ДОДАТОК А

Схема системи з хмарною технологією

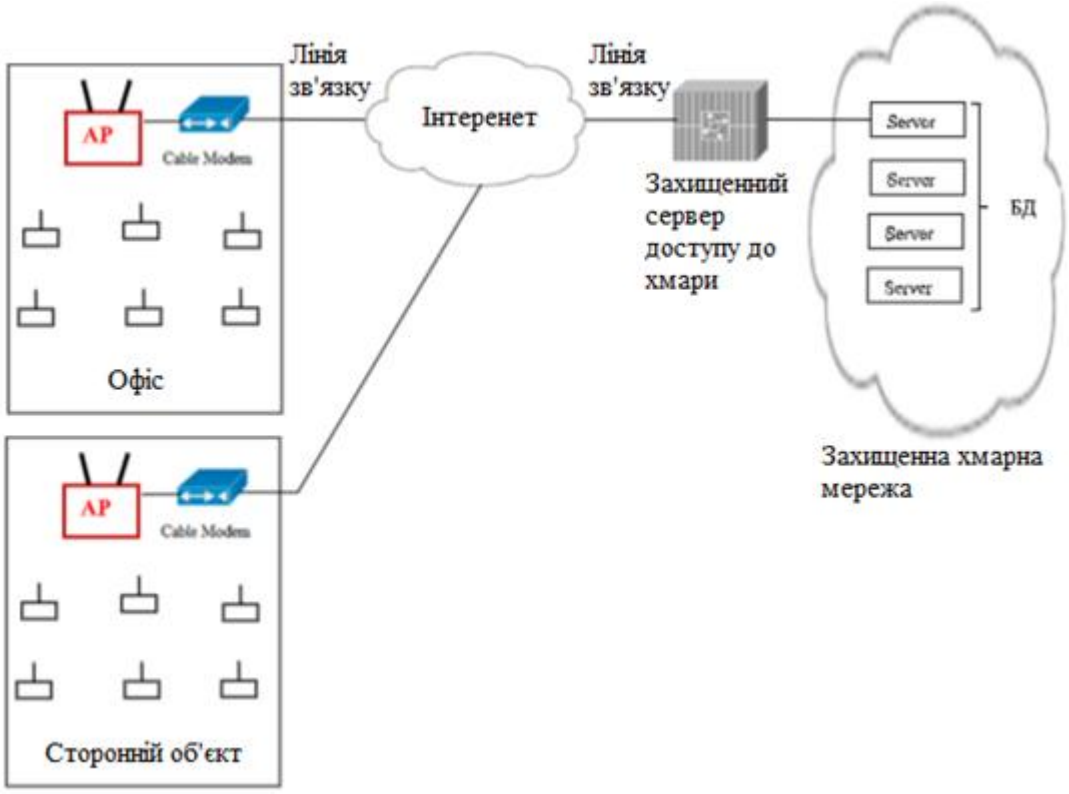

Рисунок А.1 – Схема системи для проведення аудиту

ДОДАТОК Б

Конфігурація налаштування "server.conf"

```
# Which TCP/UDP port should OpenVPN listen on?
port 1194
# TCP or UDP server?
proto tcp
# "dev tun" will create a routed IP tunnel
dev tun
# SSL/TLS root certificate (ca), certificate
# (cert), and private key (key).
ca /etc/openvpn/easy-rsa/keys/ca.crt
cert /etc/openvpn/easy-rsa/keys/server.crt
key /etc/openvpn/easy-rsa/keys/server.key # This file should be kept secret
# Diffie hellman parameters.
dh /etc/openvpn/easy-rsa/keys/dh2048.pem
# Configure server mode and supply a VPN subnet
# for OpenVPN to draw client addresses from.
# The server will take 10.8.0.1 for itself,
# the rest will be made available to clients.
# Each client will be able to reach the server
# on 10.8.0.1.
server 10.8.0.0 255.255.255.0
# Maintain a record of client <-> virtual IP address
# associations in this file. If OpenVPN goes down or
# is restarted, reconnecting clients can be assigned
# the same virtual IP address from the pool that was
# previously assigned.
ifconfig-pool-persist ipp.txt
# Uncomment this directive to allow different
# clients to be able to "see" each other.
;client-to-client
# The keepalive directive causes ping-like
```

```
# messages to be sent back and forth over
# the link so that each side knows when
# the other side has gone down.
# Ping every 10 seconds, assume that remote
# peer is down if no ping received during
# a 120 second time period.
keepalive 10 120
# For extra security beyond that provided
# by SSL/TLS
# The server and each client must have
# a copy of this key.
# The second parameter should be '0'
# on the server and '1' on the clients.
tls-auth ta.key 0 # This file is secret
# Select a cryptographic cipher.
# This config item must be copied to
# the client config file as well.
;cipher BF-CBC        # Blowfish (default)
cipher AES-128-CBC # AES
;cipher DES-EDE3-CBC # Triple-DES
# Enable compression on the VPN link.
# If you enable it here, you must also
# enable it in the client config file.
comp-lzo
# It's a good idea to reduce the OpenVPN
# daemon's privileges after initialization.
# You can uncomment this out on
# non-Windows systems.
user nobody
group nogroup
# The persist options will try to avoid
# accessing certain resources on restart
# that may no longer be accessible because
# of the privilege downgrade.
```

```
persist-key
persist-tun
# Output a short status file showing
# current connections, truncated
# and rewritten every minute.
status openvpn-status.log
#For log messages
log-append openvpn.log
# Set the appropriate level of log
verb 3
```

ДОДАТОК В

Приклад файла налаштування Virtual Private Network клієнта

```
##############################################
# Sample client-side OpenVPN 2.0 config file #
# for connecting to multi-client server.     #
#                                            #
# This configuration can be used by multiple #
# clients, however each client should have   #
# its own cert and key files.                #
#                                            #
# On Windows, you might want to rename this  #
# file so it has a .ovpn extension           #
##############################################
# Specify that we are a client and that we
# will be pulling certain config file directives
# from the server.
client
# Use the same setting as you are using on
# the server.
# On most systems, the VPN will not function
# unless you partially or fully disable
# the firewall for the TUN/TAP interface.
;dev tap
dev tun
# Windows needs the TAP-Win32 adapter name
# from the Network Connections panel
# if you have more than one. On XP SP2,
# you may need to disable the firewall
# for the TAP adapter.
;dev-node MyTap
# Are we connecting to a TCP or
# UDP server? Use the same setting as
```

```
# on the server.
proto tcp
;proto udp
# The hostname/IP and port of the server.
# You can have multiple remote entries
# to load balance between the servers.
remote 192.168.1.2 1194
;remote my-server-2 1194
# Choose a random host from the remote
# list for load-balancing. Otherwise
# try hosts in the order specified.
;remote-random
# Keep trying indefinitely to resolve the
# host name of the OpenVPN server. Very useful
# on machines which are not permanently connected
# to the internet such as laptops.
resolv-retry infinite
# Most clients don't need to bind to
# a specific local port number.
nobind
# Downgrade privileges after initialization (non-Windows only)
;user nobody
;group nogroup
# Try to preserve some state across restarts.
persist-key
persist-tun
# If you are connecting through an
# HTTP proxy to reach the actual OpenVPN
# server, put the proxy server/IP and
# port number here. See the man page
# if your proxy server requires
# authentication.
;http-proxy-retry # retry on connection failures
;http-proxy [proxy server] [proxy port #]
```

```
# Wireless networks often produce a lot
# of duplicate packets. Set this flag
# to silence duplicate packet warnings.
;mute-replay-warnings
# SSL/TLS parms.
# See the server config file for more
# description. It's best to use
# a separate .crt/.key file pair
# for each client. A single ca
# file can be used for all clients.
ca ca.crt
cert client.crt
key client.key
# Verify server certificate by checking
# that the certicate has the nsCertType
# field set to "server". This is an
# important precaution to protect against
# a potential attack discussed here:
# http://openvpn.net/howto.html#mitm
# To use this feature, you will need to generate
# your server certificates with the nsCertType
# field set to "server". The build-key-server
# script in the easy-rsa folder will do this.
ns-cert-type server
# If a tls-auth key is used on the server
# then every client must also have the key.
tls-auth ta.key 1
# Select a cryptographic cipher.
# If the cipher option is used on the server
# then you must also specify it here.
cipher AES-128-CBC
# Enable compression on the VPN link.
# Don't enable this unless it is also
# enabled in the server config file.
```

```
comp-lzo
# Set log file verbosity.
verb 3
log mylog.log
# Silence repeating messages
;mute 20
```