

The Crime Of Penetrating Systems And Information Networks.

Prepared by : Rashed Hasan Husain Ayyash

Supervisor : Prof.Nabeh Saleh

Abstract:

expansion of the spread of cybercrime has become a reality in the light of the information revolution and the tremendous technological development on the various means of communication, but there is a problem raised by cybercrime is the adequacy of legislative rules to confront cybercrime and ways to prevent them.

Palestinian legislator has dealt with this type of crime in accordance with the Palestinian Law on Cybercrime No. (10) of 2018, which criminalizes and punishes crimes committed through the computer. The researcher concluded that the crime of penetration is the process that happened through the illegal entry of the computer system and the electronic networks, through which access to the data and confidential information of each dealing with it.

crime of penetration is carried out by the information criminal, and no one can call himself a hacker. He has certain characteristics that distinguish him from other experts such as competence and skill that qualify him to deal with the computer and its components. The researcher came out with a number of results,

the most important of which is: The crime of penetration is considered a crime in itself, even if it did not commit any destructive action such as disrupting the computer system, destroying the data or destroying it and other destructive acts that the criminal may resort to. According to the (4th)Paragraph of the article number (1) of the Palestinian Electronic Crimes Law No. 10 of 2018. The main recommendations of this study are: Creating a good information environment that saves safety and reliable Palestinian computer within the latest technological means Which was adopted by Article (4) of the Ministerial Resolution No. (16) for the year 2015 regarding the internal procedures of the Palestinian emergency response team.