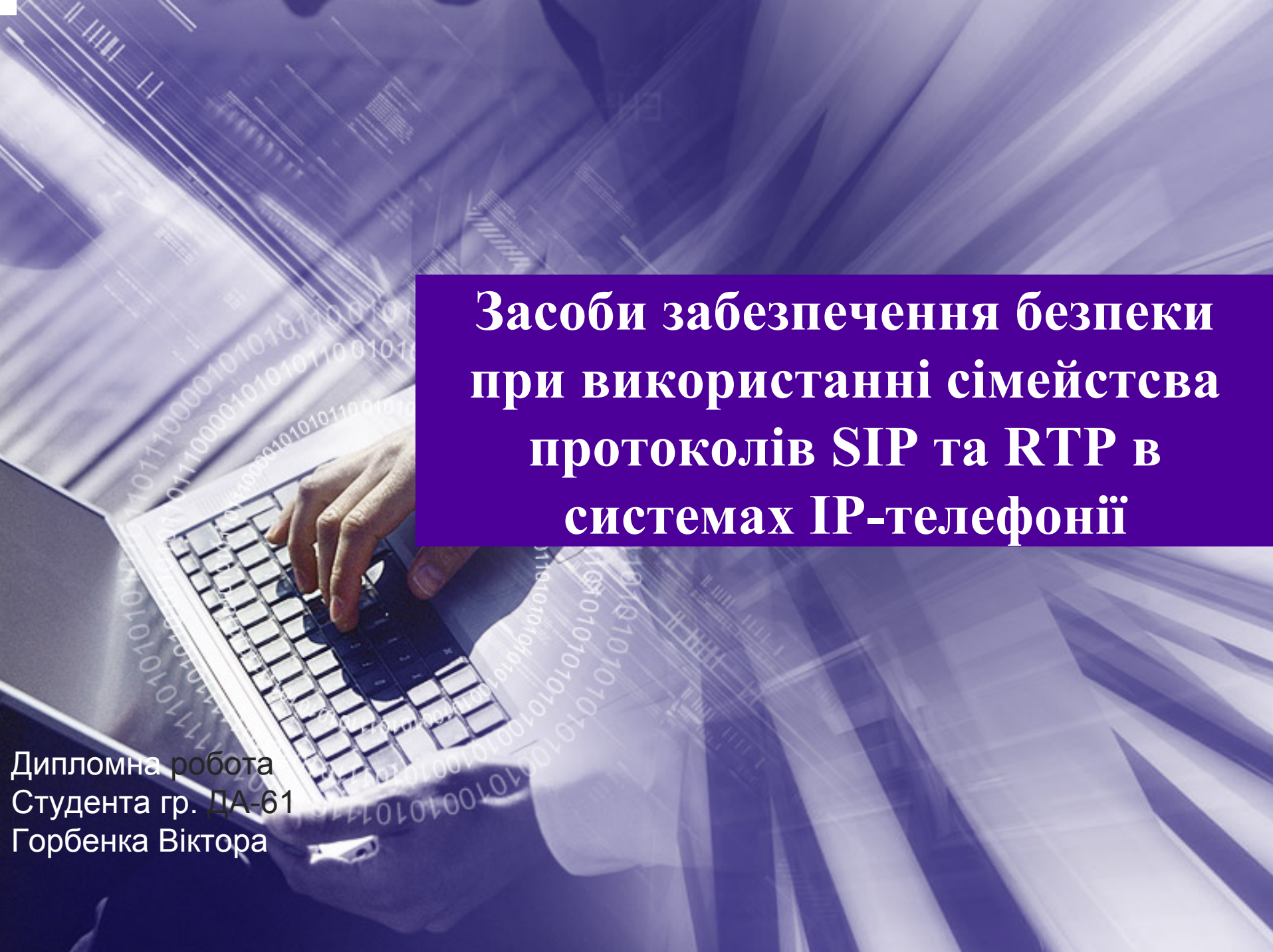


Засоби забезпечення безпеки при використанні сімейстсва протоколів SIP та RTP в системах IP-телефонії

Дипломна робота
Студента гр. ДА-61
Горбенка Віктора

Мета роботи

Визначення рекомендацій щодо шляхів забезпечення інформаційної безпеки при використанні сімейства протоколів SIP/RTP в системах IP-телефонії

Етапи робіт

1. Виявлення та систематизування можливих загроз в системах IP-телефонії
2. Аналіз та визначення засобів захисту сигнальних протоколів
3. Визначення та систематизування засобів захисту систем IP-телефонії
4. Аналіз різних реалізацій систем IP-телефонії
5. Визначення практичних рекомендації для розробки та впровадження систем захисту IP-телефонії

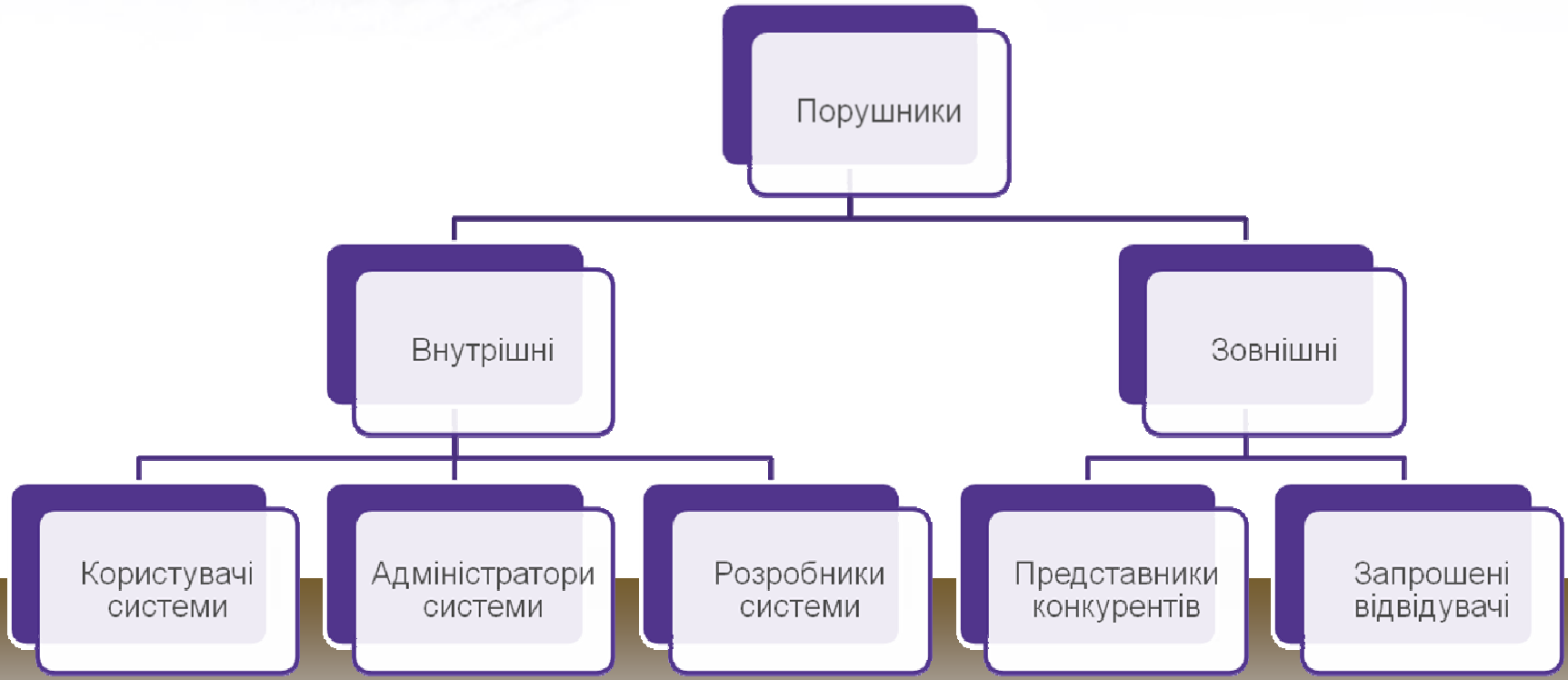
Актуальність

Make more money

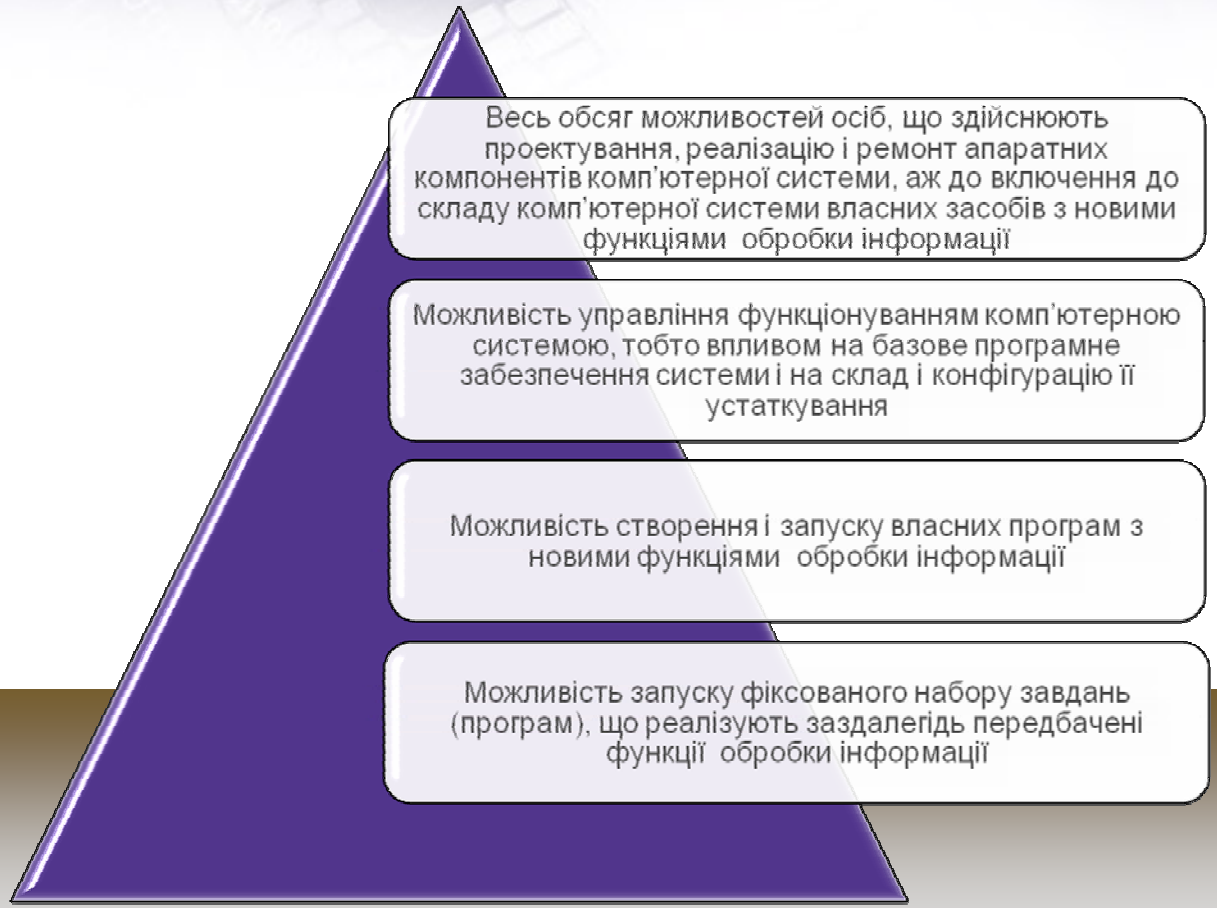
Аналіз можливих загроз та їх класифікація

Загроза	Конфіденційність	Цілісність	Доступність
Перехоплення даних	Так	Так	Ні
Відмова в обслуговуванні	Ні	Так	Так
Крадіжка сервісів та махінації з рахунком	Так	Так	Ні
Атаки на абонентські вузли	Так	Так	Так
Атаки на вузли системи	Так	Так	Так
Незамовлені виклики	Ні	Так	Так

Модель порушника



Ієрархія порушників



Безпека протоколів

Засоби організації безпеки SIP

Методи автентифікації: PSK – приватні ключі PKI – інфраструктура відкритих ключей	Автенти-фікація	Ціліс-ність	Конфіден-ційність
Базова автентифікація HTTP 1.0	PSK	Ні	Ні
Автентифікація HTTP 1.1	PSK	Ні	Ні
PGP	PKI	Так	Так
Безпечний MIME (s/MIME)	PKI	Так	Так
SIPS URI (TLS)	PKI	Так	Так
Ipsec	PKI	Так	Так

Безпека RTP

Для забезпечення шифрування, автентифікації та цілісності в протоколі RTP компаніями Cisco Systems та Ericson був розроблений безпечний протокол передачі реального часу SRTP.

Для шифрування та дешифрування даних використовується алгоритм AES. Використовують його у двох режимах:

- ✓ режим сегментованого розрахунку цілого числа
- ✓ режим f8

Механізми та засоби захисту систем IP-телефонії

- Фізична безпека
- Контроль доступу

- Криптографічний захист
- Мережева безпека

- Автентифікація
- Мережеві екрани та системи моніторингу

Програмні клієнти

Програма	Опера-ційні системи	Ліцензія	Протоколи/ засновано на/ сумісно з	Шифрування
AOL Instant Messenger	MS Windows, Mac OS	Freeware	SIP (Тільки у версії для MS Windows) RTP	Невідомо
BitWise IM	Linux, Mac OS X, Windows	Freeware / Closed Proprietary		Blowfish
Brosix	MS Windows	Freeware / Closed Proprietary		Невідомо
Cisco IP Communicator	Windows	Closed Proprietary	SCCP (Skinny), SIP, TFTP	SRTP
Coccinella	FreeBSD, Linux, Mac OS X, Windows	GPL Free software	XMPP, IAX	TLS/SSL and SASL
CounterPath X-Lite	Windows, Mac, Linux	Freeware	SIP, STUN, ICE	Невідомо
Ekiga (раніше GnomeMeeting)	Linux, (Beta Windows support)	GPL Free software	SIP, H.323, H.263, H.264/MPEG-4 AVC, STUN, Theora, Zeroconf	Немає
Empathy	Linux	GPL Free software	SIP, XMPP (Jingle), ICE (STUN/TURN), Zeroconf	Немає
Gizmo5	Windows Windows Mobile Phone, Mac OS X, Linux, Blackberry, Nokia, PDA Java	Closed Proprietary Freeware	SIP, XMPP	SRTP
Google Talk	Mac OS X, Windows XP/2000	Freeware	XMPP	Невідомо
iChat AV	Mac	Closed Proprietary	SIP AIM ICQ XMPP H.263 H.264	Невідомо
Jabbin	Linux, Windows	GPL Free software	Libjingle, XMPP	SSL
KCall	Linux (KDE)	GPL / LGPL Free software	SIP	Невідомо
KPhone	Linux (KDE)	GPL Free software	SIP, STUN, NAPTR/SRV	SRTP
Linphone	Linux and Microsoft Windows	GPL Free software	SIP	Невідомо
Lotus Sametime	Linux and Microsoft Windows, Mac OS X	Closed Proprietary	SIP, SIMPLE, T.120 and H.323	Невідомо

Програмні клієнти

Програма	Опера-ційні системи	Ліцензія	Протоколи/ засновано на/ сумісно з	Шифрування
Mercuro IMS Client	Windows XP/Windows Vista/Windows	Closed Proprietary	SIP, XCAP, MSRP, NAPTR/SRV, Dhcp, RTP, H.263, H.264	TLS-IPsec
MindSpring (раніше Vling)	Windows 2000, Windows XP	Freeware	SIP, XMPP	Невідомо
Minisip	Windows XP, 2000, Linux, Windows	GPL / LGPL Free software	SIP	SRTP, TLS, MIKEY (DH, PSK, PKE), end to end encryption
Mirial Softphone (Mirial s.u.r.l., раніше DyLogic)	Windows 2000/XP/2003/, Mac OS X (x86)	Closed Proprietary	SIP, H.323, RTSP	DTLS-SRTP
Mumble	Windows, Mac OS X, Linux, and BSD (server only)	GPLv2	Speex, CELT	SSL
OctroTalk	Symbian, Windows Mobile, and Windows	Shareware	SIP, XMPP, STUN, ICE, Libjingle and RTP (media)	TLS and SASL
OfficeSIP Messenger	Microsoft Windows	Freeware	SIP (UDP, TCP, TLS) and RTP (media)	TLS
PhoneGaim	Linux (Linspire), Windows XP/2000	GPL free software	SIP	Невідомо
QuteCom (раніше WengoPhone)	Linux, Windows XP/2000, Mac OS X	GPL free software	SIP	AES-128
SFLphone	Linux	GPL3 free software	SIP,RTP, IAX2,STUN, SRV	Немає
SightSpeed	Mac OS X / Windows	Freeware	SIP,RTP,Proprietary P2P protocol	Невідомо
SIP Communicator	Linux, Mac, Windows XP/2000 (all java supported)	LGPL free software	SIP/SIMPLE, XMPP	Secure calls with zRTP is planned for 1.0-rc1
Sippoint Mini	Windows 2000, XP, Vista, 7	Freeware	SIP, IP-MR, SpeexWB, G.711alaw, H.264, H.263	TeamSpirit Voice&Video Engine PC

Програмні клієнти

Програма	Опера-ційні системи	Ліцензія	Протоколи/ засновано на/ сумісно з	Шифрування
Skype	Windows 2000/XP, Mac OS X, Linux, Windows Mobile, iPhone	Freeware	Proprietary P2P protocol	Так
TeamSpeak	Windows, Linux, Mac OS X (unofficial)	Freeware Closed Proprietary		Немає
Telephone	Mac OS X	BSD Free Software	SIP, STUN, ICE	Немає
Tokbox	Mac OS X, Windows XP/2000, Windows	Freeware	Невідомо	Невідомо
Tpad	Windows XP, Windows 2000, Windows Vista	Freeware Closed Proprietary	SIP, STUN	Невідомо
Twinkle	Linux	GPL free software	SIP	SRTP, ZRTP
Vbuzzer	Windows XP	Closed / Proprietary freeware	SIP	TLS
Ventrilo	Windows, Mac OS X	Freeware Closed Proprietary		Немає
Windows Live Messenger	Microsoft Windows	Freeware		Невідомо
Yahoo! Messenger	Microsoft Windows, Mac OS (8, 9, X), (Linux/FreeBSD version not VoIP capable)	Freeware	SIP (using TLS) and RTP (media	Невідомо
Zfone (раніше PGPfone)	Linux, Mac OS X, Windows	Viewable source / Proprietary license (includes time bomb provision)	SIP and RTP	SRTP, ZRTP

Визначення практичних рекомендацій щодо забезпечення інформаційної безпеки систем IP-телефонії

- Рекомендації щодо захисту абонентських пристроїв
- Автентифікація
- Рекомендації щодо забезпечення конфіденційності
- Рекомендації щодо забезпечення доступності
- Рекомендації щодо забезпечення цілісності

Висновки

✓ Було проведено аналіз механізмів та засобів забезпечення інформаційної безпеки в системах IP-телефонії
✓ Були проаналізовані можливі загрози в системах IP-телефонії
✓ Був проведений аналіз можливостей протоколів IP-телефонії з точки зору забезпечення безпеки, а також додані механізми та засоби захисту систем IP-телефонії
✓ Були розглянуті системи IP-телефонії з точки зору забезпечення захисту конфіденціності, цілісності та доступності голосової інформації
✓ Були визначені практичні рекомендації щодо забезпечення інформаційної безпеки в системах IP-телефонії

Дякую за увагу