Аннотация

В данной магистерской диссертации представлена математическая модель атаки типа «подмена доверенного субъекта», позволяющее создание на ее основе средства для обнаружения сетевых атак.

Целью магистерской диссертации является повышение безопасности транспортных протоколов телекоммуникационных систем путем управления процедурами протокола.

Для достижения поставленной цели проведены атаки типа «угадывание идентификатора» и «прогнозирование идентификатора» протокола, исследована математическая модель атаки типа «подмена доверенного субъекта», выполнен сравнительный анализ протоколов TCP и SCTP, разработана имитационная модель СМО злоумышленника.

Аңдатпа

Бұл магистрлік диссертацияда желілік кауіпті анықтайтын әдістерді құратын, «сенімді субъекті алмастыру» шабуылының математикалық моделі көрсетілген.

Магистрлік диссертацияның мақсаты хатттаманың рәсімдерін басқару арқылы телекоммуникацияның транспорттық хаттамалардың қауіпсіздігіен жақсарту болып табылады.

Осы мақсаттарды жүзеге асыру үшін «идентификаторды табу» және «идентификаторды болжау» шабуылдары жасалды, «сенімді субъекті алмастыру» шабуылының математикалық моделі қарастырылды, TCP және SCTP хаттамаларының салыстырмалы анализі жүргізілді, шабуыл жасаушының имитациалия моделі жасалынды.

Abstract

This master thesis presents a mathematical model of an attack such as "spoofing a trusted entity", which allows to create tools based on a detection of network attacks.

The purpose of the master's thesis is to improve the safety of transport protocols telecommunication systems by managing the protocol.

To achieve this goal carried out attacks like "guessing identifier" and "forecasting identifier" protocol investigated mathematical model of attack such as "spoofing a trusted entity", the comparative analysis of TCP and SCTP, designed simulation model of network attacker.