УДК 004.771

Успанова Асель Исимхановна
техника ғылымдарының магистрі, Қазақ экономика, қаржы және халықаралық сауда университеті, Астана қ.
e-mail: esim2306@gmail.com
Абишева Айгуль Амантаевна
техника ғылымдарының магистрі, Қазақ экономика, қаржы және халықаралық сауда университеті, Астана қ.
e-mail: aigul_abisheva@mail.ru

VPN НЕГІЗІНДЕ КОРПОРАТИВТІ ЖЕЛІЛЕРДІ ҰЙЫМДАСТЫРУ: ҚҰРУ, БАСҚАРУ ЖӘНЕ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ

VPN *— жалпы қолданыста бар желі базасында құрылатын корпоративті желі және негізгі желіге ұқсас қызмет түрлерін көрсетеді. VPN-нің негізгі ерекшеліктері: мөліметтерді жоғары деңгейде қорғау және қысқартылған нөмір терудің көмегі арқылы оперативті қосылуды қамтамасыз ететін өзіндік нөмірлеу жобасы.*

Виртуалды жеке желі (VPN) - бірінші кезекте Интернет секілді желілерді қоғамдық коммуникациялық құрылымдарды алыс қашықтықта байланыстыратын жеке желі. Бұл желілер мәліметті шифрлеу сияқты тунельдік протоколдар және қауіпсіздік шаралары арқылы жеке желілердің қауіпсіздігін қамтамасыз етеді. Мәселен, VPN бас кеңселердің бөлімшелерін желіге қосылу қауіпсіздігін қамтамасыз ету үшін де қолданылуы мүмкін. Сондай-ақ VPN әртекті бірақ бір типті, мысалы IPv6 желісін IPv4 желісі арқылы, байланыстыруы мүмкін.

Жалпы VPN-дердің екі түрі бар: қашықтан басқарылатын VPN және сайт-сайт VPN. Қашықтан басқарылатын VPN жеке қолданушыларға қашықтан басқарылатын желіге қосылуға мүмкіндік береді, мысалы өзінің компаниясының интражелісіне қосылу роумингі. Сайт-сайт VPN бірнеше қолданушының байланысуын қарастырады, мәселен, филиалдардың компания желісіне қосылуы. Виртуалды желілер әрине шығындарды азайтады, себебі қауіпсіздікті күшейте отырып, қолданыстағы құрылымдарды пайдалана отырып, жалға алынатын желілерге деген сұранысты азайтады.

Түйін сөздер*: виртуалды желі; Интернет; корпоративтік желі; желілік қауіпсіздік; VPN; байланыс; шифрлау.*

VPN - это корпоративная сеть, которая основана на общедоступной сети и предоставляет аналогичные услуги для домашней сети. Основными функциями VPN являются: проект персонализированной нумерации, обеспечивающий защиту высокого уровня и мгновенный доступ к сокращенному номеру.

Виртуальная частная сеть (VPN) - это частная сеть, прежде всего, которая соединяет сети, такие как Интернет, с общественными структурами связи. Эти сети обеспечивают безопасность для отдельных сетей посредством туннельных протоколов, таких как шифрование данных и меры безопасности. Например, VPN также можно использовать для обеспечения безопасности доступа к сети в головном офисе. VPN также может связывать разные, но одного типа сети, например, IPv6 через сеть IPv4.

Как правило, существует два типа VPN: удаленный VPN и VPN для веб-сайтов. Удаленный VPN позволяет отдельным пользователям подключаться к удаленной сети, например, к роумингу во внутренней сети своей компании. Веб-сайт VPN учитывает подключения нескольких пользователей, например, партнерский доступ к сети компании. Виртуальные сети, конечно, снижают затраты, поскольку они повышают безопасность за счет снижения спроса на арендуемые линии с использованием существующих структур.

Ключевые слова*: виртуальная сеть; Интернет; корпоративная сеть; безопасность сети; VPN; связь; шифрование.*

A VPN is a corporate network that is based on a public network and provides similar services for a home network. The main VPN functions are: a personalized numbering project, providing high-level security and instant access to the abbreviated number.

A virtual private network (VPN) is a private network, primarily that connects networks, such as the Internet, to public communication structures. These networks provide security for individual networks through tunneling protocols, such as data encryption and security measures. For example, VPN can also be used to provide secure access to the network at the head office. VPN can also connect different, but the same type of network, for example, IPv6 over an IPv4 network.

Typically, there are two types of VPN: remote VPN and VPN for websites. Remote VPN allows individual users to connect to a remote network, for example, roaming on their company's internal network. The VPN website takes into account connections of several users, for example, partner access to the company's network. Virtual networks, of course, reduce costs, because they increase security by reducing the demand for leased lines using existing structures.

Keywords*: virtual network; Internet; corporate network; network security; VPN; communication; encryption.*

Бүгінде корпоративтік әлеуметтік желілер ұйымдардың бірыңғай ақпараттық кеңістігі қалыптастырылатын негізгі құралдардың бірі болып табылады. Корпоративтік әлеуметтік желі компания қызметкерлері арасында беделді тәуекелдерсіз байланыс орнатуға көмектеседі.

Корпоративтік әлеуметтік желі байланыс ақпараттарына ыңғайлы қол жеткізу арқылы жұмыс уақытын үнемдейді және бөлімдер арасында байланысын жақсартуға мүмкіндік береді. KeepKeys жүйесі корпоративті деректерді қорғауға, әр қызметкердің құпия сөзіне қол жеткізуді шектеуге және басқаруға бағытталған. Сіз жаңа сайтты жыл сайынғы жеңілдікті әкімшілігімен ала аласыз. VPN кеңінен айтсақ, Интернет желісі сияқты басқа желілердің желісіне қосылуды қамтамасыз ететін технология [1]. Виртуалды желідегі байланыс төменгі деңгейлі сенімге ие негізгі арналар арқылы жүзеге асырылады және шифрлау құралдарын пайдалану арқылы деректердің қауіпсіздігі барынша қамтамасыз етіледі. Бұл салыстырмалы түрде арзан және жеңілдетілген технология соңғы кезде танымал болып келеді. Корпоративтік компьютерлік желілер қазіргі заманғы компаниялардың ажырамас бөлігі болып табылады. Осындай желілердің көмегімен ақпаратты тез және қауіпсіз түрде жіберуге және қабылдап алуға болады. Олар бір ғимаратта орналасқан немесе географиялық үлестірілген бір кәсіпорынның компьютерлері арасында байланыс орнатады. Мұндай желілерді құрудың бірнеше жолы бар. Соңғы уақытқа дейін жергілікті желі жүйесі (LAN) ең танымал болды, бұл шектеулі компьютерлерді біріктірді. Олар файл алмасудың ең жоғары жылдамдығын және ақпараттың абсолюттік қауіпсіздігін қамтамасыз етеді, өйткені оның ағындары жалпыға қол жетімді болмайды. Осы типтегі құрылымдарды пайдалану тегін. LAN-ның кемшіліктеріне қашықтағы пайдаланушыларды қосуға қабілетсіздігі мен жоғары шығындарды жатқызуға болады. Ғаламдық желілер мен дербес компьютер жүйелерінің көп бөлігін қамтитын кең ауқымды желі (WAN) желілерінің үстіне салынған виртуалды жеке желі (VPN) LAN желілеріне лайықты балама болып табылады. Олардың күмәнсіз артықшылықтарына құру қарапайымдылығын (және, тиісінше, төмен құны), әлемнің түрлі бөліктеріндегі бірнеше абоненттерді қосу мүмкіндігін және деректерді жіберу қауіпсіздігін жатқызуға болады. Икемділігі мен үнемділігі арқасында, VPN желілері нарықтан белсенді түрде LAN –ды шеттетіп жатыр. Мысалы, Forrester Research Inc. және Infonetics Research компанияларының жүргізген зерттеулері нәтижесіне сәйкес, VPN желілерін пайдалану мен қолдауға жіберілетін шығын LAN технологиясын пайдалана отырып салынған логистикалық құрылымдардан үш есе төмен. Осылайша, виртуалды жеке желі оңай таралады және көптеген филиалдары бар компаниялар үшін, сондай-ақ қызметкерлері көбінесе іс-сапарда жүріп немесе үйден жұмыс істейтін компаниялар үшін ең жақсы нұсқа болып табылады. Желіге жаңа офисті немесе қашықтағы қызметкерді қосу қосымша байланыс шығындарынсыз жүзеге асырылады. Сонымен қатар, виртуалды жүйені бастапқы ұйымдастыру ең аз ақшалай шығындарды талап етеді. Болашақта қаржы салымдары интернет-провайдердің қызметтеріне ақы төлеуге ғана талап етіледі. Виртуалды жеке желінің белгілі бір кемшіліктері де бар. Мәселен, оларды пайдаланатын фирмалар жіберілетін деректердің қауіпсіздігін қамтамасыз етуі керек, себебі, жіберу процесінде құжаттар дүниежүзілік ғаламтор, яғни Интернет арқылы өтеді. Бұл мәселені шешу үшін жіберу кезінде файлдардың қорғауын қамтамасыз ететін арнайы деректерді шифрлау алгоритмдері қолданылады. Сонымен қатар, виртуалды құрылымда файл алмасу жылдамдығы оның жеке әріптестеріне қарағанда айтарлықтай төмен. Бірақ аз көлемдегі ақпаратты жіберу үшін бұл жеткілікті болуы мүмкін. Зерттеумен айналысатын Forrester Research Inc. ұйымының деректеріне сәйкес, кәсіпорындардың 41% -ы кеңсе желілерін пайдаланады, себебі олар қашықтан қолжетімділік мәселелерін шеше алады, 30% -ы оларды қаражат үнемдеуі үшін бағалайды, ал 20% - жұмысты жеңілдететіні үшін таңдайды.

Компания жұмысының ерекшеліктері мен нақты тапсырмаларына байланысты, Virtual Private Network желісін төмендегі үлгілердің біреуі арқылы құруға болады:

– *Remote Access*. Бұл жағдайда кеңсе мен қашықтағы пайдаланушы арасында кәсіпорынның ресурстарына Интернет арқылы үй компьютерінен қосылатын қауіпсіз арна жасалады. Мұндай жүйелерді құру оңай, бірақ олардың баламаларына қарағанда қауіпсіздігі кем, оларды қашықтан жұмыс істейтін қызметкерлер саны көп кәсіпорындар пайдаланады.

– *Интранет*. Бұл нұсқа ұйымның бірнеше филиалын біріктіруге мүмкіндік береді. Деректерді жіберу үдерісі ашық арналарда жүзеге асырылады. Интранет компанияның қарапайым филиалдары мен мобильдік кеңселері үшін пайдаланылуы мүмкін. Бірақ бұл

әдіс барлық байланыстырылатын кеңселерде серверлердің орнатылуын талап ететінін ескеру керек.

– *Extranet*. Кәсіпорын ақпараттарына қол жеткізу клиенттерге және басқа сыртқы пайдаланушыларға беріледі. Дегенмен, олардың жүйені пайдалану мүмкіндіктері айтарлықтай шектеулі. Абоненттерге арналмаған файлдар шифрлау құралдарымен сенімді қорғалады. Бұл өз тұтынушыларына белгілі бір ақпаратқа қол жеткізуді қамтамасыз етуді қажет еттеін компаниялар үшін дұрыс шешім.

– *Клиент / Сервер*. Бұл параметр бір сегменттегі бірнеше түйін арасындағы деректермен алмасуға мүмкіндік береді. Бір физикалық желі аумағында бірнеше логикалық желілерді (мысалы, қаржы бөлімі, персоналға қызмет көрсету бөлімі үшін жеке құрылымдар, және т.б.) құруды қажет ететін ұйымдарда ең танымал болып келеді. Бөлу кезінде трафикті қорғау үшін шифрлау қолданылады [1].

Біз айтып өткендей, деректерді қорғау оларды шифрлау, аутентификациялау және қол жеткізуді бақылауды қамтиды. Ең танымал кодтау алгоритмдері болып DES, Triple DES және AES табылады. Бұрын-соңды болмаған қауіпсіздік бірыңғай компонентке деректерді жинақтайтын және қосылысты (туннель) қалыптастыратын арнайы хаттамалар арқылы қамтамасыз етіледі, сонымен қатар қалыптасқан туннельдің ішіндегі ақпаратты шифрлайды. Қазіргі таңда төмендегі хаттамалар жиынтығы ең кең таралған: PPTP (Point-to-Point Tunneling Protocol) - түпнұсқалықты, қысуды және деректерді шифрлауды қамтамасыз ететін туннельдік протокол [3]. Microsoft корпорациясы PPTP хаттамасы үшін MPPE шифрлау әдісін пайдалануды ұсынады. Бұдан басқа, ақпарат ашық, шифрланбаған түрде берілуі мүмкін. Деректер инкапсуляциясы GRE және IP тақырыптарын қосу арқылы жүзеге асырылады. L2TP (Layer Two Tunneling Protocol) - бұл PPTP және L2F хаттамаларын біріктіру арқылы әзірленген хаттама. PPTP-ге қарағанда файлды жақсырақ қорғауды қамтамасыз етеді. Шифрлау IPSec протоколы (IP-қауіпсіздік) немесе 3DES арқылы жүзеге асырылады [2]. Деректерді жіберудің максималды қауіпсіздігін екінші нұсқа ұсынады, бірақ оны пайдалану қосылу жылдамдығының төмендеуіне және орталық процессордың жүктемесін арттыруға әкеледі. Адресатқа ақпарат өзгеріссіз жеткізілу үшін аутентификация қажет. Бұл амал MD5 және SHA1 алгоритмдері арқылы орындалады және құжаттардың тұтастығын тексеруді, сондай-ақ нысандарды сәйкестендіруді қамтиды. Сәйкестендіру дәстүрлі логин мен пароль енгізу әрекеттері арқылы, сондай-ақ шынайы құралдардың көмегімен - олардың түпнұсқалығын тексеру үшін куәліктер мен серверлер арқылы жүзеге асырылады.

VPN жасау үшін не қажет? Кәсіпорынның қажеттіліктерін толығымен қанағаттандыратын желіні жасау, тек кәсіпқойдың қолынан келеді, сондықтан әлеуетті тапсырушыға ең бастысы - сенімді жеткізушіні (провайдерді) таңдау және техникалық тапсырманы дайындау қажет. Көптеген жағдайларда провайдерлер өз клиенттерін қызмет көрсету шартына сәйкес барлық қажетті жабдықпен қамтамасыз етеді. Бірақ тапсырыс беруші тілегі бойынша жабдықты өз бетімен сатып алуы мүмкін. Мұндай жағдайда оған стандартты желілік жабдық, сондай-ақ арнайы Virtual Private Gateway шлюзі қажет болады. Бұл шлюз туннельдер құру, деректерді қорғау, трафикті басқару және белгілі бір жағдайларда орталықтандырылған басқару үшін қажет. Осындай шлюздердің ең танымал өндірушілері «Digital Assured», «Cisco», «Intel», «Avaya», «Red Creek Communications», «Net Screen Technologies», «3com», «Nokia», «Intrusion», «Watch Guard Technologies», «Sonic Wall», «eSoft» және басқалары болып табылады. Кішігірім кеңселерге арналған шлюз құны шамамен 700-2500 долларды құрайды.

VPN негізіндегі корпоративтік желіні пайдалану және басқару. Кеңседегі желі - көптеген филиалдары мен қашықтағы пайдаланушылары бар фирмалар үшін және оңай басқарылатын, сондай-ақ қымбат емес, икемді жүйеге ие болғысы келетін компаниялар үшін қарапайым және ыңғайлы шешім. Бұл технология жаңа құрылымдық элементтерді қосуға, сондай-ақ инфрақұрылымды кеңейтусіз желілердің көлемін едәуір арттыруға мүмкіндік береді. Мұны провайдерге тартпай клиенттің өзі істей алады. Жаңа абонентті қосуға бірнеше ғана минут кетеді. Мұндай жүйелерді басқару пайдаланушыға қиындық тудырмайды, себебі Virtual Private Network желісінің әкімшілік функцияларының көпшілігі автоматтандырылған. Провайдер мамандары клиенттің серверіне қажетті бағдарламалық жасақтаманы орнатады және VPN субъектілері мен объектілерінің дерекқорын жасайды (әр субъект үшін шифрлау кілті жасалады) [2].

Содан кейін бұл дерекқор алынбалы ақпарат құралдарында сақталады және тапсырыс берушіге беріледі. Пайдаланушыға тек сәйкестендіру және кіру үшін кілттік картаны компьютерге қосу керек. Егер қауіпсіз корпоративтік желіде жұмыс жасау барысында қандай да бір мәселе туындаса, тапсырыс беруші провайдерге хабарласуы қажет, провайдер осы мәселелерді шарттың талаптарымен белгіленген мерзімде шешеді.

Сонымен, VPN - штатында қашықтан жұмыс істейтін мамандары бар, сондай-ақ басқа қалалар мен елдердегі кеңселері бар орташа және ірі компанияларға қатысты шешім. Сонымен қатар, мұндай жүйелер жасырын деректерге қол жеткізуді қажет ететін адамдары мен құрылымдық бөлімшелері жиі өзгеретін (сәйкесінше, құрылым жеткілікті деңгейде икемді болуы және оңай конфигурациялануы қажет); әртүрлі деңгейдегі деректерге қол жеткізуді қажет ететін абоненттері бар (қызметкерлер, клиенттер, жеткізушілер); бір физикалық құрылым ішінде бірнеше логикалық желілер құру қажеттілігі бар (мысалы, егер сіз кәсіпорынның әрбір бөлімшесіне өзіңіздің жүйеңізді жасауыңыз қажет болса) ұйымдары үшін өте қажет болып табылады. VPN желісінің корпоративті IP құру және қолдау үшін провайдерді таңдағанда, байланыстың тұрақты сапасына, берілген деректердің қауіпсіздігіне және белгілі бір техникалық мәселелерді шешу жылдамдығына сенімді болу маңызды.

Пайдаланылған әдебиеттер тізімі

1. Браун С. Виртуальные частные сети, Изд. McGraw-Hill Companies, Inc., Лори, 2001 г. – 508 с.
2. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях.— М.: Кудиц-образ, 2001.— 368 с.
3. Джоул Снайдер VPN: поделенный рынок // Сети.— 1999.- №11 http://www.citforum.ru/nets/articles/vpn.shtm

Успанова Асель Исимхановна
Лауазымы: техника ғылымдарының магистрі, «Ақпараттық жүйелер мен технологиялар» кафедрасының аға оқытушысы, Қазақ экономика, қаржы және халықаралық сауда университеті
Пошталық мекен-жайы: 010000, Қазақстан Республикасы, Астана қ., Жұбанов көшесі 7
Ұялы. тел: +7702 236 38 28
Абишева Айгуль Амантаевна
Лауазымы: техника ғылымдарының магистрі, «Ақпараттық жүйелер мен технологиялар» кафедрасының аға оқытушысы, Қазақ экономика, қаржы және халықаралық сауда университеті
Пошталық мекен-жайы: 010000, Қазақстан Республикасы, Астана қ., Жұбанов көшесі 7
Ұялы. тел: +7701 191 34 80
VPN негізінде корпоративті желілерді ұйымдастыру: құру, басқару және қауіпсіздікті қамтамасыз ету

Успанова Асель Исимхановна
Должность: магистр технических наук, старший преподаватель кафедры «Информационные системы и технологии», Казахский университет экономики, финансов и международной торговли
Почтовый адрес: 010000, Республика Казахстан, г. Астана, ул. Жубанова, 7
сот. тел: +7702 236 38 28
Абишева Айгуль Амантаевна
Должность: магистр технических наук, старший преподаватель кафедры «Информационные системы и технологии», Казахский университет экономики, финансов и международной торговли
Почтовый адрес: 010000, Республика Казахстан, г. Астана, ул. Жубанова, 7
сот. тел: +7701 191 34 80
Организация корпоративных сетей на основе VPN: построение, управление, безопасность

Uspanova Assel Isimkhanovna
Position: Master of Technical Sciences, Associate Senior Lecturer, Department of «Information Systems and Technologies», Kazakh University of Economics, Finance and International Trade
Mailing address: 010000, Republic of Kazakhstan, Astana, Zhubanov St. 7
Mob.phone:+7702 236 38 28
Abisheva Aigul Amantaevna
Position: Master of Technical Sciences, Associate Senior Lecturer, Department of «Information Systems and Technologies», Kazakh University of Economics, Finance and International Trade
Mailing address: 010000, Republic of Kazakhstan, Astana, Zhubanov St. 7
Mob.phone:+7701 191 34 80
Organization of corporate networks based on VPN: building, management, security