ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5

©Л.Н. Гумилев атындағы Еуразия ұлттық университеті, 2024

ӘОЖ 004.056

ТЕЛЕКОММУНИКАЦИЯЛЫҚ ҰЙЫМДАР ҮШІН ҚАУІПСІЗ VPN СЕРВЕР ҚОЛДАНЫСТАРЫ

Жандабергенова Ләззат Мұратқызы
zhandabergenovalyako@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық университетінің Ақпараттық қауіпсіздік кафедрасының магистранты, Астана, Қазақстан
Ғылыми жетекші – Сантеева С.Ә.

Аңдатпа: Мақалада қауіпсіз және заманауи VPN телекоммуникациялық ұйымдар үшін маңызды және қазіргі таңда қолданысқа ие екендігіне шолу келтірілген.

Түйінді сөздер: Телекоммуникация, заманауи VPN, сервер, шифрлану, киберқауіп, құпия ақпарат, қауіпсіздік.

Технологияның дамуы әртүрлі салаларға, соның ішінде телекоммуникация саласына көптеген өзгерістер әкелді. Телекоммуникация ұйымдары деректердің үлкен көлемімен айналысады және олардың желісін ықтимал қауіпсіздік бұзылуларынан қорғауды қамтамасыз ету үшін қауіпсіз және заманауи VPN серверін қажет етеді.

VPN Интернет сияқты жалпыға ортақ желі арқылы қауіпсіз және жеке желі қосылымын жасауға мүмкіндік береді. Пайдаланушылар құпия ақпаратқа VPN арқылы деректерді ұстап алу немесе ұрлаудан қорықпай қол жеткізе алады және бөлісе алады. VPN пайдалану арқылы пайдаланушылар желідегі байланыстар үшін қосымша қауіпсіздік деңгейін қамтамасыз ететін негізгі қоғамдық желіден бөлек нысан ретінде жұмыс істейтін виртуалды желіні құра алады. Қауіпсіз және заманауи VPN серверін енгізу арқылы телекоммуникация ұйымдары өз операцияларының тиімділігі мен қауіпсіздігін жақсарта алады, шығындарды азайтады және бәсекеге қабілеттілігін арттырады.

Виртуалды желі ол пайдаланатын негізгі байланыс арналарына тәуелсіз жұмыс істейді. Оған кіретін пайдаланушы оны иеленбейді, себебі физикалық желі (бір-бірімен байланыстырылған компьютерлерден немесе құрылғылардан тұратын) басқа біреуге тиесілі. Жеке желі тек шектеулі тұлғалардың қатысуына мүмкіндік береді. Барлық мүшелер және олардың жіберілген ақпараты VPN жүйесінде анықталуы мүмкін. Рұқсат етілмеген тұлғалардан деректерді қорғау үшін шифрлау қолданылады. VPN рұқсат етілмеген пайдаланушыларға қол жеткізуді бұғаттап, трафиктің шығуын тексеріп және жіберілген деректердің желіде шифрланбағанын қамтамасыз ету арқылы ақпараттың құпиялылығын сақтауға жауапты [2].

VPN серверлері пайдаланушы мен интернет арасында тасымалданатын деректерді қорғау үшін шифрлау алгоритмдерін пайдаланады. Ең жиі қолданылатын шифрлау протоколдары PPTP, L2TP/IPSec және OpenVPN болып табылады. Бұл протоколдар қауіпсіздіктің әртүрлі деңгейлерін ұсынады, бірақ OpenVPN ең қауіпсіз болып саналады. Пайдаланушы мен VPN сервері арасында жіберілетін деректер рұқсат етілмеген тұлғалардың ұстамауын қамтамасыз ету үшін екі жағынан да шифрланады. VPN серверін пайдаланудың негізгі артықшылықтарының бірі - белгілі бір аймақта шектелуі мүмкін мазмұнға қол жеткізу мүмкіндігі. Мысалы, белгілі бір веб-сайттар бұғатталған елде орналасқан пайдаланушы сол веб-сайттарға кіру үшін басқа елде орналасқан VPN серверін пайдалана алады. VPN сервері делдал ретінде әрекет етеді, пайдаланушының интернет-трафикін серверлері арқылы бағыттайды, бұл пайдаланушы басқа елде орналасқандай көрінеді [1].

Қауіпсіз және заманауи виртуалды жеке желі (VPN) бірнеше себептерге байланысты телекоммуникация ұйымдары үшін өте маңызды, ең алдымен деректердің құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етумен айналысады. Телекоммуникация ұйымдары құпия деректермен, соның ішінде тұтынушы ақпаратымен, қаржылық транзакциялармен және меншікті желі конфигурацияларымен айналысады. Қауіпсіз VPN орындар арасында жіберілетін деректерді шифрлайды, оларды рұқсатсыз кіруден немесе

зиянды әрекеттерден қорғайды. Бұл шифрлау деректер ұсталса да, шифрлау кілттерінсіз оның түсініксіз болып қалуын қамтамасыз етеді. VPN желілері жалпыға ортақ желі арқылы жеке желіні қамтамасыз етеді, бұл телекоммуникация ұйымдарына географиялық тұрғыдан шашыраңқы кеңселер, деректер орталықтары және қашықтағы қызметкерлер арасында қауіпсіз байланыс орнатуға мүмкіндік береді. Бұл сезімтал ішкі байланыстар мен деректер алмасулардың жеке және сыртқы қауіптерден оқшауланuын қамтамасыз етеді [2]. 1-кестеде VPN серверлерін пайдалану себептері қосымша келтірілді.

Кесте 1 - VPN серверлерін пайдалану себептері

Себеп	Сипаттама
Қашықтан жұмыс істеу	Ұйым қызметтері мен құжаттамасына үйден сенімді қол жеткізу үшін
Қашықтағы кеңселерді қосу	Бір кәсіпорынның ішіндегі басқа қашықтағы кеңселермен сенімді қосылу үшін
Компания бөлімдері	Бір компанияның ішінде әртүрлі ведомстволарды, оның ішінде халықаралық бөлімдерді қосу
Жалпыға қолжетімді Wi-Fi	Хакерлер ақпаратты ұстап, ұрлай алатын дәмханалар мен метро сияқты жерлерде жалпыға қолжетімді Wi-Fi желілерін пайдалану кезінде деректерді қорғау үшін
Блокталған веб-сайттар	Белгілі бір аймақтарда блокталған веб-сайттарға қатынасу үшін.
Анонимділік	Жеке басын онлайн режимінде қорғау және қажет болған жағдайда олардың орналасқан жері туралы ақпаратты жасыру үшін
Нысаналы жарнама	Мақсатты жарнама жасау үшін пайдаланылатын іздеу тарихының болмауы үшін
Шығындарды үнемдеу	Қаржыны үнемдеу үшін, мысалы, түрлі өңірлерде әртүрлі баға белгілеуді пайдалану үшін орналасқан жері туралы ақпаратты өзгерту арқылы авиабилеттерді сатып алу кезінде

Қашықтан жұмыс істеу үрдісінің артуымен телекоммуникация ұйымдарының қызметкерлері көбінесе қашықтағы орындардан ішкі ресурстар мен жүйелерге қауіпсіз қол жеткізуді қажет етеді. Заманауи VPN қауіпсіз қашықтан қол жеткізуге мүмкіндік береді, бұл қызметкерлерге деректер қауіпсіздігін бұзбай, корпоративтік желіге кез келген жерден қауіпсіз қосылуға мүмкіндік береді. Телекоммуникация ұйымдары көбінесе тұтынушы деректері мен құпиялылығын қорғауды міндеттейтін GDPR, HIPAA немесе PCI-DSS сияқты қатаң реттеуші талаптарға бағынады. Қауіпсіз VPN енгізу ұйымдарға тасымалдау кезінде құпия деректерді қорғау және олардың тек персонал үшін қолжетімді болуын қамтамасыз ету арқылы осы сәйкестік стандарттарын орындауға көмектеседі. Телекоммуникация индустриясы өңдейтін құнды деректер мен маңызды инфрақұрылымының арқасында кибершабуылдардың басты нысанасы болып табылады. Қауіпсіздікті анықтау және алдын алу жүйелері, зиянды бағдарламаны сканерлеу және көп факторлы аутентификация сияқты сенімді қауіпсіздік мүмкіндіктері бар заманауи VPN әртүрлі киберқауіптерден, соның ішінде ортадағы адам шабуылдарынан, төлем бағдарламалық қамтамасыз етуден және деректерді бұзудан қорғауға көмектеседі. Қауіпсіздік артықшылықтарына қоса, заманауи VPN желілері жиі қызмет көрсету сапасына (QoS) басымдық беру және өткізу қабілеттілігін басқару сияқты оңтайландыру мүмкіндіктерін ұсынады, бұл желі өнімділігін жақсартады және маңызды телекоммуникациялық қызметтер үшін сенімді қосылымды қамтамасыз етеді[3].

Алдағы уақытта ғылыми зерттеуде тек телекоммуникация саласындағы VPN серверінің маңыздылығы мен қолданысы туралы зерттеліп, талдау жасалады. Себебі көптеген жұмыстарда VPN серверінің ақпарттық қауіпсіздігі туралы жалпылама талдаулар жасалған. Мысалы, Николахиннің Ақпарат қауіпсіздігін қамтамасыз ету үшін VPN технологиясын

пайдалану мақаласында, Майоровтың Заманауи VPN желілері мақаласында белгілі бір саладағы емес, жалпы VPN желісіне талдау жасаған.

Қазіргі уақытта дүние жүзіндегі көптеген телекоммуникациялық ұйымдар жоғарыда аталған қиындықтар мен талаптарды шешу үшін қауіпсіз және заманауи VPN шешімдерін қолданады. Дәлел ретінде Халықаралық электрбайланыс одағы (ITU) және Телекоммуникация индустриясы қауымдастығы (TIA) сияқты жетекші салалық ұйымдар телекоммуникация желілеріндегі деректердің қауіпсіздігі мен құпиялылығын арттыру үшін VPN желілерін пайдалануды жақтайды. Cisco, Palo Alto Networks және Fortinet қоса алғанда, желілік және киберқауіпсіздік кеңістігінде қалыптасқан жеткізушілер телекоммуникация ұйымдары үшін арнайы әзірленген, жоғары өнімді шифрлау, масштабтау және сияқты мүмкіндіктері бар кеңейтілген VPN шешімдерін ұсынады. Қолданыстағы желілік инфрақұрылыммен интеграция. Еуропадағы GDPR немесе Америка Құрама Штаттарындағы Медициналық сақтандыруды тасымалдау және есеп беру актісі (HIPAA) сияқты деректерді қорғау ережелеріне сәйкестік телекоммуникация ұйымдарында VPN сияқты қауіпсіз байланыс арналарын енгізуді қажет етеді. Осы ережелерді сақтау VPN пайдаланудың күшті көрсеткіші болып табылады[4].

Қорытындылай келе, телекоммуникация ұйымдары үшін қауіпсіз және заманауи VPN маңыздылығын асыра айту мүмкін емес. Ол құпия деректерді қорғауда, нормативтік талаптардың сақталуын қамтамасыз етуде, киберқауіптерден қорғауда, қашықтан қол жеткізуге мүмкіндік беруде және желі өнімділігін арттыруда маңызды рөл атқарады. Телекоммуникация индустриясында VPN шешімдерін кеңінен қолдану олардың қауіпсіздік пен операциялық маңызды мәселелерді шешудегі дәлелденген тиімділігін көрсетеді.

Қолданылған әдебиеттер тізімі

1. Исмаэль Буарфа, Жетілдірілген цифрлық қорғауға арналған корпоративтік VPN архитектурасы, 2022ж., қол жеткізу режимі: https://medium.com/@ismaelbouarfa/corporate-vpn-architectures-for-enhanced-digital protection-517b68a2daa8 (қаралған күні 17.03.2024).
2. Винсент Х. Хиндман, Жетілдірілген цифрлық қорғауға арналған корпоративтік VPN архитектурасы, 2022ж., қол жеткізу режимі: https://www.pqmconsultants.com/vpn/ (қаралған күні 18.03.2024).
3. Ұйымға арналған виртуалды жеке желіні жобалау және енгізу, 2019 ж., қол жеткізу режимі: https://www.lawyersnjurists.com/article/design-implementation-virtual-private-network-organization/ (қаралған күні 18.03.2024).
4. А.Ю. Николахин, АҚПАРАТ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН VPN ТЕХНОЛОГИЯСЫН ПАЙДАЛАНУ, қол жеткізу режимі: https://nirit.org/wp-content/uploads/2018/12/60-68.pdf (қаралған күні 19.03.2024)

ӘОЖ 004.056

АВТОМАТТАНДЫРЫЛҒАН ЖҮЙЕЛЕРДЕ ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУДА ЕКІ ФАКТОРЛЫ АУТЕНТИФИКАЦИЯ ҚОЛДАНЫСЫ

Жансейітова Мөлдір Әбдірзаққызы
zhanseiitovamoldir@gmail.com
Л.Н.Гумилев атындағы Еуразия ұлттық университетінің Ақпараттық қауіпсіздік кафедрасының магистранты, Астана, Қазақстан
Ғылыми жетекші – Сантеева С.Ә.

Аңдатпа: Бұл жұмыс екі факторлы аутентификация әдістерін сипаттайды және оны автоматтандырылған басқару жүйесіндегі қолдану тиімділіктерін, артықшылықтарын қарастырады.

Кілттік сөздер: ақпараттық қауіпсіздік, 2FA (екі факторлы аутентификация),фишинг,аутенфикация.