Обозначает также явление спонтанного распространения такой информации или фразы.

Примеры:



14. Информационная война.



18. Классификация хакеров как нарушителей информационной безопасности.

