Краснодарское высшее военное училище имени генерала армии С.М. Штеменко

Доклад на тему:

АЛГОРИТМ ПРОАКТИВНОЙ ЗАЩИТЫ FTP-СЕРВЕРА ОТ КОМПЬЮТЕРНЫХ АТАК

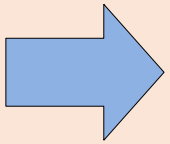
Докладчик: преподаватель Лебедкина Т.В.

Область применения алгоритма: алгоритм относится к области информационной безопасности вычислительных сетей и может быть использован в системах обнаружения атак с целью оперативного выявления и противодействия несанкционированным воздействиям на FTP-серверы, в сетях передачи данных типа «Internet».

Основная задача заключается в активном противодействии вредоносным воздействиям, за счет, предотвращения дальнейшей передачи данных злоумышленником по установленному сетевому соединению на время, которое может быть использовано службами информационной безопасности для реализации необходимых мер защиты

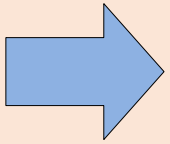
Недостатки известных алгоритмов

Относительно низкая результативность защиты FTP-сервера от несанкционированных воздействий



блокирование после заданного количества ошибок попыток авторизации, что может привести к новым попыткам несанкционированного доступа уже с учетом полученной информации о системе защиты FTP-сервера

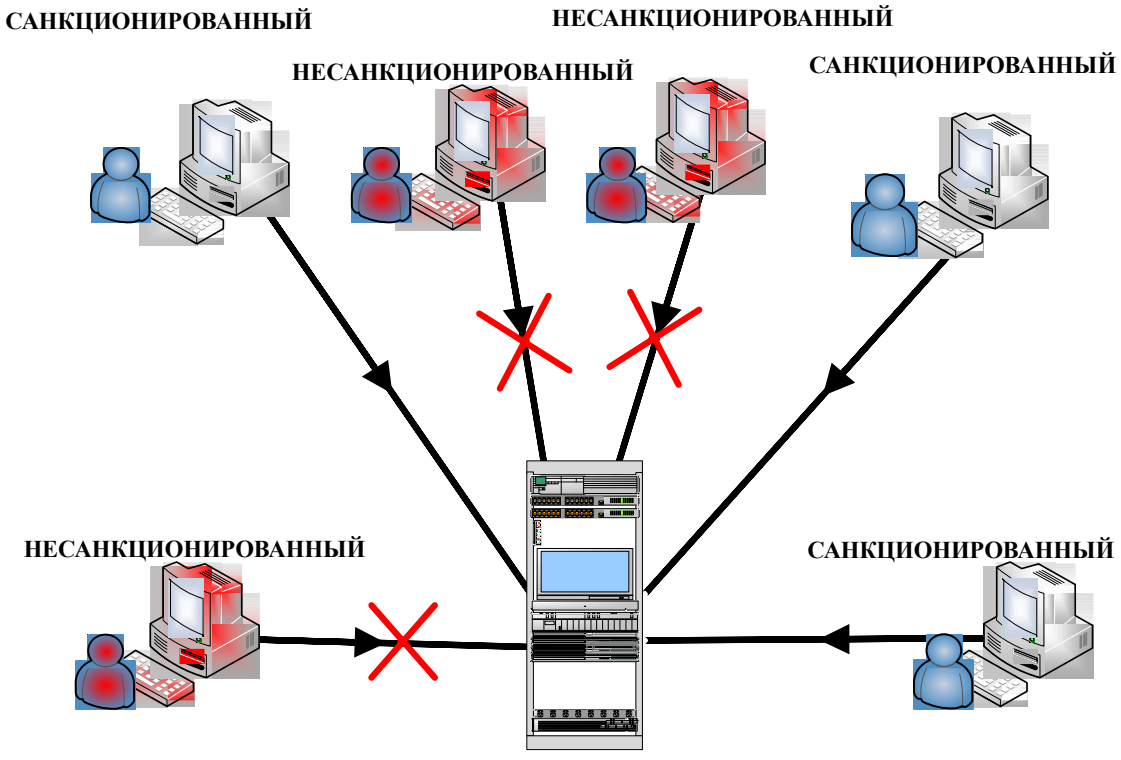
Относительно узкая область применения



разрыв соединения в случае обнаружения несанкционированных воздействий

АЛГОРИТМ ПРОАКТИВНОЙ ЗАЩИТЫ FTP-СЕРВЕРА ОТ КОМПЬЮТЕРНЫХ АТАК

Назначение алгоритма: конфигурация параметров соединений FTP-сервера и клиентов в условиях КА, обеспечивающая повышение результативности защиты за счет снижения возможностей злоумышленника по подбору имен и паролей FTP-клиентов.



Санкционированный клиент находится в состоянии установленной связи

Несанкционированный клиент находится в заблокированном состоянии

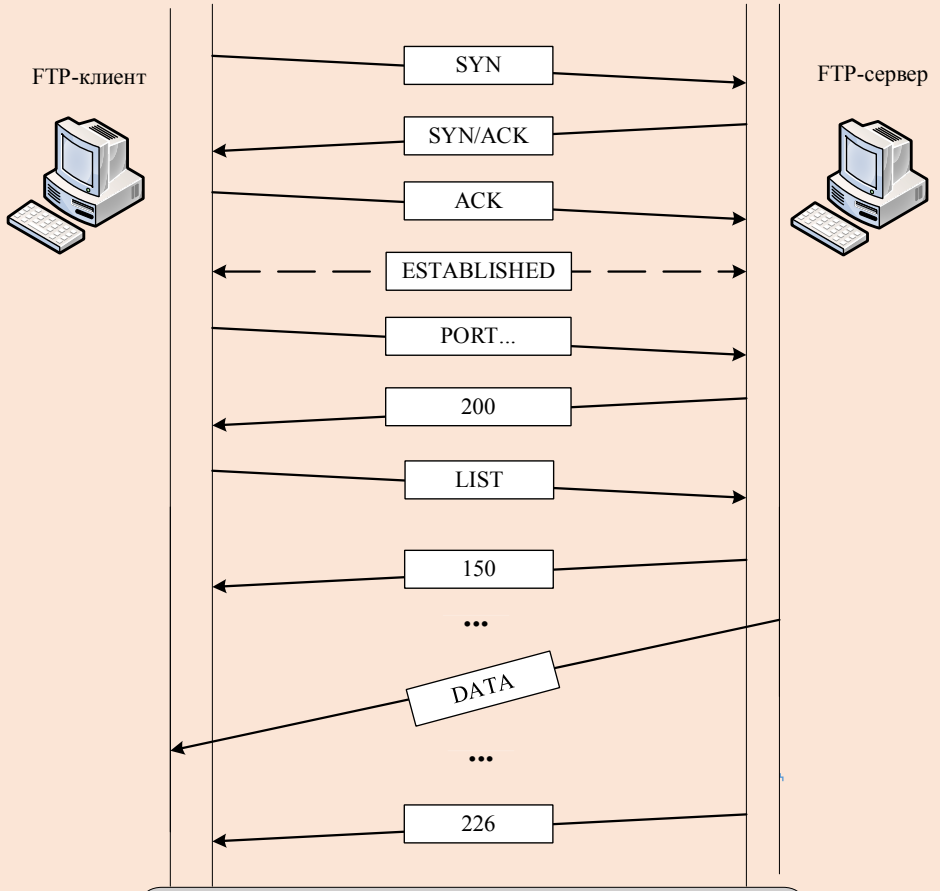
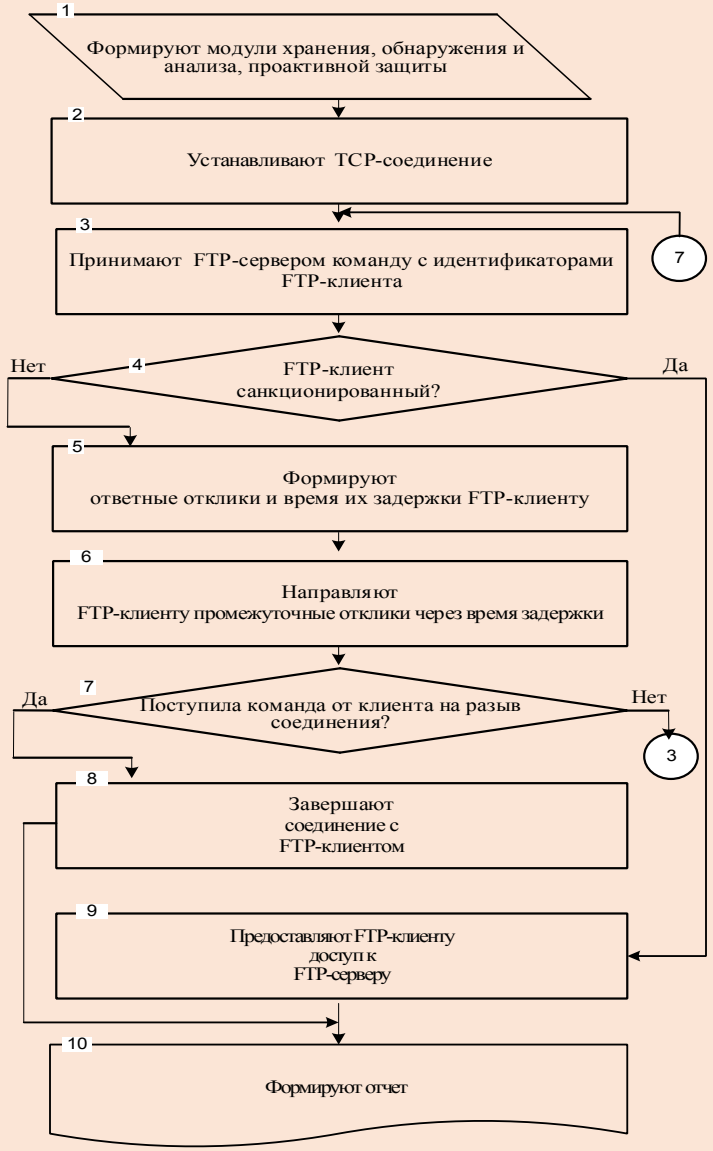


Схема установления сетевого соединения и работы FTP

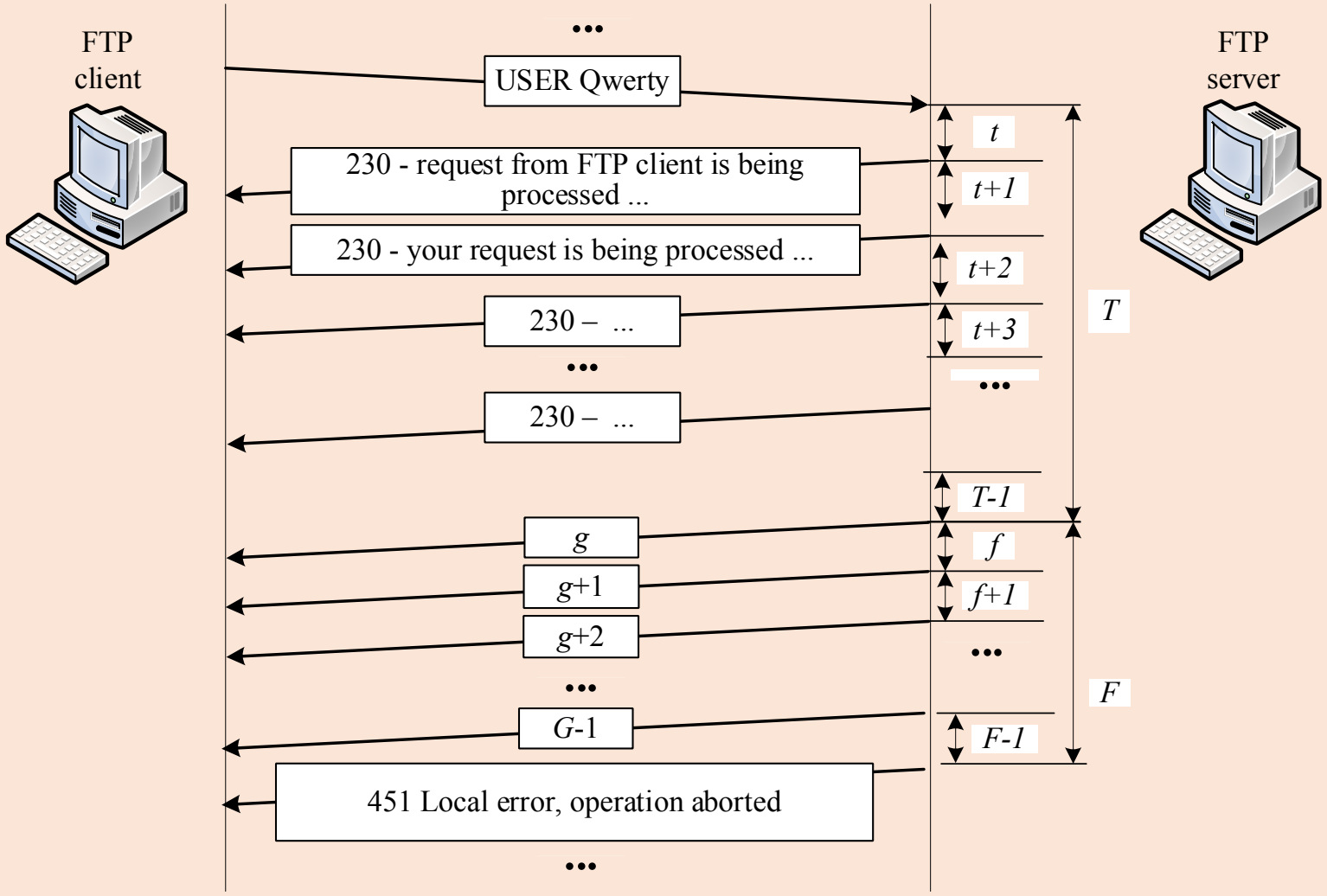
АЛГОРИТМ ПРОАКТИВНОЙ ЗАЩИТЫ FTP-СЕРВЕРА ОТ КОМПЬЮТЕРНЫХ АТАК



Блок-схема последовательности действий, реализующая алгоритм проактивной защиты FTP-сервера от компьютерных атак

Этапы алгоритма проактивной защиты FTP-сервера от КА

1	Формирование модуля хранения, модуля обнаружения и анализа, модуля проактивной защиты
2	Установление сетевого соединения FTP-клиентов с FTP-сервером
3	Направление команды с идентификаторами FTP-клиента и сравнивнение с опорными идентификаторами санкционированных FTP-клиентов
4	Формирование ответного отклика FTP-клиенту с ложным сообщением о временной ошибке, с определенным временем задержки



Фрагмент процесса авторизации FTP клиента в момент формирования и направления ему промежуточных откликов от FTP сервера

Применение ложных сообщений о временной ошибке в алгоритме является механизмом для увеличения продолжительности времени принудительного диалога со злоумышленником, обеспечивающем дискомфорт для него, а для системы защиты дополнительный временной ресурс, позволяющий ей принять дополнительные меры защиты.

ВЫВОДЫ

В алгоритме проактивной защиты FTP-сервера от КА обеспечивается повышение результативности защиты снижением возможностей злоумышленника по подбору имен и паролей, санкционированных FTP-клиентов. Это достигается имитацией канала связи с плохим качеством, обеспечивающем значительное увеличение времени для проведения атак с подбором пароля, за счет направления FTP-клиенту, не прошедшему успешную авторизацию, фрагментированного ответного отклика с ложным сообщением о временной ошибке, фрагменты которого направляются через малые интервалы времени задержки, после множества промежуточных откликов.

Разработанный алгоритм может быть использован в системах обнаружения и предупреждения КА с целью противодействия несанкционированным воздействиям в вычислительных сетях.

Спасибо за внимание