Conclusion:

1. While the solution of the two-dimensional equation of the optimal duration of construction-installation works in the formula (1) is proposed by the method of incremental approximation, the one-dimensional equation of the optimal duration is given by the formula (5).
2. As a result of the calculation, it was determined that the production norm is more than 100% when the optimal duration is between K_{opt} and $\sqrt{a}$.

References

1. Organization and management of construction production. (2004). Baku
2. Golubova, O.S. Golubova O.S., Korban L.K. (2016). Valitsky. Economics of construction: textbook. Minsk: Novoe znanie, c.574
3. Uchaev P.N. Chevychelov, S. P. (2014). Optimization of engineering solutions in examples and problems: Old Oskol: TNT.c.176
4. Sobolev, V.I. (2006). Optimization of construction processes: a textbook. Rostov-on-Don: Phoenix, c.256
5. Farzaliyev S.A, Quluzade S.R (2023). Possibilities of organizing the construction of multi-storey monolithic reinforced concrete buildings by the flow method. Scientific works/Elmi eserler, AzUAC, N1. s.36-41

Məqaləyə istinad: Fətullayev R.F. Axınabənzər tikinti istehsalatının optimal qısa müddəti. Elmi Əsərlər/Scientific works, AzMİU, s. 146-152, N2, 2024
For citation: Fatullayev R.F. Optimal short duration of flow construction production.. Elmi Əsərlər/Scientific works, AzUAC. p.146-152, N2, 2024

Redaksiyaya daxil olma/Received 11.2.2024
Çapa qəbul olunma/Accepted for publication 11.04.2024

http://doi.org/10.58225/sw.2024.2-153-158

VİPNET-DƏ QOVŞAQLARIN QARŞILIQLI ƏLAQƏSİNİN İŞLƏNMƏSİ

Nurəliyev Camaləddin Ağabala oğlu- assistent, İnformasiya texnologiyaları və sistemləri kafedrası, AzMİU, camal.nuraliyev@gmail.com
Xurşudov Dursun Qədir oğlu-baş müəllim, İnformasiya texnologiyaları və sistemləri kafedrası, AzMİU, dursuncosqun@gmail.com
Məmmədli Məryam İqbal qızı- assistent, İnformasiya texnologiyaları və sistemləri kafedrası, AzMİU, maryammammadli@gmail.com

Xülasə. Texnologiyanın sürətli inkişafı dövründə informasiya təhlükəsizliyi problemləri ən kəskin şəkildə ortaya çıxır. Avtomatlaşdırılmış informasiya emalı və idarəetmə sistemlərindən istifadə informasiyanın icazəsiz girişdən qorunmasını artırmışdır. Kompüter sistemlərində informasiya təhlükəsizliyinin əsas problemləri onların kütləvi informasiya vasitələri ilə ciddi şəkildə bağlı olmaması ilə əlaqədar yaranır. Rabitə kanalları üzərindən asanlıqla və tez surətdə kopyalana və ötürülə bilər. İnformasiya sistemi pozucuların həm xarici, həm də daxili təhdidlərinə məruz qalır.Kompüter şəbəkələrində işləyərkən informasiya təhlükəsizliyinin əsas problemlərini üç növə bölmək olar:
• Məlumatın ələ keçirilməsi (məlumatların məxfiliyinin pozulması),
• Məlumatın dəyişdirilməsi (əsl mesajın təhrif edilməsi və ya başqa məlumatla əvəz edilməsi),
• Müəllifliyin dəyişdirilməsi (məlumatların oğurlanması və müəllif hüquqlarının pozulması). Bu gün kompüter sistemlərinin icazəsiz girişdən qorunması, hardware ilə müqayisədə proqram təminatı və kriptoqrafik mexanizmlərin artan rolu ilə xarakterizə olunur. İnformasiya təhlükəsizliyi sahəsində yeni problemlər artıq nisbətən yüksək hesablama mürəkkəbliyinə malik protokol və mexanizmlərdən istifadəni tələb edir. Bu problemlərin həlli yolu virtual özəl şəbəkələrin (VPN) yaradılmasıdır.
Açar sözlər: İnformasiya,məlumat,komputer, təhlükəsizlik,VPN

INTERACTION PROCESSING OF NODES IN VIPNET

Nuraliyev Jamaleddin Aghabala- assistant, department of Information Technologies and Systems, AzUAC, jamal.nuraliyev@gmail.com
Khurshudov Dursun Gadir-head teacher, department of Information Technologies and Systems, AzUAC, dursuncosqun@gmail.com
Mammadli Maryam Iqbal- assistant, department of Information Technologies and Systems, AzUAC, maryammammadli@gmail.com

Abstract. In the period of rapid development of technology, information security problems emerge most acutely. The use of automated information processing and management systems has increased the protection of information from unauthorized access. The main problems of information security in computer systems arise due to the fact that information is not strictly connected with mass media. It can be easily and quickly copied and transmitted over communication channels. The information system is exposed to both external and internal threats of intruders.The main problems of information security when working in computer networks can be divided into three types: • interception of information (violation of confidentiality of information),
• changing information (distorting the original message or replacing it with other information),
• change of authorship (theft of information and violation of copyright). Today, the protection of computer systems against unauthorized access is characterized by the increasing role of software and cryptographic mechanisms compared to hardware. New problems in the field of information security require the use of protocols and mechanisms with relatively high computational complexity. The solution to these problems is the creation of virtual private networks (VPN).
Keywords: Information, data, computer, security, VPN

Giriş: Məlumatların ötürürülməsində Simsiz texnologiyalardan istifadə geniş yayılmışdır. İşçilərin mobilliyi günü gündən artır - onlar ofisdə işləyərkən, ezamiyyətdə və məzuniyyətdə olarkən simsiz texnologiyalardan istifadə edirlər. Hazırda dünyanın istənilən yerindən korporativ resurslara çıxış imkanı verən simsiz İnternetə çıxış (Wi-Fi, WiMAX, GPRS/EDGE, peyk rabitə kanalları) təmin etmək üçün müxtəlif texnologiyalardan istifadə olunur. Korporativ resursların istifadəçilərinin bu mobilliyi informasiya təhlükəsizliyinin təmin edilməsi üçün yeni problemlər yaradır:

- müəssisənin LAN şəbəkəsinin simsiz seqmentinə girişə nəzarət;
- simsiz kanal vasitəsilə ötürülən məlumatların qorunmasının (məxfilik və bütövlüyünün) təmin edilməsi;
- mobil işçi cihazlarını şəbəkə hücumlarından qorumaq.

Bu simsiz əlaqələrin qorunması üçün ViPNet texnologiyasının həlli təklif edilir [1]. ViPNet texnologiyası bütövlükdə şəbəkə, onun seqmentləri və hər bir şəbəkə müştərisi üçün inteqrasiya edilmiş təhlükəsizlik vasitələri ilə VPN (Virtual Şəxsi Şəbəkə) yaratmaq və idarə etmək üçün yüksək effektiv vasitədir. ViPNet seriyalı proqram paketi IP şəbəkələrinə tətbiq edildikdə, metodundan, yerindən və ayrılmış ünvan növündən asılı olmayaraq VPN-ə daxil olan kompüterlər arasında şəffaf qarşılıqlı əlaqəni təmin edən istənilən konfiqurasiyalı virtual təhlükəsiz şəbəkələrin (VPN) yaradılması üçün universal proqram vasitəsidir. Virtual təhlükəsiz şəbəkədə iştirak edən hər bir kompüterdə müvafiq proqram təminatının quraşdırılması ilə ən yüksək səviyyəli mühafizə və tam təhlükəsiz əməliyyatları təmin edilir. Hər bir kompüterin digər kompüterlərlə mübadilə etdiyi informasiya, əlaqədə iştirak etməyən digər kompüterlər üçün əlçatmaz olur. Kompüterin özündə olan informasiyanı VPN-də iştirak etməyən heç bir kompüterdən əldə edilə bilməz. VPN-də iştirak edən kompüterlərdən giriş müvafiq bağlantıların, açarların, filtr parametrlərinin olması ilə müəyyən edilir və tam olaraq idarə olunur[2].

ViPNet virtual şəbəkəsi kompüterlərdə (şəbəkə qovşaqlarında) aşağıdakı proqram təminatının quraşdırılması ilə qurulur:
ViPNet Client və ViPNet Coordinator.
ViPNet texnologiyasına aşağıdakı komponentlər daxildir:

- ViPNet Client proqram təminatı – abunəçinin iş yerində quraşdırılır, ötürülən məlumatların və iş yerinin mühafizəsini təmin edir;
- Təhlükəsiz mesajlaşma – mesajların şifrələnmiş formada ötürülməsi;
- Təhlükəsiz fayl mübadiləsi – faylların şifrələnmiş formada ötürülməsi;
- Biznes poçtu – şifrələmə və rəqəmsal imzadan istifadə etməklə e-poçt mesajlarının mübadiləsi;
- Faylın avtomatik işlənməsi – faylların hərflərə avtomatik çevrilməsi və Biznes poçtu vasitəsilə ötürülməsi;
- Poçtun avtomatik emalı – qoşmaları qovluqlara yükləmək imkanı ilə Business Mail məktublarının avtomatik işlənməsi.

ViPNet Client şəbəkənin qorunmasını və fərdi kompüterlərin VPN-ə daxil edilməsini təmin edir. ViPNet Coordinator proqramı olan kompüter adətən yerli şəbəkələrin və onların seqmentlərinin sərhədlərində quraşdırılır və aşağıdakıları təmin edir:

- Lokal şəbəkələrdə və ya onların seqmentlərində yerləşən açıq və qorunan kompüterlərin ona ayrılmış ünvan növündən asılı olmayaraq VPN-ə daxil edilməsi[4];
- Şəbəkələrin şəbəkə hücumlarından ayrılması və qorunması, həmçinin ona qoşulmuş digər şəbəkə qovşaqlarının statusu haqqında ViPNet Client ilə kompüterə bildirişlərin verilməsi;

ViPNet şəbəkə kompüterləri IP protokolunu dəstəkləyən istənilən növ lokal şəbəkələrin daxilində yerləşdirilə bilər. İstənilən növ şəbəkə bağlantısına icazə verilir. Bu, XDSL bağlantısı vasitəsilə Ethernet şəbəkəsi və ya PPPoE, adi Dial UP və ya ISDN vasitəsilə PPP, GPRS mobil şəbəkəsi və ya Simsiz cihazlar, MPLS və ya VLAN şəbəkələri ola bilər. ViPNet proqramı avtomatik olaraq müxtəlif keçid qatı protokollarını dəstəkləyir[3].

ViPNet şəbəkəsindəki kompüterlər şəbəkədə ya avtonom şəkildə, yəni heç bir firewalldan istifadə etmədən və ya müxtəlif firewalllar və ünvan tərcüməsi (NAT) funksiyalarını yerinə yetirən digər qurğular vasitəsilə işləyə bilər [6].

Böyük lokal şəbəkələr daxilində virtual şəbəkə proqram təminatından istifadə etməklə informasiya cəhətdən müstəqil, qarşılıqlı əlçatmaz və ya qismən üst-üstə düşən qapalı (müstəqil) kompüter qrupları yaradıla bilər [4].

Virtual şəbəkə proqram təminatı VPN-də iştirak edən yerli şəbəkə kompüterlərini asanlıqla İnternetə qoşmağa imkan verir, həm təhlükəsiz bağlantılar üçün, həm də İnternetdən bu kompüterlərə (həm qorunan, həm də açıq) girişi tamamilə istisna etməklə və onların İnternetin açıq resurslarına çıxışını təşkil edir [5]. Qorunan trafik üçün onu edilən parametrlərə uyğun olaraq filtrləmək də mümkündür.

Lokal şəbəkədəki bəzi kompüterlərdə proqram təminatı quraşdırmaq mümkün deyilsə və ya istəmirsə, belə kompüterlərin xarici şəbəkələrdə trafikinin qorunması işi ViPNet Coordinator proqram təminatına həvalə edilə bilər, bu halda bu kompüterlər üçün oxşar koordinatora və ya birbaşa son kompüterə təhlükəsiz tunel yaradılır [5].

Virtual şəbəkə üçün bütün proqramların əsasını xüsusi ViPNet drayveri təşkil edir. Həmin drayver əməliyyat sisteminin şəbəkə interfeyslərinin sürücüləri ilə birbaşa qarşılıqlı əlaqəsini, həmçinin proqramın əməliyyat sistemindən asılı olmamasını və ondakı sənədsiz imkanları təmin edir. ViPNet Driver kompüterdən gələn və gedən bütün IP trafikini əldə edərək idarə edir[7].

ViPNet proqramı ilə təchiz edilmiş digər kompüterlərlə şəbəkədə qarşılıqlı əlaqə qurarkən proqram bu cür kompüterlər arasında təhlükəsiz VPN tunellərinin qurulmasını təmin edir. Bu halda, iki kompüter arasındakı bütün IP trafiki şifrələnir və trafiki eyni proqram təminatına malik olanlar da daxil olmaqla digər kompüterlər üçün əlçatmaz edir. Şifrələmə GOST 28147-89 tərəfindən tövsiyə olunan alqoritmə uyğun olaraq yerinə yetirilir. Açarın uzunluğu isə 256 bit olur. Ancaq fərqli bir şifrələmə alqoritmi də seçmək mümkündür[8]. Sertifikatlaşdırma Mərkəzinin (SM) əsas funksiyaları bunlardır:

• İmza açarlarının yaradılması və Səlahiyyətli şəxslər sertifikatlarının verilməsi, həmçinin onlara sertifikatın verilməsi üçün rəhbərə sorğunun formalaşdırılması;
• Qonşu şəbəkələrin rəhbər və şəxslərinin sertifikatlarının sertifikatlaşdırma mərkəzinə idxalı;
• İstifadəçi imza açarlarının yaradılması və müvafiq sertifikatların verilməsi, şəbəkə istifadəçilərinin sertifikatların verilməsi üçün müraciətlərə baxılması;
• Qeydiyyat mərkəzləri ilə qarşılıqlı əlaqə;
• Sertifikatların ləğvi, dayandırılması və yenilənməsi üzrə əməliyyatların aparılması. Ləğv edilmiş sertifikatların siyahılarının yayılması;
• İş jurnallarında qeydlərin aparılması və verilmiş sertifikatların siyahılarının saxlanılması;
• İstifadəçilərin sertifikatlarının və məxfi açarlarının aparat yaddaş daşıyıcılarında qeyd edilməsi;
• Digər istehsalçıların sertifikatlaşdırma mərkəzi ilə çarpaz sertifikatlaşdırma (SM "Crypto-Pro", SM "Signal-COM", "Standard SM" və s.)

Sertifikatlaşdırma mərkəzləri GOST R 34.10-2001 alqoritmi əsasında imza açarları və onların sertifikatlaşdırılması imkanını təmin edir. Sertifikatlar X.509 v3 formatında yaradılır və PKCS standartlarından istifadə etməklə saxlanıla bilər.

ViPNet Administrator dəstinə daxil olan proqram təminatı ViPNet Client proqramı ilə birlikdə kompüterlərdə quraşdırılır. Bu, ViPNet Administrator komponentlərinin şəbəkə mühafizəsi və onların vahid təhlükəsiz ViPNet şəbəkəsinə daxil edilməsi məqsədilə edilir.

Qovşaqlar arasında təhlükəsiz VPN tunel əlaqələri yaratmaq üçün iki növ IP protokolu istifadə olunur (IP/241 və IP/UDP).

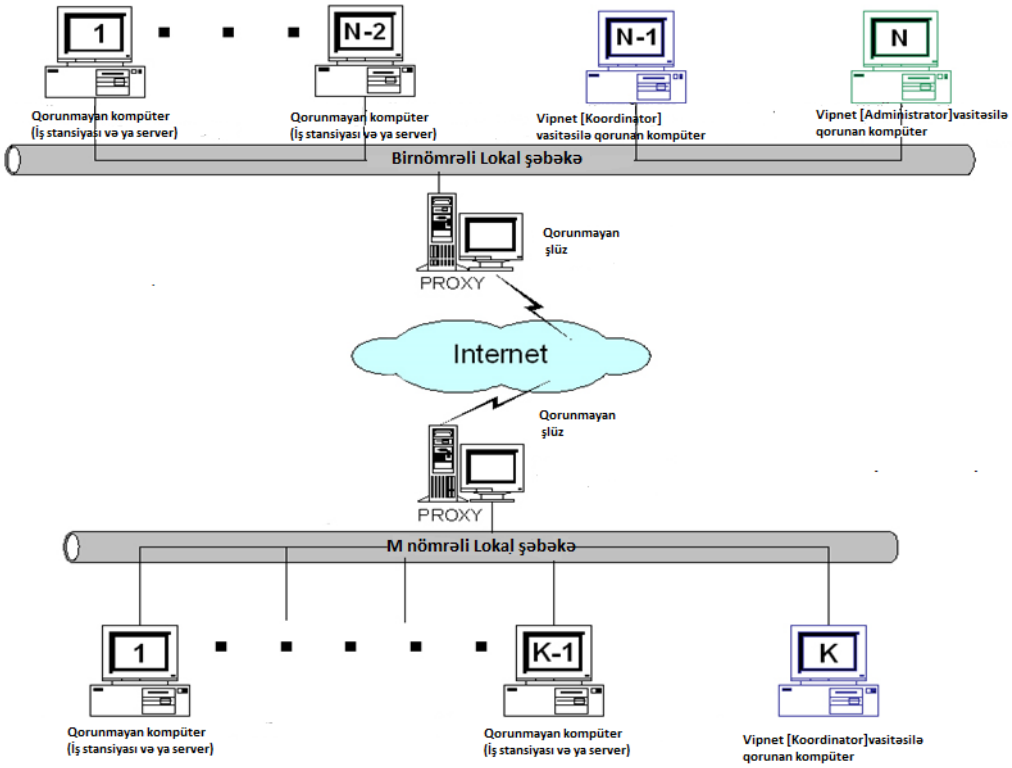
Hər bir kompüter cütü arasındakı açarlar həm Mərkəz tərəfindən yaradılan məlumatdan (simmetrik açar paylama sxemi), həm də hər bir kompüter tərəfindən yaradılan məlumatdan (asimmetrik açar paylama sxemi) asılıdır[3].

Bu əsas struktur bir tərəfdən Mərkəzdən etibarlı şəkildə idarə olunan, digər tərəfdən isə istifadəçi məlumatı baxımından Mərkəz üçün tamamilə əlçatmaz olan ViPNet əsasında korporativ virtual şəbəkələr qurmağa imkan verir.

Virtual şəbəkənin və əlaqələrin etibarlı idarə edilməsi, qovşaqlar arasında açar informasiyanın yaradılması və paylanması Şəbəkə İdarəetmə Mərkəzi (ŞİM), Sertifikatlaşdırma və Açar Mərkəzi (SAM) və ya ViPNet Manager proqramlarından istifadə etməklə həyata keçirilir.ViPNet Meneceri və

şəbəkə obyektləri öz aralarında informasiyanın idarə olunmasını, habelə poçt məlumatlarının mübadiləsini TCP/IP üzərindən xüsusi nəqliyyat protokolundan istifadə etməklə yerinə yetirir[4].
Abunəçi stansiyanın digər şəbəkə qovşaqlarının vəziyyəti haqqında onlarla qarşılıqlı əlaqədə olması barədə bildiriş bu abunəçi stansiyanın ViPNet Menecerində qeydiyyatdan keçdiyi koordinator tərəfindən standart olaraq həyata keçirilir. Bu koordinator həmişə verilmiş abunəçi nöqtəsi ilə əlaqəli bütün şəbəkə qovşaqları haqqında tam məlumata malikdir. Bununla belə, istifadəçi, lazım gələrsə, IP ünvan serveri kimi onun üçün mövcud olan istənilən digər koordinatoru seçə bilər. Bu halda abunəçi stansiya da ona qoşulmuş qovşaqların əksəriyyəti haqqında məlumat əldə edə və onlara özü haqqında məlumat verə biləcək[3].

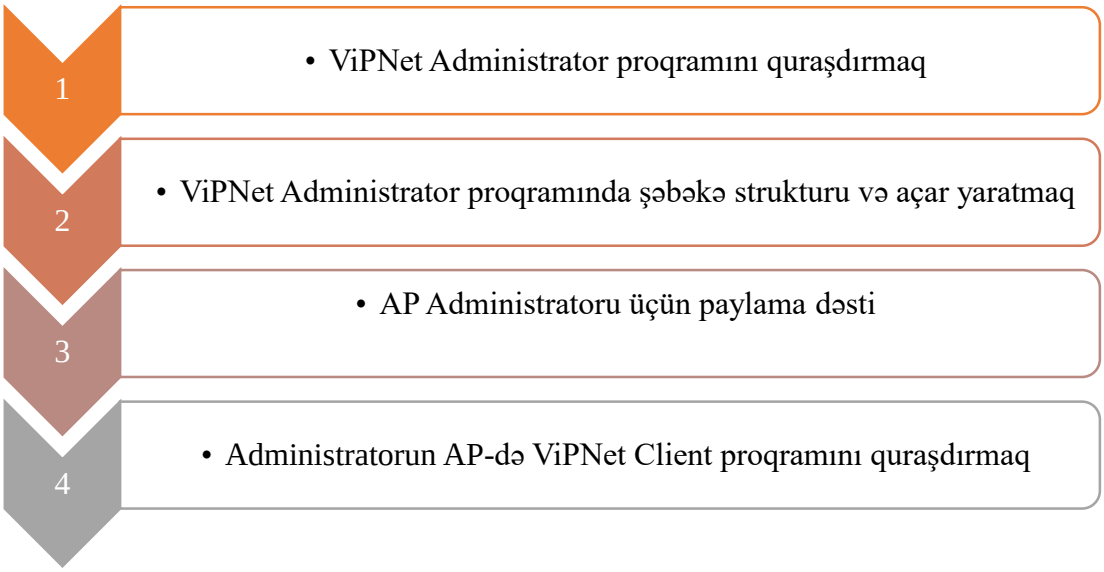
Təhlükəsiz avtomatlaşdırılmış şəbəkənin qurulması. Aşağıdakı şəkildə ViPNet [Administrator] proqramı paylanmış şəbəkənin kompüterlərindən birində (təhlükəsizlik administratoru) quraşdıraq.



Şəkil 1. Təhlükəsiz avtomatlaşdırılmış şəbəkənin struktur sxemi [6]

Bizə Proqram təminatı aşağıdakıları yerinə yetirməyə imkan verir:
• VPN şəbəkəsinin topologiyasını (məntiqi konfiqurasiya) qurmaq və VPN şəbəkə obyektləri üçün əsas məlumatları yaratmaq, VPN şəbəkə obyektlərinə adlar təyin etmək və onlar arasında əlaqələrə icazə vermək və ya imtina etmək [6].
• VPN şəbəkəsinin obyektlərində yenilənmiş istinad və açar informasiyanın sonradan paylanması və VPN şəbəkəsinin dəyişdirilməsi (obyektlərinin əlavə edilməsi və ya silinməsi).
• Quraşdırılmış proqramın yeni versiya yaradılarsa, (ViPNet [Müştəri] və ViPNet [Koordinator]) mərkəzi şəkildə yeniləmək.
ViPNet [Koordinator] proqramı yerli şəbəkə şlüzlərində (PROXY serverləri) quraşdırılmışdır. Belə kompüterlərin IP ünvanları statik olmalıdır. Proqram təminatı aşağıdakı funksiyaları yerinə yetirir[7]:
• Başqa LAN-lardakı kompüterlərlə bu LAN-ın kompüteri arasında məlumat mübadiləsini yerinə yetirmək üçün ViPNet [Koordinatoru] təhlükəsiz əlaqə tunelləri yaradır;
•Tunellər öz LAN-dakı kompüterləri arasında açıq məlumat mübadiləsini bu LAN-ın ViPNet [Koordinatoru]- və mobil istifadəçinin ViPNet proqramı [Müştəri] ilə təhlükəsiz qorunan əlaqəyə çevirir;

• Kənar LAN-dakı kompüterlər və qorunan mobil istifadəçilər bu LAN-dakı hər kompüterə daxil ola bilməyəcəklər[5];
• "Onların" tunelli kompüterlərinin uzaq LAN və qorunan mobil istifadəçilərin resurslarına çıxışını məhdudlaşdırır (müəyyən LAN-dakı hər bir kompüter uzaq LAN-dakı kompüterlərə və qorunan mobil istifadəçilərə daxil ola bilməyəcək)[8];
•IP ünvan serveridir, yəni qorunan mobil istifadəçiləri digər VPN obyektlərinin (aktiv və ya qeyri-aktiv) cari vəziyyəti və onların IP ünvanları haqqında məlumatlandıran köməkçi masasıdır;
•yeniləmələrin (proqram təminatı, arayış və əsas məlumatlar) yayılması üçün serverdir;
• VPN obyektləri arasında "fayl mübadiləsi" vasitəsilə göndərilən poçt mesajlarının (əgər Business Mail proqramı istifadə olunursa) və faylların göndərilməsi üçün server-routerdir;
• İnternetdən LAN-a icazəsiz girişin qarşısını alan Firewalldır.
Bütün bu sadaladığımız funksiyalar şlüz proqramı (PROXY server) tərəfindən həyata keçirilməlidir.
ViPNet Administratorunun qurulması. ViPNet Administrator tərəfindən qorunan iş mühiti yaratmaq üçün ağağıdakı şəkildə göstərilən ardıcıllıqları yerinə yetirmək lazımdır:



Şəkil 2. ViPNet Administrator tərəfindən qorunan iş mühiti [6]

Fərqli şəbəkələrin Şəbəkə İdarəetmə Mərkəzləri iyerarxik sistemi təşkil edilirsə, onda biz ViPNet Administratorunun quraşdırılmasına aparıcı şəbəkədən başlayırıq. Administratorun iş stansiyasını şəbəkə idarəçiliyinə hazırlamaq üçün aşağıdakıları etməliyik:
• ŞİM proqramında şəbəkənizin strukturunu yaradın, o cümlədən administrator abunəçi nöqtəsini yaradaq (onu ŞİM və SAM proqram tapşırıqlarında qeydiyyatdan keçirək). Bütün qovluqları yaradaq.
• SAM proqramında administratorun AP üçün açar paylama dəstini yaradaq.
Yaradılmış paylama dəstini SAM-dəki müvafiq menyudan ViPNet Client proqramının sonrakı quraşdırılması üçün qovluğa köçürək(VPNet Administrator proqram təminatı quraşdırma qovluğunun\SS alt qovluğu);
• ViPNet Client proqramını administratorun AP-də quraşdıraq və administratorun AP açar dəstini yaradaq. ViPNet Client proqram təminatının quraşdırılması proqramı kompüterdə ViPNet Administrator proqramının quraşdırıldığını aşkar edərsə, defolt olaraq o, ViPNet Administrator proqramının quraşdırılması qovluğunun .\SS alt qovluğunda ViPNet Client proqramını quraşdırmağı təklif edəcək.

Administratorun iş yerində IP trafikinin qorunması tələb olunmursa, ViPNet Client əvəzinə ViPNet CryptoService quraşdırıla bilər. ViPNet CryptoService-in düzgün işləməsini təmin etmək üçün ViPNet CryptoService quraşdırma sihirbazında aşağıdakı proqram quraşdırma yolunu göstərin: ViPNet Administrator proqram təminatı quraşdırma qovluğunun SS alt qovluğu[6].
Bu andan etibarən administratorun iş stansiyası şəbəkəni idarə etməyə tam hazır olacaq[7].