

МОДЕЛИРАНЕ НА КОРПОРАТИВНА ГЛОБАЛНА IP МРЕЖА С МУЛТИМЕДИЙНИ УСЛУГИ

Йоана Иванова

MODELLING AN ENTERPRISE GLOBAL IP NETWORK WITH MULTIMEDIA SERVICES

Yoana Ivanova

Резюме: Целта на разработката е изграждане на симулационен модел на корпоративна глобална IP мрежа с мултимедийни услуги с използване на софтуер за симулация на мрежи Cisco Packet Tracer. Разгледани са протоколи за реализиране на услугата VoIP и предоставяне на мултимедийно съдържание на крайните потребители при гарантирано високо качество на гласовите и мултимедийните услуги. Резултатът от изследването е симулационен модел, реализиран с мрежови устройства на Cisco, които са избрани поради предимствата им в сравнение други модели устройства. Приложните приноси се изразяват в намаляване на оперативните разходи и осигуряване на надеждна защита и устойчивост при максимално натоварване на мрежата.

Ключови думи: глас върху IP пакети, мултимедийни услуги, сигнализационни протоколи.

Abstract: The aim of this paper is building a simulation model of an enterprise global IP network with multimedia services using the network simulation software Cisco Packet Tracer. They are examined protocols for the realization of the VoIP service and providing multimedia content to end users with guaranteed high quality of voice and multimedia services. The result of the research is a simulation model implemented using Cisco networking devices that are selected due to their advantages compared to other device models. The applied contributions are expressed in reducing the operational costs and ensuring reliable protection and stability when the load of the network is maximum.

Keywords: Voice over IP, multimedia services, signalling protocols.

1. ВЪВЕДЕНИЕ

Технологичната обстановка през последните години се променя непрекъснато и осезаемо, както за индивидуалните потребители, така и за корпорациите. В сферата на телекомуникациите усилията са насочени към обединяване на няколко отделни услуги в една, което се нарича конвергенция. В това отношение с най-бързи темпове се развиват цифровите приложения, корпоративните системи и домашните забавления, което се обяснява с развиването на IP стандартите за мрежи и приложения.

От една страна технологичното развитие е свързано с увеличаване на видовете устройства и приложения, а от друга – с повишаване на капацитета и устойчивостта на компютърните мрежи. Конвергенцията присъства и в корпоративната инфраструктура и се изразява в обединяване на гласови и компютърни мрежи, осигуряване на видеоконферентна връзка, както и на допълнителни услуги, свързани с физическа и киберсигурност.

Симулационното моделиране е предпочитан метод за провеждане на изследвания в сферата на сигурността поради своите възможности за моделиране на сложни системи във виртуална среда при оптимална финансова инвестиция и минимален риск [1]. Най-новите устройства на Cisco са разработени така, че да осигуряват високо качество и сигурност, поради което в разработката моделът на IP мрежа с мултимедийни услуги е създаден със софтуер за симулация на мрежи Cisco Packet Tracer.

При изграждане на глобална мрежа (WAN – Wide Area Network) е необходимо да се направи анализ, свързан с:

- Потребителските потребности.
- Пропускателна способност на комуникационния канал (C) – представлява максималното количество информация (I) в битове, което може да премине през канала за единица време (t). Максимално достижимата ѝ стойност зависи от широчината на пропусканата честотна лента на канала (B) и отношението на средните мощности на сигнала и шума ($P_c/P_{ш}$). Може да се изчисли по Теоремата на Шенон – Хартли [$C = B \cdot \log_2(1 + P_c/P_{ш})$].
- Финансов разход – предвижда се на база на цената на технологиите.
- По отношение на представения модел на корпоративна глобална мрежа се акцентира върху:

- Организацията на информационните масиви.
- Сървъри за достъп до базата данни.
- Изследване на мултимедийния трафик.
- Осигуряване на стабилна и постоянна връзка.
- Гарантиране на информационната сигурност - понятието „информационно общество“ все по-широко се използва в последните години. Характеризира се с приложението на информационни и комуникационни технологии във всички икономически и социални сфери, както и с висока заетост в сферата на услугите[2]. Това налага да бъдат предприети мерки за ефективно и безпроблемно реализиране на комуникациите.

Едно от възможните решения е протоколният стек TCP/IP (Transfer Control Protocol/Internet Protocol), който се използва за унификация на комуникацията сървър-потребител. TCP гарантира последователността на приемане на пакетите от данни, докато IP извършва адресация и маршрутизация на цифрово компресирани пакети.

Всеки сървър се идентифицира чрез свой IP адрес. Въпреки че IP е технология, чието основно предназначение е преносът на глас, данни и мултимедия, съществуват проблеми, свързани със сигурността и осигуряване на високото качество на услугите, което налага да се използват и специални протоколи за сигурност.

2. ПРЕДОСТАВЯНЕ НА ГЛАСОВИ УСЛУГИ И МУЛТИМЕДИЙНО СЪДЪРЖАНИЕ С ВИСОКО КАЧЕСТВО

В процеса на моделиране на комуникационна мрежа в симулационна среда е възможно да бъдат направени специфични настройки (продължителност на симулацията, начално време, средства за защита, протоколи и др.). В настоящия раздел на разработката предстои да бъдат разгледани протоколи за предоставяне на гласови услуги и мултимедийно съдържание с високо качество.

Протоколите за предоставяне на гласови услуги в IP мрежа се обединяват под наименованието VoIP (Voice over Internet Protocol). Част от тях управляват процеса на транспортиране на IP пакети в мрежата:

- RTP (Real-time Transport Protocol) - стандартизиран в документа RFC-3550 на IETF. Този протокол и неговият сигнализационен протокол RTCP наблюдават и управляват процеса на доставяне на данните без да гарантират високо качество на услугите (QoS). Функциите на RTP се изпълняват в терминалите (крайните потребители).

- RTCP (Real Time Control Protocol) - сигнализационен протокол за RTP, описан в документа на IETF RFC-3550. Той доставя на RTP данни за състоянието на мрежата и за качеството на услугите (QoS - Quality of Service), като в конкретния случай се има предвид качеството на телефонен разговор.

- RSVP (Resource reSerVation Protocol) - управляващ протокол, който гарантира високо качество на услугите. Той се поддържа от хостовете на IP мрежата – терминали и

рутери, но не е маршрутизиращ протокол. Той формира таблици в рутерите, които съдържат данните за резервираните ресурси по различни маршрути.

Сигнализационните протоколи също са от голямо значение за реализиране на услугата VoIP, тъй като поддържат услугата “Глас върху IP пакети“ [3, 4, 5]:

- SCTP (Stream Control Transmission Protocol) - в превод означава протокол за управление на потока и представлява транспортен механизъм за предаване на сигнализационни съобщения между компонентите на протокола SIP, между които се пренася голям сигнализационен трафик.

- SDP (Session Description Protocol) - протокол за описание на сесия (документ RFC 2327 на IETF), чрез който се установяват мултимедийни сесии и се генерират съобщения до участниците в сесията (покани за участие, потвърждения, излизане от сесията). За всеки различен тип информация (видео, звук) се изисква установяване на отделна сесия.

- SAP (Session Announcement Protocol) - описан е в документа RFC 2974 на IETF и служи за обявяване на сесии, в които има множество участници (multicast sessions). Например, когато се провежда конференция, протоколът съобщава за сесии с голяма продължителност, голям териториален обхват и голям брой участници.

- SIP (Session Initiation Protocol) - протокол от приложния слой на протоколния стек TCP/IP, чиито функции са управление на установяването, поддържането и прекратяването на мултимедийни сесии между крайните потребители. SIP е протокол за инициране на сесии, опериращ на нивото на приложния слой от OSI модела, който се използва при провеждането на IP и Интернет конферентни разговори (broadcast и multicast), както и за изпращане на кратки съобщения. SIP може да бъде използван и при мобилни клиенти в съчетание с WLAN и VoIP технологии за установяване на телефонни връзки в мрежата. Конкретно в случая с VoIP сесиите са с продължителността на телефонен разговор и се прекратяват след това. Сесията може да бъде модифицирана по време на разговора. Например, ако бъде поканен трети участник в разговора (three-way calling – три-посочно повикване). Днес SIP е стандартен протокол за IP телефония, стандартизиран в множество документи на IETF.

- H.323 - протокол, чието предназначение е изграждане на мултимедийна комуникационна система, базирана на пакетен обмен. Но QoS не е гарантирано [6].

- Протоколите за осигуряване качеството на услугите в IP мрежа са:

- IntServ – протокол за интегриране на услугите, който представя всички услуги в реално време.

- DiffServ – протокол за диференциране на услугите, за който е характерно, че пакетите се обработват по метода на „приоритетните опашки“, т.е. с предимство при обработката са пакети, които пренасят информация в реално време (телефонен разговор, телевизионно изображение и др.). Потребителите се разделят на групи, а ресурсите се разпределят според класа на всяка група.

Предоставянето на мултимедийно съдържание (видео, аудио, данни, интерактивни приложения) на крайните потребители се осъществява чрез IPTV (Internet Protocol Television), който се нарича мобилна телевизия и гарантира високо качество на следните услуги:

- гледане на телевизия срещу заплащане.
- масова телевизия.
- гледане на поискване.
- интерактивна телевизия.

- протокол за трансфер на файлове – FTP (File Transfer Protocol).
- протокол за предаване на новинарски емисии - NNTP (Network News Transfer Protocol).
- протокол за пренос - трансфер на електронна поща - SMTP (Simple Mail Transfer Protocol)
- протокол за сваляне на електронна поща от пощенския сървър към текущия - POP (Post Office Protocol)/ POP3.
- протокол за осъществяване на връзка със сървъри на отдалечени разстояния – Telnet.
- протоколи за поточно предаване на мултимедия - работят през Интернет с помощта на Windows Media Player.
- протоколи за чат на живо - Facebook, Google Talk, Jabber, AIM и т.н. използват свободния XMPP (Jabber) комуникационен протокол.
- протоколи за аудио и видео конференции – мрежов протокол RTP.
- протоколи за осигуряване на защитена криптирана връзка (протоколи за VPN) - PPTP (Point to Point Tunneling Protocol) и L2TP (Layer Two Tunneling Protocol) [7, 8].

3. РЕАЛИЗИРАНЕ НА МРЕЖАТА И ОЦЕНКА НА НЕОБХОДИМИТЕ РЕСУРСИ

Архитектурното развитие изисква моделиране, което ни помага да разберем връзката между изискванията от една страна и архитектурната концепция от друга [9]. Предложеният вариант за изграждане на глобална корпоративна IP мрежа с мултимедийни услуги е реализиран с технологии на Cisco и включва:

- ASR 1000 Series Router - Cisco Aggregation Services Router, който е мощен и компактен маршрутизатор за целите на бизнеса. Той предлага следните услуги и функции: защитна стена, IPsec (Internet Protocol Security), VPNs, DPI (Deep-packet Inspection) и др. Допълнително предимство на този протокол е редуциране на разходите за експлоатация и оперативните разходи на клиентите.
- Cisco IP/TV 3430 Archive Server - предоставя и възможност да се използва предварително записан видеоклип на VOD (Video on Demand или Audio and Video on Demand) основа.
- Catalyst 2960S 24 GigE, 2 x SFP LAN Lite – WS – C2960S – 24TS – S – тези комутатори осигуряват високо ниво на защита на бизнес операциите, надеждност и устойчивост дори в условия на максимално натоварване.
- Cisco VoIP Phones - изборът на висококачествени VoIP телефони е голям [10].

За по-голяма яснота преди да бъде представена цялостната схема на мрежата, е показана легенда на отделните елементи, от които ще бъде изградена (Фиг. 1).

Концептуалният модел на корпоративна глобална IP мрежа с мултимедийни услуги е представен на Фиг. 2. Той може да бъде реализиран с използване на симулационен софтуер Cisco Packet Tracer (Фиг. 3).

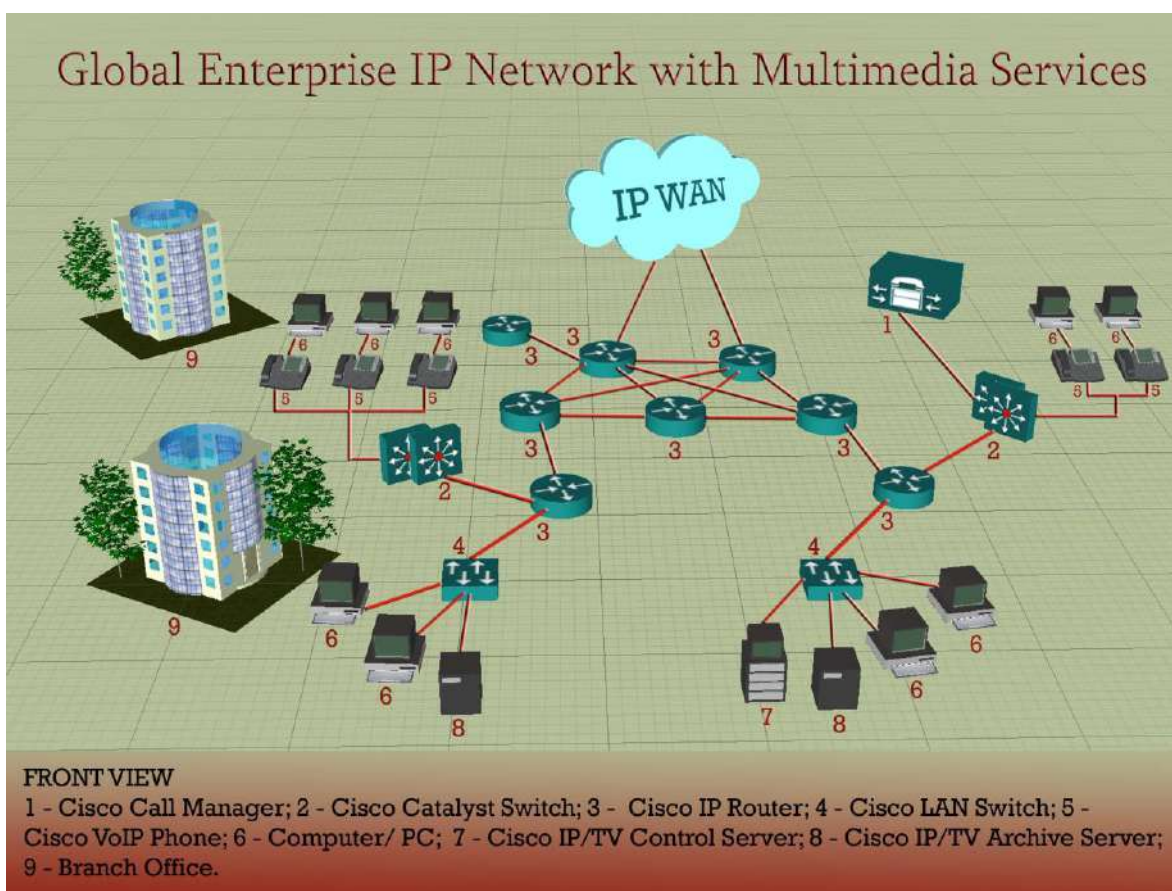
Необходимо е да има обратна връзка относно верността на конфигурацията. Когато не са установени проблеми и грешки в Realtime Mode (в долния десен ъгъл) се изписва Last Status: Successful. Пример за адресна конфигурация на компютър PC A е показан на Фиг. 4. Physical може да се види как изглежда самото устройство, като на Фиг. 5 е показан конкретен пример за Multilayer Switch 1 3560-24PS.

При избран симулационен режим (Simulation Mode) вдясно от работното пространство се отваря Simulation Panel. В него могат да бъдат редактирани филтрите (Event List Filters), като активни да останат само някои (например ARP и ICMP). ARP софтуерът поддържа таблица със съответствията между IP и Ethernet адресите. Тази таблица се създава динамично. Когато ARP получи заявка за съпоставяне на IP адрес, той проверява

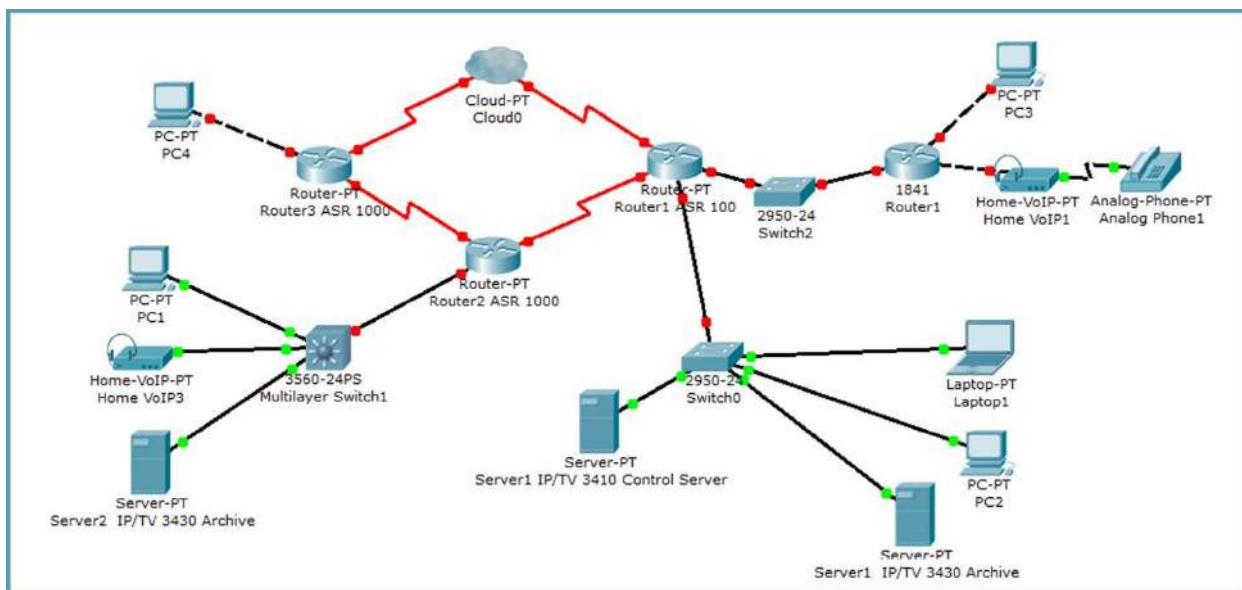
дали този адрес е в таблицата. Ако намери адреса, връща Ethernet адреса на изпратилия заявката софтуер.



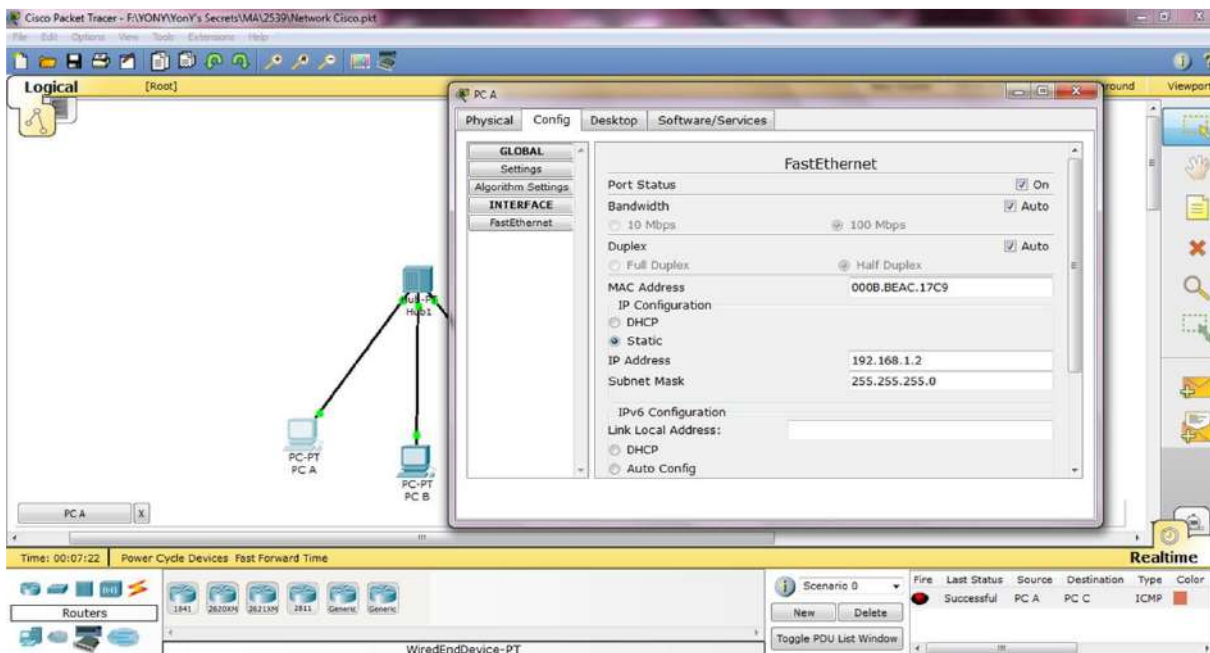
Фиг. 1. Легенда на мрежовите елементи.



Фиг. 2. Концептуален модел на корпоративна глобална IP мрежа с мултимедийни услуги.



Фиг. 3. Модел на корпоративна глобална IP мрежа с мултимедийни услуги, изграден в Cisco Packet Tracer.

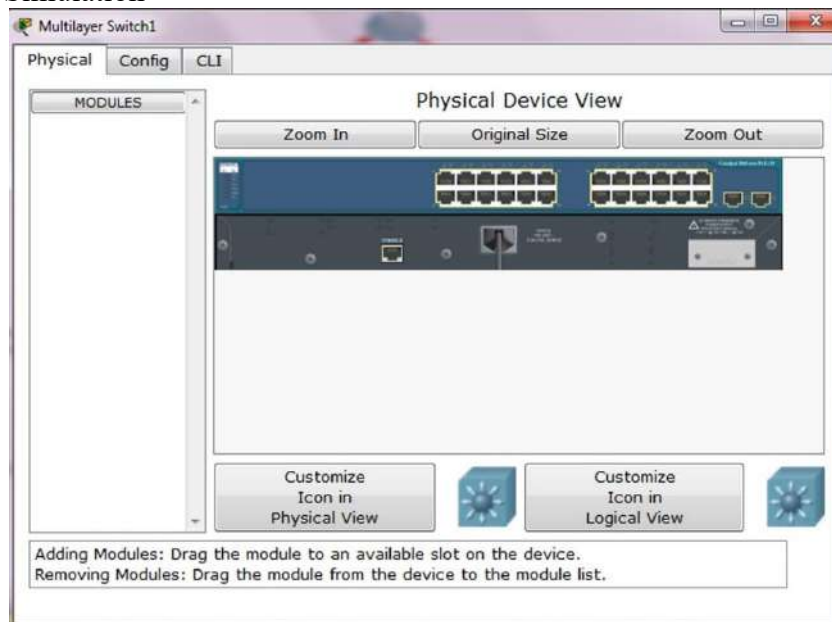


Фиг. 4. Адресна конфигурация на компютър в Cisco Packet Tracer.

Ако адресът не е в таблицата, ARP изпраща единичен пакет до всеки хост от Ethernet сегмента. Този пакет съдържа IP адреса, за който се търси съответстващия Ethernet адрес. Ако някой от получаващите хостове идентифицира IP адреса като свой, той отговаря като изпраща Ethernet адреса си на изпратилия заявката хост. Отговорът след това се съхранява в ARP таблицата [11].

За да бъде създаден сценарий първо се активира иконка Add Simple PDU и последователно се кликва върху устройството, което е избрано да бъде източник, а след това и върху устройството, което ще изпълнява функцията на приемник или крайна точка. Симулацията се стартира с натискане на бутона Auto Capture/Play, а разположеният под

него плъзгач се явява регулатор на скоростта. Симулацията може да бъде изтрита с помощта на бутона Reset Simulation



Фиг. 5. Multilayer Switch 1 3560-24PS в Cisco Packet Tracer.

4. ЗАКЛЮЧЕНИЕ

IP мултимедийните мрежи и тяхната оптимизация от гледна точка на разнообразие, високо качество и възможности на гласовите и мултимедийните услуги, са от съществено значение за развитието на съвременното информационно общество. Услугите, които предоставят достъп до мултимедийно съдържание в реално време, спомагат за усъвършенстване на телекомуникациите чрез реализиране на широкомащабна телеконференция, провеждане на Web – базирани обучения в Интернет, както и на видео-телеобучения с възможност за задаване на въпроси по телефона.

Поради еволюцията на кибер заплахите е необходимо да бъде осигурена надеждна защита на мрежите чрез намиране на оптималната комбинация от антивирусен софтуер, протоколи за сигурност, мрежови устройства, защитни стени и др. [12, 13]. В съвременната динамична среда за сигурност, свързана с развитието на информационните технологии, се налага използването на модерни социални приложения. Тези продукти дават възможност да се наблюдава разрастването на мрежата и свободно да се навигира през различни връзки и мрежи [14].

Процесът на изграждане на мрежовия модел е първият етап от цялостното изследване на дадена система в избрана симулационна среда. На този етап се проверява доколко е правилна конфигурацията и дали при стартиране на симулацията се наблюдава проблем със свързаността или съвместимостта на използваните мрежови устройства. Необходимо е внимателно запознаване с опциите за настройка на устройствата и входните параметри, за да може да се даде посока на изследването, т.е. с негова помощ да се реши конкретен проблем.

На следващ етап от изследването може да бъде проведена симулация на кибератака върху системата с цел предварително да се установи доколко тя е устойчива на негативно въздействие от такъв характер. В случай, че предприетите мерки за защита на мрежата се окажат недостатъчно ефективни, следва да се проведе нова серия от експерименти с други

средства за защита. На практика финансовата инвестиция в професионален симулационен продукт е оправдана, тъй като разходите за възстановяване на системата при евентуално реализиране на кибератака биха я надвишили многократно.

ЛИТЕРАТУРНИ ИЗТОЧНИЦИ:

1. ЧЕРВЕНЯКОВ, Стоян и Иван ХРИСТОЗОВ. Възможности за въвеждане на нови подходи и информационни технологии във военното образование. В: *Сборник доклади от Юбилейна научна конференция „140 години военно образование - традиции и перспективи“*. Велико Търново: Национален военен университет „Васил Левски“, 2019, с. 120-130. ISBN 978-954-753-283-0. CHERVENYAKOV, Stoyan i Ivan HRISTOZOV. Vazmozhnosti za vvezhdane na novi podhodi i informatsionni tehnologii vav voennoto obrazovanie. V: *Sbornik dokladi ot YUbileyna nauchna konferentsiya „140 godini voenno obrazovanie - traditsii i perspektivi“*. Veliko Tarnovo: Natsionalen voenen universitet „Vasil Levski“, 2019, s. 120-130. ISBN 978-954-753-283-0.
2. ЧЕРВЕНЯКОВ, Стоян. Информацията като фактор на международната сигурност в условията на информационното общество. В: *Сборник доклади от годишната научна конференция на факултет „Национална сигурност и отбрана“, Военна академия „Г. С. Раковски“ 17-18 май 2018 г.* 2018, (1), с. 103-106. ISBN 978-619-7478-05-1. CHERVENYAKOV, Stoyan. Informatsiyata kato faktor na mezhdunarodnata sigurnost v usloviyata na informatsionnoto obshtestvo. V: *Sbornik dokladi ot godishnata nauchna konferentsiya na fakultet „Natsionalna sigurnost i otbrana“, Voenna akademiya „G. S. Rakovski“ 17-18 may 2018 g.* 2018, (1), s. 103-106. ISBN 978-619-7478-05-1.
3. КЪДРЕВ, Васил и Ангел ГУШЕВ. *Комутиционна и мултиплексна техника*. София: Висше транспортно училище „Т. Каблешков“, 2011. ISBN 978-954-12-0190-9. KADREV, Vasil i Angel GUSHEV. *Komutatsionna i multipleksna tehnika*. Sofiya: Visshe transportno uchilishte „T. Kableshkov“, 2011. ISBN 978-954-12-0190-9.
4. КЪДРЕВ, Васил, Анушка СТАНЧЕВА и Росен ПАСАРЕЛСКИ. Анализ на влиянието на средствата за мрежова и информационна конфиденциалност върху сигнализацията в телекомуникационните мрежи. *Сборник доклади от Научна конференция „Актуални проблеми на сигурността“ 26-27 Октомври 2017 г.* Велико Търново: Издателски комплекс на НВУ „Васил Левски“, 2017, с. 454-464. ISSN 2367-7473. KADREV, Vasil, Anushka STANCHEVA i Rosen PASARELSKI. Analiz na vliyanieto na sredstvata za mrezhova i informatsionna konfidentsialnost varhu signalizatsiyata v telekomunikatsionnite mrezhi. *Sbornik dokladi ot Nauchna konferentsiya „Aktualni problemi na sigurnostta“ 26-27 Oktomvri 2017 g.* Veliko Tarnovo: Izdatelski kompleks na NVU „Vasil Levski“, 2017, s. 454-464. ISSN 2367-7473.
5. КЪДРЕВ, Васил и Росен ПАСАРЕЛСКИ. Аспекти на влиянието на сигурността и сигнализацията върху QOS при VOIP. *Сборник доклади от Научна конференция „Актуални проблеми на сигурността“ 25-25 октомври 2018 г.* Велико Търново: Издателски комплекс на НВУ „Васил Левски“, 2018, с. 612-622. ISSN 2367-7473. KADREV, Vasil i Rosen PASARELSKI. Aspekti na vliyanieto na sigurnostta i signalizatsiyata varhu QOS pri VOIP. *Sbornik dokladi ot Nauchna konferentsiya „Aktualni problemi na sigurnostta“ 25-25 oktomvri 2018 g.* Veliko Tarnovo: Izdatelski kompleks na NVU „Vasil Levski“, 2018, s. 612-622. ISSN 2367-7473.
6. ПЕНЕВ, Николай. *Съвременни комуникационни системи и технологии. Възможности, приложение, развитие*. София: Ваньо Недков, 2008. ISBN 978-954-9462-27-2. PENEV, Nikolay. *Savremenni komunikatsionni sistemi i tehnologii. Vazmozhnosti, prilozhenie, razvitie*. Sofiya: Vanyo Nedkov, 2008. ISBN 978-954-9462-27-2.
7. ШИНДЕР, Дебора Литълдзон. *Компютърни мрежи*. София: Софтпрес, 2003. ISBN 978-954-685-254-0. SHINDER, Debora Litaldzhon. *Kompyutarni mrezhi*. Sofiya: Softpres, 2003. ISBN 978-954-685-254-0.
8. КОМЪР, Брайан. *TCP/IP Мрежи и административане*. София: Инфодар, 1999. ISBN 954-8485-55-9. KOMAR, Bruyan. *TCP/IP Mrezhi i administrativane*. Sofiya: Infodar, 1999. ISBN 954-8485-55-9.
9. ALEKSANDROVA, Veselina, Anna GUNCHEVA, Miroslav KOCHANKOV, Vania TAGAREVA and Violeta VASILEVA. An approach for defining the system design of information infrastructure. In: *Human Systems Integration Approach to Cyber Security. Proceedings of International Conference, 28-29 September 2015, Sofia, Bulgaria*. 2016, pp. 145-155. ISBN 978-954-9348-77-4.
10. Design Zone-Design Guides. Cisco [online]. [viewed 02 January 2020]. Available from: <https://www.cisco.com/c/en/us/solutions/design-zone.html>
11. НИКОЛОВ, Атанас и Иван ХРИСТОЗОВ. Корпоративна защита на информацията. Подход и решения. *Годишник на Военна академия-ИПИО*. София: Военна академия „Георги Стойков Раковски“, Институт за перспективни изследвания за отбраната, 2005, с. 194-204. ISSN 1312-0816. NIKOLOV, Atanas i Ivan HRISTOZOV. Korporativna zashtita na informatsiyata. Podhod i resheniya. *Godishnik na Voenna akademiya-IPIO*. Sofiya: Voenna akademiya „Georgi Stoykov Rakovski“, Institut za perspektivni izsledvaniya za otbranata, 2005, s. 194-204. ISSN 1312-0816.
12. НИКОЛОВ, Атанас и Иван ХРИСТОЗОВ. Проблеми и предизвикателства пред изграждането на национална система за киберсигурност. *Военен журнал*. 2015, (3), с. 7-13. ISSN 0861-7392. NIKOLOV, Atanas i Ivan HRISTOZOV. Problemi i predizvikatelstva pred izgrazhdaneto na natsionalna sistema za kibersigurnost. *Voenen zhurnal*. 2015, (3), s. 7-13. ISSN 0861-7392.

13. АЛЕКСАНДРОВА, Веселина, Илина АРМЕНЧЕВА и Георги ПАВЛОВ. Прилагане на технология за цифрово видео в динамична среда за сигурност. В: *Сборник доклади от Научна конференция „Актуални проблеми на сигурността” 16-18 октомври 2013.* 2013, (4), с. 94-103. ISBN 978-954-753-200-7. ALEKSANDROVA, Veselina, Iilina ARMENCHEVA i Georgi PAVLOV. Prilagane na tehnologiya za tsifrovo video v dinamichna sreda za sigurnost. V: *Sbornik dokladi ot Nauchna konferentsiya „Aktualni problemi na sigurnostta” 16-18 oktombri 2013.* 2013, (4), s. 94-103. ISBN 978-954-753-200-7.

Информация за автора/ите:

Асистент, Инж. Йоана Атанасова Иванова, Департамент „Телекомуникации“ НБУ, ул. Монтевидео 21, e-mail: yivanova@nbu.bg

Contacts:

Assistant, Eng. Yoana Atanasova Ivanova, New Bulgarian University, Department Telecommunications, Sofia, 21 Montevideo St., e-mail: yivanova@nbu.bg

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 22.07.2019

Дата на приемане за публикуване (Date of adoption for publication): 27.09.2019