МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Завідувач кафедри
_____ І.С. Скарга-Бандурова
«____»_____ 20__ р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА

ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

Засоби системи безпеки корпоративної мережі закладу освіти

Освітній рівень"бакалавр"
Спеціальність 125 "Кібербезпека"

Науковий керівник роботи: _____ (підпис) Д.О.Недзельський (ініціали, прізвище)

Консультант з охорони праці: _____ (підпис) Я.О.Критська (ініціали, прізвище)

Здобувач вищої освіти: _____ (підпис) А.М.Коваль (ініціали, прізвище)

Група: КБ-16д

Сєвєродонецьк 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітній рівень бакалавр
Спеціальність 125 "Кібербезпека"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Т.в.о. завідувача кафедри _____
_____ С.О. Сафонова
«_____» _____20____р.

З А В Д А Н Н Я
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) БАКАЛАВРА

Коваля Андрія Миколайовича
(прізвище, ім'я, по батькові)

1. Тема роботи Засоби системи безпеки корпоративної мережі закладу освіти

керівник проекту (роботи) Недзельський Дмитро Олександрович, к.т.н., доц.
(прізвище, м.'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від «30» 04 2020 р. № 73/15.15
2. Строк подання студентом роботи 10.06.2020
3. Вихідні дані до роботи Матеріали переддипломної практики, відомості про серверні розробки, теоретичний аналіз загроз, теоретичні відомості про захист мереж, середа розробки Microsoft Windows Server 2012

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Огляд інфраструктури захисту на прикладному рівні, створення базової конфігурації безпеки корпоративної мережі з використанням ос windows server 2012, моделювання безпеки корпоративної мережі за допомогою параметрів політики домену, охорона праці, висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці	Критська Я.О. ст. викл. кафедри КНІ		

7. Дата видачі завдання 30.04.2020

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Розробка технічного завдання	01.05.2020-07.05.2020	
2	Аналіз завдання, робота з літературою	08.05.2020-13.05.2020	
3	Розробка частини проекту "Охорона праці"	13.05.2020-15.05.2020	
4	Розробка та тестування системи	15.05.2020-01.06.2020	
5	Оформлення пояснювальної записки та презентації	2.06.2020-09.06.2020	

Здобувач вищої освіти _____ А.М.Коваль
(підпис) (прізвище та ініціали)

Науковий керівник _____ Д.О.Недзельський
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Пояснювальна записка дипломної роботи бакалавра: 89 с., 20 рис., 7 табл., 1 додаток, 19 бібліографічних джерел посилань.

Дипломна робота присвячена розробці системи безпеки корпоративної мережі яка працює під управлінням Windows Server 2012 і входить у домен на основі Active Directory.

Метою даної дипломної роботи є аналіз інфраструктури захисту корпоративної мережі на прикладному рівні. Розглянуто базову конфігурацію безпеки корпоративної мережі з використанням ОС Windows Server 2012. Для посилення захисту налаштованої за замовчуванням ОС необхідно використовувати об'єкти групової політики. Розглянуто параметри групової політики ОС Windows Server 2012. За допомогою параметрів політики домену побудовано модель безпеки корпоративної мережі.

Ключові слова: корпоративна мережа, windows server 2012, комп'ютерна мережа, протокол, операційна система, сервер

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

БД – база даних

ОС – операційна система

ПК – персональний комп’ютер

GPO – об’єкти групової політики

IP – адреса пристрою підключеного до мережі

IT – інформаційні технології

TCO – сукупна вартість володіння

ВСТУП

Розвиток IT дозволяє підвищити ефективність діяльності компаній, а також відкриває нові можливості для взаємодії з потенційними клієнтами на основі загальнодоступних мереж, в тому числі Інтернету. Утворення Web-сайту – своєрідного представництва в Інтернеті - є тільки першим кроком на цьому шляху. Активне ведення комерційних операцій в Мережі являє собою масовий доступ користувачів електронних послуг до Internet – додатків та проведення електронних транзакцій мільйонами користувачів Мережі. Розміщення Internet-додатків всередині корпоративної мережі може нанести збиток безпеці IT-інфраструктурі оскільки відкриття доступу створить потенційну можливість для несанкціонованого проникнення зловмисників до мережі підприємства.

Забезпечення інформаційної безпеки повинно містити в собі розв`язання таких завдань як безпечний доступ до Web-серверів та Web-додатків, аутентифікація та авторизація користувачів, забезпечення цілісності та конфіденційності даних, реалізація електронного цифрового підпису тощо.

Організації потребують надійних, гнучких та безпечних методів та засобів для отримання та використання відкритої та конфіденційної інформації чисельними групами людей – своїми співробітниками, партнерами, клієнтами та постачальниками. Проблема міститься у забезпеченні доступу до такої інформації тільки авторизованими користувачами. Доцільно використовувати інтегровану систему управління доступу користувачів до чутливої інформації у широкому діапазоні точок доступу та додатків. Така система вирішує проблеми контролю доступу, з якими стикаються організації, забезпечуючи при цьому зручний доступ та високу безпеку.

1 ОГЛЯД ІНФРАСТРУКТУРИ ЗАХИСТУ НА ПРИКЛАДНОМУ РІВНІ

1.1 Управління ідентифікацією та доступом

Для реалізації зростаючих потреб електронного бізнесу необхідно побудувати надійне, з точки зору безпеки, середовище для здійснення електронного бізнесу у режимі on-line. Технології, які дають можливість здійснювати електронний бізнес, виконують чотири основні функції (рис. 1.1):

– аутентифікацію або перевірку автентичності користувача;

– управління доступом, яке дозволяє авторизованим користувачам отримувати доступ до необхідних ресурсів;

– шифрування, яке гарантує, що зв’язок між користувачем та базовою інфраструктурою захищений;

– безвідмовність, яка означає, що користувачі не можуть пізніше відмовитися від виконання транзакції (частіше реалізується за допомогою цифрового підпису та інфраструктури відкритих ключів [1].

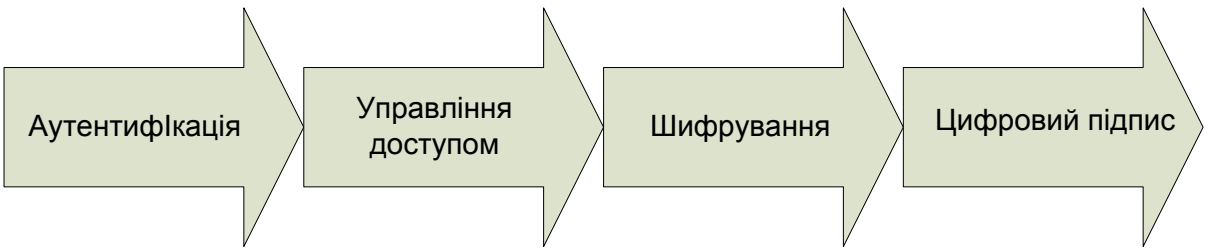


Рисунок 1.1 -Технології які забезпечують електронний бізнес

Тільки розв’язання, яке дозволяє виконувати всі чотири функції, може створити доручене середовище, яке може забезпечити реалізацію електронного бізнесу.

Управління доступом є критичним компонентом загальної системи безпеки. Система управління доступом забезпечує авторизованим

користувачам доступ до належних ресурсів. Проектування цієї інфраструктури вимагає тонкого балансу між надаванням доступу до критичних ресурсів тільки авторизованим користувачам та забезпечення необхідної безпеки цих ресурсів, які відомі великому колу користувачів.

1.2 Особливості та управління доступом

У розподіленій корпоративній мережі зазвичай застосовуються два методи управління доступом:

– управління доступом мережі (регулює доступ до ресурсів внутрішньої мережі організації);

– управління Web-доступом (регулює доступ до серверів та їх вмісту).

Всі запити на доступ до ресурсів проходять через один або більше списків контролю доступу ACL (Access Control List).

ACL являє набор правил доступу, які задають для набору ресурсів, що захищаються. Ресурси з низьким ризиком будуть мати менш суворі правила доступу, в той час високо критичні ресурси повинні мати більш суворі правила доступу. ACL, по своїй суті, визначають політику безпеки [2].

Доступ до ресурсів мережі можна регулювати шляхом утворення списків контролю доступу Login AC, які дозволяють визначити конкретні дозволи та умови для отримання доступу до ресурсів внутрішньої мережі.

Утворюючи конкретні списки контролю Web ACL адміністратори безпеки визначають, які користувачі можуть отримати доступ до Web-серверів організації та їх змісту. Управління доступом спрощується при застосуванні єдиної централізованої інфраструктури контролю та управління доступом, яка може дозволити користувачу «самообслуговування», доручаючи їм такі завдання управління, як реєстрація, редагування профілю, відновлення паролю та управлення підпискою. Вона може забезпечити делегування адміністрування, передачу функції управління користувачам,

особам, які найбільше обізнані про конкретну групу користувачів як у бізнес-підрозділах організації так і у клієнтів та у підрозділах бізнес- партнерів. Для полегшення підтримки системи безпеки масштабу виробництва, засоби управління доступом можуть отримувати дані користувачів та політик, які вже зберігаються в таких існуючих сховищах даних як каталоги LDAO та реляційні БД.

Централізовані системи управління доступом випускаються низкою компаній, такими як Secure Compyting, RSA Security Inc., Baltimore та інші.

Розглянемо функціонування системи управління доступом на прикладі системи Premier Access компанії Secure Computing. Ця система здійснює управління Web та доступом мережі всіх користувачів, включаючи внутрішніх користувачів, віддалених співробітників, клієнтів, постачальників та бізнес- партнерів. Вона базується на політиці безпеки, яка дозволяє персоналізувати права доступу користувачів. Користувачі отримують доступ тільки до тих ресурсів на які було надано дозвіл, у відповідності з їх правами доступу через Web-доступ, VPN-доступ або віддалений доступ з використанням серверів Radius. В системі реалізовані засновані на застосуванні каталогів процеси аутентифікації, авторизації та адміністрування дій користувачів. Система підтримує різноманітні типи аутентифікаторов – від багаторазових паролів до біометричних засобів аутентифікації. Перевага віддається засобам суворої аутентифікації [3].

Засоби управління користувачами дозволяють управляти великою кількістю користувачів. Сервер реєстрації дає можливість самим користувачам реєструватися у мережі, використовуючи стандартні Web-браузери. В процесі реєстрації користувачу призначаються ролі. Ролі є ярликами, ідентифікуючими групи користувачів, які розподіляють однакові права доступу. Таким чином, ролі визначають набір правил доступу, які застосовуються до конкретних груп користувачів. Категорування користувачів за ролями можна виконати на основі їх функціональних обов’язків.

1.3 Засоби управління мережним доступом

В системі управління доступом використовуються так звані агенти. Агент системи - це програмний модуль, інстальований на відповідний сервер у рамках корпоративної мережі (рис. 1.2) [4].

В якості таких агентів виступають агенти віддаленого доступу, агенти VPN-доступу, агенти серверів RADIUS, Novel,RAS,Citrix та ін. При спробі користувача підключитися до внутрішньої мережі, агенти системи перехоплюють запит користувача на вхід у мережу.

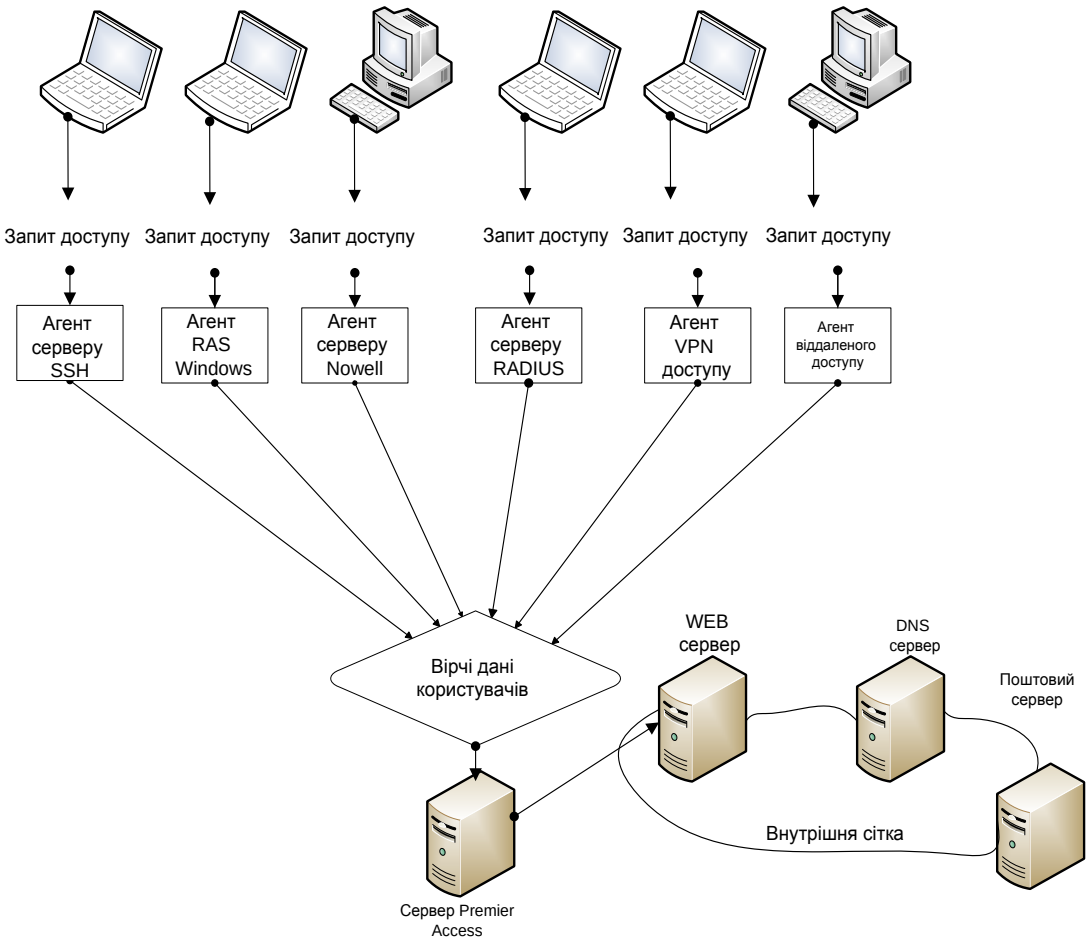


Рисунок 1.2 - Схема управління доступом до мережі

Агенти діють як точки аутентифікації користувачів UAPs (User Authentication Points) на лініях комунікації з сервером Premirer Access. У відповідь на запит користувача агент запитує у користувача його вірчі дані –

ідентифікатор користувача та аутентифікатор. Відповідаючи на запит агента, користувач вводить свої дані. Ці вірчі дані передаються AAA-серверу (Authentication, Authorization, Accounting).

AAA-сервер порівнює ідентифікатор ID користувача та сертифікат з даними, які зберігаються у каталозі LDAP, з метою перевірки їх тотожності. Якщо ідентифікатор ID користувача співпадає із збереженим, запис користувача у БД перевіряється по ролі (або ролям) та ресурсам, до яких вони авторизуються. Для аутентифікації можуть застосовуватися фіксований пароль, апаратний або програмний аутентифікатори. Якщо користувач успішно проходить всі шаги підтвердження своєї справжності, він отримує доступ до ресурсу мережі.

1.4 Засоби управління Web-доступом

Система PremierAccess використовує універсальний Web-агент UWA (Universal Web Agent), який інсталює на хост-машині кожного Web-ресурсу, який захищається. На розгляненому прикладі у якості користувача виступає бізнес-партнер, який запитує доступ до Web-ресурсу компанії (рис. 1.3) [5].

Управління Web-доступом реалізується у вигляді процесу, який складається з двох етапів:

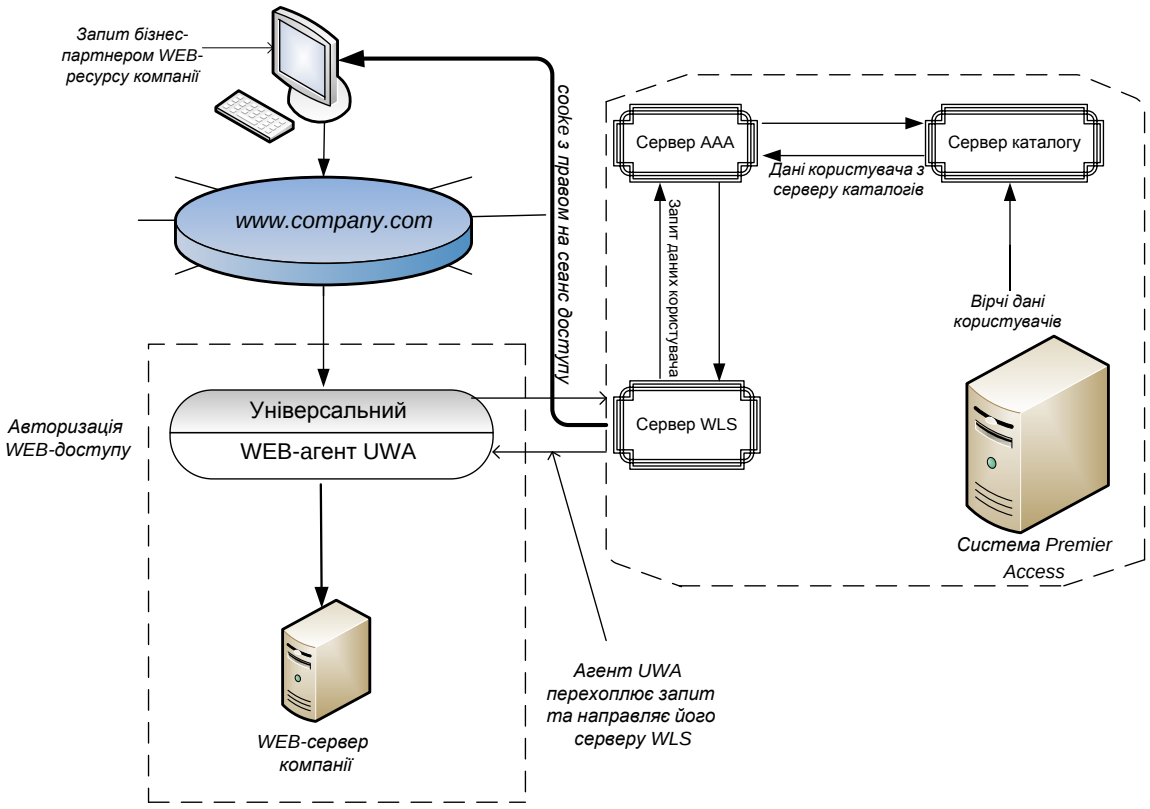


Рисунок 1.3 - Схема управління Web-доступом

– користувач намагається увійти у систему, використовуючи сервер WLS (Web Login Server). Запит користувача на доступ до захищеного Web-ресурсу компанії перехоплюється агентом UWA, який для обробки цього запиту звертається до серверу WLS. Сервер WLS запитує результат аутентифікації у сервера AAA. У випадку успішної аутентифікації сервер WLS генерує сеанс cookie, який містить сеанс ідентифікатора користувача;

– користувач намагається отримати доступ до Web-ресурсу. Сервер WLS використовує сеансів ідентифікатор в cookie для запиту у AAA-серверу даних сеансу користувача. Щоб виконати запит на доступ, сервер WLS передає користувачу сеансів cookie з правами на сеанс. Агент UWA отримує сеанс ID, потім отримує від AAA-сервісу дані сеансу. Базуючись на ролях користувача та політиці доступу він приймає рішення, надати або заборонити користувачу доступ до Web-ресурсу.

При будуванні систем управління доступом важливе значення мають:

– засоби та протоколи аутентифікації віддалених користувачів;

– засоби управління доступом за схемою однократного входу з авторизацією Single Sing-On;

– інфраструктури управління відкритими ключами PKI.

1.5 Організація захищеного віддаленого доступу

Віддалений доступ до комп'ютерних ресурсів став актуальним та значущим, як і доступ у режимі безпосереднього підключення. Віддалений доступ до корпоративної мережі здійснюється з незахищеного зовнішнього оточення через відкриті мережі, тому засоби будування захищеної корпоративної мережі повинні забезпечувати безпеку мережної взаємодії при підключенні до мережі віддалених комп'ютерів.

Віддалений доступ до корпоративної мережі можливий через глобальну комп'ютерну мережу або середовище передачі інформації, утворену ланцюгом з телефонної та глобальної комп'ютерної мережі. Доступ через глобальну мережу Internet є достатньо ефективним способом, причому для підключення віддаленого користувача Internet може використовуватись канал телефонного зв'язку. Основні переваги віддаленого доступу корпоративної мережі через Internet:

– забезпечення масштабуємої підтримки віддаленого доступу, яке дозволяє мобільним користувачам зв'язуватися з провайдером, а потім через Мережу входити у свою корпоративну мережу;

– скорочення витрат на інформаційний обмін через відкрите зовнішнє середовище (віддалені користувачі, підключившись до Internet, зв'язуються з мережею своєї організації з мінімальними витратами);

– управління трафіком віддаленого доступу здійснюється так само як і іншим трафіком Internet.

У корпоративній мережі для взаємодії з віддаленими користувачами виділяється сервер віддаленого доступу, який слугує:

– для установки з’єднання з віддаленим комп’ютером;

– аутентифікації віддаленого користувача;

– управління віддаленим з’єднанням;

– посередництва при обміні даними між віддаленим комп’ютером та корпоративною мережею.

Серед протоколів віддаленого доступу до локальної мережі найбільше розповсюдження отримав протокол «точка-точка» PPP (Point-to–Point Protocol), який є відкритим стандартом Internet. Протокол PPP призначений для встановлення віддаленого з’єднання та обміну інформацією по встановленому каналу пакетами мережного рівня, інкапсульованими у PPP-кадри. Використовуємий у протоколі PPP метод формування кадрів забезпечує одночасну роботу через канал віддаленого зв’язку декількох протоколів мережного рівня.

Протокол PPP підтримує наступні функції:

– аутентификацію віддаленого користувача та серверу віддаленого доступу;

– компресії та шифрування даних, що передаються;

– виявлення та корекції помилок.

На основі протоколу PPP побудовані протоколи PPTP, L2F,L2TP. Ці протоколи дозволяють створювати захисні канали для обміну даними між віддаленими комп’ютерами і локальними мережами, функціонуючими за різноманітними протоколами мережного рівня - IP, IPX або NetBEUI. Для передачі за телефонними каналами зв’язку пакети цих протоколів інкапсулюються у PPP-кадри. При необхідності передачі через Internet захищені PPP-кадри інкапсулюються у IP-пакети мережі Internet. Криптозахист трафіку можливий як у каналах Internet так і на протязі всього шляху між комп’ютером віддаленого користувача та сервером віддаленого доступу локальної мережі [6].

1.5.1 Протоколи аутентифікації віддалених користувачів

Контроль доступу користувачів до ресурсів корпоративної мережі повинен здійснюватися у відповідності із політикою безпеки організації, якій належить ця мережа. Ефективне розмежування доступу до мережних ресурсів може бути забезпечено тільки при надійній аутентифікації віддалених користувачів. Вимоги до надійності аутентифікації віддалених користувачів повинні бути вельми високими, тому що при взаємодії з фізично віддаленими користувачами значно складніше забезпечити доступ до мережних ресурсів. У відмінності від локальних користувачів віддалені користувачі не проходять процедуру фізичного контролю при допуску на територію організації.

При віддаленій взаємодії важлива аутентифікації не тільки користувачів, а і обладнання, оскільки підміна користувача або маршрутизатора приводить до одних і тих же наслідків – дані з корпоративної мережі передаються не тим особам, яким вони призначалися.

Для забезпечення надійної аутентифікації віддалених користувачів, необхідно виконання наступних вимог:

– проведення аутентифікації обох взаємодіючих сторін - як віддаленого користувача так і серверу віддаленого доступу - для виключення маскування зловмисників;

– оперативне узгодження використовуємих протоколів аутентифікації;

– здійснення динамічної аутентифікації взаємодіючих сторін у процесі роботи віддаленого з’єднання;

– застосування криптозахисту таємних паролів для виключення перехвату та несанкціонованого використання аутентифікуючої інформації.

Протокол PPP має вбудовані засоби, які можуть бути використані для організації аутентифікації при віддаленій взаємодії. У стандарті RFC 1334 визначається два протоколи аутентифікації:

– по паролю PAP (Password Authentication Protocol);

– по рукостисканню – CHAP (Challeng Handshake Authentication Protocol).

У процесі встановлення віддаленого з'єднання кожна із взаємодіючих сторін може запропонувати для застосування один із стандартних протоколів аутентифікації - PAP або CHAP. Іноді компанії створюють власні протоколи аутентифікації віддаленого доступу, які працюють разом з протоколом PPP, ці фірмові протоколи є модифікаціями протоколів PAPA та CHAP.

Широке застосування для аутентифікації за одноразовими паролями отримав протокол S/Key. В програмних продуктах, які забезпечують зв'язок по протоколу PPP, протоколи PAP та CHAP, як правило, підтримуються у першу чергу.

В процесі аутентифікації приймають участь дві сторони – яку перевіряють і яка перевіряє. Протокол PAP використовує для аутентифікації передачу перевіряємою стороною ідентифікатора і паролю у вигляді відкритого тексту. Якщо перевіряюча сторона виявляє співпадіння ідентифікатора та паролю із записом, який є в наявності у БД легальних користувачів то процес аутентифікації рахується успішно завершеним, після чого перевіряємій стороні надсилається відповідне повідомлення. В якості сторони, чия справжність перевіряється, як правило, виступає віддалений користувач, а в якості перевіряючої сторони – сервер віддаленого доступу.

Для ініціалізації процесу аутентифікації на базі протоколу PAP сервер віддаленого доступу після встановлення сеансу зв'язку надсилає віддаленому комп'ютеру пакет LCP (Link Control Protocol) – протокол управління каналом, який вказує на необхідність застосування протоколу PAP. Далі здійснюється обмін пакетами PAP. Віддалений комп'ютер передає по каналу зв'язку перевіряючій стороні ідентифікатор та пароль, які введені віддаленим користувачем. Сервер віддаленого доступу за отриманим ідентифікатором користувача обирає еталонний пароль з БД системи захисту та порівнює його з отриманим паролем. Якщо вони співпадають, тоді ідентифікація вважається успішною, про що повідомляється віддаленому користувачу.

Слідує відмітити, що протокол аутентифікації PAP, згідно якого ідентифікатори передаються по лініях зв’язку у незашифрованому виді, доцільно застосовувати тільки разом з протоколом, орієнтованим на аутентифікації за одноразовим паролем, наприклад, спільно з протоколом S/Key. Інакше пароль, який передається за каналом зв’язку, може бути перехоплений зловмисником та використаний повторно, з метою маскування під санкціонованого віддаленого користувача.

В протоколі CHAP використовується таємний статичний пароль. У відмінності від протоколу PAP в протоколі CHAP пароль кожного користувача для передачі за лініями зв’язку шифрується на основі випадкового числа, яке отримано від сервера. Така технологія забезпечує не тільки захист паролю від крадіжки, але і захист від повторного використання зловмисником перехоплених пакетів із зашифрованим паролем. Протокол CHAP застосовується тільки у сучасних мережах частіше ніж PAP, тому що він використовує передачу паролю по мережі у захищеній формі, як слідство, більш безпечною.

Шифрування паролю у відповідності з протоколом CHAP виконується за допомогою криптографічного алгоритму хешування і тому є незворотнім. У стандарті RFC 1334 для протоколу CHAP у якості хеш-функції визначений алгоритм MD5, який виробляє із вхідної послідовності якої завгодно довжин 16-байтове значення. Хоча мінімальною довжиною секрету є 1 байт, для підвищення криптостійкості рекомендується використовувати секрет довжиною не менше 16 байт. Специфікація CHAP не виключає можливості використання інших алгоритмів рахування хеш - функцій.

Для ініціалізації процесу аутентифікації по протоколу CHAP сервер віддаленого доступу після встановлення сеансу зв’язку повинен надіслати віддаленому комп’ютеру пакет LCP, який вказує на необхідність застосування протоколу CHAP, а також, необхідного алгоритму хешування. Якщо віддалений комп’ютер підтримує запропонований алгоритм хешування, то він повинен відповісти пакетом LCP про узгодження із запропонованими параметрами. Інакше виконується обмін пакетами LCP для

узгодженого алгоритму хешування. Після цього починається аутентифікація на основі обміну пакетами протоколу CHAP.

В протоколі CHAP визначені пакети чотирьох типів:

– виклик (Challenge);

– відгук (Response);

– підтвердження (Success);

– відмова (Failure).

Протокол CHAP використовує для аутентифікації віддаленого користувача результат шифрування довільного слова - виклика за допомогою унікального секрету Цей секрет є в наявності як у перевіряючої так і у перевіряємої сторони. Процедура аутентифікації починається з відправки сервером віддаленого доступу пакету Виклик (рис. 1.4).

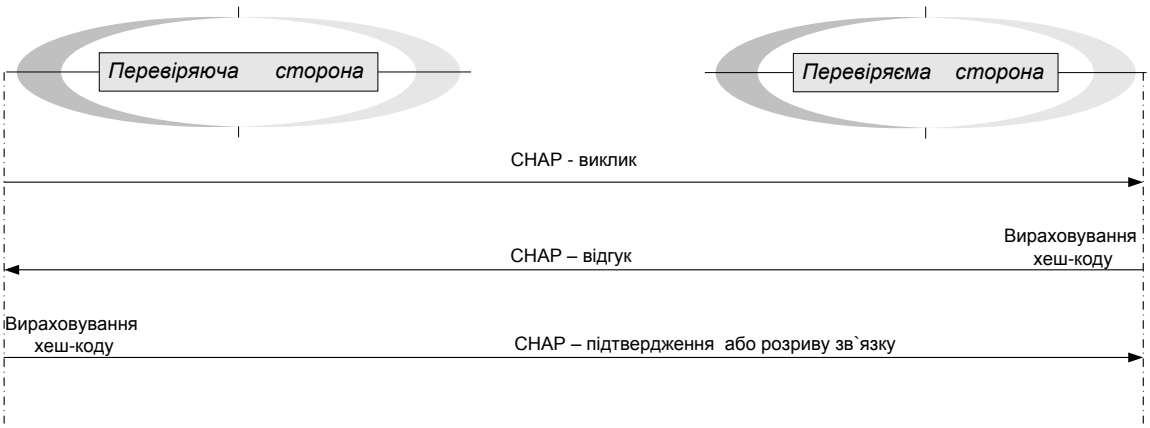


Рисунок 1.4 - Кроки процесу аутентифікації по протоколу CHAP

Віддалений комп’ютер, отримавши пакет «Виклик», зашифровує його за допомогою односторонньої функції та відомого йому секрету, отримуючи в результаті дайджест. Дайджест повертається перевіряючій стороні у вигляді пакету «Відгук».

Оскільки використовується одностороння хеш-функція, то по перехопленим пакетам «Виклик» і «Відгук» вирахувати пароль віддаленого користувача практично неможливо.

Отримавши пакет «Відгук», сервер віддаленого доступу порівнює вміст результату з отриманим пакету «Відгук» з результатом, вирахуваним

самостійно. Якщо ці результати співпадають, то аутентифікації вважається успішною і сервер надсилає віддаленому комп'ютеру пакет «Підтвердження».

Інакше сервер віддаленого доступу надсилає пакет «Відмова» та розриває сеанс.

Пакет «Виклик» повинен бути відправлений сервером повторно, якщо у відповідь на нього не отримано пакет «Відгук». Крім того пакет «Виклик» може відправлятися періодично на протязі сеансу віддаленого зв'язку для проведення динамічної аутентифікації, щоб переконатися, що протидіюча сторона не була підмінена. Відповідно пакет «Відгук» повинен відправлятися перевіряємій стороні у відповідь на кожний прийнятий пакет «Виклик».

Одним з найбільш розповсюджених протоколів аутентифікації на основі одноразових паролей є стандартизований в Интернеті протокол S/Key. Цей протокол реалізований у багаточисельних системах, які потребують перевірку автентичності віддалених користувачів, наприклад у системі TACACS+ компанії Cisco.

Перехоплення одноразового паролю, який передається по мережі у процесі аутентифікації, не надає зловмиснику можливості повторно використати цей пароль, тому що при наступній перевірці справжності необхідно надавати вже інший пароль. Тому схема аутентифікації на основі одноразових паролів, наприклад S/Key, дозволяє передавати по мережі одноразовий пароль у відкритому виді, і таким чином, компенсує основний недолік протоколу аутентифікації PAP.

Однак, слідує відмітити, що протокол S/Key, не виключає необхідності завдання таємного паролю для кожного користувача. Цей секретний пароль використовується тільки для генерації одноразових паролів. Для того щоб зловмисник не зміг за перехопленим одноразовим паролем вирахувати секретний вихідний пароль, генерація одноразових паролів виконується за допомогою односторонньої функції. В якості такої односторонньої функції у специфікації протоколу S/Key визначений алгоритм хешування MD4 (Message Digest Algorithm 4) Деякі реалізації протоколу S/Key у якості

односторонньої функції використовують алгоритм хешування MD5 (Message Digest Algorithm 5).

Розглянемо основну ідею протоколу S/Key, на наступному прикладі. Нехай віддаленому користувачу (перевіряємій стороні) для регулярного проходження аутентифікації призначається випадковий ключ К, в якості її таємного постійного паролю. Потім перевіряючи сторона виконує процедуру ініціалізації списку одноразових N=100 паролів. В ході даної процедури перевіряючи сторона, за допомогою односторонньої функції h вираховує по ключу К перевірочне значення ω_{101} для 1-го одноразового пароля. Для вираховування значення ω_{101} ключ К підставляють у якості аргументу функції h і дана функція рекурсивно виконується 101 раз:

$$\omega_1 = \eta(\mathrm{K}), \omega_2 = \eta\left(\eta(\mathrm{K})\right), \omega_3 = \eta\left(\eta\left(\eta(\mathrm{K})\right)\right), ...,$$
$$\omega_{101} = \eta\left(\eta\left(\eta(...\eta(\mathrm{K})...\ )\right)\right) = \eta^{101}(\mathrm{K}).$$

Ідентифікатор користувача і відповідний цьому користувачу секретний ключ К, а також несекретні числа N та ω_{101} зберігаються у БД перевіряючої сторони. Число N є номером одноразового паролю для чергової аутентифікації із списку одноразових паролів. Слідує відмітити, що після використання кожного такого паролю номер N зменшується на одиницю.

У процесі чергової аутентифікації, яка проводилась після ініціалізації, перевіряєма сторона надає перевіряючій стороні свій ідентифікатор, а та повертає відповідне цьому ідентифікатору число N. У нашому прикладі N=100. Потім перевіряєма сторона вираховує за своїм секретним ключем К одноразовий пароль та надсилає його перевіряючій стороні.

$$\omega'_{100} = h\left(h\left(h(...h(K)...)\right)\right) = h^{100}(K).$$

Отримавши значення ω'_{100}, перевіряюча сторона виконує на ним 1 раз односторонню функцію $\omega'_{101} = h(\omega'_{100})$. Далі перевіряюча сторона порівнює отримане значення ω'_{101} із значенням ω_{101} з БД. Якщо вони співпадають, це означає, що і $\omega'_{100} = \omega_{100}$ і, як слідство, аутентифікація є успішною.

У випадку успішної аутентифікації перевіряючи сторона замінює БД для перевіряємої сторони число ω'_{100}, а число N на N=N-1. З урахуванням, того що при успішній аутентифікації номер одноразового паролю N для чергової аутентифікації зменшився на 1, в БД перевіряючої сторони сумісно з ідентифікатором і секретним ключем К перевіряємої сторони буде зберігатися числа (N-1) та ω_{100}. Тут під ω_{100} розуміється отриманий від перевіряємої сторони, при успішній аутентифікації, останній одноразовий пароль. Після використання чергового списку одноразових паролів процедура ініціалізації повинна виконуватися знову [7].

Іноді бажано, щоб користувач мав можливість сам призначати секретний постійний пароль. Для втілення такої можливості специфікація S/Key передбачає режим вираховування одноразових паролів не тільки на основі секретного пароля, а і на основі генерує мого, перевіряючою стороною, випадкового числа. Таким чином, у відповідності із протоколом S/Key за кожним користувачем закріплюється ідентифікатор та секретний постійний пароль.

Перед тим як проходити аутентифікацію, кожен користувач повинен спочатку пройти процедуру ініціалізації чергового списку одноразових паролів, а саме фазу парольної ініціалізації. Дана фаза виконується по запиту користувача на сервері віддаленого доступу.

Для прискорення процедури аутентифікації певне число одноразових паролів, наприклад декілька десятків, може бути враховано і зберігатися на віддаленому комп'ютері у зашифрованому вигляді.

Протокол аутентифікації на основі одноразових паролів S/Key застосовують для поліпшення характеристик протоколів централізованого контролю доступу до мережі віддалених користувачів TACACS та RADIUS.

1.5.2 Централізований контроль віддаленого доступу

Для управління віддаленими з’єднаннями невеликої локальної мережі достатньо одного серверу віддаленого доступу. Однак, якщо локальна мережа об’єднує відносно великі сегменти та число видалених користувачів істотно збільшується, то одного серверу віддаленого доступу недостатньо.

Розглянемо чи вирішується задача контролю доступу до мережі віддалених користувачів у відповідності із звичайною схемою, коли віддалені користувачі намагаються отримати доступ до мережних ресурсів, які знаходяться під управлінням декількох різних ОС. Користувач додзвонюється до свого серверу віддаленого доступу і RAS виконує для нього процедуру аутентифікації, наприклад за протоколом CHAP. Користувач логічно входить у мережу за звертається до необхідного серверу, де знову проходить аутентифікацію та авторизацію, в результаті чого отримує чи не отримує дозвіл на виконання запитаної операції. Неважко помітити, що така схема незручна користувачу, тому що йому приходиться декілька разів виконувати аутентифікацію - при вході в мережу на сервері віддаленого доступу, а потім ще кожен раз при зверненні до кожного ресурсного серверу мережі. Користувач вимушений запам’ятовувати декілька різних паролів. Крім того, він повинен знати порядок проходження різних процедур аутентифікації в різних ОС. Виникають, також, труднощі з адмініструванням такої мережі. Адміністратор повинен заводити облікову інформацію щодо кожного користувача на кожному сервері. Ці розрізнені БД важко підтримувати у коректному стані. При звільненні співробітника важко виключити його зі всіх списків. Виникають труднощі при призначенні паролів, суттєво ускладнюється аудит.

Відмічені труднощі долаються при установці в мережі централізованої служби аутентифікації та авторизації. Для централізованого контролю доступу виділяється окремий сервер – сервер аутентифікації. Але в Windows Server 2012 ця технологія вже слугує для перевірки автентичності віддалених

користувачів, визначення їх повноважень, а також фіксації та накопичування реєстраційної інформації, зв’язаної з віддаленим доступом.

Проте в більшості випадків сервери віддаленого доступу потребують посередництва для взаємодії з центральною БД системи захисту,наприклад службою каталогів.

Більшість мережних ОС та служб каталогів зберігають еталонні паролі користувачів з використанням одностороннього хешування, що не дозволяє серверам віддаленого доступу, стандартно реалізуючих протоколи PAP та CHAP, витягти відкритий еталонний пароль для перевірки відповіді.

Роль посередника у взаємодії між серверами віддаленого доступу та центральної БД системи захисту може бути покладено на сервер аутентифікації. Централізований контроль віддаленого доступу до комп’ютерних ресурсів за допомогою серверу аутентифікації виконується на основі спеціалізованих протоколів. Ці протоколи дозволяють об’єднати використовуємі сервери віддаленого доступу та сервер аутентифікації в одну підсистему на основі взаємодії з центральною БД системи захисту. Сервер аутентифікації створює єдину точку спостереження та перевірки всіх віддалених користувачів та контролює доступ до комп’ютерних ресурсів у відповідності з встановленими правилами.

До найбільш популярних протоколів централізованого контролю доступу до мережі віддалених користувачів відносяться протоколи TACACS (Terminal Access Controller Access Control System) та RADIUS (Remote Authentication Dial-In User Service). Вони призначені, в першу чергу, для організації, в центральній мережі яких використовується декілька серверів віддаленого доступу. В цих системах адміністратор може управляти БД ідентифікаторів та паролів користувачів, надавати їх привілеї доступу та вести облік звернень до системних ресурсів.

Протоколи TACACS та RADIUS потребують застосування окремого серверу аутентифікації, який для перевірки автентичності користувачів та визначення їх повноважень може використовувати не тільки власну БД, а також мати взаємодію із сучасними службами каталогів, наприклад з NDS

(Novell Directory Services). Сервери TACACS та RADIUS виступають у якості посередників між серверами віддаленого доступу, який приймає дзвінки від користувачів, з однієї сторони, та мережними ресурсними серверами з іншої. Реалізації TACACS та RADIUS можуть слугувати посередниками для зовнішніх систем аутентифікації.

Розглянемо особливості централізованого контролю віддаленого доступу на прикладі протоколу TACACS (рис. 1.5).

Система TACACS виконана в архітектурі клієнт-сервер. В комп'ютерній мережі, яка включає в себе декілька серверів віддаленого доступу, встановлюється один сервер аутентифікації, який називають сервером TACACS. На сервері TACACS формується центральна база облікової інформації про віддалених користувачів (імена, паролі та повноваження) [8].

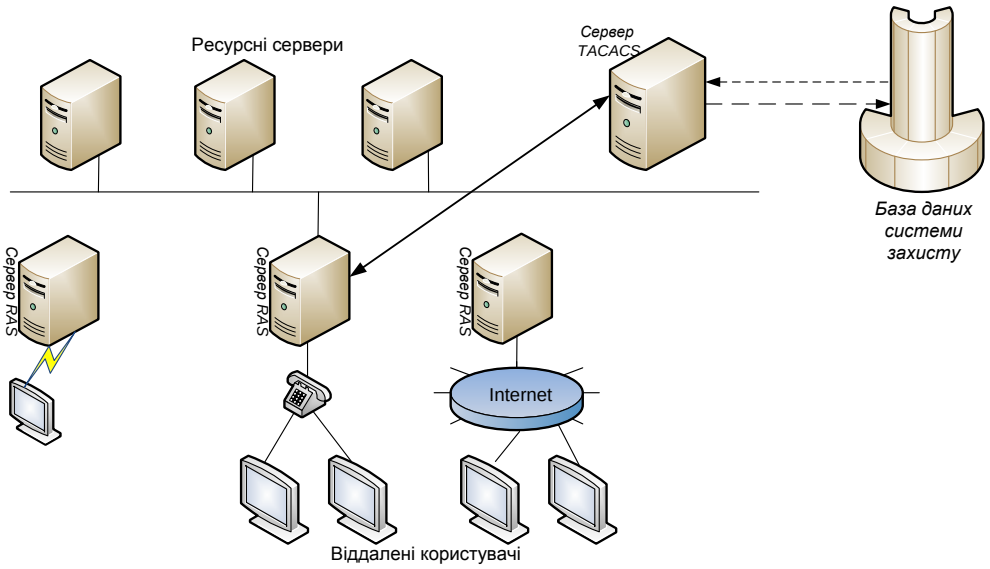


Рисунок 1.5 - Схема централізованого контролю віддаленого доступу

У повноваженнях кожного користувача задаються підмережі, комп'ютери та сервіси, з якими він може працювати, а також різноманітні види обмежень, наприклад тимчасові обмеження. На цьому сервері ведеться БД аудиту, в якій накопичується реєстраційна інформація щодо кожного

логічного входу, тривалість сесії, а також часу використовування ресурсів мережі.

Клієнтами мережі TACACS є сервери віддаленого доступу, які приймають запити на доступ до ресурсів мережі від віддалених користувачів. В кожний сервер вбудоване програмне забезпечення (ПЗ), яке реалізує стандартний протокол, за яким вони взаємодіють з сервером TACACS, цей протокол також називається TACACS.

Протокол TACACS стандартизує схему взаємодії серверів віддаленого доступу з сервером TACACS на базі завдання можливих типів запитів, відповідей та з'єднань. Визначені запити, з якими клієнти можуть звертатися до серверу TACACS. Сервер на кожен запит повинен відповісти відповідним повідомленням. Протокол задає декілька типів з'єднань, кожне з яких визначається як послідовність пар запит-відповідь, орієнтована на рішення окремої задачі.

Визначено три типи з'єднання:

– Auth - виконується тільки аутентифікація;

– Login – виконується аутентифікація і фіксується логічне з'єднання з користувачем;

– Slip – виконується аутентифікація, фіксується логічне з'єднання, підтверджується IP-адреса клієнта.

За допомогою Auth сервери віддаленого доступу перенаправляються серверу TACACS потік запитів на логічне підключення користувачів до мережі в цілому. З'єднання Login слугує для перенаправлення запитів серверу TACACS на логічне підключення користувачів до окремих комп'ютерів локальної мережі.

При з'єднанні Auth сервер віддаленого доступу надсилає на сервер TACACS тільки одне повідомлення – пакет Auth на який сервер TACACS відповідає повідомленням Replay.

Сервер TACACS на основі наявних у нього даних перевіряє пароль та повертає відповідь у виді пакету Replay, де повідомляє про успішну або

неуспішну аутентифікації. У відповідності з протоколом TACACS пароль передається між сервером віддаленого доступу та сервером аутентифікації у відкритому вигляді. Тому протокол TACACS необхідно застосувати сумісно з протоколом аутентифікації за одноразовими паролями.

На підставі отриманих від серверу TACACS вказівок сервер віддаленого доступу виконує процедуру аутентифікації та дозволяє або не дозволяє віддаленому користувачу логічно вийти у мережу.

Сервер TACACS може виконувати аутентифікації та авторизацію віддалених користувачів різноманітними способами:

– використовуючи вбудований механізм аутентифікації тієї ОС, під управлінням якої працює сервер;

– використовувати централізовані довідкові системи ОС;

– використовувати системи аутентифікації, які основані на одноразових паролях;

– передавати запити іншим системам аутентифікації.

Слід відмітити, що недоліки протоколу TACAC зв’язані з відкритою передачею паролю по мереж, вилучені компанією Cisco у версії яка має назву TACACS+. У відповідності з протоколом TACACS+ пароль для передачі шифрується за допомогою алгоритму MD5. TACACS+ передбачає роздільне зберігання БД аутентифікаційної, авторизованої та облікової інформації, в тому числі на різних серверах. Поліпшено взаємодію з системою Kerberos.

Іншою розповсюдженою системою централізованої аутентифікації при віддаленому доступі є система RADIUS. За своїми функціональними можливостями протоколи TACACS та RADIUS практично еквівалентні та є відкритими стандартами, однак протокол RADIUS став більш популярним серед виробників систем централізованого контролю віддаленого доступу. Це пов’язано з тим, що засноване на ньому серверне ПЗ розповсюджується безкоштовно. Крім того, протокол RADIUS менш складний у реалізації.

1.6 Постановка завдання дослідження

Метою даної дипломної роботи є аналіз інфраструктури захисту корпоративної мережі на прикладному рівні.

У дипломній роботі необхідно вирішити наступні питання й завдання:

- розглянути базову конфігурацію безпеки корпоративної мережі;
- розглянути параметри групової політики ОС Windows Server 2012;
- побудувати модель безпеки корпоративної мережі;
- вибір і опис апаратних ресурсів запроектованої мережі;
- оцінка ефективності й продуктивності функціонування.

2 СТВОРЕННЯ БАЗОВОЇ КОНФІГУРАЦІЇ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ОС WINDOWS SERVER 2012

У кожному новому випуску операційної системи компанія Майкрософт прагне поліпшити набір параметрів безпеки за замовчуванням. Операційна система (ОС) Windows Server 2012 успадковує удосконалення в цій галузі, що з'явилися в Windows Server 2008, також пропонує нові компоненти забезпечення безпеки.

Розглянемо настройку параметрів безпеки для забезпечення більшого захисту клієнтських комп'ютерів; операційну систему яка налаштована за замовчуванням і яка приєднана до домену Active Directory Domain Services (AD DS); процедури щодо введення в силу приписаних параметрів безпеки, які збільшують захищеність Windows Server 2012.

Тепер, для посилення захисту налаштованої за замовчуванням ОС досить використовувати об'єкти групової політики (GPO). У попередніх розробках Майкрософт передбачалася необхідність імпортувати INI-файли шаблонів безпеки, а також вручну вносити зміни у розділ «Адміністративні шаблони» деяких GPO. Ці файли та шаблони більше не потрібні. Однак, INI-файли шаблонів безпеки все ж таки включено до складу засобу GPOAccelerator з даного набору, і їх можна використовувати для посилення безпеки одиночних комп'ютерів.

Щоб застосувати рекомендовані параметри, необхідно:

– створити потрібну структуру підрозділів (OU);

– за допомогою засобу GPO Accelerator створити потрібні об'єкти GPO;

– за допомогою консолі керування груповою політикою (GPMC) зв'язати і впорядкувати об'єкти GPO.

Об'єкти GPO представляють комбінацію перевірених параметрів, які підвищують безпеку клієнтських комп'ютерів під управлінням Windows 7 у двох наступних середовищах:

- корпоративний клієнт (EC);
- особливі параметри безпеки і обмежена функціональність (SSLF).

2.1 Середа корпоративних клієнтів

Середа корпоративних клієнтів (середа EC) - це домен на основі Active Directory Domain Services (AD DS), а також служби Active Directory Domain Services (AD DS) управляють клієнтськими комп'ютерами з ОС Windows Server 2012. Управління клієнтськими комп'ютерами здійснюється через групову політику, яка застосовується на рівні сайтів, доменів та підрозділів. Групова політика являє централізовану інфраструктуру в рамках Active Directory Domain Services (AD DS), яка дозволяє виконувати зміни на рівні каталогів та управляти настройками користувачів і комп'ютерів, в тому числі безпекою та користувацькими даними. Базова конфігурація середовища EC передбачає підвищену безпеку і рівень функціональності операційної системи і додатків, достатній для більшості підприємств [8].

2.2 Середовища з особливими параметрами безпеки

Базова конфігурація середовища з особливими параметрами безпеки і обмеженою функціональністю (середовища SSLF) передбачає створення високозахищеного середовища на базі комп'ютерів з ОС Windows Server 2012. Важливість забезпечення безпеки в середовищі настільки велика, що допускається значна втрата функціональності і керованості.

При розгортанні параметрів SSLF на клієнтських комп'ютерах зростає кількість звернень до служби підтримки зі скаргами на обмеження у функціональності. Хоча ступінь захищеності даних і мереж в подібному середовищі буде вище, деякі служби не будуть працювати. Наприклад, буде заборонено роботу служб віддаленого робочого столу, які дозволяють інтерактивно підключатися до робочих місць і програмам на віддалених комп'ютерах.

2.3 Особливі параметри безпеки

При використанні комп'ютерних мереж на яких дозволено підключення до зовнішніх ресурсів, наприклад до Інтернету, зростає відповідальність підходу до безпеки проектування систем і мереж, а також параметрами комп'ютерів. Такі переваги, як автоматизація процесів, віддалене адміністрування, віддалений доступ, цілодобова доступність, підключення з будь-якої точки світу і незалежність від кінцевого обладнання забезпечують бізнесу чималі конкурентні переваги, однак, вони ж і збільшують потенційну загрозу [9].

Найчастіше, кроків які здійснює адміністраторами, досить для запобігання несанкціонованого доступу до даних, перебоїв в обслуговуванні та нецільового використання ресурсів. В особливих випадках, наприклад у військових, державних і банківських структурах, потрібно забезпечити окреме ступінь захисту деяких або всіх серверів, систем і даних. Конфігурація SSLF проектувалася саме під ці умови.

2.4 Обмежена функціональність

Особливі параметри безпеки конфігурації SSLF можуть обмежити доступну функціональність. Це відбувається за рахунок того, що користувачам дозволяється виконувати лише вузький набір дій, необхідних для конкретних завдань. Доступ дозволяється тільки до затверджених програм, служб та елементів інфраструктури. Скорочуються і можливості з налаштування, тому що в рамках цієї конфігурації відключається багато сторінок властивостей, які звичні користувачам.

Далі розглянемо області підвищеної безпеки і обмеженої функціональності, що вводиться конфігурацією SSLF, а саме:

- обмеження доступу до служб і даних;
- обмеження доступу в мережу;
- посилений захист мережі.

2.4.1 Обмеження доступу до служб і даних

Дія ряду параметрів конфігурації SSLF полягає в тому, що допустимі користувачі не зможуть отримати доступ до служб і даних, якщо забудуть або невірно введуть пароль. Через це може зрости кількість звернень до служби підтримки, проте, завдяки їм зловмисникам буде складніше провести атаку на комп'ютери під управлінням Windows Server 2012 [10]. Серед даних параметрів можна виділити:

- відключення облікових записів адміністратора;
- більш жорсткі вимоги до паролів;
- більш жорстка політика обмеження прав облікового запису;
- більш жорстка політика для наступних параметрів групи.

2.4.2 Обмеження доступу до мережі

Надійність мережі і можливість встановлювати підключення - необхідна умова успішного бізнесу. Адміністратори не забороняють можливості, необхідні для роботи в мережі. Серед параметрів конфігурації SSLF, які підвищують безпеку мережі, але можуть призвести до відмов у мережевому доступі, можна відзначити:

– обмеження мережевого доступу до клієнтських систем;

– виключення імен комп'ютерів зі списків перегляду;

– контроль над винятками брандмауера Windows;

– засоби забезпечення безпеки підключення, наприклад підписування пакетів.

2.4.3 Посилений захист мережі

Типова атака на мережеві служби - атака відмови в обслуговуванні (DoS). У результаті такої атаки або не вдається підключитися до даних, або відбувається надмірне споживання системних ресурсів і падіння продуктивності. Конфігурація SSLF забезпечує захист доступу до системних об'єктів і механізму розподілу ресурсів, що дозволяє захиститися від цього типу атак. Серед параметрів SSLF, які дозволяють не допустити DoS-атаки, можна відзначити:

– контроль розподілу квот пам'яті для процесів;

– контроль створення об'єктів;

– контроль можливості налагоджувати програми;

– контроль профілювання процесів.

Кожен з пунктів вносить свій внесок у вірогідність того, що параметри безпеки SSLF не дозволять потрібним програмам працювати, а користувачам - звертатися до необхідних служб і даних. З цієї причини дуже важливо провести повномасштабне тестування цих параметрів після їх введення.

2.4.4 Технологія комплексного захисту Hyper–V 3.0

Windows Server 2012 і Hyper-V - фундаментальні будівельні блоки приватної «хмари» Microsoft. Разом з новітньою серверною операційною системою Microsoft поставляється гіпервизор Hyper-V 3.0, в якому відбулися численні зміни. Hyper-V 3.0 може стати першою платформою віртуалізації Microsoft, зі своїми перевагами цілком зіставними з VMware vSphere.

Серед змін Hyper-V - кілька нових функцій, спрямованих на підвищення безпеки. Віртуалізація мережі Network Virtualization - перший крок Microsoft до централізовано-програмованих мереж Software-Defined Networking (SDN). У SDN управління мережевим трафіком покладається на програми, виконувані не так на фізичному обладнанні мережі. В результаті ми отримуємо більш гнучке управління і точну настройку мережі. З точки зору безпеки, завдяки SDN і віртуалізації мережі компанії і постачальники послуг «хмари» можуть надійніше ізолювати віртуальні машини на мережевому рівні.

У Hyper-V 3.0 також реалізовано безліч дрібних, але не менш важливих змін, що відносяться до безпеки. Наприклад, це розширюваний комутатор віртуальної мережі, нова група адміністраторів Hyper-V і вдосконалене шифрування дисків BitLocker.

2.4.5 Віртуалізація мережі

Завдяки віртуалізації мережі можливості ізолювання віртуальних машин розширюються з вузла на мережевий рівень. Ізоляція - необхідна умова багатоабонентських «хмарних» рішень, в яких програми та служби різних компаній або підрозділів розміщуються в одному фізичному сервері та мережевої інфраструктури. Подібно до того, як віртуалізація сервера дає можливість встановити декілька ізольованих віртуальних машин на одному вузлі, віртуалізація мережі Hyper-V 3.0 дозволяє запускати кілька ізольованих віртуальних мереж в одній фізичній мережі. У віртуалізації мережі задіяний програмний рівень абстракції, розташований поверх фізичної мережі і заснований на концепції віртуальних підмереж. Віртуальна підмережа утворює кордон широкомовної передачі пакетів, і тільки віртуальні машини в одному віртуальному підмережі можуть встановлювати зв'язок один з одним. Таким чином, за допомогою віртуальних підмереж адміністратори можуть організувати різні ізольовані домени широкомовної передачі між віртуальними машинами.

2.5 Структура параметрів безпеки

Структура параметрів безпеки являє собою початкову точку для сценаріїв, а також рекомендації щодо усунення проблем. Далі розглянемо базову структура безпеки:

- структура підрозділів політик безпеки;
- структура об'єктів GPO політик безпеки.

2.5.1 Структура підрозділів політик безпеки

Структура безпеки заснована на підрозділах (OU). Підрозділ - це контейнер у рамках домену на основі Active Directory Domain Services (AD DS). Підрозділ може включати в себе користувачів, групи, комп'ютери та інші підрозділи. Якщо один підрозділ містить у собі інші, воно є батьківським. Підрозділ, що міститься в батьківському, називається дочірнім.

До підрозділів можна прив'язати об'єкти GPO, і тоді параметри з цих об'єктів будуть застосовані до користувачів та комп'ютерів, що містяться у такому підрозділі і його дочірніх підрозділах. З метою адміністрування можна делегувати адміністративні повноваження кожному з підрозділів.

Контроль над одним або декількома підрозділами можна делегувати за допомогою майстра делегування в оснащенні Active Directory - користувачі і комп'ютери консолі управління (MMC).

Одне з ключових завдань при проектуванні підрозділів - забезпечити фундамент для безперешкодного впровадження групових політик, які повинні застосовуватися до всіх комп'ютерів в Active Directory Domain Services (AD DS). Завдяки цьому забезпечується відповідність всіх комп'ютерів необхідним стандартам. Крім того, структура підрозділів повинна дозволяти вказувати параметри безпеки для окремих типів користувачів. Наприклад, розробникам може знадобитися рівень доступу, не потрібний звичайним користувачам, а у користувачів переносних ПК можуть бути інші вимоги до безпеки, ніж у користувачів настільних комп'ютерів.

Нижче наведена проста структура підрозділів, яка належить конфігурації ЕС і може не відповідати вимогам конкретного середовища [11].

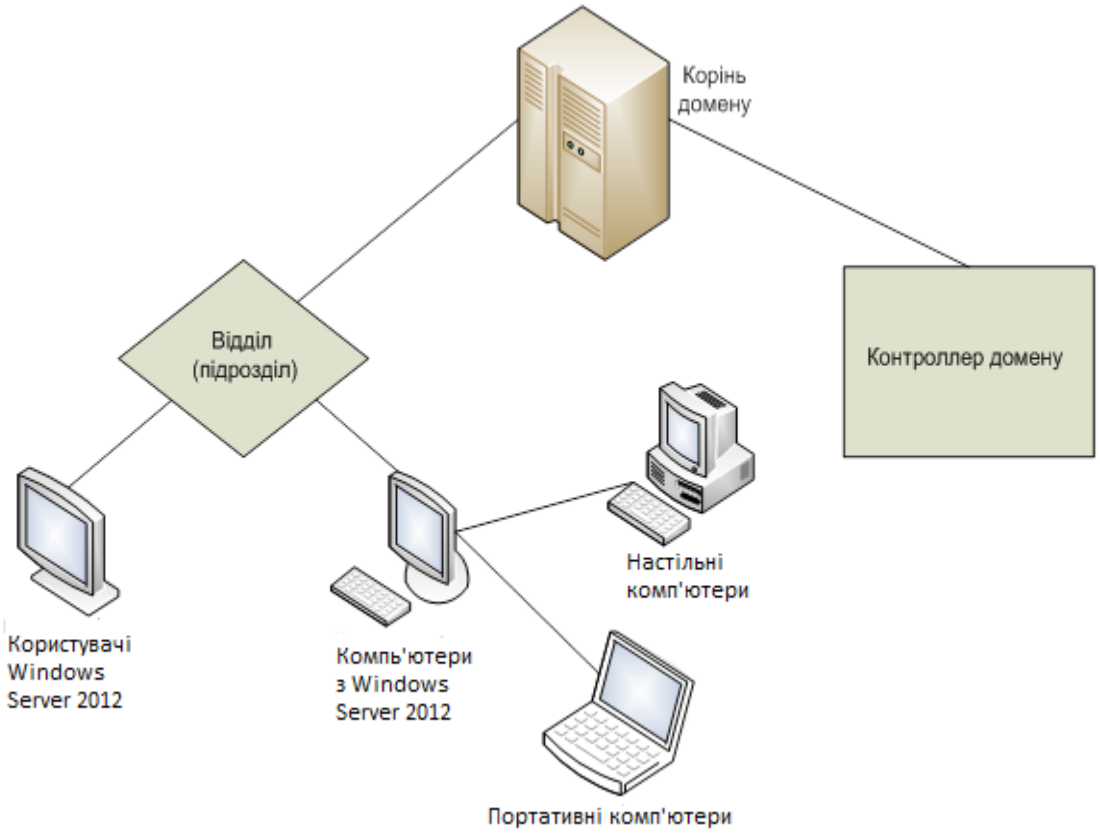


Рисунок 2.1 - Приклад структури підрозділів для комп'ютерів під управлінням Windows Server 2012

Підрозділ «Відділ».

Вимоги до параметрів безпеки в рамках організації часто різні. Тому має сенс створити одну або кілька підрозділів, що представляють відділи. Це дозволить застосовувати потрібні параметри з об'єктів GPO до комп'ютерів і користувачам з конкретних відділів.

Підрозділ «Користувачі Windows Server 2012».

Містяться облікові записи користувачів середовища ЕС.

Підрозділ «Комп'ютери з Windows Server 2012».

Містяться дочірні підрозділи для кожного типу клієнтських комп'ютерів під управлінням Windows Server 2012 в середовищі ЕС, тому при проектуванні структури підрозділів були виділені наступні:

Підрозділ настільних ПК.

Містяться настільні комп'ютери, постійно підключені до мережі.

Підрозділ переносних ПК.

Містяться переносні комп'ютери мобільних користувачів, які не завжди підключені до мережі.

2.5.2 Структура об'єктів GPO політик безпеки

Об'єкт GPO - це набір параметрів групової політики, а саме файлів, створюваних оснащенням «Групова політика». Параметри зберігаються на рівні домену і поширюються на користувачів і комп'ютери, що входять у сайти, домени та підрозділи.

Об'єкти GPO дозволяють ввести в дію потрібні параметри політики, права користувачів і поведінку комп'ютерів на всіх клієнтських комп'ютерах. Використання групової політики замість ручного конфігурування дозволяє вносити зміни і керувати ними відразу для великої кількості комп'ютерів і користувачів.

На рисунку 2.2 розглядається порядок старшинства об'єктів GPO, які застосовані до комп'ютеру, що входить в дочірній підрозділ, починаючи від самого нижчого пріоритету (1) та до вищого (5).

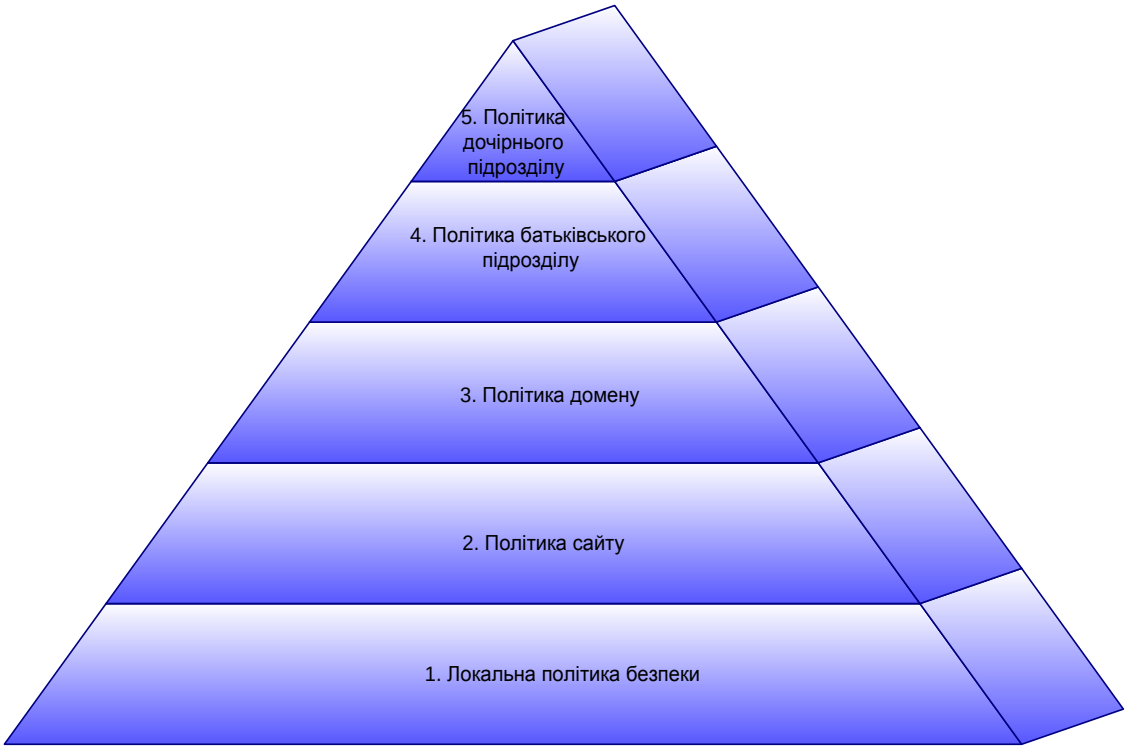


Рисунок 2.2 - Порядок старшинства об'єктів GPO

Спочатку застосовується групова політика, задана локально на кожному з комп'ютерів під управлінням Windows Server 2012. Після цього застосовуються об'єкти GPO рівня сайту, потім рівня домену.

До клієнтських комп'ютерів під управлінням Windows Server 2012, об'єкти GPO застосовуються в напрямку від батьківського підрозділи до самого внутрішнього дочірнього. Останній із застосовуваних об'єктів GPO належить тому підрозділу, до якого безпосередньо входить комп'ютер. Такий порядок обробки - спочатку локальні налаштування, потім параметри сайту, домену, батьківського підрозділи і, нарешті, дочірнього - важливий, оскільки більш пізній об'єкт GPO замінює параметри з більш ранніх. До користувачів об'єкти GPO застосовуються рівно так само.

При проектуванні групової політики необхідно пам'ятати про наступне:

– адміністратор повинен визначити порядок, в якому кілька об'єктів GPO прив'язуються до підрозділу, інакше групова політика буде за замовчуванням вводитися в тому порядку, в якому об'єкти прив'язувалися. Порядок старшинства прив'язаних об'єктів відображається у списку Link

Order (порядок прив'язки) консолі GPMC. Якщо один і той же параметр налаштований в декількох політиках, пріоритет матиме політика, що йде в списку першою;

– об'єкту GPO можна встановити параметр Enforced (примусовий). Проте, в цьому випадку інші об'єкти GPO не зможуть перевизначити параметри, що містяться в такому GPO;

– сайту, домену або підрозділу Active Directory можна призначити параметр Block policy inheritance (блокувати спадкування політики). У цьому випадку будуть проігноровані параметри з об'єктів GPO, розташованих вище за ієрархією Active Directory, якщо тільки вони не відзначені прапором Enforced (примусовий). Іншими словами, параметр Enforced має пріоритет над параметром Block policy inheritance;

– параметри групової політики застосовуються до користувачів і комп'ютерів в залежності від положення цих об'єктів в ієрархії Active Directory Domain Services (AD DS). У деяких випадках може знадобитися, щоб до об'єктів, що становлять користувачів, політики застосовувалися в залежності від розташування об'єкта, який представляє відповідний комп'ютер. Тоді стане в нагоді режим замикання групової політики, в рамках якого параметри групової політики користувача застосовуються залежно від комп'ютера, з якого користувач виконав вхід.

Рекомендовані об'єкти GPO. Для структури підрозділів потрібно мінімум 4 об'єкти GPO, що представляють такі параметри:

– параметри політики домену;

– параметри політики для підрозділу користувачів Windows Server 2012;

– параметри політики для підрозділу настільних ПК;

– параметри політики для підрозділу переносних ПК.

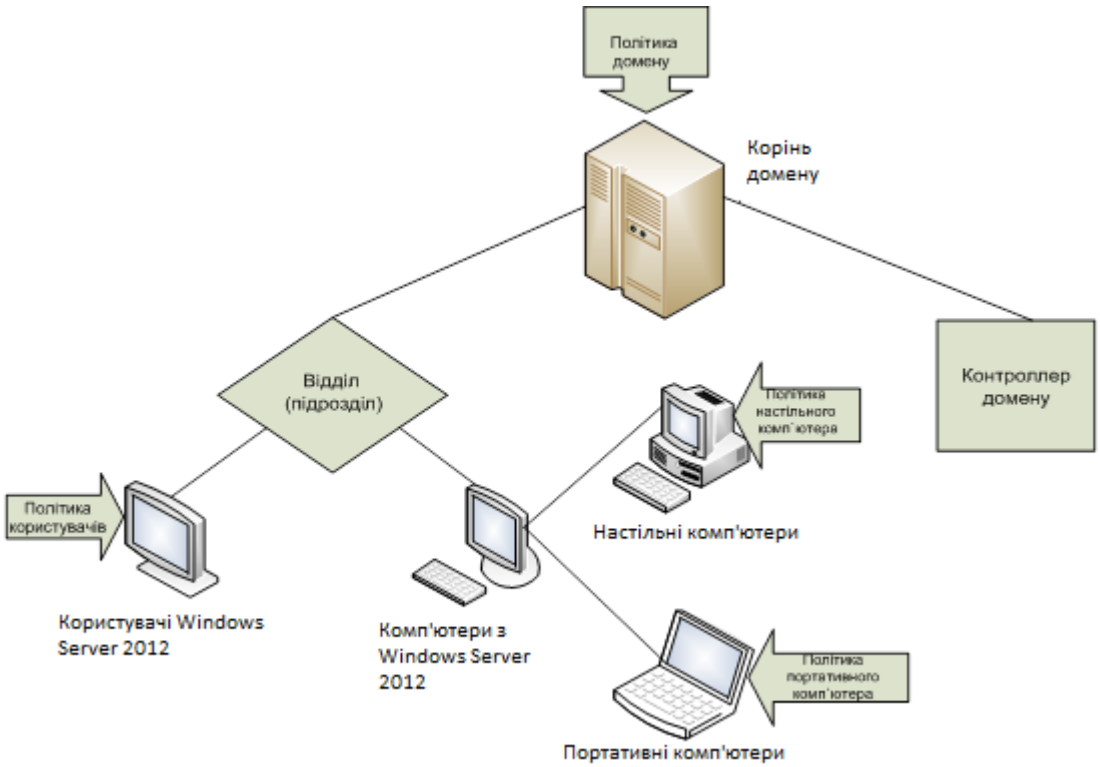


Рисунок 2.3 - Приклад структури підрозділів та об'єктів GPO для комп'ютерів під управлінням Windows Server 2012

У прикладі на рисунку 2.3 переносні комп'ютери входять до підрозділу «Мобільні комп'ютери». У першу чергу в них застосовується їх власна локальна політика безпеки. Оскільки в нашому прикладі тільки один сайт, на рівні сайтів об'єктів GPO немає, так що наступною застосовуваної політикою стає доменний об'єкт GPO і останнім застосовується об'єкт GPO «Політика переносного ПК» [12].

Щоб розібратися з порядком старшинства, розглянемо приклад, в якому параметр Allow logon through Remote Desktop Services (дозволити вхід в систему через служби віддаленого робочого столу) необхідно застосувати до наступного підрозділам і групами користувачів:

– підрозділ комп'ютерів з Windows Server 2012 - група Адміністратори;

– підрозділ переносних ПК - групи Користувачі віддаленого робочого столу і Адміністратори.

У цьому випадку користувач, чий обліковий запис входить до групи Користувачі віддаленого робочого столу, може підключитися до переносного

ПК за допомогою віддаленого робочого столу, оскільки підрозділ переносних ПК є дочірнім по відношенню до підрозділу «Комп'ютери з Windows Server 2012», а параметри дочірнього підрозділу мають більший пріоритет.

Якщо в об'єкті GPO для підрозділу «Комп'ютери з Windows Server 2012» включити параметр політики No Override (не перекривати), підключитися за допомогою віддаленого робочого столу до переносного комп'ютера зможуть тільки учасники групи Адміністратори. Це відбувається тому, що параметр No Override не дозволяє дочірньому підрозділу перевизначити політику, призначену раніше.

3 МОДЕЛЮВАННЯ БЕЗПЕКИ КОРПОРАТИВНОЇ МЕРЕЖІ ЗА ДОПОМОГОЮ ПАРАМЕТРІВ ПОЛІТИКИ ДОМЕНУ

На рівні домену вводиться відносно невелике число параметрів. Вони розташовані у вузлі Server Configuration (конфігурація сервера) редактора об'єктів групової політик. Його підвузол Windows Server Settings (конфігурація Windows Server) містить наступні групи параметрів:

– Password Policy Settings (політика паролів);

– Account Lockout Policy Settings (політика блокування облікового запису) (рис. 3.1).

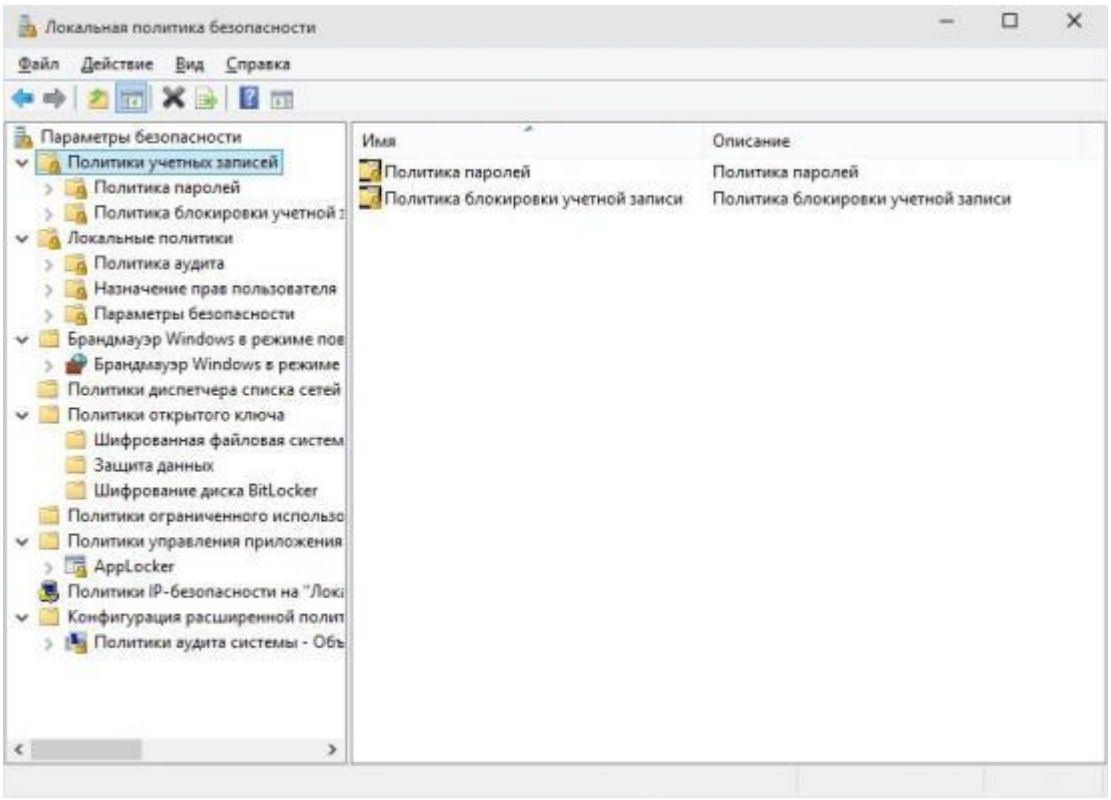


Рисунок 3.1- Політика облікових записів

3.1 Політика паролів

Складні, регулярно змінювані паролі знижують вірогідність успішного підбору пароля. Політика паролів контролює складність і термін використання кожного пароля. Її параметри задаються груповою політикою на рівні домену.

Параметри політики паролів в редакторі GPO розташовані за наступним шляхом.

Server Configuration \ Windows Server Settings \ Security Settings \ Account Policies \ Password Policy (Конфігурація сервера \ Конфігурація Windows Server \ Параметри безпеки \ Політики облікових записів \ Політика паролів) (рис. 3.2).

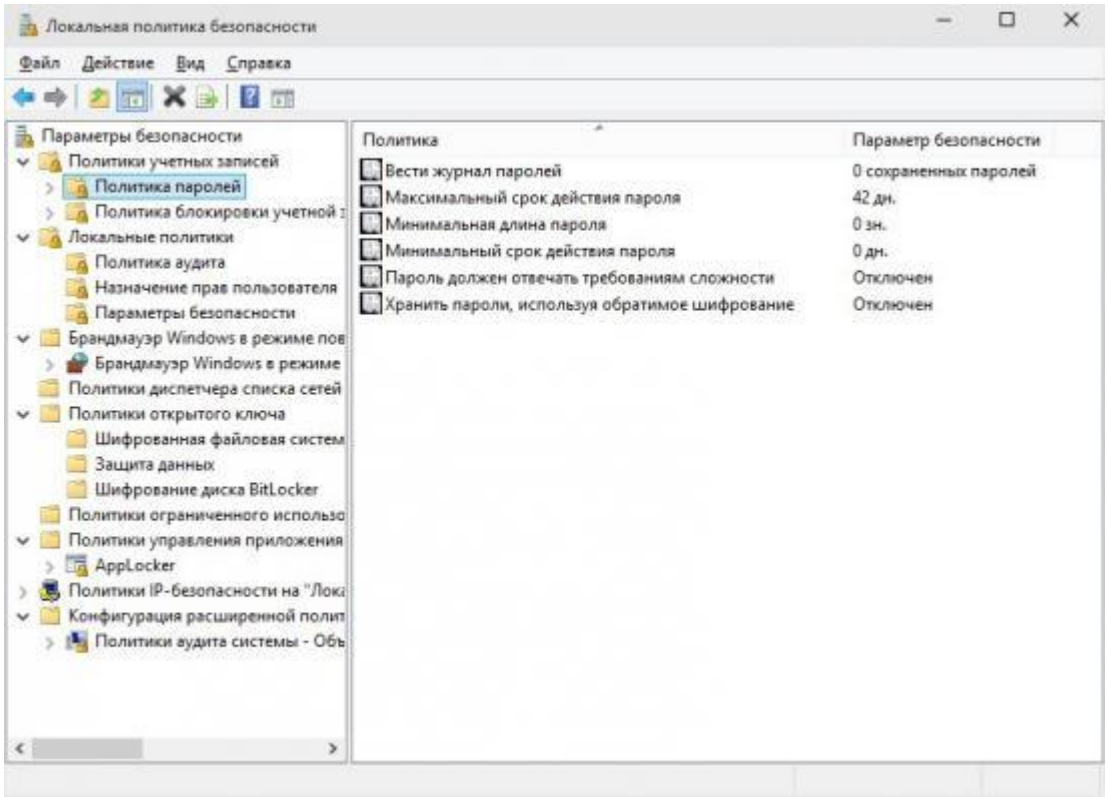


Рисунок 3.2 - Політика паролів

Крім перерахованих політик пароля, в деяких організаціях потрібний централізований контроль усіх користувачів. За допомогою групової

політики можна задати мінімальний і максимальний термін дії пароля. Однак, якщо пароль потрібно міняти надто часто, користувачам вдасться обійти вимоги параметра Enforce password history (вести журнал паролів), якщо він встановлений у вашому середовищі. Або, якщо мінімально дозволена довжина пароля занадто велика, може збільшитися число звернень до служби підтримки з приводу забутого пароля.

Користувачі можуть змінити свій пароль у проміжку між мінімальним і максимальним терміном його дії. Однак, конфігурація SSLF передбачає, що змінювати пароль дозволяється тільки за запитом самої операційної системи, який видається після закінчення його максимального терміну дії у 42 дня. Для досягнення такого ступеня контролю можна відключити кнопку Зміна пароля діалогового вікна Безпека Windows, яке з'являється при натисканні клавіш CTRL + ALT + DEL.

3.2 Політика блокування облікового запису

Ця політика в Active Directory Domain Services (AD DS) відповідає за блокування облікового запису користувача. Користувач буде заблокований і не зможе увійти в систему, якщо протягом певного часу зробить певну кількість невдалих спроб входу. Спроби входу відстежуються контроллерами домену, і їх число порівнюється з числом дозволених. Період, на який блокується обліковий запис, залежить від параметрів політики. Ці параметри дозволяють захиститися від підбору пароля і знижують вірогідність успішної атаки на мережеве середовище. Параметри політики блокування облікового запису у редакторі GPO розташовані за наступним шляхом.

Server Configuration \ Windows Server Settings \ Security Settings \Account Policies \ Account Lockout Policy (Конфігурація сервера \ Конфігурація Windows Server\ Параметри безпеки \ Політики облікових записів \ Політика блокування облікового запису) (рис. 3.3).

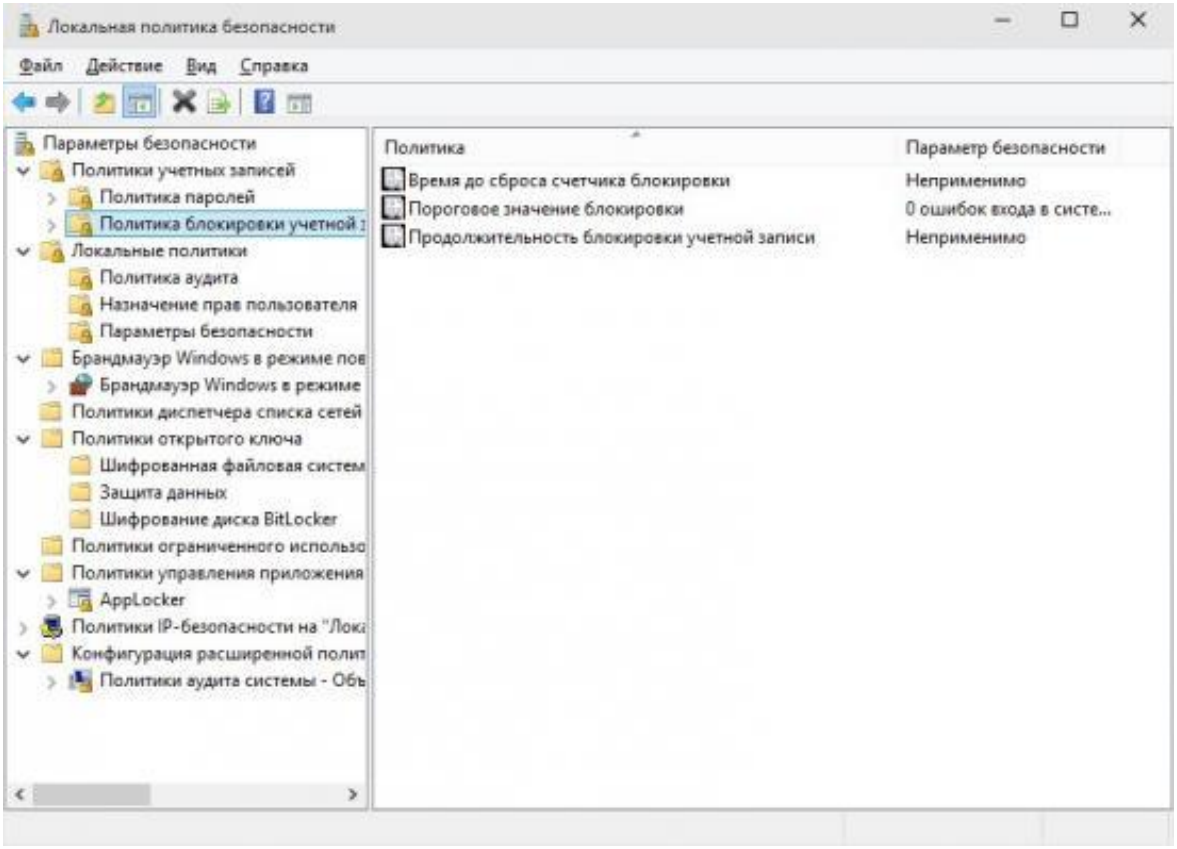


Рисунок 3.3- Політики облікових записів

3.3 Параметри політики комп'ютерів

Параметри безпеки, описані в цьому розділі, застосовуються до настільних і переносних комп'ютерів домену. Вони належать до вузла Server Configuration (конфігурація сервера) редактора об'єктів групової політики і згруповані у дочірні вузли Windows Server Settings (конфігурація Windows Server) і Administrative Templates (адміністративні шаблони).

Розглянемо наступні параметри цих вузлів:

– Audit Policy Settings (політика аудиту);

– User Rights Assignment Settings (призначення прав користувача);

– Security Options Settings (параметри безпеки);

– Event Log Security Settings (параметри безпеки журналів подій);

– Windows Server Firewall with Advanced Security Settings (параметри брандмауера Windows Server у режимі підвищеної безпеки);

– Administrative Templates (адміністративні шаблони).

3.4 Політика аудиту

Політика аудиту визначає ті події, що мають відношення до безпеки, облік яких потрібно вести - так, щоб ряд дій користувача або системи залишав записи в певних категоріях. Можна відстежити, хто звертався до об'єкта, коли користувачі входили в систему і завершували роботу, або які зміни були внесені в параметри політики аудиту. З цих причин схему ведення аудиту рекомендується розробити і впровадити в робочому середовищі.

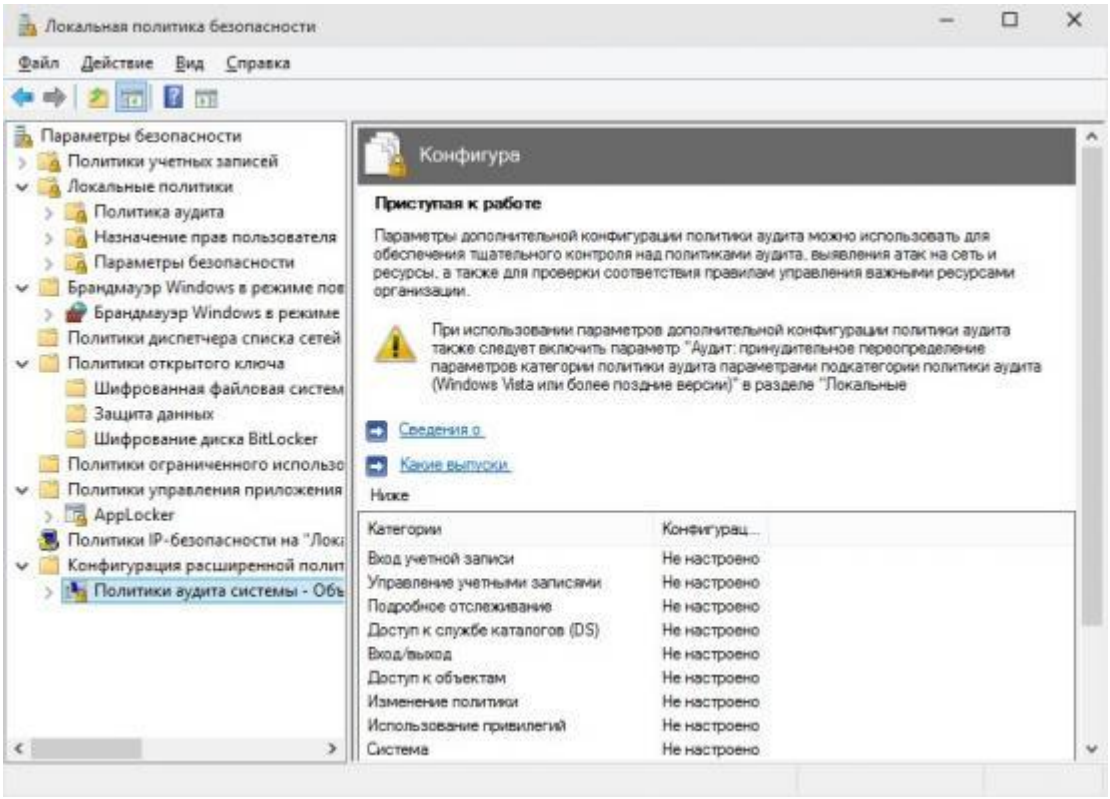


Рисунок 3.4- Конфігурація розширеної політики аудиту

Приступаючи до впровадження політики аудиту, потрібно перш за все встановити, які категорії подій треба відстежувати. В ОС Windows Server 2012 представлено дев'ять категорій політики аудиту, що і в попередніх версіях Windows, плюс одна нова категорія Global Object Access Auditing (аудит доступу до глобальних об'єктів).Account Logon (вхід облікового запису).

Подія генерується за фактом перевірки облікових даних. Воно відбувається на тому комп'ютері, якому належать ці облікові дані. Наприклад, у разі облікового запису домену подія генерується на контролері домену, а в разі локального облікового запису - на локальному комп'ютері. У рамках домену більшість подій цієї категорії буде міститися в журнал безпеки контроллера домену, на якому створені облікові записи.

Account Management (управління обліковими записами). Це категорія допомагає відстежувати спроби створення нових користувачів і груп, їх перейменування, включення або виключення, а також зміну паролів. Аналіз записів цього аудиту дозволяє виявити зловмисні, випадкові або санкціоновані створення облікових записів користувачів і груп.

Detailed Tracking (докладний відстеження). Ця категорія дозволять вести детальне відстежання таких подій, як активація програми, завершення роботи процесу, створення копії дескриптора і непрямий доступ до об'єктів. Включення параметра Audit process tracking (аудит відстеження процесів) призведе до запису великого числа подій, так що звичайне значення цієї політики - No Auditing (немає аудиту).

DS Access (доступ до DS). Ця категорія застосовна тільки до контролерів домену. Тому вона і всі її підкатегорії встановлені в No Auditing (немає аудиту).

Logon / Logoff (події входу і виходу з системи). Ця категорія дозволяє відстежувати події створення та припинення сеансів входу. Події відбуваються на комп'ютері, до якого здійснюється доступ. Так, при інтерактивному вході подія відбудеться на комп'ютері, де здійснено вхід, а

при мережному - на комп'ютері, де розташовані ресурси, до яких проводиться звернення.

Якщо параметру Audit logon events (аудит подій входу в систему) задати значення No auditing (немає аудиту), буде важко встановити, хто саме звертався до будь-яких комп'ютерів або намагався це зробити.

Object Access (доступ до об'єктів). Цей параметр політики не призведе до появи будь-яких подій. Він лише визначає, чи слід вести аудит звернень користувачів до тих об'єктів, наприклад файлів, папок, розділам реєстру або принтерів, для яких зазначене системна таблиця управління доступом (SACL).

Таблиця SACL складається із записів управління доступом (ACE). Кожен запис складається з трьох елементів:

– відстежується учасник безпеки (користувач, комп'ютер або група);

– відслідковують типи доступу, що утворюють маску доступу;

– параметр, який вказує, відстежувати чи тільки невдалі спроби звернень, тільки успішні або обидві категорії.

Якщо задати параметру Audit object access (аудит доступу до об'єктів) значення Success (успіх), запис аудиту буде створюватися кожен раз, коли користувачеві дозволяється доступ до об'єкта, якому привласнена таблиця SACL. Якщо ж поставити значення Failure (відмова), запис буде створюватися кожен раз, коли користувачеві відмовляється у доступі до об'єкту до присвоєної таблицею SACL.

При створенні таблиць SACL слід вносити в них тільки ті дії, які реально потрібно відстежувати. Наприклад, для виконуваних файлів можна включити параметр Write and Append Data auditing (аудит запису і дозапису даних), тому що це дозволить відстежувати зміну або заміну таких файлів, а комп'ютерні віруси впроваджуються у виконувані файли.

Policy Change (зміна політики). Тут можна призначити аудит кожного випадку внесення змін до політики призначення прав користувачів, політики брандмауера Windows, політики довіри чи самі політики аудиту.

Рекомендовані параметри дозволять відслідковувати ситуації, в яких проводиться спроба підвищити рівень своїх привілеїв - наприклад, спроба додати привілеї Debug programs (налагодження програм) або привілеї Back up files and directories (архівування файлів і каталогів).

Privilege Use (використання привілеїв). Ця категорія контролює аудит випадків використання наданих привілеїв. Якщо задати цьому параметру значення Success (успіх), буде створюватися запис аудиту кожного разу, коли користувач успішно користується своїм правом. Якщо задати значення Failure (відмова), запис буде створюватися кожен раз, коли користувачеві не вдається скористатися привілеєм.

System (система). Ця категорія визначає спосіб аудиту системних подій, які завершилися успіхом або невдачею. Аналіз її записів може допомогти у виявленні спроб несанкціонованого доступу до системи. Під системними подіями розуміються запуск і завершення роботи комп'ютерів, переповнення журналів подій і інші події з області безпеки, які впливають на систему цілком.

Global Object Access Auditing (аудит доступу до глобальних об'єктів). Ця категорія дозволяє задати глобальну таблицю управління доступом (SACL) для файлової системи або реєстру комп'ютеру цілком.

В ОС Windows Server 2012 можна зручно контролювати застосування цієї політики аудиту через групову політику за допомогою розділу Advanced Audit Policy Configuration (розширена конфігурація політики аудиту).

3.5 Призначення прав користувача

До готових привілейованих груп ОС Windows Server 2012, можна призначати будь-яким користувачам або групам права, яких у них немає. Щоб задати для права значення No one (ніхто), увімкніть параметр, але не додавайте до нього користувачів та групи. Щоб задати для права значення

Not Defined (не визначено), не вмикайте параметр. Параметри призначення прав користувачів у редакторі GPO операційної системи Windows Server 2012 розташовані за наступним шляхом.

Server Configuration \ Windows Server Settings \ Security Settings \ Local Policies \ User Rights Assignment (Конфігурація сервера \ Конфігурація Windows Server \ Параметри безпеки \ Локальні політики \ Призначення прав користувача) (рис. 3.5).

Параметри безпеки поширювані на комп'ютери під управлінням Windows Server 2012 за допомогою групової політики, дозволяють включати або відключати можливості і компоненти операційної системи, наприклад доступ до приводів компакт-дисків або запит на вхід в систему. Вони також контролюють цифрове підписання даних, імена облікових записів адміністратора і гостя і спосіб установки драйверів. Ці параметри в редакторі GPO розташовані за наступним шляхом.

Server Configuration \ Windows Server Settings \ Security Settings \ Local Policies \ Security Options (Конфігурація сервера \ Конфігурація Windows Server \ Параметри безпеки \ Локальні політики \ Параметри безпеки) (рис. 3.6).

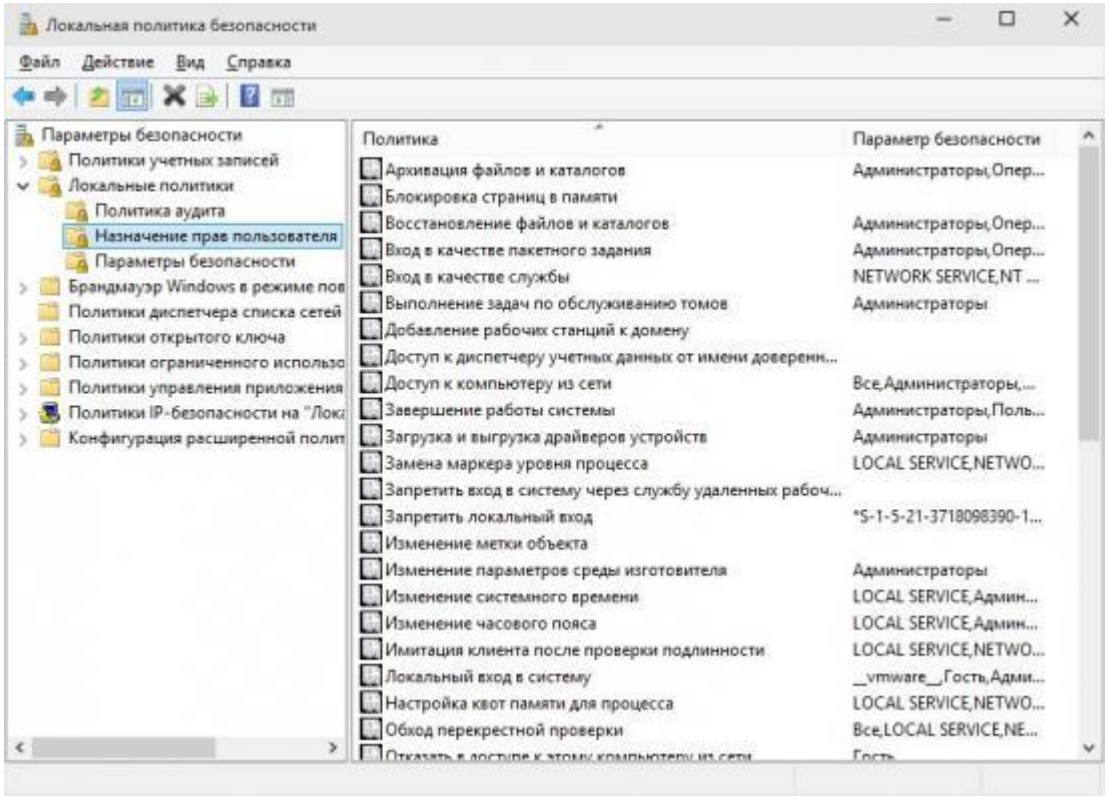


Рисунок 3.5- Призначення прав користувача

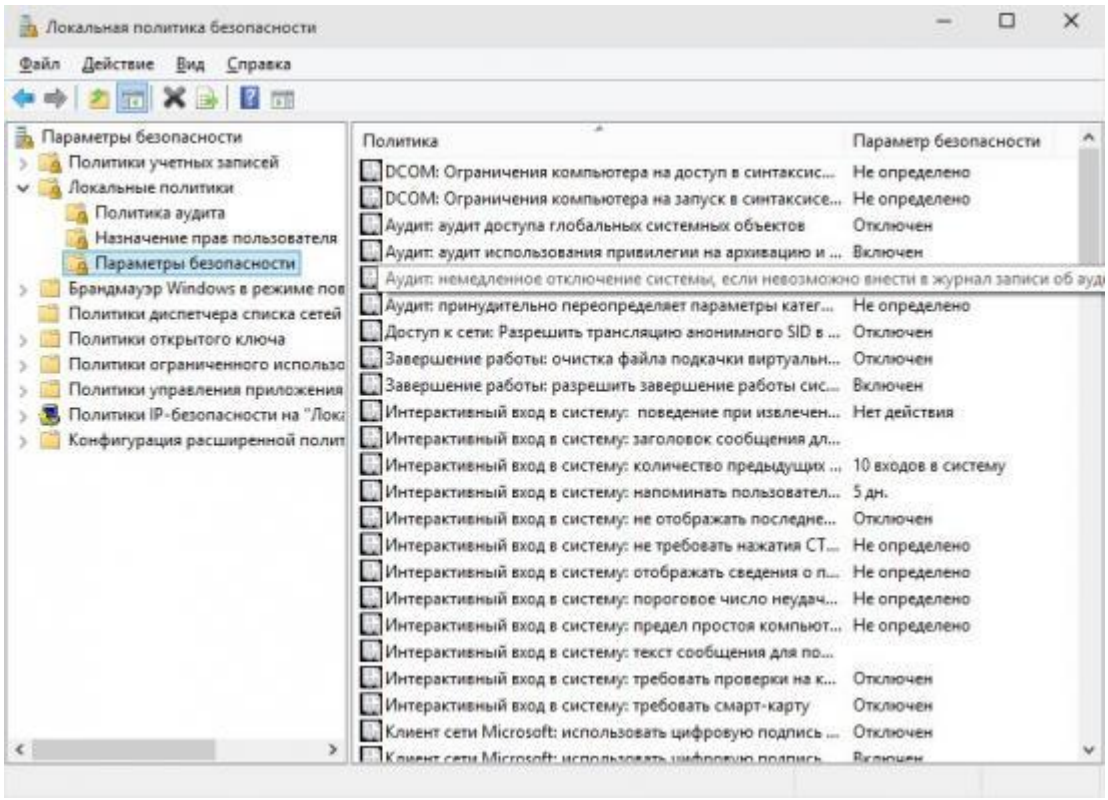


Рисунок 3.6- Параметри безпеки

Параметри які представляють собою записи реєстру та не відображаються в редакторі конфігурацій безпеки (SCE), редакторі групових політик або консолі GPMC відзначені префіксом MSS. Ці параметри включені в ту частину групової політики, де розташовані шаблони безпеки. Якщо відповідна політика видаляється, ці настройки не видаляються разом з нею. Їх потрібно видалити вручну за допомогою редактора реєстру, наприклад Regedt32.exe.

Ці додаткові параметри можна додати в редактор SCE, внісши зміни у файл Sceregvl.inf (знаходиться в папці% windir% \ inf) та повторно зареєструвавши файл Scecli.dll. І оригінальні, і додаткові параметри безпеки розташовані в розділі Local Policies \ Security Options (Локальні політики \ Параметри безпеки). За допомогою редактора SCE можна визначити шаблони безпеки, що застосовуються до окремих комп'ютерів. Шаблони безпеки можуть містити політики пароля, політики блокування, політики протоколу Kerberos, політики аудиту, параметри журналів подій, значення записів реєстру, режими запуску служб, дозволи для служб, права користувачів, обмеження на участь в групах, дозволи на розділи реєстру та дозволу на файлову систему. Редактор SCE можна знайти у багатьох оснащеннях MMC і засобах адміністрування, у тому числі оснащення шаблонів безпеки, оснащенні аналізу і настройки безпеки, редакторі групової політики, параметрах локальної безпеки, політики безпеки домену та контролера домену.

Якщо політики підписування блоків повідомлень сервера (SMB) включені, то при спробі клієнта SMB версії 1 почати на сервері негостьові або неанонімні сеанси сервера дозволяється використовувати підписи безпеки. Наступні сеанси успадковують вже встановлений ланцюжок підписів.

Проблемною є ситуація, коли на контролері домену під керуванням Windows Server 2012 включені наступні політики:

– Computer Configuration \ Windows Settings \ Security Settings \ Local Policies \ Security Options \ Microsoft network server: Digitally sign

communications (always) (Конфігурація сервера \ Конфігурація Windows Server \ Параметри безпеки \ Локальні політики \ Параметри безпеки \ Сервер мережі Microsoft: використовувати цифровий підпис (завжди) (рис.3.7);

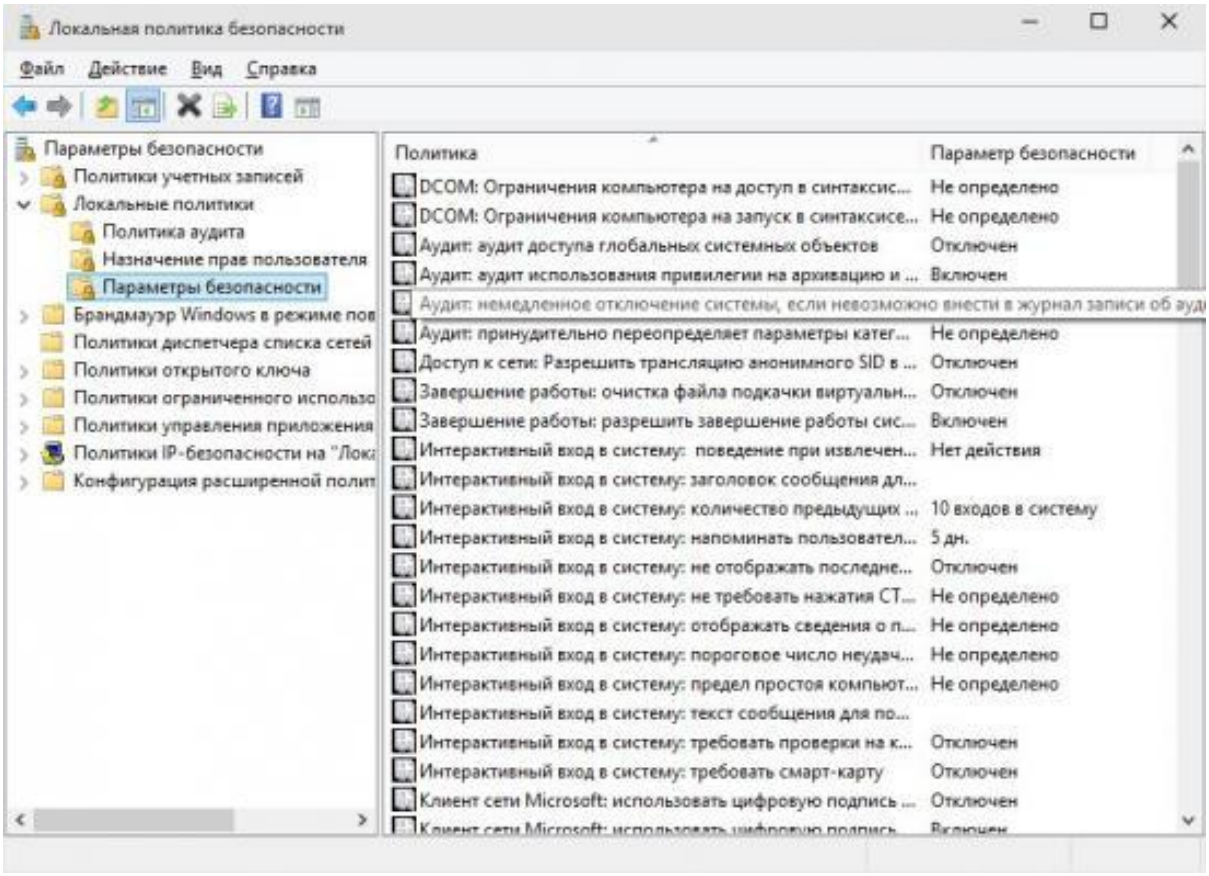


Рисунок 3.7- Параметри безпеки

– Server Configuration \ Windows Server Settings \ Security Settings \ Local Policies \ Security Options \ Microsoft network server: Digitally sign communications (if client agrees) (Конфігурація сервера \ Конфігурація Windows Server \ Параметри безпеки \ Локальні політики \ Параметри безпеки \ Сервер мережі Microsoft: використовувати цифрову підпис (за згодою клієнта) (рис. 3.8).

У розділ «Локальні політики» (Локальные политики або Local Policies) входить вузол «Параметри безпеки» (Security Options). Він надає 60 додаткових параметрів безпеки, об'єднаних у наступні категорії: аудит, доступ до мережі, завершення роботи, інтерактивний вхід у систему, клієнт мережі Microsoft, консоль відновлення, контролер домена, сервер мережі

Microsoft, мережна безпека, мережний доступ, системна криптографія, системні об'єкти, пристрої, облікові записи і член домена.

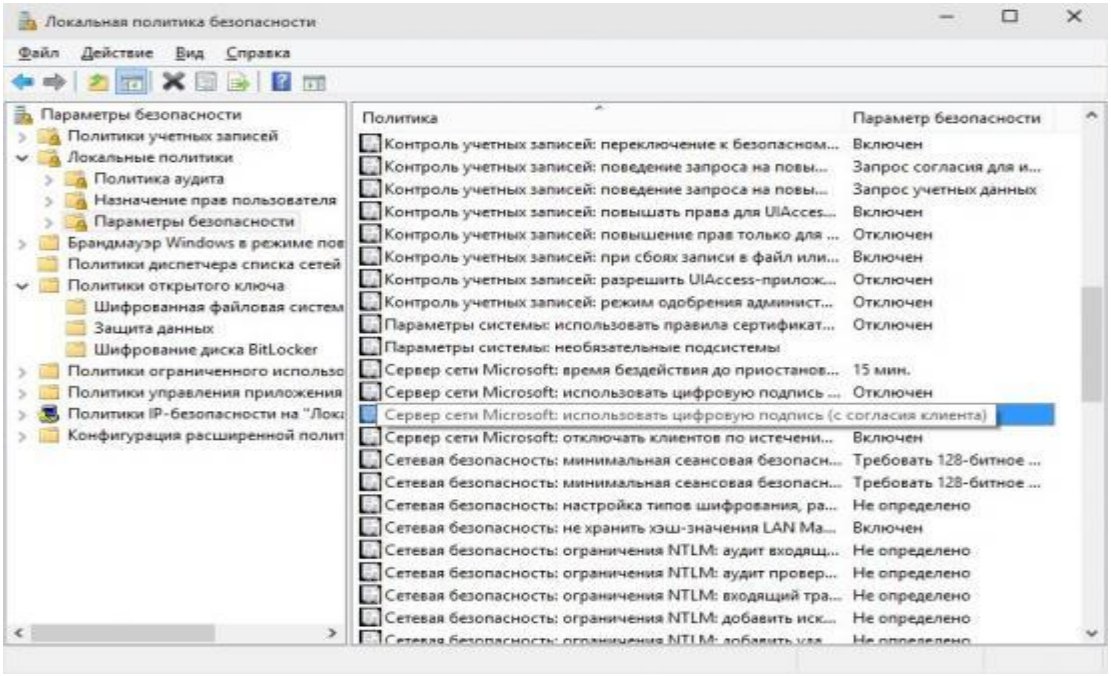


Рисунок 3.8 - Використання цифрового запису (із згоди клієнта)

При цьому в тому ж домені на клієнтських комп'ютерах під управлінням ОС Windows Vista з пакетом оновлень 1 (SP1) або Windows Server 2008 містить такі політики:

– Server Configuration \ Windows Server Settings \ Security Settings \ Local Policies \ Security Options \ Microsoft network client: Digitally sign communications (always) (Конфігурація сервера \ Конфігурація Windows Server \ Параметри безпеки \ Локальні політики \ Параметри безпеки \ Клієнт мережі Microsoft: використовувати цифровий підпис (завжди) (рис. 3.9);

– Електронний цифровий підпис (ЕЦП) — вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

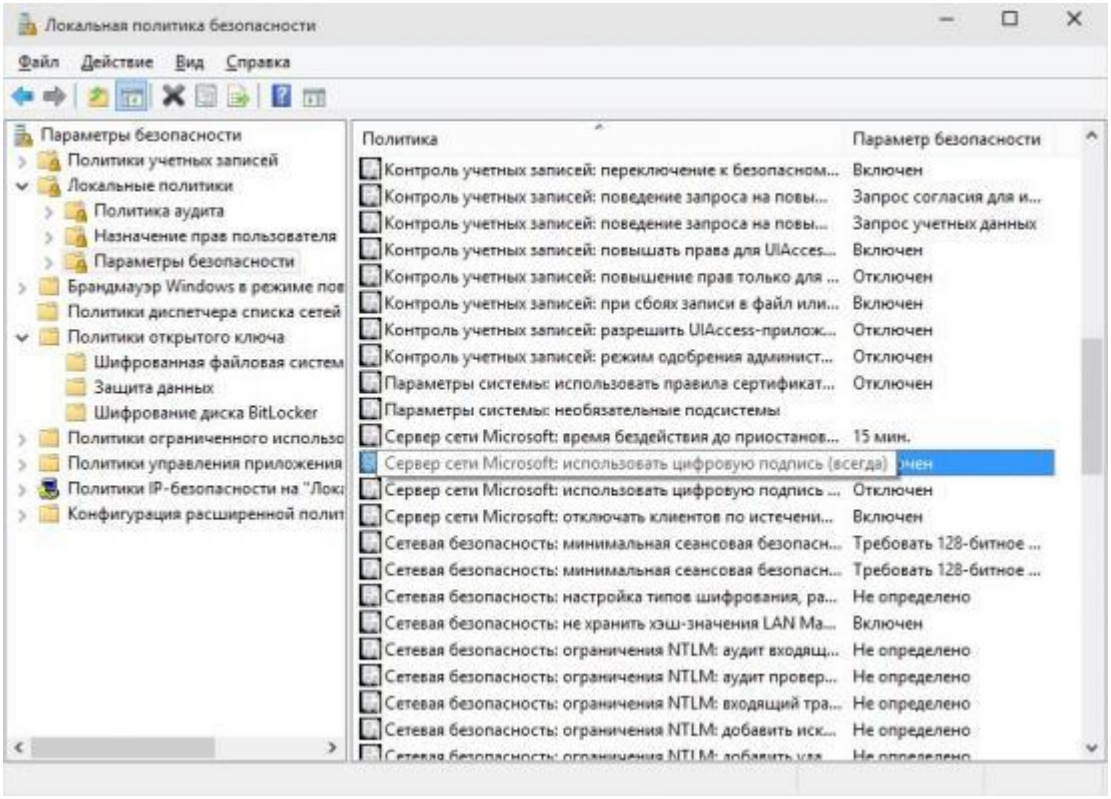


Рисунок 3.9 - Використання цифрового запису (завжди)

Перевірка справжності диспетчера мережі NT (NT LAN Manager, NTLM) використовується багатьма корпоративними мережами незважаючи на те, що у Windows є більш безпечні протоколи перевірки автентичності. В Windows Server 2012 R2 з'явилися нові політики, з допомогою яких можна встановити, де в мережі використовується перевірка автентичності NTLM, і обмежити її. Перший крок в обмеженні протоколу NTLM - розібратися, які комп'ютери та програми використовують його для перевірки автентичності. Зробити це можна, включивши певні політики безпеки аудиту комп'ютерів під управлінням ОС Windows Server 2012. Аналізуючи журнал подій, можна дізнатися, які програми вдасться налаштувати на використання більш надійного протоколу, а також встановити, які комп'ютери або домени зможуть працювати без протоколу NTLM. Встановити характер використання протоколу NTLM, можна за допомогою параметрів групової політики Windows Server 2012 R2

У журнал подій поміщуються записи про події, що відбуваються в системі, а в журнал безпеки - події аудиту. Розділ групової політики, що

відповідає за журнали, дозволяє контролювати такі параметри журналів як максимальний розмір, права доступу, налаштування і способи забезпечення схоронності.

Брандмауер зі складу Windows Server 2012 по своїй структурі дуже схожий на брандмауер з ОС Windows 10. Контроль за його конфігурацією здійснюється у розділі редактора об'єктів групової політики:

Computer Configuration \ Windows Settings \ Security Settings\ Windows Firewall with Advanced Security (Конфігурація комп'ютера \ Конфігурація Windows \ Параметри безпеки \ Брандмауер Windows в режимі підвищеної безпеки) (рис. 3.11).

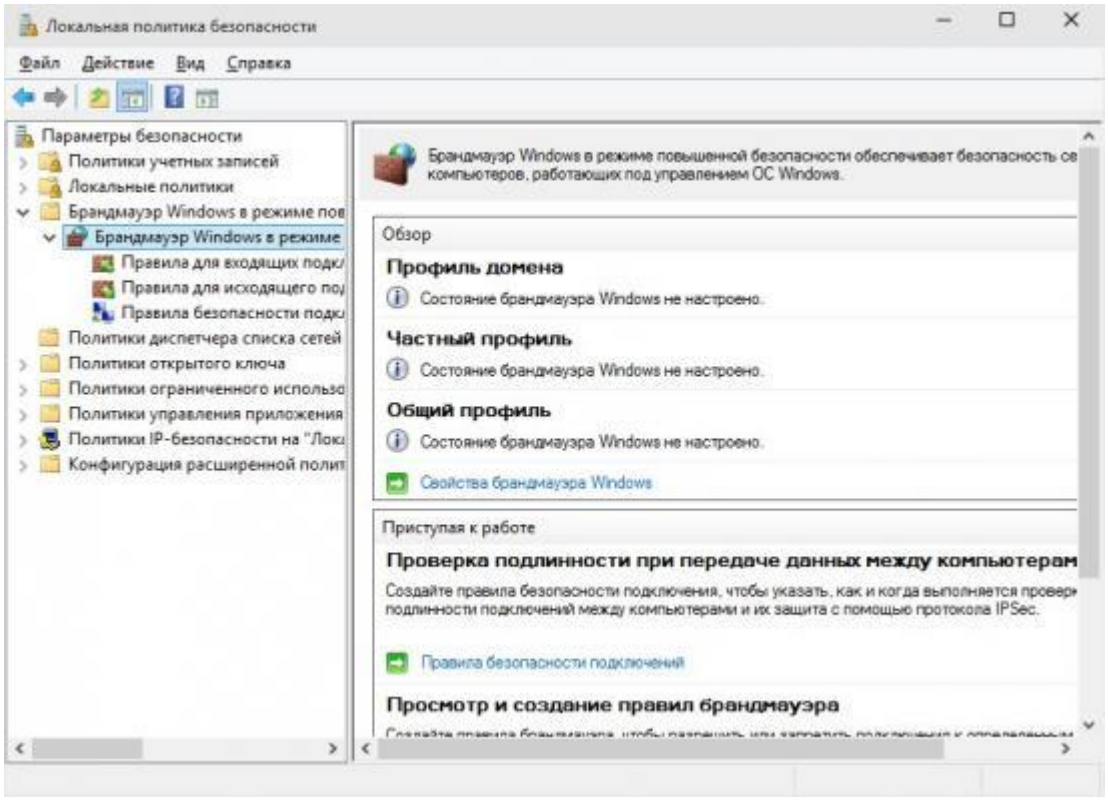


Рисунок 3.10 - Брандмауер Windows в режимі підвищеної безпеки

Для установки цих параметрів треба активувати посилання Windows Firewall Properties (властивості брандмауера Windows), яка знаходиться у розділі «Windows Firewall with Advanced Security» (брандмауер Windows в режимі підвищеної безпеки) редактора об'єктів GPO. У діалоговому вікні Windows Firewall with Advanced Security можна задати параметри доменного,

приватного й загального профілів. Для кожного профілю можна задати загальні налаштування в розділі State (стан), після чого в розділі Settings (налаштування) натиснути кнопку Customize (налаштувати) для їх зміни.

Профіль домену набуває чинності, коли комп'ютер підключається до мережі і проходить перевірку автентичності на контроллері домену, якому належить комп'ютер. Рекомендовані параметри брандмауера в режимі підвищеної безпеки для конфігурації ЕС включають дозвіл на роботу віддаленого робочого столу і віддаленого помічника. У середовищі SSLF всі вхідні комунікації за замовчуванням блокуються, а локальні правила брандмауерів ігноруються комп'ютерами. Щоб змінювати або доповнювати правила, потрібно використовувати редактор об'єктів GPO.

Щоб побачити правила, встановлені для профілю домену, в розділі «Windows Firewall with Advanced Security» редактора об'єктів GPO треба активувати посилання Inbound Rules (правила для вхідних підключень).

Приватний профіль буде використовуватися, тільки якщо користувач з правами локального адміністратора призначить його мережі, раніше використав загальний профіль. Рекомендовані параметри брандмауера в режимі підвищеної безпеки для конфігурації ЕС включають дозвіл на роботу віддаленого робочого столу. Щоб побачити правила, встановлені для приватного профілю, в розділі «Windows Server Firewall with Advanced Security» редактора об'єктів GPO треба активувати посилання Inbound Rules (правила для вхідних підключень).

Загальний профіль за замовчуванням застосовується для комп'ютера, не підключеного до домену. Його параметри повинні накладати найсильніші обмеження, оскільки комп'ютер підключається до публічної мережі, де безпека практично не можна. У конфігураціях ЕС і SSLF всі вхідні підключення за замовчуванням блокуються, і немає правил, які дозволяли б додаткові види комунікацій.

Параметри розділу Windows Server Update контролюють спосіб розповсюдження оновлень і виправлень на комп'ютери з ОС Windows Server 2012. Оновлення завантажуються з веб-сайту Windows Server Update, але з

метою додаткового адміністративного контролю можна вказати веб-сайт інтрамережі, з якого їх слід завантажувати.

Служби оновлення Windows Server Update Services (WSUS) - це інфраструктура, побудована на технологіях Microsoft Windows Server Update і Software Update Services (SUS). Через неї поширюються критичні оновлення Windows, що дозволяють усунути знайдені загрози стабільності в операційних системах Windows.

Служби WSUS усувають необхідність встановлювати оновлення вручну. Замість цього пропонується динамічна система повідомлень на основі інтернет-серверу, що сповіщає про оновлення, що вийшли для систем Windows. Служби Windows Server Server Update Services пропонують такі можливості.

Адміністративний контроль синхронізації вмісту інтрамережі. Служба синхронізації розміщується на сервері і отримує останні критичні оновлення з веб-сайту Windows Server Update. При появі там нових оновлень сервер служб WSUS за заданим розкладом автоматично завантажує їх та поміщує на зберігання.

Внутрішній сервер оновлень Windows Server Update. Цей простий у використанні сервер веде себе як віртуальний сервер Windows Server Update. На ньому розміщені служби синхронізації і засоби адміністрування оновлень. Він обслуговує HTTP-запити на отримання оновлень від клієнтських комп'ютерів. Сервер також може зберігати критичні оновлення, отримані від служби синхронізації, і надавати клієнтським комп'ютерам доступ до них.

Адміністративний контроль оновлень. Перед розгортанням по інтрамережі організації оновлень, отриманих з веб-сайту Windows Server Update, їх можна перевірити і затвердити. Розгортання відбувається за розкладом, заданим адміністратором. Якщо служби WSUS працюють на кількох серверах, можна задати, які комп'ютери до яких серверів будуть звертатися. Це досягається через групову політику в рамках середовища Active Directory або зміною значень реєстру.

Автоматичне оновлення комп'ютерів (робочих станцій і серверів). Компонент автоматичного оновлення Windows можна налаштувати на автоматичну перевірку наявності оновлень, що опубліковані на веб-сайті Windows Server Update. У службах WSUS ця можливість використовується для розгортання оновлень з сервера, розташованого у внутрішній мережі.

У розділі Windows Server Update існує кілька параметрів. ДЛ включення цієї служби, необхідно налаштувати: Configure Automatic Updates (налагодження автоматичного оновлення), No auto-restart for scheduled Automatic Updates installations (не виконувати автоматичне перезавантаження при запланованій автоматичній установці оновлень) і Reschedule Automatic Updates scheduled installations (перенесення запланованої автоматичної установки оновлень) . Використання четвертого параметра, Specify intranet Microsoft server update service location (вказати розміщення служби оновлень в інтрамережі), не обов'язково і залежить від конкретних умов.

4 ОХОРОНА ПРАЦІ

Основним завданням для безпечного навчання є розробка технічних, санітарно-гігієнічних і організаційних заходів, спрямованих на усунення причин виробничого травматизму, професійної захворюваності, підвищення продуктивності праці, на зниження дії на довкілля.

На робочому місці користувача ПК виникають небезпечні та шкідливі фактори: підвищений рівень шуму, несприятливі мікрокліматичні умови, недостатній рівень освітленості, шкідливі речовини, підвищений рівень електромагнітних випромінювань радіочастот, висока напруга електричної мережі, статична електрика та інші. Робота з ПК супроводжується також підвищеним ступенем напруженості трудового процесу. До хімічно небезпечних факторів, що постійно діють на користувача ПК, відноситься виникнення активних часток у результаті іонізації повітря при роботі комп'ютера. Біологічні шкідливі виробничі фактори в даному приміщенні відсутні. Неправильна організація робочого місця сприяє загальній і локальній напрузі м'язів шиї, тулуба, верхніх кінцівок, скривленню хребта й розвитку остеохондрозу.

4.1 Опис приміщення

Для комп’ютерної лабораторії вибране приміщення з наступними геометричними параметрами: ширина – 4 м, довжина – 6.25 м, площа – 25м2 , висота стелі – 3,2 м. Будівля та приміщення спорудженні згідно з вимогами [1]. Приміщення комп’ютерної лабораторії обладнане чотирма робочими місцями для програмістів. Об'єм виробничого приміщення для програмістів, операторів відео термінальних пристроїв на одного працівника складає 19,5 м3 , площа приміщень — 6 м2 з урахуванням максимального числа

працівників в одну зміну. План комп'ютерної лабораторії зображений на рис. 4.1

Основний виробничий процес полягає в розробці алгоритмів, технічної документації та написанні програмного забезпечення, що потребує використання ЕОМ. В комп'ютерної лабораторії розташовані чотири робочих місця. Всі вони обладнанні ПК з рідкокристалічним дисплеєм, і кожне місце приєднане до локальної мережі. На столі додатково встановлено телефон-факс. Ще в лабораторії знаходиться два БФП. Для освітлення використовується шість світильників. Кожен світильник містить дві люмінесцентні лампи типу ЛБ-40-1. Вікна комп'ютерної лабораторії є досить старими. В приміщенні відсутня спеціальна вентиляція і звукоізоляція. Все обладнання, яке розташовано в комп'ютерній лабораторії, підключене до джерела живлення під напругою в 220 В.

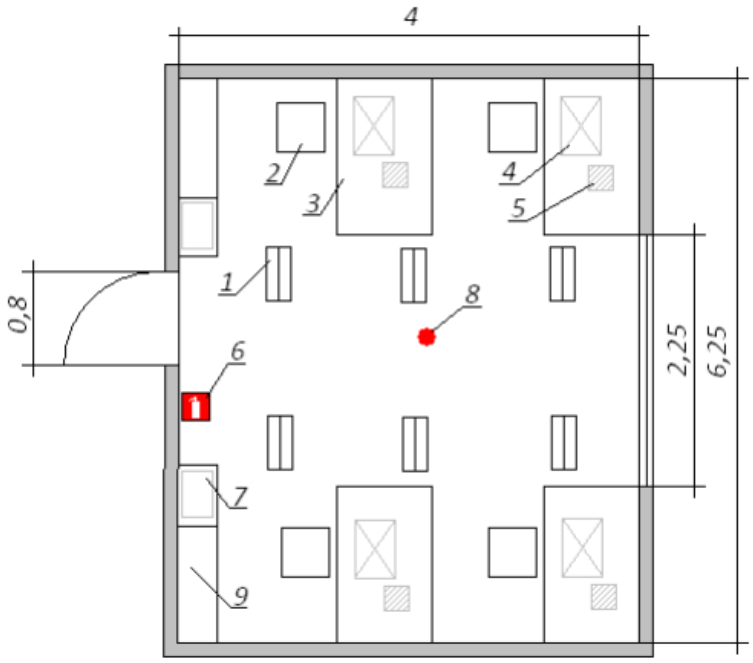


Рисунок 4.1 – План комп'ютерній лабораторії: 1 – світильник; 2 – стілець; 3 – стіл; 4 – персональний комп'ютер (ПК); 5 – телефон – факс; 6 – вогнегасник; 7 – багатофункціональній пристрій (БФП); 8 – протипожежні датчики; 9 – шафа

4.2 Напруженість праці користувача ПЕОМ

Робота програміста пов’язана з значним зоровим навантаження, що вимагає забезпечення належного освітлення. В даному приміщенні рівень природного освітлення є достатнім, а рівень штучного – понижений. Інженер-програміст працює з ЕОМ та іншим офісним обладнанням, що є джерелом небезпеки ураження електричним струмом. Трудова діяльність програміста пов’язана з постійним перебуванням в приміщенні, тому для комфортних умов праці необхідно створити належний мікроклімат в комп’ютерній лабораторії. Згідно нормативним документам [2] та [3] можна виділити такі шкідливі виробничі чинники, що діють на працівника даної комп’ютерної лабораторії:

1) недостатній рівень штучного освітлення;
2) мікроклімат робочої зони: температура, відносна вологості, швидкість руху повітря;
3) підвищений рівень шуму на робочому місці;
4) небезпечна напруга в електричному ланцюзі;
5) підвищений рівень вібрації.

Далі проведемо аналіз перших трьох шкідливих та небезпечних виробничих чинників, що діють в комп’ютерній лабораторії на програміста. Виконаємо якісний та кількісний аналіз цих чинників. Також, розробимо заходи з охорони праці, для цих трьох шкідливих виробничих чинників, які забезпечують покращення умов праці для програміста в комп’ютерній лабораторії.

4.2.1 Рівень штучного освітлення

Основним документом, який регламентує норми освітленості є [4]. В комп'ютерній лабораторії розташовані шість світильників по дві люмінесцентні лампи ЛБ40-1 в кожному. Джерелом живлення світильників є електрична мережа у 220 В. Фактична величина освітленості даного робочого приміщення становить всього Е=210-220 Лк. Категорія виконуваних робіт програміста відноситься до робіт високої точності з присвоєнням розряду III в. Тому нормативне значення загального освітлення робочого приміщення повинно бути Е = 300-500 Лк. Отже, необхідно вжити заходів для збільшення освітленості приміщення. Освітлення на робочому місці програміста повинно бути таким, щоб працівник міг без напруги зору виконувати свою роботу. Розрахунок освітленості робочого місця зводиться до вибору системи освітлення, визначенню необхідного числа світильників, їхнього типу і розміщення. Відповідно до вибраного розрядом зорових робіт допустиме значення освітленості робочої поверхні приймається Е = 400 лк. Для покращення освітлення комп'ютерній лабораторії будуть використовуватися світлодіодні лампи, а саме LITWELL LED-T8S-120 світловий потік яких Фл=1500лм.

4.2.2 Мікроклімат робочої зони: температура, відносна вологості, швидкість руху повітря

Відповідно до [3] праця програміста за важкістю відноситься до легкої фізичної роботи категорії Іа. Основним документом, який регламентує норми мікроклімату робочої зони є [5]. Комп'ютери і офісна техніка є джерелом істотних тепловиділень, що може привести до підвищення температури і зниження відносної вогкості в приміщенні. В приміщеннях, де встановлені

комп'ютери, повинні дотримуватися певні параметри мікроклімату. В санітарних нормах встановлені величини параметрів мікроклімату, що створюють комфортні умови. (див. табл. 4.1). Значення параметрів оптимальних та допустимих параметрів мікроклімату згідно з [5] для приміщень, та фактичних параметрів представленні в таблиці 4.1 .

Таблиця 4.1 – Оптимальні та допустимі параметри мікроклімату

Період року	Параметр мікроклімату	Значення		
		Оптимальне	Допустиме	Фактичне
Холодний	Температура повітря в преміщенні	21,0-23,4°С	23,5-25,4°С	16,1-18,0°С
	Відносна вологість	40-60%	75%	35%
	Швидкість руху повітря	0,1м/с	до 0,1м/с	0,1м/с
Теплий	Температура повітря в приміщенні	21,0-23,4°С	23,5-25,4°С	26,7-27,4°С
	Відносна вологість	40-60%	55%	55%
	Швидкість руху повітря	0,1 м/с	0,2-0,1м/с	0,1м/с

Для забезпечення комфортних умов використовуються як організаційні методи (раціональна організація проведення робіт залежно від пори року і доби, чергування праці і відпочинку), так і технічні засоби (вентиляція, кондиціонування повітря, опалювальна система). Значення фактичної вологості повітря в приміщенні в холодний період - 35%, не потрапляє в діапазон допустимих значень. Отже, в холодну пору року в приміщенні необхідно використовувати зволожувачі повітря, а також для підвищення

температури потрібно встановите додаткове опалення. В теплу пору року для пониження температури потрібно встановити кондиціонер.

4.2.3 Рівень шуму на робочому місці

Підвищений рівень шуму в комп’ютерній лабораторії спричинений чотирма ПК, двома багатофункціональними пристроями, а також гудінням пускового реле світильників. Фактичне значення рівня шуму становить 88-92 дБ, коли допустимий рівень звуку становить ≤ ГДР, а саме 50 дБ. Методи вимірювання шуму та допустимі рівні звукового тиску у октавних смугах частот, еквівалентні рівні звуку на робочому місці регламентовані [6]. Шум погіршує умови праці здійснюючи шкідливу дію на організм людини. Працюючі в умовах тривалої шумової дії випробовують дратівливість, головні болі, запаморочення, зниження пам'яті, підвищену стомлюваність, пониження апетиту, болі у вухах і т.і. Такі порушення в роботі ряду органів і систем організму людини можуть викликати негативні зміни в емоційному стані людини аж до стресових ситуацій. Під впливом шуму знижується концентрація уваги, порушуються фізіологічні функції, з'являється стомленість у зв'язку з підвищеними енергетичними витратами і нервово-психічною напругою, погіршується мовна комутація. Все це знижує працездатність людини і її продуктивність, якість і безпеку праці. Для пониження рівня шуму необхідна додаткова звукоізоляція. У якості звукоізолюючих матеріалів, які застосовують у конструкціях перекриттів для зниження передачі структурного (ударного) звуку переважно використовують мати та плити із скляного та мінерального волокна, м'які плити з деревних стружок, картон, гуму, утеплений лінолеум, а також заміна вікон на звукоізолюючі.

4.2.4 Розрахунок для покращення рівня штучного освітлення

Для покращення освітлення комп’ютерній лабораторії будуть використовуватися світлодіодні лампи, а саме LITWELL LED-T8S-120 світловий потік яких Фл=1500лм.

Відповідно до вибраного розрядом зорових робіт допустиме значення освітленості робочої поверхні приймається E = 400 лк.

Для розрахунку освітлення КЛ скористаємося методом світлового потоку. Для визначення кількості світильників визначимо світловий потік, що падає на поверхню по формулі 4.1:

$$F = \frac{EkSZ}{\eta} \tag{4.1}$$

де F - світловий потік, Лм;

E - нормована оптимальна освітленість, Лк, E=400 Лк;

S - площа освітлюваного приміщення (у нашому випадку S = 25 м2);

Z - коефіцієнт мінімальної освітленості, характеризує нерівномірність освітлення. Приймається при найвигіднішому розташуванні світильників, коли світловий потік використається для освітлення робочої зони найбільш раціонально, (Z = 1.1);

k - коефіцієнт запасу, що враховує зменшення світлового потоку лампи в результаті забруднення світильників у процесі експлуатації (його значення визначається по таблиці коефіцієнтів запасу для різних приміщень і в нашому випадку k = 1.2);

η - коефіцієнт використання світового потоку від світильника, що показує, яка частина світлового потоку лампи досягає освітлюваної поверхні, у тому числі завдяки відбиттю світлового потоку від стін, стелі й робочої поверхні.

Для визначення коефіцієнта η потрібно розрахувати індекс приміщення i за формулою 4.2:

$$i = \frac{s}{h(A + B)} \tag{4.2}$$

де S - площа приміщення, S = 25 м2;

h - висота підвісу світильників над робочою поверхнею, м;

A - ширина приміщення, A = 4 м;

B - довжина приміщення, B = 6,25 м.

Висота підвісу знаходить за формулою 4.3:

$$h = H - h_{св} - h_p \tag{4.3}$$

де H – геометрична висота КЛ, H=3 м;

$$3{,}2 – 0{,}3 – 0{,}9 = 2м$$

$$i = \frac{25}{2{,}9(4+6{,}25)} = 0{,}84$$

По показнику приміщення та коефіцієнтам світлового потоку від підлоги – 10% (0,1), від стін – 30% (0,3) та від стелі – 50% (0,5) визначаємо для світлодіодної лампи LITWELL LED-T8S-120 значення коефіцієнта використання світлового потоку η= 0,51.

Підставимо всі значення у формулу 4.1 для визначення світлового потоку:

$$F = \frac{400 * 1.2 * 25 * 1.1}{0.51} = 25882Лм$$

Розрахуємо необхідну кількість ламп по формулі 4.4:

$$N = \frac{F}{F_л} \quad (4.4)$$

де N - визначається число ламп;

F - світловий потік, F = 25882 Лм;

Fл- світловий потік лампи, Fл = 1500 Лм.

$$N = \frac{25882}{1500} = 18 \text{ шт.}$$

Отже, для освітлення використаємо 6-ть світильників, кожен світильник комплектується 3-ма лампами. Розміщуються світильники двома рядами, по три в кожному ряду.

Згідно з [4], дане приміщення не відноситься до тих, що потребують аварійного освітлення.

4.3 Ергономіка робочого місця

Проектування робочих місць, забезпечених відео терміналами, відноситься до числа важливих проблем ергономічного проектування в області обчислювальної техніки. Робоче місце і взаємне розташовує всіх його елементів повинне відповідати антропометричним, фізичним і психологічним вимогам. Велике значення має також характер роботи. Зокрема, при організації робочого місця програміста повинні бути дотримані наступні основні умови: оптимальне розміщення устаткування, що входить до складу робочого місця і достатній робочий простір, що дозволяє здійснювати всі необхідні рухи і переміщення. Ергономічними аспектами проектування відео термінальних робочих місць, зокрема, є: висота робочої поверхні, розміри простору для ніг, вимоги до того, що розташовує

документів на робочому місці (наявність і розміри підставки для документів, можливість різного розміщення документів, відстань від очей користувача до екрану, документа, клавіатури і т.і.), характеристики робочого крісла, вимоги до поверхні робочого столу, можливість регулювання елементів робочого місця . Головними елементами робочого місця програміста є стіл і крісло. Основним робочим положенням є положення сидячи. Робоча поза сидячи викликає мінімальне стомлення програміста. Раціональне планування робочого місця передбачає чіткий порядок і постійність розміщення предметів, засобів праці і документації. Те, що потрібне для виконання робіт частіше, розташоване в зоні легкої досяжності робочого простору. Моторне поле – простір робочого місця, в якому можуть здійснюватися рухові дії людини. Максимальна зона досяжності рук - це частина моторного поля робочого місця, обмеженого дугами, описуваними максимально витягнутими руками при 80 русі їх в плечовому суглобі. Оптимальна зона - частина моторного поля робочого місця, обмеженого дугами, описуваними передпліччями при русі в ліктьових суглобах з опорою в точці ліктя і з відносно нерухомим плечем (див. рис 4.2).

Оптимальне розміщення предметів праці і документації в зонах досяжності: 1. Системний блок розміщується в передбаченій ніші столу. 2. Дисплей розміщується в зоні а (в центрі). 3. Сканер в зоні а/б (зліва). 4. Документація: необхідна при роботі – в зоні легкої досяжності долоні – в, а у висувних ящиках столу – література, невживана постійно. 5. Клавіатура – в зоні г/д. 6. «миша» – в зоні в справа. 6. Принтер знаходиться в зоні а (справа). Зони досяжності рук в горизонтальній площині: а – зона максимальної досяжності; б – зона досяжності пальців при витягнутій руці; в – зона легкої досяжності долоні; г – оптимальний простір для грубої ручної роботи; д – оптимальний простір для тонкої ручної роботи.

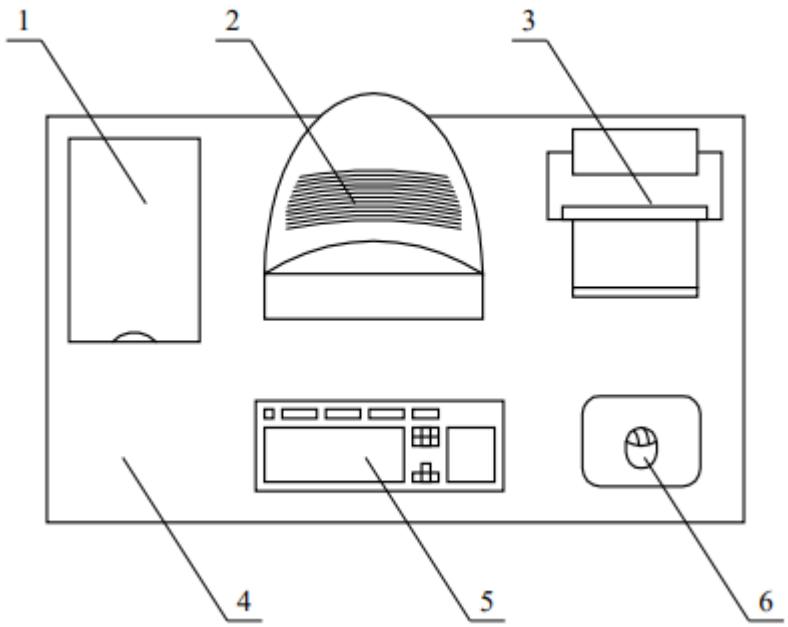


Рисунок 4.2 – Приклад розміщення основних і периферійних складових ПК на робочому столі програміста: 1 – сканер, 2 – монітор, 3 – принтер, 4 – поверхня робочого столу, 5 – клавіатура, 6 – маніпулятор типу «миша».

Для комфортної роботи стіл повинен задовольняти наступним умовам : 1. висота столу повинна бути вибрана з урахуванням можливості сидіти вільно, в зручній позі, при необхідності спираючись на підлокітники; 2. нижня частина столу повинна бути сконструйована так, щоб програміст міг зручно сидіти, не був вимушений підтискати ноги; 3. поверхня столу повинна володіти властивостями, що виключають появу 1 2 3 4 5 6 відблисків в полі зору програміста; 4. конструкція столу повинна передбачати наявність висувних ящиків (не менше 3 для зберігання документації, лістингів, канцелярських обладнань); 5. висота робочої поверхні рекомендується в межах 680-760 мм. Висота поверхні, на яку встановлюється клавіатура, повинна бути біля 650 мм. Велике значення надається характеристикам робочого крісла. Так, висота сидіння над рівнем підлоги, що рекомендується, знаходиться в межах 420-550 мм. Поверхня сидіння м'яка, передній край закруглює, а кут нахилу спинки - регульований. Необхідно передбачати при проектуванні можливість різного розміщення документів: збоку від відео-терміналу, між монітором і клавіатурою і т.п. Крім того, у випадках, коли

відео-термінал має низьку якість зображення, наприклад помітні мигтіння, відстань від очей до екрану роблять більше (біля 700мм), ніж відстань від ока до документа (300-450мм). Взагалі при високій якості зображення на відео-терміналі відстань від очей користувача до екрану, документа і клавіатури може бути рівним. Положення екрану визначається: 1. Відстанню прочитування (0,6 - 0,7 м). 2. Кутом прочитування, напрямом погляду на 20° нижче горизонталі до центру екрану, причому екран перпендикулярний цьому напряму. Повинна також передбачатися можливість регулювання екрану: 1. По висоті +3 см. 2. По нахилу від -10° до +20° щодо вертикалі. 3. В лівому і правом напрямах. Велике значення також надається правильній робочій позі користувача. При незручній робочій позі можуть з'явитися болі в м'язах, суглобах і сухожиллях. Вимоги до робочої пози користувача відеотерміналу наступні: 1. Голова не повинна бути нахилена більш ніж на 20°. 2. Плечі повинні бути розслаблені. 3. Лікті – під кутом 80° - 100°. 4. Передпліччя і долоні рук – в горизонтальному положенні. Причина неправильної пози користувачів обумовлена наступними чинниками: немає хорошої підставки для документів, клавіатура знаходиться дуже високо, а документи - низько, нікуди покласти руки і кисті, недостатній простір для ніг. В цілях подолання вказаних недоліків даються загальні рекомендації: краще пересувна клавіатура; повинні бути передбачені спеціальні пристосування для регулювання висоти столу, клавіатури і екрану, а також підставка для рук. Істотне значення для продуктивної і якісної роботи на комп'ютері мають розміри знаків, густину їх розміщення, контраст і співвідношення яскравості символів і фону екрану. Якщо відстань від очей оператора до екрану дисплея складає 60 - 80 см, то висота знаку повинна бути не менше 3мм, оптимальне співвідношення ширини і висоти знаку складає 3:4, а відстань між знаками – 15.20% їх висоти. Співвідношення яскравості фону екрану і символів – від 1:2 до 1:15. Під час користування комп'ютером медики радять встановлювати монітор на відстані 50-60 см від очей. Фахівці також вважають, що верхня частина відеодисплея повинна бути на рівні очей або трохи нижче. Коли людина дивиться прямо перед

собою, його очі відкриваються ширше, ніж коли він дивиться вниз. За рахунок цього площа огляду значно збільшується, викликаючи обезводнення очей. До того ж якщо екран встановлений високо, а очі широко відкриті, порушується функція моргання. Це значить, що очі не закриваються повністю, не омиваються слізною рідиною, не одержують достатнього зволоження, що приводить до їх швидкої стомлюваності. Створення сприятливих умов праці і правильне естетичне оформлення робочих місць на виробництві має велике значення як для полегшення праці, так і для підвищення її привабливості, що позитивно впливає на продуктивність праці. 1.5 Висновки Аналіз умов праці в розглянутому робочому приміщенні показав, що умови праці з ПЕОМ відповідають вимогам, оскільки площа та об’єм не менше нормативних значень, рівні шуму, вібрації і загазованості не перевищують нормативних обмежень. Запропоновані світлодіодні світильники мають строк служби 50 тисяч годин, що значно краще ніж у люмінесцентних ламп, де строк рівний 10 - 20 тисяч годин, і крім того залежить від кількості переключень. З іншого боку світильники є економічнішими на 44 % (світло-діодна лампа 20 +/- 1 Вт, люмінесцентна 36 +/- 1Вт), більш ударостійкі, не містять токсичних речовин і не мають спеціальних вимог щодо утилізації. Ці лампи створюють оптимальні умови для зорової роботи інженера-програміста, а порівняно невисока температура нагрівання підвищує рівень пожежної безпеки. Значення фактичної вологості повітря в приміщенні в холодний період - 35%, не потрапляє в діапазон допустимих значень. Отже, в холодну пору року в приміщенні необхідно використовувати зволожувачі повітря, а також для підвищення температури потрібно встановите додаткове опалення. Для пониження температури в теплу пору року потрібно встановити кондиціонер.

4.4 Навантаження та напруженість процесу праці

Під час виконання більшості робіт використовують ПК та периферійні пристрої (лазерні та струменеві), що надають навантаження на окремі системи організму. Такі перекоси у напруженні різних систем організму, що трапляються під час роботи з ПК, зокрема, значна напруженість зорового аналізатора і довготривале малорухоме положення перед екраном, не тільки не зменшують загального напруження, а навпаки, призводять до його посилення і появи стресових реакцій. Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м'язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Встановлюють режим праці та відпочинку користувачів ПК, враховуючі психофізіологічну напруженість їхньої праці, динаміку функціонального стану систем організму та працездатності. Раціональний режим праці та відпочинку повинен передбачати запровадження регламентованих перерв, рівномірний розподіл навантажень протягом усього дня праці, регулярні комплекси вправ для очей, рук, хребта, поліпшення мозкового кругообігу та психофізіологічне розвантаження. З метою запобігання перевантаження організму як в цілому, так і окремих його функціональних систем, передусім зорового та рухового аналізаторів, центральної нервової системи, передбачити обмеження загального часу щоденної роботи з ПК.

4.5 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені

питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.5.1 Аналіз небезпечних та шкідливих факторів при виробництві (експлуатації) виробу

Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання НПАОП 0.00-7.15-18 [7] «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями», які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема персональні комп’ютери (ПК) та периферійні пристрої.

Основними робочими характеристиками персонального комп'ютера є наступні:

- робоча напруга U = +220В ± 5%;
- робочий струм I = 2А;
- споживана потужність P = 350 Вт.

Робоче місце має відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [8].

4.5.2 Пожежна безпека

Пожежа — це неконтрольоване горіння, яке супроводжується виділенням тепла, світла, диму та інших продуктів. Горіння виникає за таких трьох умов: наявності окисника, наявності горючої речовини, наявності температури, за якої горюча речовина може самостійно горіти. Якщо немає хоча б однієї із цих умов, горіння стає неможливим. На цьому постулаті ґрунтується переважна більшість профілактичних заходів, спрямованих на відвернення пожеж. Описуючи пожежовибухонебезпечність середовища, зазначають пожежовибухонебезпечні властивості речовин і матеріалів, які використовують під час виконання дипломних (кваліфікаційних) робіт (горючість, верхня та нижня концентраційні границі спалахування, температура спалаху). Приміщення оснащено системою автоматичної пожежної сигналізації, має 1 вогнегасник ВП-5 із зарядом вогнегасної речовини 8-12 кг, відповідно до вимог чинного законодавства України. Проходи до засобів пожежогасіння вільні, не захаращуються та у разі потреби забезпечувати евакуацію всіх людей, які перебувають у приміщенні через один евакуаційний вихід з дверима на шляху евакуації, що відчинятися в напрямку виходу з будівлі від робочого місця. В приміщенні наявна затверджена «План-схема евакуації з кабінету (приміщення)».

Пожежна безпека при застосуванні ЕОМ забезпечується:

1) системою запобігання пожежі,

2) системою протипожежного захисту,

3) організаційно-технічними заходами.

Згідно ДСТУ Б В.1.1-36:2016 [9] таке приміщення, площею 25 м2, відноситься до категорії "В" (пожежонебезпечної) та для протипожежного захисту в ньому проектом передбачено устаткування автоматичною пожежною сигналізацією із застосуванням датчиків-сповіщувачів РІД-1 (сповіщувач димовий ізоляційний) в кількості 1 шт., і застосуванням первинних засобів пожежогасіння.

Горючими матеріалами в приміщенні, де розташовані ЕОМ, є:

1) поліамід – матеріал корпусу мікросхем, горюча речовина, температура самозаймання 420º С,

2) полівінілхлорид – ізоляційний матеріал, горюча речовина, температура запалювання 335º С, температура самозаймання 530º С,

3) склотекстоліт ДЦ – матеріал друкарських плат, важкогорючий матеріал, показник горючості 1.7А, не схильний до температурного самозаймання,

4) пластикат кабельний №.489 – матеріал ізоляції кабелів, горючий матеріал, показник горючості більше 2.1,

5) деревина – будівельний і обробний матеріал, з якого виготовлені меблі, горючий матеріал, показник горючості більше 2.1, температура запалювання 255º С, температура самозаймання 399ºС.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор і ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол.

ВИСНОВКИ

У даній дипломній роботі було проведено аналіз інфраструктури захисту корпоративної мережі на прикладному рівні. Розглянуто базову конфігурацію безпеки корпоративної мережі з використанням ОС Windows Server 2012. Для посилення захисту налаштованої за замовчуванням ОС використані об'єкти групової політики. Розглянуто параметри групової політики ОС Windows Server 2012. Політика паролів контролює складність і термін використання кожного пароля, її параметри задаються груповою політикою на рівні домену. За допомогою групової політики можна задати мінімальний і максимальний термін дії пароля. Користувачі можуть змінити свій пароль у проміжку між мінімальним і максимальним терміном його дії. Політика блокування облікового запису відповідає за блокування облікового запису користувача. Користувач буде заблокований і не зможе увійти в систему, якщо протягом певного часу зробить певну кількість невдалих спроб входу. Спроби входу відстежуються контролерами домену і їх число порівнюється з числом дозволених. Період, на який блокується обліковий запис, залежить від параметрів політики. Ці параметри дозволяють захиститися від підбору пароля і знижують вірогідність успішної атаки на мережу.

Побудовано модель безпеки корпоративної мережі за допомогою параметрів політики домену для забезпечення більшого захисту клієнтських комп'ютерів, операційна система яких налаштована за замовчуванням і які приєднані до домену Active Directory Domain Services.

Необхідно зазначити, що зроблено в результаті проведеної роботи: Виконаний аналіз умов праці, шкідливих та небезпечних чинників, з якими стикається робітник. Визначено параметри і певні характеристики приміщення для роботи над проектом, описаним у кваліфікаційній роботі, описані заходи для того, щоб робоче приміщення відповідало необхідним нормам, було комфортним і безпечним для робітника. Приведені

рекомендації щодо організації робочого місця, а також інформацію щодо пожежної та електробезпеки. Наведена схема, розраховані розміри приміщення та наведені значення температури, вологості й рухливості повітря, необхідна кількість і потужність ламп та інші параметри, значення яких впливає на умови праці робітника, наведені інструкції з охорони праці, техніки безпеки при роботі на комп’ютері.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1) Вито, А. Основы организации сетей Cisco. Том 1. [Текст] / А.Вито. – М.: ИНФРА-М, 2004. – 512 с.

2) Литтлджон, Д. Основы компьютерных сетей [Текст]/ Д. Литтлджон. – М.: Real-book, 2003.– 650 с.

3) Столлингс, В. Современные компьютерные сети [Текст] / В. Столлингс. – СПб.: Питер, 2003. – 783 с. – ISBN 5-94723-327-4.

4) Хелд, Г. Технологии передачи данных [Текст] / Г. Хилд. – СПб.: Питер, 2003. – 720 с. – ISBN 5-94723-472-6.

5) Столлингс, В. Передача данных [Текст] / В. Столлингс. – СПб.: Питер, 2004. – 752 с. – ISBN 5-94723-647-8.

6) Халсалл, Ф. Передача данных, сети компьютеров и взаимосвязь открытых систем. [Текст] / Халсалл Ф. – М.: Радио и связь, 1995. – 408 с. ISBN 5-256-0006002.

7) Куроуз, Дж. Компьютерные сети [Текст] / Дж. Куроуз. – СПб.: Питер, 2004. – 765 с. – ISBN 5-8046-0093-1.

8) Таненбаум, Э. Компьютерные сети [Текст] / Э. Таненбаум. – СПб.: Питер, 2011. – 992 с. – ISBN 978-5-318-00492-6.

9) Кеннеди, К. Принципы коммутации в локальных сетях. [Текст] / К. Кеннеди, К. Гамильтон.- Cisco, 2003. – 976 с. – ISBN 5-8459-0464-1.

10) Оливер, И. Сети и удаленный доступ. Протоколы, проблемы, решения [Текст] / И. Оливер. – ДМК Пресс, 2002. – 336 с. – ISBN 5-94074-080-4.

11) «Будинки і споруди. Будинки адміністративного та побутового призначення». ДБН В.2.2-28:2010. [Електронний ресурс]: ДБН В.2.2-28:2010. Режим доступу: http://document.ua/budinki-i-sporudi.-budinki-administrativnogo-ta-pobutovogo-pnor19583.html. – Дата доступу : 10.04.2015.

12) ССБТ «Небезпечні і шкідливі виробничі фактори. Класифікація». ДСТУ 12.0.003-74*. [Електронний ресурс]: ДСТУ 12.0.003-74*. – М., 1980 –

Режим доступу: http://www.budinfo.org.ua/doc/1810987.jsp. – Дата доступу: 15.04.2015.

13) «Гігієнічна класифікація праці за показниками шкідливості та небезпечності факторів виробничого середовища, важкості та напруженості трудового процесу». Наказ Міністерства охорони здоров'я України 08 квітня 2014 року N 248–. [Електронний ресурс]: – Режим доступу: http://golovbukh.ua/regulations/2340/2592/2593/332659/. – Дата доступу : 20.04.2015.

14) «Державні будівельні норми. Природне та штучне освітлення». ДБН В 2.5.28- 2006. [Електронний ресурс]: ДБН В 2.5.28-2006. – Режим доступу: http://www.info-build.com.ua/normativ/detail.php?ID=45079. – Дата доступу: 25.04.2015

15) «Державні санітарні норми мікроклімату виробничих приміщень». ДСН 3.3.6.042-99. [Електронний ресурс]: ДСН 3.3.6.042-99.– Режим доступу: http://mozdocs.kiev.ua/view.php?id=1972. – Дата доступу: 1.05.2015.

16) «Санітарні норми виробничого шуму, ультразвуку та інфразвуку». ДСН 3.3.6.037-99. [Електронний ресурс]: ДСН 3.3.6.037-99. – Режим доступу : http://document.ua/sanitarni-normi-virobnichogo-shumu-ultrazvuku-ta-infrazvukunor4878.html. – Дата доступу : 7.05.2015

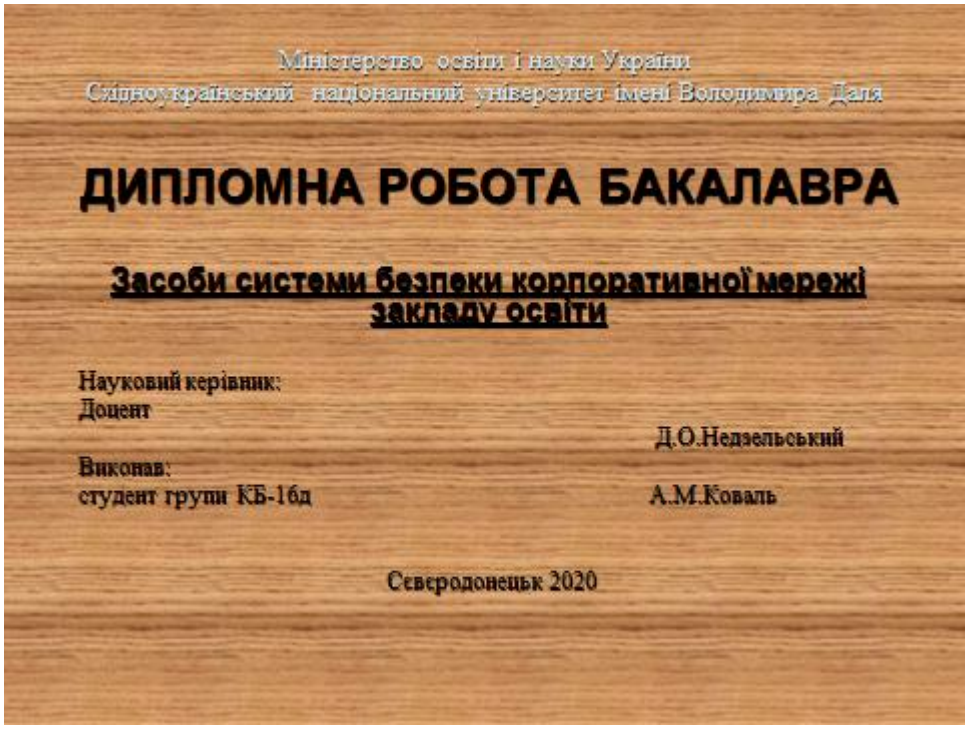
17) НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристро-ями». Зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за № 508/31960. Режим доступу: www. URL: https://zakon.rada.gov.ua/laws/show/z0508-18

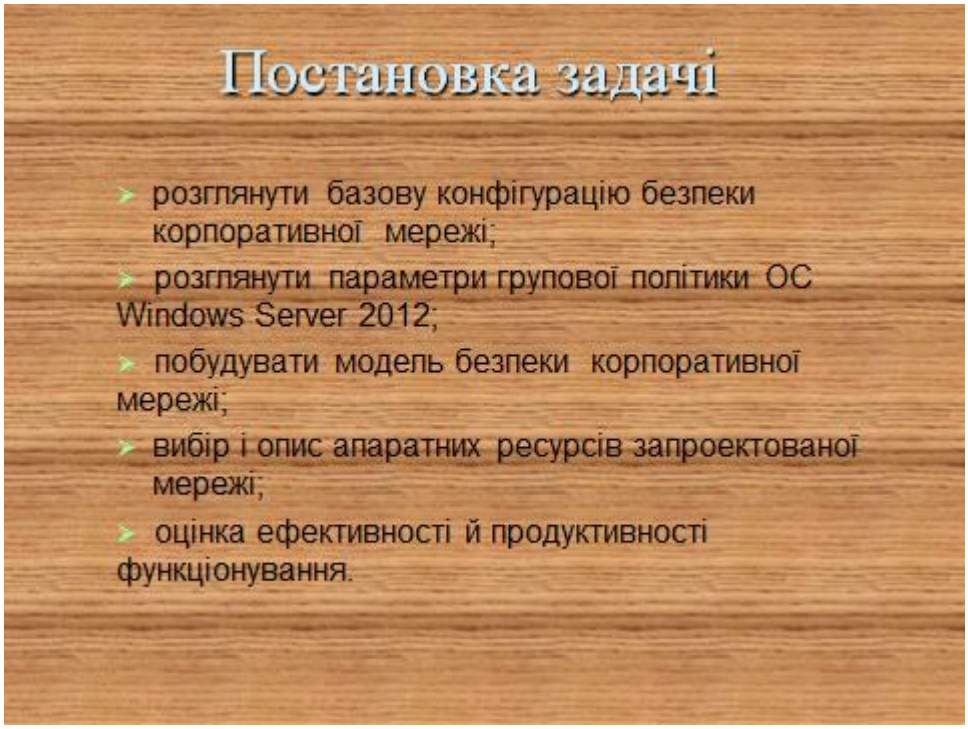
18) Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПІН 3.3.2.007-98. Затверджено Постановою Головного державного санітарного лікаря України 10 грудня 1998 р. N 7. Режим доступу: www. URL: https://zakon.rada.gov.ua/rada/show/v0007282-98

19) ДСТУ Б В.1.1-36:2016 «Визначення категорій приміщень, будинків та зовнішніх установок за вибухопожежною та пожежною небезпекою». Наказ від 15.06.2016 №158. Режим доступу: http://zakon.rada.gov.ua/rada/show/v0158858-16. - – Дата доступу : 15.06.2016

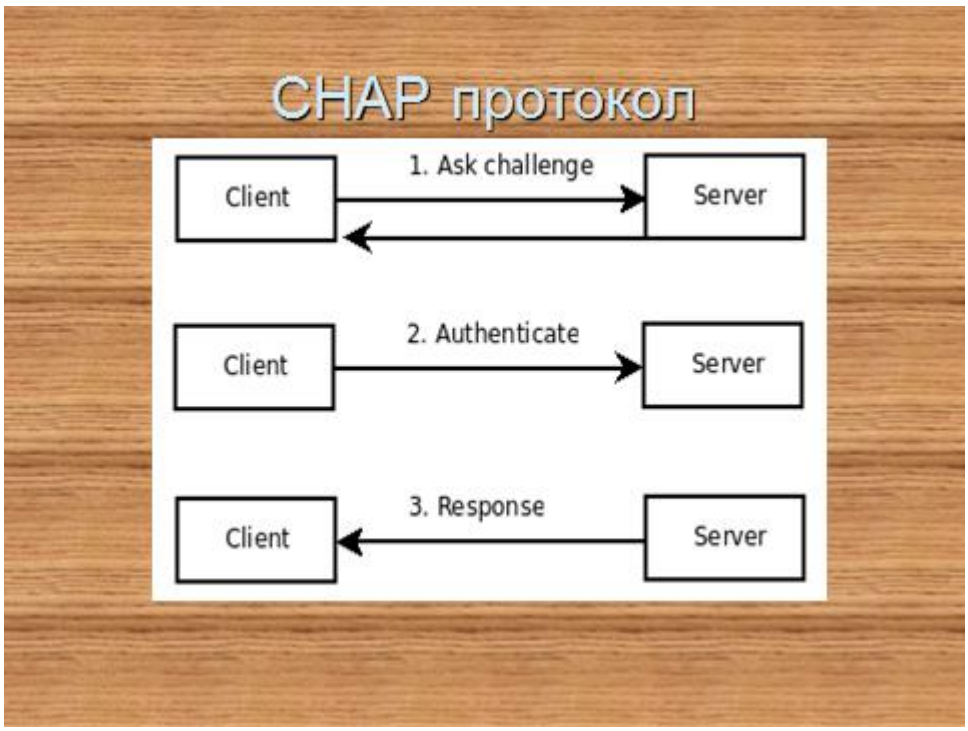
Додаток А

Комп’ютерна презентація





Порядок старшинства об'єктів GPO



Active Directory – універсальна система захисту

active directory («активний каталог», ad) - ldap-сумісна реалізація служби каталогів корпорації microsoft для операційних систем сімейства windows nt. active directory дозволяє адміністраторам використовувати групові політики для забезпечення однаковості настройки користувальницької робочої середовища, розгортати програмне забезпечення на безлічі комп'ютерів через групові політики або за допомогою system center configuration manager (раніше microsoft systems management server), встановлювати оновлення операційної системи, прикладного та серверного програмного забезпечення на всіх комп'ютерах в мережі, використовуючи службу оновлення windows server. active directory зберігає дані і налаштування середовища в централізованій базі даних. мережі active directory можуть бути різного розміру: від декількох десятків до декількох мільйонів об'єктів.

Hyper – V 3.0 система включающая в себя множество технологий

Технологія RSS, за умови, що вона підтримується мережним адаптером хоста, дозволяє обробляти входить мережевий трафік хоста декількома ядрами доступних фізичних процесорів. Однак, трафік усередині ВМ як і раніше обробляється одним віртуальним процесором. У Windows Server 2012 завдяки vRSS з'явилася можливість розподіляти обробку мережевого трафіку по різних віртуальним процесорам ВМ. Це особливо важливо в сценаріях, коли на хості запущено трохи або взагалі одна ВМ, але дуже інтенсивно обробна мережеві потоки. Подібна ситуація характерна, наприклад, для різних шлюзів, спеціалізованих пристроїв на базі Windows Server. Щоб задіяти vRSS, на хості повідомлений бути мережевий адаптер з підтримкою VMQ.

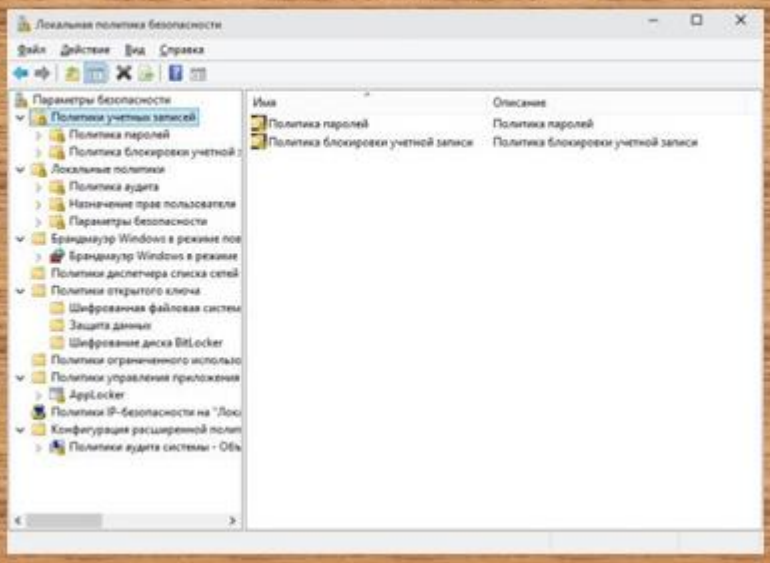
У Windows Server 2012 для кожного порту Hyper-V Extensible Switch можна задати ACL, тим самим дозволивши або заборонивши трафік на конкретний MAC-адресу або IP-адреса, в одну або в обидві сторони. У Windows Server 2012 R2 в налаштуваннях ACL з'явилася можливість додатково вказати протокол, порт, а також задати ознака stateful для, наприклад, розширеного аналізу трафіку.

Віртуалізація мережі

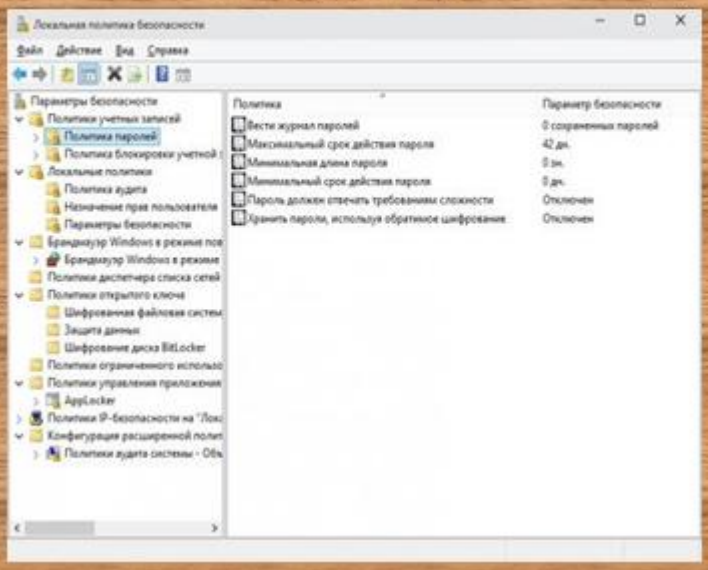
Віртуалізація мережі - це технологія, механізм віртуалізації який дозволяє абстрагуватися від фізичного рівня роботи з мережею до рівня логічного, тобто до рівня програмних софтверних механізмів. Також під виртуализацией розуміється і типова консолідація, але тут вона носить трохи інший характер. Під консолідацією мережі мається на увазі можливість створити кілька, безліч віртуальних мереж поверх загальною телекомунікаційного середовища, простіше кажучи - поверх звичайних мережевих адаптерів. Таким чином можна рознести інфраструктуру поверх дуже великої кількості обладнання. Рішення швидше для провайдерів, ніж для середніх компаній, або для великих компаній з складною гетерогенної інфраструктурою.

Однак віртуальні мережі - це, звичайно, добре - але що на рахунок безпеки? Та й питання масштабованості закритими не назвеш такою технологією. І ось для цього в технологіях віртуалізації мережі є поняття ізоляції - простими словами це механізм, який дозволяє працювати безлічі ізольованих мереж поверх загального фізичного каналу таким чином, що жоден канал не знає про існування один одного і веде себе так, як ніби він працює поверх власного виділеного фізичного каналу. Це дуже важливий момент, оскільки він дозволяє реалізовувати такі нині популярні тренди, як BYOIP (Bring Your Own IP) і BYON (Bring Your Own Network) на практиці. Ці підходи цікаві в першу чергу для провайдерів і є можливість повністю перенести і зберегти всю мережеву адресацію при міграції інфраструктури в хмару на базі System Center 2012 SP1 і Windows Server 2012 SP1, а другий механізм дозволяє також перенести і всю конфігурацію мережі за рахунок її віртуалізації (самої мережі та її компонентів - шлюзів, адрес, віртуальних адаптерів, створення логічних комутаторів і категоризація портів мережних адаптерів за певними параметрами і т.п.).

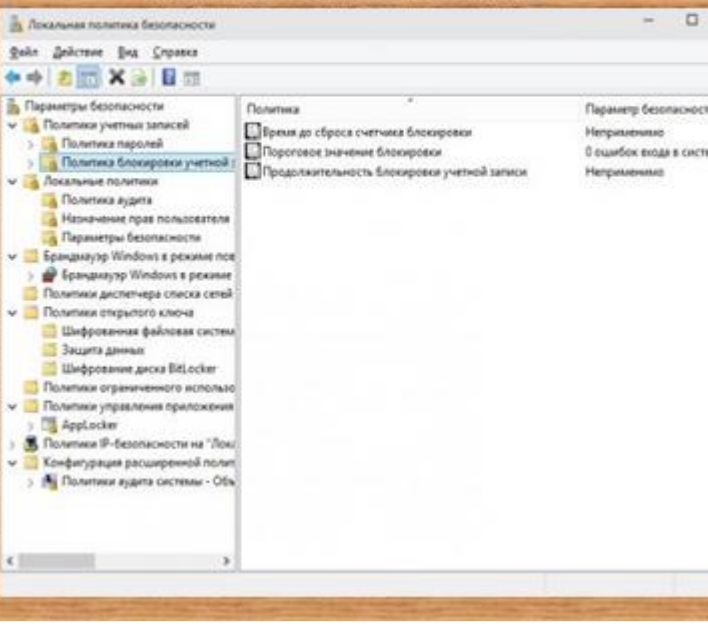
Групова політика облікових записів



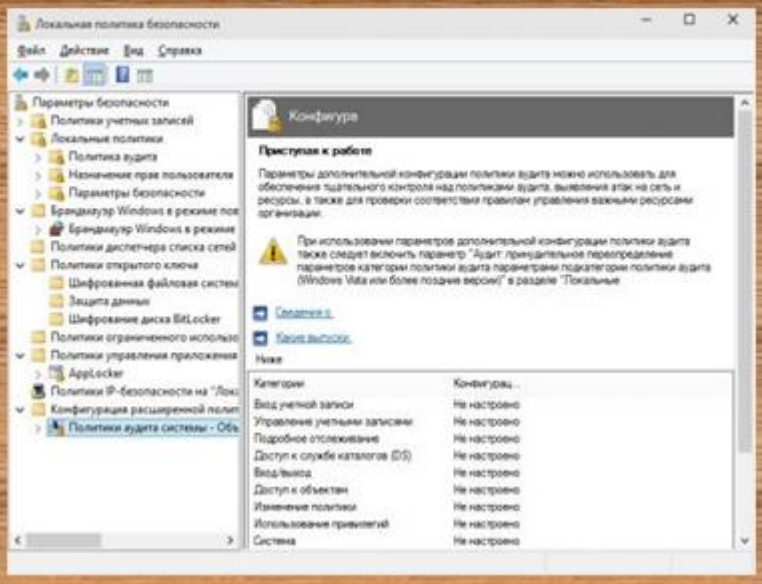
Політика паролів



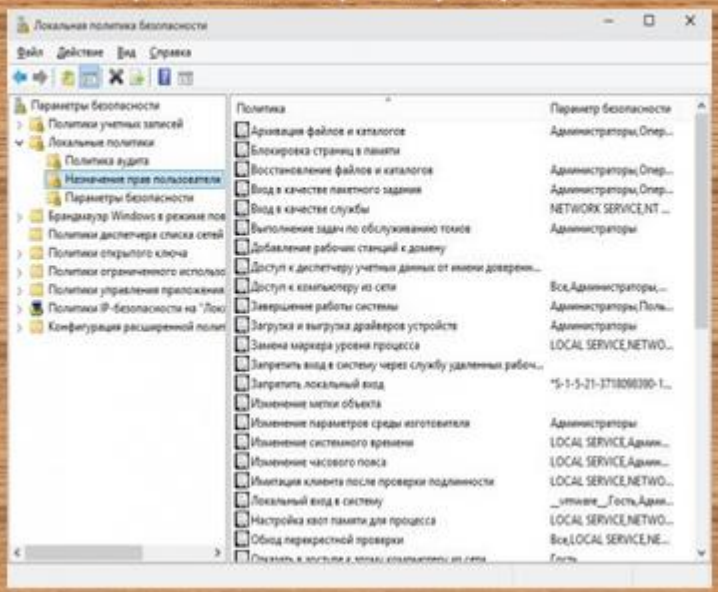
Політики облікових записів



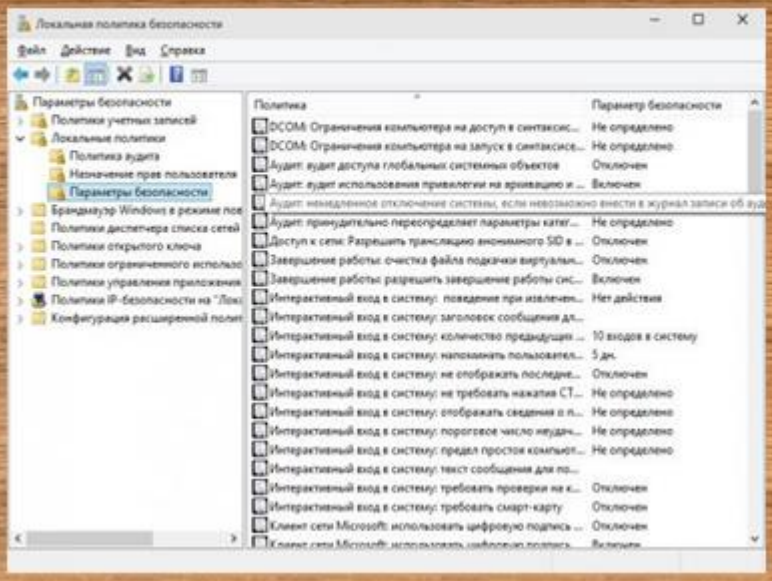
Конфігурація розширеної політики аудиту



Призначення прав користувача



Параметри безпеки



Висновки

У даній дипломній роботі було проведено аналіз інфраструктури захисту корпоративної мережі на прикладному рівні. Розглянуто базову конфігурацію безпеки корпоративної мережі з використанням ОС Windows Server 2012. Для посилення захисту налаштованої за замовчуванням ОС використані об'єкти групової політики. Розглянуто параметри групової політики ОС Windows Server 2012. Політика паролів контролює складність і термін використання кожного пароля, її параметри задаються груповою політикою на рівні домену. За допомогою групової політики можна задати мінімальний і максимальний термін дії пароля. Користувачі можуть змінити свій пароль у проміжку між мінімальним і максимальним терміном його дії. Політика блокування облікового запису відповідає за блокування облікового запису користувача. Користувач буде заблокований і не зможе увійти в систему, якщо протягом певного часу зробить певну кількість невдалих спроб входу. Спроби входу відстежуються контролерами домену і їх число порівнюється з числом дозволених. Період, на який блокується обліковий запис, залежить від параметрів політики.