Міністерство освіти і науки України
Київський університет імені Бориса Грінченка

В. Л. Бурячок, А. О. Аносов, В. В. Семко,
В. Ю. Соколов, П. М. Складанний

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

Підручник

Київ – 2019

БКК 39.973.26-018.2(4Укр)я73
Б 91
УДК 004.7.056.5(477)(075.8)

Рекомендовано вченою радою
Київського університету імені Бориса Грінченка
до друку та використання в навчальному процесі
(протокол №3 від 28.04.2019 року)

Автори:
В. Л. Бурячок, доктор технічних наук, професор
А. О. Аносов, кандидат військових наук, доцент
В. В. Семко, доктор технічних наук, доцент
В. Ю. Соколов, старший викладач
П. М. Складанний, старший викладач

Рецензенти:
О. А. Смірнов, доктор технічних наук, професор
В. В. Бараннік, доктор технічних наук, професор

Б 91 Бурячок В. Л. Технології забезпечення безпеки мережевої інфраструктури. [Підручник] / В. Л. Бурячок, А. О. Аносов, В. В. Семко, В. Ю. Соколов, П. М. Складанний. – К.: КУБГ, 2019. – 218 с.

У підручнику висвітлено основні способи боротьби з уразливостями різних телекомунікаційних технологій, розкрито методи організації захищеної передачі даних у незахищеному середовищі, докладно розглянуто спеціалізоване мережеве обладнання, що застосовується для проектування корпоративних проводових телекомунікаційних систем та мереж, а також для забезпечення (з урахуванням загроз) їх безпеки.

Виклад зорієнтовано на аспірантів та магістрантів вищих навчальних закладів, які навчаються за спеціалізацією «Безпека інформаційно-комунікаційних систем» спеціальності 125 «Кібербезпека» галузі знань 12 «Інформаційні технології».

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DHCP – dynamic host configuration protocol
FTP – file transfer protocol
IP – internet protocol
MAC – media access control
VLAN – virtual local area network

АРМ – автоматизоване робоче місце
АС – автоматизована система
АСУ – автоматизована система управління
БД – база даних
ЕОМ – електронна обчислювальна машина
ЕЦП – електронний цифровий підпис
ЗЛ – зловмисник
ІБ – інформаційна безпека
ІКСМ – інформаційно-комунікаційні системи та мережі
ІС – інформаційна система
ІТС – інформаційно-телекомунікаційна система
КІ – карта ідентифікації
ЛОМ – локальна обчислювальна мережа
МЕ – міжмережевий екран
ОС – операційна система
ПЕОМ – персональна електронна обчислювальна машина
ПЗ – програмне забезпечення
ПК – персональний комп’ютер
РПЗ – руйнуючі програмні засоби
СУБД – система управління базами даних
ТРМ – територіально розподілена мережа
ЦП – центральний процесор

ПЕРЕДМОВА

«Хто володіє інформацією, той володіє світом», – цій цитаті Н. Ротшильда більше двохсот років, однак саме сьогодні її популярність виросла в рази. Зважаючи, що історія розвитку інформаційного суспільства тісно переплетена з інформаційними операціями саме заходи з маніпуляції інформацією, дезінформації конкуруючих сторін та/або введення їх одна одну в оману стали останнім часом невід'ємною частиною внутрішньої й зовнішньої політики переважної більшості держав земної кулі. Головну роль у цих процесах останнім часом відіграє інтернет – п'ята влада світу. Саме інтернет-технології допомагають користувачам швидше, дешевше і ефективніше користуватися всіма перевагами мережевої інфраструктури й саме тому все частіше вислів Н. Ротшильда звучить у новому трактуванні: «Хто володіє інтернетом, той володіє світом». Й це зрозуміло, бо саме вибухове зростання обсягів інформації, до якої завдяки новітнім інтернет-технологіям отримали доступ пересічні громадяни та винайдення потужних комп'ютерів, електронною артерією яких стали сучасні інформаційно-телекомунікаційні (ІТ) системи і мережі – сприяло як глобальній інтелектуалізації та розвитку промисловості, так й суттєво розширило можливості міжнародного бізнесу.

Разом з тим, як відомо, впровадження сучасних інтернет-технологій у всі сфери діяльності світового суспільства призвело й до значної залежності передусім критично-важливих галузей та секторів світової економіки від загроз антропогенного і техногенного характеру, а також природних катаклізмів. Останнім часом кількість державних і комерційних структур, які потерпають від таких дій значно збільшилась. Цьому сприяє «продуктивна робота» дійових осіб інформаційного та кіберпросторів, які, будучи підкріпленими новими можливостями щодо злому веб-сайтів, серверів додатків та баз даних, здатні заподіяти не тільки прямі фінансові збитки, а й паралізувати роботу та привести як до репутаційних втрат, так і до конкурентних переваг критично-важливі об'єкти навіть у розвинутих країнах світу.

Тобто, чим більше ІТ технології розвиваються й інтегруються у наше повсякденне життя, тим більш важливою стає інформаційна безпека (ІБ). Підтвердженням цьому можуть слугувати: статистичні дані, оприлюднені корпорацією WASC (Web Application Security Consortium), згідно яких уразливими до хакерських атак є понад 96,85% веб-сайтів, а також твердження фахівців з ІБ на кшталт міжнародної організації CERT (Computer Emergency Response Team), які вважають, що кількість інцидентів в інфосфері та кількість виявлених уразливостей

кожного року суттєво збільшується. За їх твердженнями та низкою статистичних даних і в прикладному та системному програмному забезпеченні (ПЗ), і в серверних додатках домінують, як видно, уразливості на кшталт відмови в обслуговуванні, компрометації системи та підвищення привілей.

Для унеможливлення впливу таких і ним подібних уразливостей на інфраструктуру країн світу та захисту їх від низки різноманітних загроз нині витрачаються великі кошти. Але, доволі часто буває так, що при цьому, придбавши коштовне антивірусне ПЗ та коштовні апаратні брандмауери, – переважна більшість замовників не отримує майже нічого, окрім теоретичних доказів того, що вкладені кошти роблять їх мережі від хакерських атак більш захищеними.

Щоб вберегтися від зайвих втрат значна кількість світових державних і комерційних структур намагаються будувати нині не тільки ефективну, але і безпечну мережеву інфраструктуру, адміністратор якої повинен розуміти як принципи роботи та взаємодії, так і роль та вплив кожного з компонентів цієї інфраструктури на їх інформаційну захищеність. Одним з можливих способів реалізації цього завдання є така, доволі популярна в усьому світі послуга, як «тестування на проникнення» (тести на подолання системи захисту, penetration testing, pentest). Вона означає санкціоновану спробу обійти існуючий комплекс засобів захисту власних ІТ систем і мереж, яка дозволить: дізнатися можливості здійснення загроз безпеці інформації; оцінити наслідки спрямованої хакерської атаки; визначити уразливості в захисті інформаційної системи; оцінити ефективність засобів захисту інформації; оцінити ефективність менеджменту ІБ; оцінити ймовірний рівень кваліфікації порушника для успішної реалізації атаки; отримати аргументи для обґрунтування подальшого вкладення ресурсів в ІБ й виробити список контрзаходів, щоб знизити можливість реалізації атак.

Зважаючи на те, що технологія pentest не може гарантувати виявлення тестувальником усіх «дірок» в системі безпеки замовника та використання їх тестувальником з метою наживи у майбутньому, – завдання забезпечення безпеки інформаційних систем на об’єктах інформаційної діяльності й, передусім, ІТ систем (мереж) органів влади та критичної інфраструктури (соціальних фондів та різних державних реєстрів), а також об’єктивної оцінки рівня безпеки цих структур повинне вирішуватись комплексно на всіх рівнях мережевої інфраструктури та комп’ютерних ресурсів, які й розглянуто в цьому викладі.

Автори висловлюють щиру подяку професору Хорошко В. О. (Національний авіаційний університет) та професору Рибальському О. В. (Національна академія внутрішніх справ України), зауваження і поради яких дали можливість суттєво покращити цей підручник та уникнути ряду помилок.

ГЛАВА 1.
ОРГАНІЗАЦІЙНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

1.1. Принципи організації безпеки мережевої інфраструктури

Проблема дослідження критичних ситуацій і факторів, які можуть становити певну небезпеку для інформації, а також пошуку і обґрунтування заходів і засобів по її виключенню або зниженню, характеризується наступними особливостями:

– великою кількістю факторів небезпечних ситуацій і необхідністю виявлення джерел і причин їх виникнення;

– необхідністю виявлення і вивчення повного спектру можливих заходів і засобів протидії небезпечним факторам для забезпечення безпеки інформації.

З іншого боку, існує загроза інформації, що захищається. У літературі визначення загрози сформульоване в такий спосіб: «Загроза інформації, що захищається, це є сукупність явищ, факторів і умов, що створюють небезпеку порушення статусу інформації». Тобто загроза інформації обумовлена цілком певними факторами, сукупністю явищ і умов, які можуть виникнути в конкретній ситуації.

Стосовно інформаційної системи усю безліч загроз можна розбити на дві групи: зовнішні та внутрішні, кожна з яких, у свою чергу, ділитися на навмисні та випадкові загрози, які можуть бути явними або прихованими.

Виявлення і аналіз загроз інформації, що захищається, є відповідальним етапом при побудові системи захисту інформації. Більшість фахівців вживають термін «загрози безпеки інформації». Але безпека інформації – це стан захищеності інформації від впливів, що порушують її статус. Отже, безпека інформації означає, що інформація перебуває в такому захищеному вигляді, який здатний протистояти будь-яким дестабілізуючим впливам.

Види та властивості інформації, як предмета захисту

Розглянемо, які види та властивості має інформація, як відображається інформація. Будь-якого виду інформація передається за допомогою повідомлень, що формуються як послідовність знаків та символів або параметрів фізичних процесів, які відображаються на матеріальних носіях: папері, лініях зв’язку, магнітних та оптичних носіях тощо.

За способом відображення, прийнятним для людини, інформація поділяється на такі основні види: звукова, текстова, числова, графічна, комбінована інформація.

Відповідно Закону України «Про інформацію» № 1642-III (1642-14) від 06.04.2000 р. інформацію розмежовують на:

– статистичну – це офіційна документована державна інформація, що дає кількісну характеристику подій і явищ, які відбуваються в економічній, соціальній, культурній та інших галузях життя України;

– масову – привселюдно поширювана друкована й аудіовізуальна інформація;

– державних органів і органів місцевого та регіонального самоврядування – офіційна документована інформація, яка створюється у процесі поточної діяльності законодавчої, виконавчої і судової влади, органів самоврядування;

– інформацію про особу – це сукупність документованих або привселюдно повідомлених відомостей про особу;

– довідково-енциклопедичного характеру – систематизовані, документовані або привселюдно оголошені зведення про суспільне, державне життя і навколишнє природне середовище;

– соціологічну – документовані або привселюдно повідомлені відомості про ставлення окремих громадян і соціальних груп до суспільних подій і явищ, процесів, фактів;

– науково-технічну – документовані чи привселюдно оголошені зведення про вітчизняні та закордонні досягнення науки, техніки, виробництва, отримані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та суспільної діяльності.

В загальному комплексі заходів щодо забезпечення інформаційної безпеки важливе місце займають заходи пов’язані із безпосереднім захистом інформації, що спрямована на реалізацію законних інтересів громадян, юридичних осіб, державних органів та здійснення ними своїх завдань і функцій, від загроз, реалізація яких може нанести політичні, економічні, моральні та інші збитки особі, суспільству або державі. В цьому сенсі інформація поділяється:

Відкрита інформація – інформація, право доступу до якої встановлено правовими нормами і правилами.

Інформація з обмеженим доступом – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами. До інформації з обмеженим доступом належать конфіденційна і таємна інформації.

Конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава, і порядок доступу до якої встановлюється ними.

Таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

Інформація нам потрібна для того, щоб приймати правильні рішення. Вона, як відображення реального (матеріального) світу, повинна мати такі властивості:

1. Об'єктивність інформації. Інформація – це відображення зовнішнього світу, а він існує незалежно від нашої свідомості і бажань. Інформація об'єктивна, якщо вона не залежить, від чиєїсь думки, судження.

2. Достовірність інформації. Інформація є достовірною, якщо вона відображає справжній стан справ. Об'єктивна інформація завжди достовірна, але достовірна інформація може бути як об'єктивною, так і суб'єктивною.

3. Повнота інформації. Інформацію можна назвати повною, якщо її достатньо для розуміння і прийняття рішення. Неповна інформація може привести до помилкового висновку або рішення.

4. Точність інформації визначається ступенем її близькості до реального стану об'єкта, процесу, явища і т. ін. Навіть події, що відбувалися на наших очах, з часом забуваються, і спогади піддаються спотворенню.

5. Актуальність (своєчасність) інформації – важливість, суттєвість для теперішнього часу. Тільки вчасно отримана інформація може принести необхідну користь.

6. Корисність (цінність) інформації. Це ступінь важливості стосовно до потреб конкретних людей.

7. Своєчасність інформації полягає у зменшенні її цінності з часом. Старіє інформацію не сам час, а поява нової інформації, що уточнює, доповнює або відкидає повністю або частково більш ранню.

8. Стислість, компактність – зручна форма представлення, яка полегшує розуміння і засвоєння інформації.

Загалом будь-яку інформацію можна характеризувати з точки зору її об'єктивності, достовірності, повноти, актуальності та корисності, своєчасності та стислості. Захист інформації з обмеженим доступом полягає не лише в захисті засобів обробки інформації, а в організації захисту для підтримки певних властивостей інформації. Такими властивостями є конфіденційність, цілісність та доступність.

Конфіденційність інформації – це властивість інформації бути недоступною для несанкціонованого ознайомлення. Конфіденційність властива лише інформації з обмеженим доступом (позначається в НД ТЗІ – ІзОД). Конфіденційність інформації забезпечується ще режимними заходами та, за потреби, криптографічними засобами.

Цілісність інформації – це властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення. Забезпечення цієї властивості стосується будь-якої інформації важливої для особи, суспільства, держави незалежно від режиму доступу до цієї інформації.

Доступність інформації – це властивість інформації бути захищеною від несанкціонованого блокування. Забезпечення цієї властивості, як і цілісності, стосується усякої інформації важливої для особи, суспільства, держави незалежно від режиму доступу до цієї інформації

Для людино-машинних систем організаційного управління, а саме такими є захищені ІТС, також відзначимо характерні особливості інформації:

– цільове призначення – інформація завжди використовується для досягнення певних цілей;

– способи і формат представлення – найбільш розповсюдженими способами представлення є візуальний та звуковий, формати представлення залежать від конкретних умов та мети обробки інформації;

– надмірність – за наявності можливих помилок необхідна надмірність інформації хоча це і призводить до збільшення її обсягу, часу її обробки і т. ін.;

– швидкодія – швидкість обробки інформації, яка особливо важлива для систем реального часу;

– періодичність – значна частина інформації характеризується періодичністю при її використанні і в процесах її обробки;

– детермінованість або ймовірносні характеристики – інформація завжди є або чітко визначеною (точною чи достовірною) або наближеною;

– витрати – будь-які операції над інформацією завжди супроводжуються певними витратами (час, гроші і т. ін.);

– цінність – будь-яка інформація завжди щось коштує;

– надійність та достовірність – одні з основних властивостей інформації при її практичному використанні;

– статичність та динамічність – інформації завжди притаманні ці фізичні властивості;

– ступінь таємності – як показує життя, завжди існує розподіл інформації за ступенем її таємності.

Як показує аналіз історичних фактів та досвід останніх років, постійно винаходяться нові види і форми обробки інформації. А з іншого боку паралельно винаходяться все нові і нові види і форми її захисту. Однак цілком її ніяк не вдається захистити і, напевно, не вдасться взагалі. Інакше кажучи, можна говорити про деяке складне становище в забезпеченні безпеки в інформаційних технологіях.

Не зупиняючись на соціальних, правових і економічних аспектах проблеми, систематизуємо наукові і технічні передумови ситуації з забезпеченням інформаційних технологій.

1. Збільшення обсягів інформації, що накопичується, зберігається та оброблюється за допомогою ЕОМ. При цьому мова йде не тільки і не стільки про різке і буквальне збільшення самих обсягів, але і розширення арсеналу методів, способів і можливостей її зосередження і збереження, наприклад, коли в єдиних базах даних може зосереджуватися інформація всілякого призначення і приналежності. Особливо розширилися можливості подібного роду з виникненням глобальної мережі інтернет.

2. Сучасні комп'ютери за останні роки отримали гігантську обчислювальну потужність. Причому повсюдне поширення мережних технологій об'єднало окремі машини в локальні мережі, що спільно використовують загальні ресурси, а застосування технології «клієнт-сервер» перетворило такі мережі в розподілені обчислювальні середовища. Тепер безпека мережі починає залежати від безпеки всіх її компонентів, і зловмиснику досить порушити роботу однієї з них, щоб скомпрометувати всю мережу. Сучасні телекомунікаційні технології об'єднали локальні мережі в глобальні. Це привело до появи такого унікального явища як інтернет. І саме розвиток інтернету викликав сплеск інтересу до проблеми безпеки і змусив, принаймні частково, переглянути її основні положення.

3. Маючи гігантську обчислювальну потужність сучасні комп'ютери за останні роки (що може показатися парадоксальним) стали набагато простіше в експлуатації. Це означає, що користуватися ними стало набагато простіше і що все більша кількість нових користувачів одержує доступ до комп'ютерів. Звичайно, в такій ситуації комерційні питання вирішуються у першу чергу, а питання забезпечення безпеки інформації вирішуються в останню.

4. Широке розповсюдження отримало певне (фактично негативне) відношення до даних, що містять персональні дані абонентів, партнерів або співробітників та комерційні таємниці компаній, яке полягає в наступному:

– багато компаній не здогадуються про те, що їхні бази даних крадуть;

– крадіжка та заподіяний збиток мають латентний характер;

– якщо факт крадіжки даних встановлений, більшість компаній замовчують заподіяний збиток;

– технології, що дозволяють чітко персоніфікувати дії користувачів і розмежовувати їхні права, невідомі більшості керівників;

– можливості захисту даних від системних адміністраторів також маловідомі, керівники воліють вважати їх найбільш лояльними співробітниками;

– бюджети на інформаційну безпеку, як правило, невеликі. Це не дозволяє вирішити проблему комплексно (введення штатних одиниць, що відповідають за інформаційну безпеку, захист інформації, формування й реалізацію політик безпеки, навчання персоналу, встановлення систем захисту і т. ін.).

Проблема ускладняється також і тим, що керівники організації та технічні фахівці зазвичай оперують різними поняттями: перші – фінансово-економічними, другі – технічними. Внаслідок цього, розуміння керівництвом важливості придбання і встановлення засобів захисту інформації трапляється рідко, і найчастіше буває сформованим за результатами інцидентів, що трапляються через порушення безпеки інформації.

5. Прогрес в області апаратних засобів супроводжується ще більш бурхливим розвитком програмного забезпечення. Як показує практика, більшість розповсюджених сучасних програмних засобів (у першу чергу – операційних систем), незважаючи на великі зусилля розробників у цьому напрямку, не відповідають навіть мінімальним адекватним вимогам безпеки.

6. Практично зникає розходження між даними і програмами, що виконуються, за рахунок появи і широкого поширення віртуальних машин і різних інтерпретаторів. Тепер будь-який розвинутий додаток від текстового процесора до браузера не просто обробляє дані, а інтерпретує інтегровані в них інструкції спеціальної мови програмування, тобто по суті це є окремою машиною. Це істотно збільшує можливості ЗЛ по створенню засобів проникнення в чужі системи та ускладнює захист, тому що вимагає здійснення контролю взаємодії ще на одному рівні – рівні віртуальної машини чи інтерпретатора.

7. Зловмисні програми (віруси, інтернет-хробаки, трояни, різноманітне шпигунське та рекламне ПЗ) завдали чималої шкоди за останні декілька років, незважаючи на те, що обсяг коштів, які залучено до її вирішення крупними компаніями і організаціями, постійно зростав упродовж останніх років. Причому розвиток проблем із зловмисними програмами за останні роки надбав незмінного характеру і необхідно констатувати, що проблема продовжує погіршуватись.

8. Має місце істотний розрив між теоретичними моделями безпеки, що оперують абстрактними поняттями типу об'єкт, суб'єкт і т. ін., і сучасними інформаційними технологіями. Це призводить до невідповідності між моделями безпеки і їхнім впровадженням у засобах обробки інформації. Крім того, багато засобів захисту, наприклад, засоби боротьби з комп'ютерними вірусами чи засоби міжмережного екранування (firewall) узагалі не мають системної наукової бази. Таке положення є наслідком відсутності загальної теорії захисту інформації, комплексних моделей безпеки обробки інформації, що описують механізми дій ЗЛ в реальних умовах, а також відсутності систем, що дозволяють ефективно перевірити адекватність тих чи інших рішень в області безпеки. Наслідком цього є те, що практично всі системи захисту засновані на аналізі результатів успішних атак, що заздалегідь визначає їх відставання від реальної ситуації.

9. У сучасних умовах надзвичайно важливим є обґрунтування вимог безпеки, створення нормативної бази, яка не ускладнює задачі розробників, а, навпаки, встановлює обов'язковий рівень безпеки. Існує ряд міжнародних стандартів, що намагаються вирішити цю проблему, однак аж до останнього часу вони не могли претендувати на те, щоб стати посібником до дій, чи хоча б закласти фундамент безпечних інформаційних технологій майбутнього. У різних країнах, у тому числі і в Україні, розроблені документи, що являють собою лише деяке наслідування закордонним стандартам десятилітньої давнини. В умовах повальної інформатизації і комп'ютеризації найважливіших сфер економіки і державного апарата нашій країні просто необхідні нові рішення в цій області.

10. Нарешті, глобальна безпека. В останні роки у світі різко загострилися проблеми, що пов'язані з забезпеченням безпечної діяльності людей узагалі. В умовах політичної та економічної нестабільності у світі зараз постійно виникають різні негативні явища від локальних воєн до міжнародного тероризму. Тому різко ускладнилася проблема забезпечення економічної, матеріальної і навіть фізичної безпеки людини. Забезпечення ж перерахованих видів безпеки виявилося прямо пов'язаним з інформаційною безпекою внаслідок широкого використання інформаційних технологій практично в усіх областях людської діяльності.

Унаслідок сукупної дії перерахованих факторів перед розробниками сучасних інформаційних систем, призначених для обробки важливої інформації, виникають наступні задачі, що вимагають негайного та ефективного рішення:

1. Забезпечення безпеки нових типів інформаційних ресурсів. Оскільки комп'ютерні системи тепер прямо інтегровані в інформаційні структури сучасного суспільства, засоби захисту повинні враховувати сучасні форми представ-

лення інформації (гіпертекст, мультимедіа і т. ін.). Це означає, що системи захисту повинні забезпечувати безпеку на рівні інформаційних ресурсів, а не окремих документів, файлів чи повідомлень.

2. Організація довіреної взаємодії сторін (взаємної ідентифікації/ автентифікації) в інформаційному просторі. Розвиток локальних мереж і інтернет диктує необхідність здійснення ефективного захисту при віддаленому доступі до інформації, а також взаємодії користувачів через загальнодоступні мережі. Цю задачу потрібно вирішити в глобальному масштабі, незважаючи на те, що сторони, які беруть участь, можуть знаходитися в різних частинах планети, функціонувати на різних апаратних платформах і в різних ОС.

3. Захист від автоматичних засобів нападу. Досвід експлуатації існуючих систем показав, що сьогодні від систем захисту вимагаються зовсім нові функції, а саме, можливість забезпечення безпеки в умовах будь-якої їх взаємодії з подібними засобами, в тому числі і при появі усередині їх програм, що здійснюють деструктивні дії – комп'ютерних вірусів, автоматизованих засобів зламу, агресивних агентів. На перший погляд здається, що ця проблема вирішується засобами розмежування доступу, однак це не зовсім так, що підтверджується відомими випадками поширення комп'ютерних вірусів у «захищених» системах.

4. Інтеграція захисту інформації в процес автоматизації її обробки як обов'язковий елемент. Для того, щоб бути затребуваними сучасним ринком інформаційних систем, засоби безпеки не повинні істотно погіршувати характеристики існуючих застосувань і сформованих технологій обробки інформації, а, навпаки, повинні стати невід'ємною частиною цих засобів і технологій.

5. Розробка сучасних ефективних, адекватних та надійних математичних моделей безпеки.

Як неважко зрозуміти, ці задачі знаходяться під безперервною увагою і вимагають свого вирішення, оскільки зрозуміло, що і сучасний стан і подальший розвиток та поширення інформаційних технологій у сфері критичних систем, що обробляють важливу інформацію, виявляються під безперервною загрозою.

Принципи організації інформаційної безпеки

При організації ефективного та надійного захисту потрібно керуватися системою принципів. Під принципами захисту інформації розуміються основні ідеї і найважливіші рекомендації з питань організації та здійснення робіт для ефективного захисту інформаційних ресурсів ІКСМ. Використання даних принципів дозволяє ефективно організувати роботу з захисту інформації.

В загальному принципі, захист інформації можна умовно розділити на дві основні групи: правові принципи; організаційні принципи.

Правові принципи захисту інформації. Правове регулювання захисту інформації спирається на принципи інформаційного права. Дані принципи, що базуються на положеннях основних конституційних норм, закріплюють інформаційні права і свободи, і так само гарантують їх здійснення. Крім того, основні правові засади захисту інформації ґрунтуються на особливостях і юридичних властивостях інформації як повноцінного об'єкту правовідносин. Узагальнено, до правових принципів захисту інформації відносяться: легітимність (законність); пріоритет міжнародного права над внутрішньодержавним; економічна доцільність.

Організаційні принципи захисту даних. Роль організаційного захисту інформації в системі заходів безпеки визначається своєчасністю та правильністю прийнятих управлінських рішень, способів і методів захисту інформації на основі діючих нормативно-методичних документів.

Організаційні методи захисту передбачають проведення організаційно-технічних та організаційно-правових заходів, і також включають в себе наступні принципи захисту інформації:

– науковий підхід до організації захисту інформації;

– планування захисту ;

– керування системою захисту;

– безперервність процесу захисту інформації;

– мінімальна достатність організації захисту;

– системний підхід до організації та проектування систем та методів захисту інформації;

– комплексний підхід до організації захисту інформації;

– відповідність рівня захисту цінності інформації;

– гнучкість захисту;

– багатозональність захисту, що передбачає розміщення джерел інформації в зонах з контрольованим рівнем її безпеки;

– багаторубіжність захисту інформації;

– обмеження числа осіб, які допускаються до захищеної інформації;

– особиста відповідальність за збереження довіреної інформації.

Побудова системи забезпечення безпеки інформації в АС і її функціонування повинні здійснюватися у відповідності з наступними основними принципами.

Законність. Передбачає здійснення захисних заходів і розробку системи безпеки інформації в АС відповідно до чинного законодавства в області інформації, інформатизації та захисту інформації, інших нормативних актів по безпеці, затверджених органами державної влади в межах їх компетенції, із застосуванням усіх дозволених методів виявлення і припинення правопорушень при роботі з інформацією.

Системність. Системний підхід до захисту інформації в АС передбачає облік усіх взаємозалежних, взаємодіючих і мінливих у часі елементів, умов і факторів, суттєво значимих для розуміння та вирішення проблеми забезпечення інформаційної безпеки в АС.

При створенні системи захисту повинні враховуватися всі слабкі і найбільш уразливі місця системи обробки інформації, а також характер, можливі об'єкти та напрямки атак на систему з боку порушників, шляхи проникнення в розподілені системи та несанкціонованого доступу до інформації. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення та несанкціонованого доступу до інформації, але і з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеки.

Комплексність. Комплексне використання методів і засобів захисту комп'ютерних систем передбачає узгоджене застосування різнорідних засобів при побудові цілісної системи захисту, що перекривають всі істотні (значимі) канали реалізації загроз і не залишаючи слабких місць на стиках окремих її компонентів. Захист повинен будуватися ешелоновано. Зовнішній захист повинен забезпечуватися фізичними засобами, організаційними, технологічними і правовими заходами.

Безперервність захисту. Захист інформації – не разовий захід і не проста сукупність проведених заходів і встановлених засобів захисту, а безперервний цілеспрямований процес, що припускає вживання відповідних заходів на всіх етапах життєвого циклу АС, починаючи із самих ранніх стадій проектування, а не тільки на етапі її експлуатації.

Більшості фізичних і технічних засобів захисту для ефективного виконання своїх функцій необхідна постійна організаційна (адміністративна) підтримка (своєчасна зміна і забезпечення правильного зберігання та застосування імен, паролів, ключів шифрування, перерозподілу повноважень і т. ін.). Перерви в роботі засобів захисту можуть бути використані зловмисниками для аналізу застосовуваних методів і засобів захисту, для впровадження спеціальних програмних і апаратних «закладок» і інших засобів подолання системи захисту після відновлення її функціонування.

Своєчасність. Передбачає попереджувальний характерзаходів забезпечення безпеки інформації, тобто постановку завдань по комплексному захисту АС і реалізацію заходів забезпечення безпеки інформації на ранніх стадіях розробки АС у цілому і її системи захисту інформації, зокрема.

Розробка системи захисту повинна вестися паралельно з розробкою та розвитком самої системи, що захищається. Це дозволить урахувати вимоги безпеки при проектуванні архітектури і, в остаточному підсумку, створити більш ефективні (як по витратах ресурсів, так і по стійкості) захищені системи.

Спадковість і вдосконалювання. Припускають постійне вдосконалювання заходів і засобів захисту інформації на основі спадковості організаційних і технічних рішень, аналізу функціонування АС і її системи захисту з урахуванням змін у методах і засобах перехоплення інформації і впливу на компоненти АС, нормативних вимог по захисту, досягнутого вітчизняного та закордонного досвіду в цій області.

Поділ функцій. Принцип поділу функцій, вимагає, щоб жоден співробітник організації не мав повноважень, що дозволяють йому одноосібно здійснювати виконання критичних операцій. Усі такі операції повинні бути розділені на частини, і їх виконання повинно бути доручено різним співробітникам. Крім того, необхідно вживати спеціальних заходів по недопущенню змови і розмежуванню відповідальності між цими співробітниками.

Розумна достатність (економічна доцільність, порівнянність можливого збитку й витрат). Передбачає відповідність рівня витрат на забезпечення безпеки інформації цінності інформаційних ресурсів, величині можливого збитку від їхнього розголошення, втрати, витоку, знищення та викривлення. Заходи і засоби забезпечення безпеки інформаційних ресурсів не повинні помітно погіршувати ергономічні показники роботи АС, у якій ця інформація циркулює. Зайві заходи безпеки, крім економічної неефективності, приводять до стомлення та роздратуванню персоналу.

Персональна відповідальність. Передбачає покладання відповідальності за забезпечення безпеки інформації і системи її обробки на кожного співробітника в межах його повноважень. Відповідно до цього принципу розподіл прав і обов’язків співробітників будується таким чином, щоб у випадку будь-якого порушення коло винуватців було чітко відоме або зведено до мінімуму.

Мінімізація повноважень. Означає надання користувачам мінімальних прав доступу відповідно до виробничої необхідності. Доступ до інформації повинен надаватися тільки в тому випадку і обсязі, у якому це необхідно співробітникові для виконання його посадових обов’язків.

Взаємодія та співробітництво. Передбачає створення сприятливої атмосфери в колективах. У такій обстановці співробітники повинні усвідомлено дотримуватись встановлених правил і сприяти в діяльності підрозділам забезпечення безпеки інформації.

Гнучкість системи захисту. Вжиті заходи і встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечувати як надмірний, так і недостатній рівень захисту. Для забезпечення можливості корегування рівня захищеності, засоби захисту повинні мати певну гнучкість. Особливо важливим така властивість є у випадках, коли встановлення засобів захисту необхідно здійснювати на вже працюючу систему, не порушуючи процесу її нормального функціонування. Крім того, зовнішні умови і вимоги із часом змінюються. У таких ситуаціях властивість гнучкості системи захисту рятує власників АС від необхідності вживання кардинальних заходів по повній заміні засобів захисту на нові.

Відкритість алгоритмів і механізмів захисту. Суть принципу відкритості алгоритмів і механізмів захисту полягає в тому, що захист не повинен забезпечуватися тільки за рахунок таємності структурної організації та алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно давати можливості її подолання (навіть авторам). Однак це не означає, що інформація про конкретну систему захисту повинна бути загальнодоступна.

Простота застосування засобів захисту. Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або з виконанням дій, що вимагають значних додаткових працезатрат при звичайній роботі зареєстрованих встановленим порядком користувачів, а також не повинно вимагати від користувача виконання рутинних малозрозумілих йому операцій (уведення декількох паролів, імен і т. ін.).

Наукова обґрунтованість і технічна реалізованість. Інформаційні технології, технічні та програмні засоби, засоби і заходи захисту інформації повинні бути реалізовані на сучасному рівні розвитку науки і техніки, науково обґрунтовані з погляду досягнення заданого рівня безпеки інформації та повинні відповідати встановленим нормам і вимогам по безпеці інформації.

Спеціалізація та професіоналізм. Передбачає залучення до розробки засобів і реалізації заходів захисту інформації спеціалізованих організацій, найбільш підготовлених до конкретного виду діяльності по забезпеченню безпеки інформаційних ресурсів, що мають досвід практичної роботи та державні ліцензії на

право надання послуг у цій області. Реалізація адміністративних заходів і експлуатація засобів захисту повинна здійснюватися професійно підготовленими співробітниками (фахівцями підрозділів забезпечення безпеки інформації).

Взаємодія та координація. Передбачають здійснення заходів забезпечення безпеки інформації на основі взаємодії всіх зацікавлених міністерств і відомств, підприємств і організацій при розробці і функціонуванні АС і її системи захисту інформації, підрозділів і фахівців, спеціалізованих підприємств і організацій в області захисту інформації, притягнутих для розробки системи захисту інформації в АС, координації їх зусиль для досягнення поставлених цілей.

Обов'язковість контролю. Припускає обов'язковість і своєчасність виявлення та припинення спроб порушення встановлених правил забезпечення безпеки інформації на основі систем і засобів захисту інформації, що використовуються.

Контроль над діяльністю будь-якого користувача, кожного засобу захисту і, відносно, будь-якого об'єкта захисту повинен здійснюватися на основі застосування засобів оперативного контролю та реєстрації і повинен охоплювати як несанкціоновані, так і санкціоновані дії користувачів.

1.2. Моделі управління мережевими ресурсами

Є дві принципово різні моделі управління користувачами і мережевими ресурсами:

– модель управління робочою групою;

– доменна модель управління.

Модель робочої групи (модель розподіленого управління)

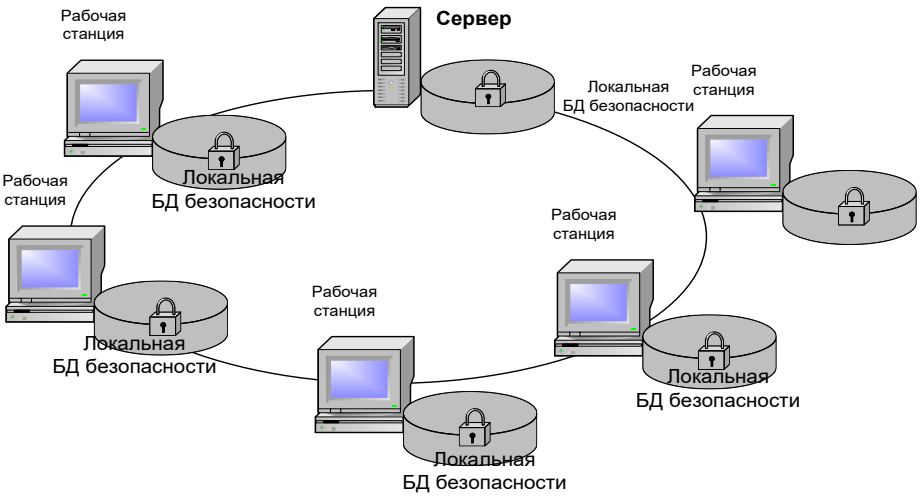


Рис. 1.1. Робоча група

Робоча група (workgroup) – логічна група мережевих комп'ютерів, що надають доступ до ресурсів, наприклад до файлів і принтерів. Робоча група використовується в *однорангових* (peer-to-peer) мережах, в яких усі комп'ютери робочої групи забезпечують рівноправний доступ до ресурсів без використання виділеного сервера. Кожен комп'ютер робочої групи, веде власну *локальну БД безпеки* (рис. 1.1), яка є списком облікових записів користувачів і інформацією про захист ресурсів комп'ютера, на якому вона знаходиться. Таким чином адміністрування облікових записів користувачів і захист ресурсів в робочій групі децентралізовано (є розподіленим).

Недоліки моделі робочої групи:

– користувачеві необхідно мати облікові записи на усіх комп'ютерах, до яких йому потрібний доступ;

– будь-які зміни облікових записів користувачів, наприклад зміна пароля або додавання нового облікового запису, необхідно виконати на кожному комп'ютері робочої групи. Якщо адміністратор забуде додати новий обліковий запис користувача на один з комп'ютерів робочої групи, новий користувач не зможе отримати доступ до його ресурсів;

– надання доступу до файлів і пристроїв виконується конкретними комп'ютерами тільки для користувачів, що мають облікові записи на кожному конкретному комп'ютері.

Переваги робочої групи:

– робочій групі не потрібний комп'ютер сервер для зберігання централізованої інформації безпеки;

– робоча група забезпечує простоту в проектуванні і супроводі: в порівнянні з доменом не потрібно трудомістке планування і адміністрування;

– робоча група зручна для невеликої кількості розташованих поруч комп'ютерів. (Використання робочої групи непрактичне в ятерах, що складаються більш ніж з 10 комп'ютерів.)

Модель домена (модель централізованого управління)

Домен (domain) – логічна група мережевих комп'ютерів, доступ до ресурсів яких виконується за допомогою центральної БД облікових записів користувачів і ресурсів до яких надається доступ (рис. 1.2). Цю базу часто називають *База даних каталогу* (directory database). Вона містить облікові записи користувачів і параметри безпеки для усього домена. БД каталогу, або просто каталог, є частиною БД служби каталогу. Служба каталогу забезпечує обробку запитів користувачів

на отримання доступу до ресурсів каталогу. Окрім файлових ресурсів і мережевих принтерів каталог про доступні мережеві служби і інші інформаційні ресурси.

У домені каталоги знаходяться на комп'ютерах, зконфігурованих як контролери домена, де задаються параметри безпеки взаємодії користувачів з доменом. Захист і адміністрування централізовані на контролерах домена. У ролі контролерів домена можуть виступати тільки комп'ютери на яких працюють операційні системи що підтримують виконання цих функцій (наприклад, Windows 2000/2003 Server). Домен не пов'язаний з певним місцем розташування або конкретним типом конфігурації мережі. Комп'ютери в домені можуть знаходитися поруч в невеликій локальній мережі або в різних країнах, зв'язуючись один з одним за допомогою різних фізичних модемів, ліній ISDN (Integrated Services Digital Network), оптоволоконних ліній, ліній Ethernet, з'єднань з ретрансляцією кадрів (frame relay), супутникових і орендованих каналів.

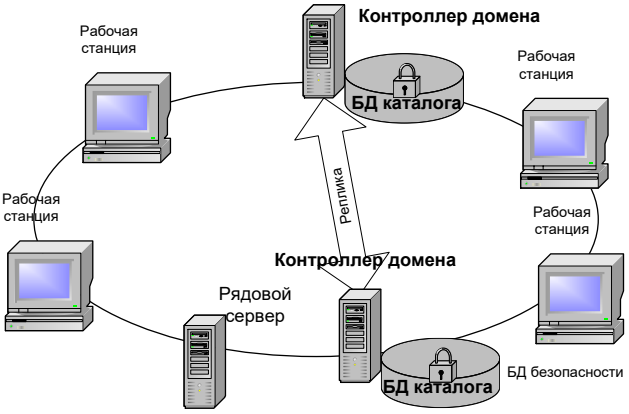


Рис. 1.2. Домен управління ресурсами

Переваги використання домена такі:

– домен дозволяє виконувати централізоване управління, оскільки уся інформація про користувачів зберігається централізовано. Змінений користувачем пароль автоматично реплікується по усьому домену;

– домен забезпечує єдиний процес входу в систему користувачів для дістування доступу до дозволених мережевих ресурсів, наприклад до файлів, принтерів і застосувань. Іншими словами, користувач входить в систему на одному комп'ютері і звертається до ресурсів іншого комп'ютера мережі впродовж часу дії відповідних дозволів;

– домен забезпечує масштабованість, що дозволяє адміністраторові управляти дуже великими мережами.

Типовий домен включає наступні комп'ютери:

– кожен контролер домена зберігає і веде копію каталогу. У домені необхідно одноразово створювати обліковий запис користувача, який заноситься в каталог. Коли користувач входить в домен, контролер перевіряє по каталогу його ім'я, пароль і повноваження. За наявності декількох контролерів домена, періодично реплікують інформацію своїх каталогів;

– рядові сервери (member server) – сервер не конфігурований як контролер домена. Він не зберігає інформацію каталогу і не виконує перевірку достовірності користувачів домена, він лише забезпечує доступ до ресурсів, таких, як теки або принтери, використовуючи базу даних каталогу для перевірки повноважень суб'єктів доступу;

– клієнтські комп'ютери – це комп'ютери клієнтів із запущеним оточенням призначеного для користувача робочого столу, що дозволяють діставати доступ до ресурсів домена.

Служби каталогів

Каталог (directory) – збережений набір інформації про об'єкти, пов'язані один з одним деяким способом. Наприклад, в телефонному довіднику зберігаються імена об'єктів і телефонні номери, що відповідають їм. Телефонний довідник також може містити адресі або іншу інформацію про об'єкт [2].

Служба каталогів – мережева служба, яка ідентифікує усі ресурси мережі і робить їх доступними користувачам. Служба каталогів відрізняється від каталогу тим, що хоча вони обидва є джерелами інформації, служба робить її доступною для користувачів. Служба каталогів працює як головний комутатор мережевої ОС. Вона управляє ідентифікацією і стосунками між розподіленими ресурсами і дозволяє їм працювати разом. Зважаючи на підтримку службою каталогів цих фундаментальних функцій ОС, мають бути тісно пов'язані з механізмами управління і безпеки ОС для забезпечення цілісності і захищеності мережі. Вони також потрібні для визначення і підтримання інфраструктури мережі організації, адміністрування системи і контролю активності користувачів інформаційної служби компанії.

Призначення служби каталогів

Служба каталогу надає засоби організації і спрощення доступу до ресурсів мережевої комп'ютерної системи. Користувачі і адміністратори можуть не знати точну назву необхідних їм об'єктів. Їм досить знати один або декілька атрибутів даних об'єктів. Користувачі звертаються до служби каталогів для запиту списку об'єктів, що відповідають відомим атрибутам (рис. 1.3). Наприклад, у відповідь

на запит «Знайти усі кольорові принтери на третьому поверсі» каталог виведе відомості про всіх об’єктів кольорових принтерів з атрибутами «кольоровий» і «третій поверх» (або у яких атрибут місця розташування рівний «третій поверх»). Служба каталогів дозволяє шукати об’єкт одному або декільком його атрибутам.

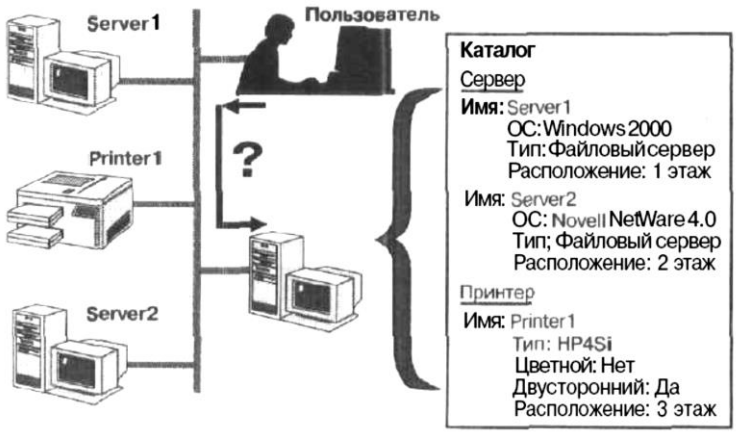


Рис. 1.3. Атрибути служби каталогів

Робота служби каталогів

Служба каталогів виконує і інші функції:

– призначення безпеки для захисту об’єктів БД від зовнішніх вторгнень або внутрішніх користувачів, що не мають доступу до цих об’єктів;

– поширення каталогу на безліч комп’ютерів мережі;

– дублювання каталогу для надання доступу більшій кількості користувачів та відмовостійкості;

– ділення каталогу на декілька сховищ, розташованих на різних комп’ютерах мережі.

Це збільшує доступний для каталогу простір в цілому і дозволяє зберігати більше об’єктів.

Служба каталогів є як інструментом адміністрування, так і інструментом користувача. При розширенні мережі доводиться управляти все більшою кількістю об’єктів ресурсів, і наявність служби каталогу стає насущною необхідністю.

Доменна модель управління мережевими ресурсами була багаторазово реалізована в мережевих операційних системах різних фірм. Прикладом однієї з найперших реалізацій на практиці цієї ідеї є служба NIS (Network Information Service).

Network Information Service

Мережева інформаційна служба NIS була розроблена і реалізована компанією Sun Microsystems у кінці 80-х років. Основна мета полягала в спрощенні управління великими парками робочих станцій під управлінням систем сімейства Unix.

Принцип роботи NIS можна описати всього однією фразою: функція системи полягає в реплікації вмісту файлів /etc/passwd, /etc/groups і /etc/hosts ведучої машини серед машин домена.

Файл /etc/passwd є БД облікових записів; окрім імен, ідентифікаторів та аутентифікаційній інформації (геша пароля) там міститься цивільне ім'я користувача і його контактна інформація.

Файл /etc/groups містить списки груп користувачів, а /etc/hosts дозволяє перетворювати імена вузлів мережі IP в адреси і назад. Таким чином, NIS можна було використати як альтернативу DNS. Оскільки NIS був набагато простіший в налаштуванні, ніж зона DNS, адміністратори багатьох приватних мереж використали його для дозволу імен робочих станцій (доступні ззовні сервери зазвичай все-таки прописувалися в DNS); аж до Solans v7 служба дозволу імен за умовчанням була налаштована на використання NIS.

Ця служба досі входить до складу великого числа UNIX систем від різних виробників.

NIS передбачає реплікацію, який з'єднується з одним провідним сервером і, можливо, декількома веденими. Інші машини домена є клієнтами і виконують окремі запити на дозвіл імені або пошук у БД, підключаючись до вказаного сервера.

Аутентифікація доступу веденого сервера до ведучого або клієнта до сервера робиться на основі секретного значення, що розділяється, і пароля користувача root, за допомогою простої схеми запит-відповідь. Клієнт аутентифікує користувачів, передаючи геш пароля по мережі у відкритому виді.

Досконаліша версія протоколу, NIS+, передбачає ієрархічну структуру БД каталогу і значно досконалішу схему аутентифікації як машин, так і користувачів, засновану на схемі Діффі-Геллмана [1]. Кожен вузол ієрархії в каталозі повинен мати власний провідний сервер і, можливо, декількох ведених (рис. 1.4).

Нині Sun відмовився від підтримки NIS/NIS+ і замінив його розподіленою аутентифікацією і повноцінною службою каталогів на основі протоколу LDAP.

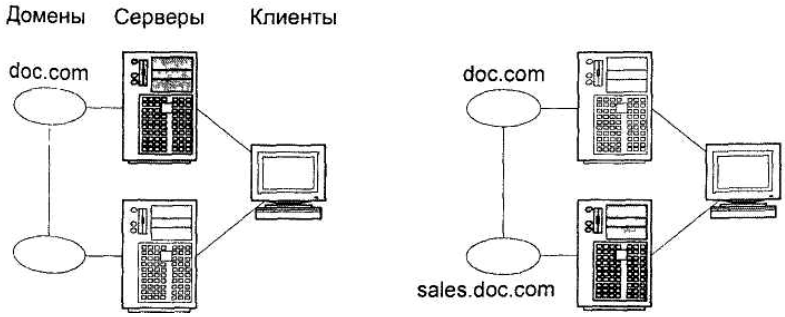


Рис. 1.4. Ведучий і ведений сервери доменів NIS+

Banyan Vines

Уперше система, що мала основні риси сучасних служб каталогів, була реалізована у кінці 80-х років компанією Banyan Vines в мережевій операційній системі Vines. Vines надавала файловий сервіс, розподілену аутентифікацію і ієрархічну службу каталогів, використовуючи нестандартні протоколи прикладного рівня і IPX як протокол мережевого рівня.

Як показав досвід експлуатації, основною перевагою Vines виявилася не служба каталогів як така, а ієрархічна структура БД облікових записів, яка сильно полегшувала управління користувачами і ресурсами. Зокрема, адміністратор мережі компанії міг делегувати адміністраторові облікових записів підрозділу право заводити, видаляти і змінювати атрибути (у тому числі забуті паролі) у записів користувачів його підрозділу, не надаючи права управляти усією іншою мережею. Контейнери служби каталогів виявилися зручним способом групування користувачів при роздачі доступу до мережевих ресурсів [12].

Ці переваги виявилися особливо важливі для великих компаній, тому цінова і ліцензійна політика Banyan Vines виявилася орієнтована саме на такі компанії. У дрібних і середніх мережах Vines не мала великого успіху; успіху також не сприяв і ефективний захист від неліцензійного використання. В середині 90-х років, після появи на ринку NDS, поширення Lotus Notes/Domino і витіснення файлових сервісів на допоміжні ролі, справи компанії пішли під гору і в 2001 році вона припинила своє існування. Проте найбільш успішні на якийсь час написання книги служби каталогів, NDS і ADS, поза сумнівом були спроектовані під враженням від Vines.

Novell Directory Service

У 1994 році на ринок вийшла нова версія мережевої ОС Novell Netware 4.0, в якій була реалізована революційна система управління обліковими записами і ряд інших важливих нововведень.

NDS (Novell Directory Service – служба каталогів Novell; у деяких статтях абревіатуру розшифровують також як Netware Directory Service) є ієрархічним реплікованим каталогом з розширюваним набором типів і атрибутів об'єктів. Набір типів об'єктів і їх атрибутів називається схемою (scheme) і змінюється при установці нових версій системи і додаткових продуктів.

Ієрархія каталогу в цілому відповідає структурі каталогу X.500. Об'єкти ідентифікуються абсолютними і відносними ієрархічними іменами.

В корені ієрархії імен розташовується псевдооб'єкт Root (корінь), атрибути якого насправді є властивостями дерева NDS в цілому (рис. 1.5). Усі інші контейнери і об'єкти NDS є нащадками Root, так що каталог завжди є деревом. Нащадками Root можуть бути країни і організації, але не об'єкти інших типів. Нащадками країни можуть бути тільки організації.

Дерево зберігається в реплікованій БД. Усі репліки доступні для модифікації. Реплікація відбувається проштовхуванням або, при поганих каналах, за розкладом, з ідентифікацією змін за допомогою тимчасових штампів. Ця схема дуже чутлива до синхронізації годинника, тому NDS підтримує спеціальну досить складну інфраструктуру синхронізації часу.

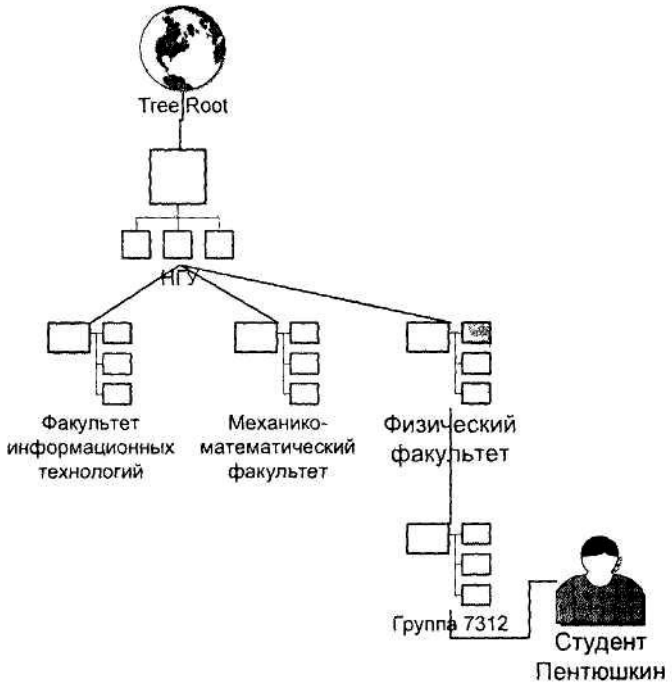


Рис. 1.5. Ієрархія контейнерів і об'єктів NDS

Служба каталогів X.500

Стандарт OSI X.500 був розроблений на початку 90-х років [11]. У чистому вигляді він не отримав застосування, але система понять і термінологія цього стандарту лежить в основі ряду популярних протоколів, передусім LDAP.

Каталог X.500 складається із записів (entry). Кожен запис містить деяку кількість іменованих атрибутів (attribute). Атрибут може мати одне або декілька значень. Деякі з атрибутів є обов'язковими, інші можуть бути відсутніми. У одному і тому ж каталозі можуть міститися записи, що мають різні списки атрибутів, тобто точний список атрибутів визначається як властивостями каталогу, так і типом конкретного запису. Найбільш важливі атрибути – CN (Common Name 'загальне ім'я') і O (Organization 'організація'). Окрім цих обов'язкових атрибутів, ресурс також може мати атрибути OU (Organization Unit 'підрозділ організації') і З (Country 'країна'). Атрибут OU може мати декілька значень.

Поєднання перерахованих атрибутів утворює DN (Distinguished Name 'помітне ім'я') запису: CN = cit/OU=Information Technology Department/O = Academy of management/C = By. Таке ім'я може бути дуже довгим, тому в якості імен зазвичай використовують абревіатури: CN=cit/OU=ITD/O=PAC/C=BY.

DN або, як його ще називають, ієрархічне ім'я однозначно ідентифікує ресурс в каталозі; при цьому загальні імена у різних ресурсів, що належать різним підрозділам, можуть співпадати, а імена організації і підрозділу, як правило, співпадають у багатьох записів. У багатьох реальних каталогах країна або країна і організація виявляються загальними у усіх записів каталогу.

DN організовують записи каталогу в ієрархічну деревовидну структуру, звану DIT (Directory Information Tree 'інформаційне дерево каталогу'). Видно, що країна за ієрархією вища, ніж організація; стандарт спочатку розроблявся з розрахунку на мережі публічного доступу, але реальні служби каталогів мали успіх, головним чином, в приватних мережах, на вершині ієрархії яких завжди знаходиться організація. У каталогах транснаціональних корпорацій, можливо, мало б сенс створювати об'єкти країн, підпорядковані організації, але X.500 такого не допускає, і національні підрозділи доводиться оформляти як звичайні підрозділи.

Більшість реальних каталогів, перш ніж вони дозволять створювати записи з тим або іншим ім'ям OU, вимагають, щоб заздалегідь був створений запис, що описує цей підрозділ. Такі записи називаються контейнерами (container).

З точки зору організації простору імен, контейнери схожі на вкладені каталоги і підкаталоги в сучасних файлових системах. Ця аналогія досить глибока, з

однією важливою відмінністю: на відміну від каталогу файлової системи і усупереч назві, контейнер зовсім не зобов'язаний містити ні підлеглі йому записи, ні навіть посилання на них; у багатьох реалізаціях зв'язок контейнера з підпорядкованими записами обумовлений тільки тим, що вони мають загальні компоненти ієрархічного імені.

Над каталогом X.500 визначені три основні операції:

– read – читання запису з вказаним ім'ям;

– list – отримання списку підпорядкованих записів вказаного контейнера; повертає список імен, а не записів;

– search – виконує пошук записів з вказаними значеннями вказаних атрибутів або записів, що взагалі мають вказаний атрибут. Допустиме використання шаблонів, наприклад символу *, який відповідає будь-якому текстовому рядку.

При вказівці імені запису або контейнера можливі два способи вказівки імені. Найпростіший полягає в тому, щоб завжди вказувати DN. Дещо складніший з точки зору реалізації, але зручніший для користувача, полягає у вказівці поточного контейнера і RDN (Relative Distinguished Name – відносного розрізняючого імені). При цьому повне ім'я буде утворено з DN поточного контейнера і RDN: так, якщо я починаю пошук з OU=FIT/O=PAC/C=BY, то цілком можна ідентифікувати ресурс CN=cit по одному тільки його загальному імені. Поточний контейнер таким чином схожий на поточний каталог у файлових системах.

Досить повно реалізацій специфікацій X.500 є протоколом LDAP (Lightweight Directory Access Protocol – полегшений протокол доступу до каталогу) [3]. Існує ряд реалізацій LDAP і його підмножин на основі різних БД, що у тому числі забезпечують доступ до БД облікових записів NIS/NIS+, NDS, ADS (Active Directory Service) і Lotus Domino.

Протокол підтримує досить гнучкі політики управління доступом до записів і атрибутів. Завдяки наявності захищених записів, протокол може використовуватися для зберігання секретних значень і аутентифікації за схемою запит-відповідь. Аутентифікація через LDAP підтримується більшістю сучасних систем сімейства Unix і деякими серверами додатків, наприклад IBM WebSphere.

Архітектура Windows 2000/2003

Windows 2000 є модульною ОС, що є колекцією невеликих, самодостатніх програмних компонентів, спільно працюючих для виконання завдань ОС. Кожен компонент виконує набір функцій, що є інтерфейсом до іншої частини системи.

Рівні, підсистеми і диспетчери Windows 2000

Архітектура Windows 2000 підтримує два основні режими; призначений (непривілейований) для користувача і режим ядра (рис. 1.6).

Рис. 1.6. Архітектура Windows 2000

Windows 2000 має два різні типи компонентів призначеного для користувача режиму: підсистеми середовища і вбудовані підсистеми.

Підсистеми середовища

Одна з можливостей Windows 2000 – здатність виконувати додатки, написані для різних ОС. Це досягається використанням *підсистем середовища* (environment subsystems), які емулюють різні ОС, надаючи необхідні для додатків API-інтерфейси. Підсистеми середовища приймають від додатків виклики API, перетворюють їх у формат, зрозумілий Windows 2000, і потім передають для обробки виконуваним службам. У таблиці 1.1 перераховані підсистеми середовища із складу Windows 2000.

Таблиця 1.1

Підсистеми середовища в Windows 2000

Підсистема середовища	**Призначення**
32-розрядна підсистема Windows 2000 на базі Windows (Win32)	Відповідає як за управління додатків Win32, так і за надання середовища для додатків Wml6 і MS – DOS. Управляє усіма операціями введення-виводу на екран між підсистемами. Це гарантує несуперечливий призначений для користувача інтерфейс незалежно від виконуваного користувачем застосування
Підсистема OS/2	Надає набір API для 16-розрядних застосувань текстового режиму OS/2
Інтерфейс переносних ОС для підсистем UNIX (POSIX)	Надає API для POSIX -приложений

На підсистеми середовища і додатка, працюючі в них, накладаються деякі обмеження:

– вони не мають прямого доступу до устаткування;

– вони не мають прямого доступу до драйверів пристроїв;

– вони не мають доступу до деяких операцій API буфера обміну;

– вони не мають доступу до деяких функцій розширень Microsoft CD – ROM (MSCDEX);

– вони не мають доступу до API перемикання завдань;

– вони обмежені в призначенні адресного простору;

– вони вимушені використати простір жорсткого диска під віртуальну пам’ять при нестачі пам’яті для ОС;

– вони працюють на нижчому пріоритетному рівні, ніж процеси режиму ядра;

– оскільки вони працюють на нижчому пріоритетному рівні, ніж процеси режиму ядра, їм менш доступні ресурси *центрального процесора* (central processing unit, CPU) чим процеси, які працюють в режимі ядра.

Вбудовані підсистеми

Безліч різних вбудованих підсистем виконує важливі функції ОС. У правій частині рис.6 показана універсальна підсистема. Ця вбудована підсистема може бути будь-якою, приклади деяких вбудованих підсистем перераховані в табл. 1.2.

Таблиця 1.2

Вбудовані підсистеми Windows 2000

Вбудована підсистема	**Призначення**
Підсистема безпеки	Контролює права і дозволи, пов’язані з обліковими записами користувачів. Відстежує, яким системним ресурсам призначений аудит. Приймає запити на вхід користувачів у систему. Ініціює аутентифікацію входу в систему.
Служба робочої станції	Мережева вбудована підсистема, що надає API для доступудо мережевої системи переадресації. Дає користувачам Windows2000 доступ до мережі.
Служба сервера	Мережева вбудована підсистема, що надає API для доступу до мережевого сервера. Надає користувачам Windows2000 доступ до мережевих ресурсів.

Режим ядра

Рівень режиму ядра має доступ до системних даних і устаткування. Режим ядра надає прямий доступ до пам’яті, програми цього режиму виконуються в захищеній області пам’яті. Він складається з чотирьох компонентів: виконуваній частині ОС Windows 2000, драйверів пристроїв, мікроядра і рівня абстрагування від устаткування (Hardware Abstraction Layer, HAL).

Виконувана частина ОС Window 2000

Виконує велику частину операцій введення-виводу і управління об'єктами, включаючи забезпечення безпеки. Він не займається введенням з клавіатури і виводом на екран – за це відповідає підсистема Microsoft Win32. Виконувана частина ОС Windows 2000 містить компоненти режиму ядра Windows 2000. Кожен з них надає два набори служб і підпрограм, що відрізняються:

– системні служби, доступні як підсистемам призначеного для користувача режиму, так і іншим виконуваним компонентам ОС;

– вбудовані підпрограми, доступні іншим компонентам в межах ОС.

Виконувана частина ОС складається з компонентів режиму ядра (табл. 1.3).

Драйвери пристроїв

Транслюють виклики драйверів в команди управління конкретними пристроями.

Таблиця 1.3

Компоненти виконуваної частини Windows 2000

Компонент	**Призначення**
Диспетчер віртуальній пам'яті (Virtual Memory Manager, VMM)	Система управління пам'яттю, яка встановлює віртуальну пам'ять і управляє нею, а також надає захищений адресний простір для кожного процесу. VMM також контролює *підкочування за запитом* (demand paging) і дозволяє використати дисковий простір для переміщення програм і даних з фізичної пам'яті та в неї.
Диспетчер міжпроцесної взаємодії (Interprocess Communication Manager, I PC)	Управляє зв'язками між клієнтами і серверами, наприклад між підсистемою середовища (яка може працювати в ролі клієнта який запитує інформацію) і компонентом служби ОС (працює в ролі сервера, який відповідає на запит інформації). Диспетчер IPC складається з двох компонентів: *засоби локального виклику процедур* (local procedure call, LPC), обслуговуючого з'єднання, коли клієнти і сервери існують на одному і тому ж комп'ютері, і *засоби віддаленого виклику процедур* (remote procedure call, RPC), обслуговуючого з'єднання, коли клієнти і сервери знаходяться на різних комп'ютерах.
Диспетчер процесів	Створює і завершує процеси і потоки. *Процес* (process) – це програма або її частина. *Потік* (thread) – певний набір команд в програмі.
Plug and Play	Забезпечує центральне управління процесами PnP. Взаємно діє з драйверами пристроїв, управляючи додаванням і запуском пристроїв.
Диспетчер живлення	Управляє API-інтерфейсами живлення, координує події, пов'язані з живленням, і генерує запити управління живленням.
Диспетчер вікон та*інтерфейс графічних облаштувань* (Graphical Device Interface, GDI)	Ці два компоненти, виконані у вигляді одного драйвера пристрої з ім'ям Win32k.sys, управляють системою дисплея. Диспетчер вікон управляє вікнами і виводом на екран, а також відповідає за введення інформації з клавіатури і миші і передає введені повідомлення додатків. GDI містить функції, потрібні для малювання і обробки графіків.
Диспетчер об'єктів	Створює, управляє і знищує об'єкти, що займають ресурси ОС наприклад процеси, потоки і структури даних.

Мікроядро

Управляє тільки мікропроцесором. Ядро координує усі функції введення-виводу і синхронізує дії здійснимих служб.

Рівень абстрагування від устаткування

Приховує деталі апаратного інтерфейсу, роблячи Windows 2000 переносимою на різну апаратну архітектуру. Містить апаратно-залежний код, відповідальний за інтерфейси введення-виводу, контролери переривань і механізм багатопроцесорної взаємодії. Дозволяє Windows 2000 працювати в системах на базі Intel і Alpha одночасно, тобто розробникам не довелося створювати дві окремі версії для кожної платформи.

Місце Active Directory в архітектурі Windows 2000

Два режими доступу до процесора – режим ядра і призначений для користувача режим – відділяють від процесів верхнього рівня низькорівневі, платформозалежні процеси, захищаючи додатки від відмінностей платформ і запобігаючи прямому доступу додатків до системного коду і даних.

Кожне застосування, у тому числі і службові, виконується в окремому модулі (module) в призначеному для користувача режимі, з якого воно просить системні служби за допомогою API, що дістає обмежений доступ до системних даних. Процес додатка починається в призначеному для користувача режимі і переноситься в режим ядра, де відбувається його фактична обробка в захищеному середовищі. Потім процес переноситься назад в призначений для користувача режим. Active Directory працює в підсистемі безпеки в призначеному для користувача режимі. Еталонний монітор безпеки (security reference monitor), працюючий в режимі ядра, є основним засобом встановлення правил безпеки однойменної підсистеми. На рис. 1.7 показано розташування Active Directory в Windows 2000.

Тісний взаємозв’язок служби каталогу і підсистеми безпеки є основою для роботи розподілених систем Windows 2000. Доступ до будь-якого об’єкту каталогу вимагає спочатку посвідчення особи (перевірки достовірності), а потім і перевірки дозволів доступу (авторизації), яка виконується компонентами підсистеми безпеки разом з еталонним монітором безпеки.

Останній управляє доступом стосовно об’єктів Active Directory.

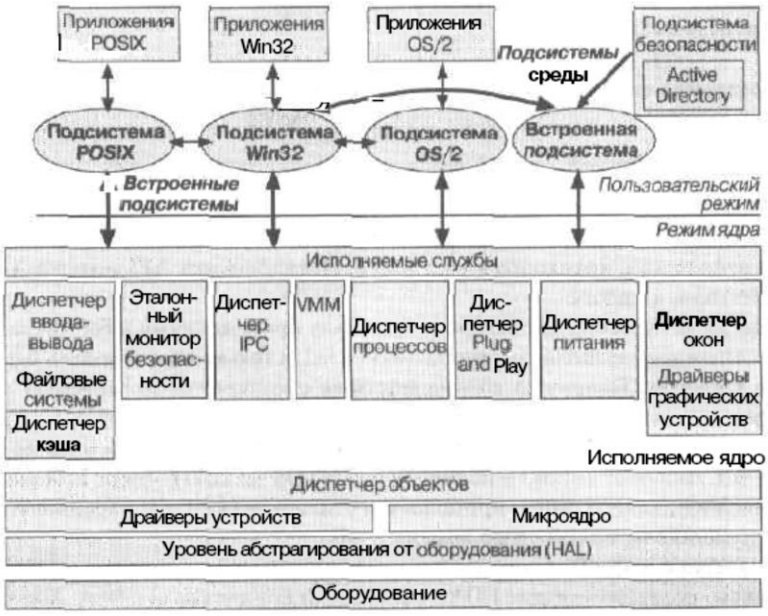


Рис. 1.7. Місце Active Directory в архітектурі Windows 2000

Архітектура Active Directory

Функціональну структуру Active Directory можна представити у вигляді багаторівневої архітектури, в якій рівні є процесами, що надають клієнтським застосуванням доступ до служби каталогу. Active Directory складається з трьох рівнів служб і декількох інтерфейсів і протоколів, спільно працюючих для надання доступу до служби каталогу. Три рівні служб охоплюють різні типи інформації, необхідної для пошуку записів у БД каталогу. Вище за рівні служб в цій архітектурі знаходяться протоколи і API-інтерфейси, що здійснюють зв'язок між клієнтами і службою каталогу.

На рис. 1.8 зображені рівні служби Active Directory і інтерфейси, що відповідають їм, і протоколи. Стрілки показують, як різні клієнти дістають за допомогою інтерфейсів доступ до Active Directory.

Рис. 1.8. Архітектура Active Directory

Нижче перераховані основні компоненти служб:

– системний агент каталогу (Directory System Agent, DSA). Вибудовує ієрархію батьківсько-дочірніх стосунків, що зберігаються в каталозі. Надає API - інтерфейси для викликів доступу до каталогу;

– рівень БД. Надає рівень абстрагування між додатками і БД. Виклики з додатків ніколи не виконуються безпосередньо до БД, а тільки через рівень БД;

– розширюване ядро зберігання. Безпосередньо взаємодіє з конкретними записами в сховищі каталогу на основі атрибуту відносного складеного імені об'єкту;

– сховище даних (файл БД NTDS.DIT) управляється за допомогою механізму зберігання БД, розташованого в теці на контролері домена;

– для адміністрування цього файлу застосовується утиліта NTDSUTIL, що зберігається в теці \Mnnt на контролері домена;

– клієнти дістають доступ до Active Directory, використовуючи механізми, підтримувані DSA;

– LDAP/ADSI. Клієнти, підтримувальні LDAP, використовують його для зв'язку з DSA. Active Directory підтримує LDAP версії 2 (описаний в RFC 1777). Клієнти Windows 2000, Windows 98 і Windows 95 зі встановленими клієнтськими компонентами Active Directory для зв'язку з DSA використовують LDAP версії 3. Хоча ADSI є засобом абстрагування API LDAP, Active Directory використовує тільки LDAP;

– API-інтерфейс обміну повідомленнями (Messaging API, MAPI). Традиційні клієнти MAPI, наприклад Microsoft Outlook, підключаються до DSA, використовуючи інтерфейс постачальника адресної книги MAPI RPC;

– диспетчер облікових записів безпеки (Security Accounts Manager, SAM). Клієнти Windows NT версії 4.0 або більш ранньою використовують інтерфейс SAM для зв'язку з DSA. Реплікація з резервних контролерів в домені змішаного режиму також виконується через інтерфейс SAM;

– реплікація (REPL). При реплікації каталогу, агенти DSA взаємодіють один з одним, використовуючи патентований інтерфейс RPC.

Можливості служби каталогів Windows 2000

Active Directory – це служба каталогів в Windows 2000 Server. Active Directory містить каталог, в якому зберігається інформація про мережеві ресурси і служби, що надають доступ до цієї інформації. Ресурси, що зберігаються в каталозі, такі, як дані, відомості про принтери, сервери, бази даних, групи, служби, комп'ютери, політику безпеки, – називаються об'єктами (object).

Active Directory вбудована в Windows 2000 Server і забезпечує:

– спрощене адміністрування;
– масштабованість;
– підтримку відкритих стандартів;
– підтримку стандартних форматів імен.

Спрощене адміністрування

Active Directory ієрархічно упорядковує ресурси в домені (domain) – логічному об'єднанні серверів і інших мережевих ресурсів в єдине ім'я домена. Домен є основною одиницею реплікації і безпеки в мережі Windows 2000.

Кожен домен включає один або декілька контролерів домена. Контролер домена (domain controller) – комп'ютер під управлінням Windows 2000 Server, доступ користувачів, що забезпечує, в мережу: вхід в систему, перевірку достовірності і доступ до каталогу і загальних ресурсів. Для простоти адміністрування усі контролери домена рівнозначні. Зміни, зроблені на будь-якому з них, реплікуються на інші контролери в домені.

Active Directory додатково спрощує адміністрування, надаючи єдину точку адміністрування усіх об'єктів мережі. Завдяки цьому адміністратор може, увійшовши до системи на одному комп'ютері, управляти об'єктами, розташованими на будь-якому комп'ютері в мережі.

Масштабованість

У Active Directory каталог заносить інформацію в розділи, що дозволяють зберігати безліч об'єктів. В результаті каталог розширюється з ростом організації. Це дозволяє переходити від невеликих установок з декількома сотнями об'єктів до більш ніж мільйонами об'єктів.

Підтримка відкритих стандартів

Active Directory відповідає концепції простору імен інтернету в частині служби каталогів Windows 2000. Це дозволяє уніфікувати і управляти безліччю просторів імен, існуючих нині в різнорідному програмному і апаратному оточенні корпоративних мереж. В якості системи іменування Active Directory використовує DNS і здатний обмінюватися інформацією з будь-яким застосуванням або каталогом, що використовує LDAP або протокол передачі гіпертексту (HTTP).

Active Directory спільно використовує інформацію з іншими службами каталогу, підтримувальними LDAP версій 2 і 3, наприклад службою каталогів Novell (Novell Directory Services, NDS).

DNS

Оскільки Active Directory для доменного іменування і служби пошуку використовує DNS, імена доменів Windows 2000 також є іменами DNS. Windows 2000 Server застосовує динамічну DNS (DDNS), що дозволяє клієнтам з динамічно призначеними адресами безпосередньо реєструватися на сервері з працюючою службою DNS і динамічно оновлювати таблицю DNS. У однорідному середовищі DDNS усуває потребу в інших службах іменування інтернету, наприклад в службі імен інтернету для Windows (Windows Internet Name Service, WINS).

Підтримка LDAP і HTTP

Active Directory відповідає стандартам інтернету і безпосередньо підтримує LDAP і HTTP.

LDAP – версія протоколу доступу до каталогу X.500, розроблений в якості альтернативи протоколу доступу до каталогів (Directory Access Protocol, DAP). Active Directory підтримує обидві версії LDAP: 2 і 3. HTTP є стандартним протоколом для відображення сторінок у всесвітній мережі інтернет. Користувачі можуть переглядати кожен об’єкт в Active Directory, як HTML-сторінку в веб-оглядачі, користуючись при запитах і перегляді об’єктів Active Directory усіма перевагами знайомої моделі веб-оглядача.

Таблиця 1.4

Стандартні формати імен, підтримувані Active Directory

Формат	Опис
RFC 822	Застосовується у формі *користувач@домен,* знайомий більшості користувачів по адресах електронної пошти інтернету
HTTP універсальний покажчик на ресурси (URL)	Застосовується у формі *Шр://домен/шлях_до_сторінки*знайомий користувачам оглядачів Vvfeb
Універсальні правила іменування LDAP URL	Застосовується у формі *\fljicrosoft.com. XLS* в мережах на основі Windows 2000 Server для звернення до загальних томів, принтерів і файлам Active Directory підтримує проект RFC 1779і використовує атрибути, як показано в наступних прикладах: LDAP://someserver.m icrosoft.com/ CN=FirstnameLastname, OU=sys, OU=product OU=division, DC=devel Де CN – ім’я; OU – ім’я підрозділу; DC – ім’я компонента домена; LDAP URL – сервер, на якому розташовані служби Active Directory і атрибут не ім’я об’єкту

1.3. Програмно-апаратні засоби забезпечення безпеки мережі

Програмні засоби забезпечення захисту інформації

Програмні засоби захисту інформації призначені для виконання логічних та інтелектуальних функції захисту і включаються або у склад програмного забезпечення автоматизованих інформаційних систем, або до складу засобів, комплексів та систем апаратури контролю. Програмні засоби захисту є найбільш поширеним видом захисту, володіючи наступними позитивними властивостями: універсальністю, гнучкістю, простотою реалізації, можливістю змінення та розвитку. Дана обставина робить їх найвразливішими елементами захисту інформаційної системи підприємства.

Важливим є захист інформації і у всесвітній мережі інтернет. Якщо раніше мережа використовувалась лише в якості середи передачі файлів та повідомлень електронної пошти, то сьогодні вирішуються складніші завдання розподіленого доступу до ресурсу. Інтернет, який раніше слугував виключно дослідницьким та учбовим групам, стає все більш популярною у діловому світі. Компанії спокушають швидкість, дешевий глобальний зв'язок, зручність для проведення спільних робіт, доступні програми, унікальна база даних мережі. Вони розглядають глобальну мережу, як доповнення до власних локальних мереж.

При роботі в мережі інтернет, для захисту інформації, на перше місце виходять міжмережеві екрани (firewalls) – найважливіший засіб захисту мережі організації. Вони контролюють мережевий трафік, що входить в мережу і що виходить з неї. Використовуючи інтерфейс налаштувань профілю доступу міжмережевого екрану, є можливість для кожного користувача створити свій профіль, який буде визначати не тільки права доступу цього користувача до мережі інтернет, але і права доступу до цього користувача з інтернету. Міжмережевий екран може блокувати передачу в мережу несанкціонованого трафіка та виконувати перевірки трафіка. Добре сконфігурований міжмережевий екран спроможний зупинити більшість відомих комп'ютерних атак [6].

Firewall здатні забезпечити захист окремих протоколів і програмних продуктів. Вони здійснюють контроль доступу ззовні до внутрішньої мережі, і окремих сегментів на основі вмісту пакетів даних, що передаються між двома сторонами, або пристроями мережею.

Міжмережеві екрани працюють з програмами маршрутизації та фільтрами всіх мережевих пакетів, щоб визначити, чи можна пропустити інформаційний пакет, а якщо можна, то відправити його до певної комп'ютерної служби за при-

значенням. Для того щоб міжмережевий екран міг зробити це, необхідно визначити правила фільтрації. Отже, міжмережевий екран є немовби віртуальним кордоном, на якому перевіряється цілісність фрагментованих пакетів даних, що передаються, їх відповідність стандарту тощо.

Часто корпоративні мережі зв'язують офіси, розкидані в місті, регіоні, країні або всьому світі. Ведуться роботи щодо захисту на мережевому рівні IP-мереж (саме такі мережі формують інтернет). Провідні постачальники міжмережевих екранів і маршрутизаторів запропонували технологію S/WAN. Вони взяли на себе впровадження і тестування протоколів, що пропонуються Робочою групою інженерів інтернет (Inernet Engineering Task Force, IETF) для захисту пакетів даних. Ці протоколи забезпечують автентифікацію й шифрування пакетів, а також засоби обміну та управління ключами для шифрування й автентифікації. Протоколи S/WAN допоможуть досягти сумісності між маршрутизаторами і брандмауерами різноманітних виробників, що дасть змогу географічно віддаленим офісам однієї корпорації, а також партнерам, що утворюють віртуальне підприємство, безпечно обмінюватися даними в інтернеті. Іншими словами, компанії зможуть створювати власні віртуальні приватні мережі (virtual private networks, VPN) і використовувати інтернет як альтернативу традиційним каналам зв'язку, які орендуються за високу плату.

Віртуальні приватні мережі (virtual private networks, VPN) – територіально розподілені корпоративні мережі, які використовують для зв'язку між окремими сегментами інтернету.

Однак міжмережеві екрани не є універсальним вирішенням усіх проблем безпеки в інтернеті. Наприклад, вони не здійснюють перевірку на віруси і не здатні забезпечити цілісність даних.

Засоби захисту VPN – це інтегровані з віртуальними мережами засоби захисту мережі, в цілому, її сегментів та кожного клієнта мережі окремо (захист TCP/IP трафіку, створюваного будь-якими додатками і програмами; захист робочих станцій, серверів WWW, баз даних і додатків; автопроцесингу, трансакцій для фінансових та банківських додатків і платіжних систем). Реалізуються в рамках програмно-апаратних рішень VVPN-шлюзів. Серед основних функцій VPN-шлюзів: автентифікація (MD5, SHA1), шифрування (DES, 3DES, AES), тунелювання пакетів даних через IP. Певні шлюзи підтримують також функції firewall.

Використання антивірусних засобів вважається необхідною умовою при підключенні до інтернету, дозволяє значно знизити втрати інформації в наслідок зараження шкідливими програмами.

Антивірус (в обчислювальній техніці) – програма, що виявляє або виявляє та знищує комп'ютерні віруси.

Вірус – програма, яка модифікує інші програми. У контексті проблем безпеки цей термін зазвичай використовується по відношенню до програм, зловмисно упроваджених у систему з метою нанесення шкоди та руйнування. Вірусна програма поширюється за рахунок самокопіювання та під'єднання копій до інших програм. Коли у системі відбувається певна подія, на яку налаштований вірус, він починає виконувати свою цільову функцію.

Мережеві антивіруси – використовують для захисту від вірусів однієї або кількох OS, протоколів та команди комп'ютерних мереж і електронної пошти. Використання автоматизованих засобів перевірки мережі на можливі уразливості в системі захисту та аудиту безпеки корпоративних серверів дозволяє встановити джерела загроз та значно понизити вірогідність ефективних атак на корпоративну мережу або персональний комп'ютер.

SKIPBridge – система, яка встановлюється на інтерфейсі внутрішня / зовнішня мережа (локальна мережа або комунікаційний провайдер). Забезпечує захист (шифрування) трафіка, що направляється з внутрішньої мережі у зовнішню на основі протоколу SKIP, а також фільтрацію і дешифрування трафіка, який поступає із зовнішньої мережі у внутрішню. IP-пакети, що приймаються із зовнішньої мережі, обробляються протоколом SKIP (розшифровуються, фільтруються відкриті пакети в режимі тільки захищеного трафіка, контролюється і забезпечується імітозахист). Пакети, які пройшли фільтрацію SKIP, за допомогою протоколу IP передаються програмному забезпеченню SKIP-Bridge. Програмне забезпечення вирішує завдання адміністративної безпеки (забезпечуючи пакетну фільтрацію), і потім системи SKIPBridge, який маршрутизує пакети на адаптер локальної мережі.

Використання Proxy та анонімних серверів дозволяє залишатись умовно анонімним при діях в мережі інтернет та знизити ризики, пов'язані із збиранням та моніторингом мережевої інформації на користь третіх осіб, потоком непотрібної та шкідливої інформації у системі.

Використання систем обмеження доступу співробітників до мережевих ресурсів інтернету, використання маршрутизаторів та надійних постачальників мережевих послуг, короткочасного каналу зв'язку дозволяє скоротити збір та моніторинг мережевої інформації на користь третіх осіб, потік непотрібної та шкідливої інформації.

Для захисту інформації у мережі також використовується шифрування. В основу шифрування покладено два елементи: криптографічний алгоритм і ключ.

Принципово новий підхід до здійснення електронних платежів сьогодні полягає в негайній авторизації і шифруванні фінансової інформації в мережі інтернет з використанням протоколів SSL (Secure Sockets Layer) та SET (Secure Electronic Transaction). Протокол SSL припускає шифрування інформації на канальному рівні, а протокол SET, розроблений компаніями VISA, MasterCard та інші, – шифрування виключно фінансової інформації. Оскільки мережа інтернет розрахована на одночасну роботу мільйонів користувачів, то в комерційних додатках «у чистому вигляді» неможливо використовувати ні традиційні системи, засновані виключно на «закритих ключах» (DES, ГОСТ 28147-89 та ін.), ні методи шифрування тільки на «відкритих ключах», в тому числі і російський стандарт електронного підпису.

Застосування одних закритих ключів неможливо у зв'язку з тим, що розкриття (перехоплення) навіть одного ключа відразу ж приведе до «злому» усієї системи захисту. Тому при реалізації електронної комерції в інтернеті разом з системами шифрування за допомогою закритих ключів використовуються системи шифрування за допомогою відкритих ключів. Це пов'язано з тим, що шифрування лише відкритими ключами вимагає великих витрат обчислювальних ресурсів. Тому краще всього шифрувати інформацію, передану по мережах, за допомогою закритого ключа, який генерується динамічно та передається іншому користувачу зашифрованим з допомогою відкритого ключа. Така система шифрування буде працювати і швидше, і надійніше.

У додатках, заснованих на використанні алгоритму SET, покупець, не розшифровуючи платіжних реквізитів продавця, розшифровує всі дані замовлення, а банк, не маючи даних про структуру замовлення, має доступ до платіжних реквізитів і продавця і покупця. Це досягається завдяки використанню подвійного (сліпого) електронного підпису, і в даній ситуації банку надсилається одна частина повідомлення, а покупцеві – інша. Крім того, протокол SET описує стандартні види фінансових транзакцій між банками, центрами авторизації і торговими точками. При шифруванні з використанням закритих ключів передбачається, що і продавець і покупець мають загальний ключ, який вони використовують для шифрування/дешифрування інформації. У шифруванні ж з використанням відкритих ключів передбачено, що і продавець і покупець мають по два ключі: один – «відкритий», який може бути відомий будь-якої третій стороні, а інший – «приватний», завжди відомий лише одній стороні – його власнику. При цьому по одному ключу неможливо відновити інший.

Також для захисту інформації використовують протоколи. Ці протоколи можна класифікувати відповідно до того, що саме вони захищають – сполучення чи

програми. Такі стандарти, як SSL і S/WAN, призначені для захисту комунікацій в інтернет; хоча SSL використовується насамперед з веб-додатками. S-HTTP і S/MIME спрямовані на забезпечення автентифікації і конфіденційності (8-HTTP – для веб-продуктів, а S/MIME – для електронної пошти). SET забезпечує тільки захист трансакцій електронної комерції.

Захист веб-продуктів: S-HTTP і SSL. Веб-застосування захищені двома протоколами – S-HTTP і SSL, які забезпечують автентифікацію для серверів і браузерів, а також конфіденційність і цілісність даних для сполучень між веб-сервером і програмою-браузером.

S-HTTP – захищений HTTP-протокол, розроблений компанією Enterprise Integration Technologies (EIT) спеціально для веб. Він дає змогу забезпечити надійний криптозахист тільки для HTTP-документів веб-сервера. Його використання неможливе для захисту інших прикладних протоколів (FTP, TELNET, SMTP тощо). S-HTTP призначений насамперед для підтримки протоколу передачі гіпертексту (HTTP), забезпечує авторизацію і захист веб-документів. SSL – розробка компанії Netscape – пропонує ті ж самі засоби захисту, але для комунікаційного каналу.

Канал – лінія зв’язку між двома вузлами мережі або вузлом і одним з його абонентів.

За SSL кодування інформації здійснюється на рівні порту.

Порт – ідентифікаційний номер, який відповідає кожному програмному застосуванню або процесу, що використовують базовий інтернет-протокол TCP як транспортний.

Захист електронної пошти. Для захисту електронної пошти в інтернеті існує безліч різноманітних протоколів, але лише кілька з них поширені.

PEM (Privacy Enhanced Mail). Це стандарт інтернету для захисту електронної пошти з використанням відкритих або симетричних ключів. Він застосовується усе рідше, оскільки не призначений для оброблення нового MIME-формату електронних повідомлень і вимагає жорсткої ієрархії сертифікаційних центрів для видачі ключів.

S/MIME. Відносно новий стандарт, у якому задіяно багато криптографічних алгоритмів, запатентованих і заліцензійованих компанією RSA Data Security Inc. S/MIME використовує цифрові сертифікати і, отже, при забезпеченні автентифікації спирається на використання сертифікаційного центру.

PGP (Pretty Good Privacy). Це родина програмних продуктів, які використовують найстійкіші криптографічні алгоритми. В їх основу покладено алгоритм RSA. PGP реалізує технологію, відому як криптографія з відкритими ключами,

яка дає змогу обмінюватися зашифрованими повідомленнями і файлами каналами відкритого зв'язку без наявності захищеного каналу для обміну ключами, а також накладати на повідомлення й файли цифровий підпис. Іншими словами, програма побудована за принципом «павутини довіри» (Web of Trust) і дає змогу користувачам розповсюджувати свої ключі без посередництва сертифікаційних центрів.

Аутентифікація електронного документа здійснюється за допомогою перевірки електронно-цифрового підпису (ЕЦП). При перевірці ЕЦП файлу перевіряється, застосовувався чи при виробленні даного цифрового підпису конкретний ключ, що належить відправнику документа, і чи не зазнав файл змін у процесі пересилання адресату. Якщо програма перевірки підпису формує запис «ЕЦП вірна», то файл «аутентифікований». При аутентифікації файлу не має значення, яку корисну інформацію він містить і чи містить взагалі. Для подальшої ідентифікації файлу – документа потрібен механізм переведення бінарної інформації, що становить файл, в читану людиною форму і певним чином трактується вміст даної форми. Очевидно, що тільки при наявності подібного механізму може бути забезпечена доказова сила електронного документа. Закон «Про електронний цифровий підпис» є підставою доказової сили цифрового підпису.

Доказова ж сила електронних документів ґрунтується на фіксації мови їх прочитання або, іншими словами, механізму ідентифікації цифр – нулів та одиниць, що утворюють документ. Найчастіше мова ідентифікації електронних документів в договірних відносинах не регламентований. Тому, за відсутності будь-яких правил, норм і вимог, ситуація необтяжливого хаосу в цьому питанні породжує додаткові ризики, які є принциповим гальмом розвитку технологій електронної комерції.

Електронний цифровий підпис (ЕЦП) є електронним еквівалентом власноручного підпису. ЕЦП служить не тільки для аутентифікації відправника повідомлення, а й для перевірки його цілісності. При використанні ЕЦП для аутентифікації відправника повідомлення застосовуються відкритий і закритий ключі. Процедура схожа на здійснювану в асиметричному шифруванні, але в даному випадку закритий ключ служить для шифрування, а відкритий – для дешифрування.

Алгоритм застосування ЕЦП складається з ряду операцій:

1. Генерується пара ключів – відкритий і закритий.

2. Відкритий ключ передається зацікавленій стороні (одержувачу документів, підписаних стороною, згенерувавашою ключі).

3. Відправник повідомлення шифрує його своїм закритим ключем і передає одержувачу по каналах зв'язку.

4. Одержувач дешифрує повідомлення відкритим ключем відправника.

Будь-якому програмному забезпеченню властиві певні уразливості, які призводять до реалізації атак. І уразливості проектування системи e-Commerce (наприклад, відсутність засобів захисту), та вразливості реалізації і конфігурації. Останні два типи вразливостей найпоширеніші і зустрічаються в будь-якій організації. Все це може призвести до реалізації різного роду атак, спрямованих на порушення конфіденційності і цілісності даних, що обробляються.

В даний час на рівні мережі застосовуються маршрутизатори і міжмережеві екрани, на рівні ж ОС – вбудовані засоби розмежування доступу. Одним із прикладів засобів виявлення атак є система RealSecure, розроблена компанією Internet Security Systems.

Наступний рівень – третій рівень прикладного програмного забезпечення (ПЗ), що відповідає за взаємодію з користувачем. Прикладом елементів цього рівня – текстовий редактор WinWord, редактор електронних таблиць Excel, поштова програма Outlook, браузер Internet Explorer [5].

Четвертий рівень системи управління базами даних (СУБД) відповідає за зберігання і обробку даних інформаційної системи. Прикладом елементів цього рівня – СУБД Oracle, MS SQL Server, Sybase і MS Access.

Система захисту повинна ефективно працювати на всіх рівнях. Інакше зловмисник зможе знайти уразливості системи і реалізувати атаку на ресурси електронного магазину. Тут допоможуть засоби аналізу захищеності та сканери безпеки.

Технічні (апаратні) засоби забезпечення захисту інформації

До технічних заходів можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у випадку порушення працездатності окремих ланок, установку устаткування виявлення і гасіння пожежі, вживання конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів, установлення резервних систем електроживлення, оснащення приміщень замками, установку сигналізації і багато чого іншого.

Вся сукупність технічних засобів захисту підрозділяється на апаратні і фізичні.

Апаратні засоби – пристрої, що вбудовуються безпосередньо в обчислювальну техніку, чи пристрою, що сполучаються з нею по стандартному інтерфейсу.

Системи будь-якої складності будуються на базі одних і тих же технічних пристроїв. При рішенні технічних завдань захисту й охорони в першу чергу необхідно вибрати основні параметри пристроїв, які забезпечать достатню надійність виконання покладених на них функцій. Система охоронної сигналізації фіксує факт несанкціонованого доступу на територію, що охороняється, передає сигнал тривоги, наприклад, на пульт охорони і вмикає виконуючі пристрої. Система охоронної сигналізації включає: датчики, пульт-концентратор, виконуючі пристрої.

Апаратні пристрої є мініатюрними пристроями, які можуть бути прикріплені між клавіатурою і комп'ютером або вбудовані в саму клавіатуру. Вони реєструють всі натиснення клавіш, зроблені на клавіатурі. Процес реєстрації абсолютно невидимий для кінцевого користувача. Щоб успішно перехоплювати всі натиснення клавіш, апаратні кейлоггери не вимагають установки ніякої програми на комп'ютері. Коли апаратний пристрій прикріплюють, абсолютно не має значення, в якому стані знаходиться комп'ютер – ввімкненому або вимкненому. Час його роботи не обмежений, оскільки він не вимагає для своєї роботи додаткового джерела живлення.

Об'єми внутрішньої незалежної пам'яті даних пристроїв дозволяють записувати до 20 млн натиснень клавіш, причому з підтримкою юнікода. Дані пристрої можуть бути виконані у будь-якому вигляді, так що навіть фахівець не в змозі іноді визначити їх наявність при проведенні інформаційного аудиту. Залежно від місця прикріплення апаратні кейлогери підрозділяються на зовнішні і внутрішні.

Сучасні комп'ютерні засоби побудовані на інтегральних схемах. При роботі таких схем відбуваються високочастотні зміни рівнів напруги і струмів, що приводить до виникнення в ланцюгах живлення, в ефірі, у близько розташованої апаратурі і комп'ютерах у мережі і т. ін. електромагнітних полів і наведень, що за допомогою спеціальних засобів (умовно назвемо їх «шпигунськими») можна трансформувати в оброблювану інформацію. Тому, зі зменшенням відстані між приймачем порушника й апаратними засобами імовірність такого роду знімання і розшифровки інформації збільшується, унаслідок чого повинні дотримуватися нормативної відстані і ставитися захисні екрани і фільтри.

SunScreen – апаратна система захисту локальних мереж. SunScreen – це спеціалізована система захисту, що вирішує завдання розвиненої фільтрації пакетів, аутентифікації і забезпечення конфіденційності трафіка. SunScreen не має IP-адреса, тому вона «невидима» із зовнішньої мережі і тому не може бути безпосере-

дньо атакована. Пристрій SunScreen містить п’ять Ethernet-адаптерів, до яких можуть приєднуватися чотири незалежних сегменти локальної мережі і комунікаційний провайдер. Для кожного сегмента забезпечується налаштування індивідуальної політики безпеки шляхом встановлення складного набору правил фільтрації пакетів (у напрямі поширення, за адресами відправника/одержувача, за протоколами і додатками, за часом доби і т. ін.). Іншою важливою рисою SunScreen є підтримка протоколу SKIP, який, з одного боку, використовується для забезпечення безпеки роботи, управління і конфігурування систем SunScreen, а з іншого – дозволяє організовувати SKIP-захист користувацького трафіка. Використання протоколу SKIP в Screen-системах дає кілька додаткових можливостей. Screen-пристрої можуть інкапсулювати весь зовнішній трафік локальних мереж, які захищаються в SKIP (проводити SKIP-тунелювання). При цьому початкові IP-пакети можуть вміщуватися в блоки даних SKIP-пакетів, а мережеві адреси всіх вузлів внутрішніх мереж можуть бути замінені на певні віртуальні адреси, що відповідають у зовнішній мережі Screen-пристроям (адресна векторизація). В результаті весь трафік між локальними мережами, які захищаються, може виглядати ззовні тільки як повністю шифрований трафік між вузлами Screen-пристроїв. Вся інформація, яка може бути в цьому випадку доступна зовнішньому спостерігачеві динаміка і оцінка інтенсивності трафіка, яка, зазначимо, може маскуватися шляхом використання стиснення даних і видачі «порожнього» трафіка.

Виходячи із викладеного, програмно-апаратні засоби мають наступну класифікацію:

– апаратно-незалежні – працюючі без участі апаратних засобів захисту інформації – пароль, програми шифрування, антивіруси;

– апаратно-залежні – забезпечення сполучених апаратних засобів захисту інформації з інших програм або ОС – драйвера, вільне ПЗ;

– автономні – частина систем захисту функціонує;

– комплексні – кілька частин системного захисту використовують загальний елемент і базу ідентифікації або використовують інформацію, отриману від інших частин системи захисту – ключ, використовується і при завантаженні комп’ютера, параметри користувача ігноруються, якщо він не прийшов на роботу, тобто не пройшов контроль;

– інтелектуальні засоби – усі системи безпеки, системи керування безпекою об’єднані в єдине ціле.

1.4. Технології забезпечення безпеки мережевої інфраструктури

Основою забезпечення захисту інформації при міжмережевій взаємодії є міжмережевий екран. Міжмережевий екран як напівпроникна мембрана, що розташовується між внутрішньою мережею (що захищається) і зовнішнім середовищем (зовнішніми мережами чи іншими сегментами корпоративної мережі) і контролює всі інформаційні потоки у внутрішній мережі і з неї. Контроль інформаційних потоків полягає в їхній фільтрації, тобто у вибірковому пропущенні через екран, можливо, з виконанням деяких перетворень і повідомленням відправника про те, що його даним у пропуску відмовлено. Фільтрація здійснюється на основі набору правил, попередньо завантажених в екран і сіткові аспекти, що є вираженням, політики безпеки організації.

Ситуації, коли корпоративна мережа містить лише один зовнішній канал, є, скоріше, виключенням, ніж правилом. Навпроти, типова ситуація, при якій корпоративна мережа складається з декількох територіально рознесених сегментів, кожний з який підключений до мережі загального користування. У цьому випадку кожне підключення повинне захищатися своїм екраном. Точніше кажучи, можна вважати, що корпоративний зовнішній межмережевий екран є складеним, і потрібно вирішувати задачу погодженого адміністрування (керування й аудиту) усіх компонентів.

1.4.1. Безпека міжмережевої взаємодії

У загальній сукупності загроз, яких зазнає інформація, оброблювана в автоматизованій системі, значне місце займають загрози, спрямовані на дані, передані по каналах і лініях зв’язку між територіально рознесеними об’єктами автоматизованої системи. На практиці при відсутності належного захисту канали (лінії) зв’язку є найбільш уразливим елементом автоматизованої системи, тому що по своїй природі та за умовами розташування допускають і пасивні, і активні атаки порушника.

Під пасивною атакою у цьому випадку розуміється перехоплення, у ході якого порушник тільки стежить за переданими повідомленнями без втручання в потік. Основні типи перехоплення спрямовані на:

– розкриття змісту повідомлення, тобто порушення конфіденційності;

– аналіз потоку повідомлень (трафіка), під яким розуміється аналіз заголовків повідомлень із метою визначення місця розміщення та ідентифікаторів

об’єктів, що беруть участь у передачі, навіть якщо зміст повідомлень порушникові незрозуміло, а також визначення довжини повідомлень і частоти їх передачі для визначення характеру переданих даних.

При активній атаці порушник впливає на передані повідомлення, переслідуючи наступні цілі:

– зміна потоку повідомлень, тобто знищення, затримка, дублювання та більш пізній повтор, підробка повідомлень, тобто порушення цілісності і автентичності повідомлень;

– переривання потоку повідомлень, тобто знищення або затримка всіх переданих повідомлень;

– ініціювання хибного з’єднання, тобто спроба порушити протокол аутентифікації шляхом передачі хибних ідентифікаторів, або записи і передачі попередніх повідомлень по ініціюванню з’єднань.

Слід відмітити особливості зазначених типів атак. Пасивне перехоплення практично неможливо виявити, але йому легко перешкодити. Активним атакам складно запобігти, але їх можна надійно виявити.

Таким чином, при розробці методів, що забезпечують захист передачі даних, слід забезпечити:

1) запобігання розкриття змісту інформації;

2) запобігання аналізу потоку;

3) виявлення зміни потоку повідомлень;

4) виявлення переривання передачі повідомлень;

5) виявлення ініціювання хибного з’єднання.

Існує два основні методи вирішення завдань захисту передачі даних: канальні (лінійні) і абонентські (міжкінцеві). Перші забезпечують захист потоку даних незалежно для кожного каналу, у той час як останні – єдиний захист кожного повідомлення при передачі його від джерела до адресата.

Канальні методи забезпечують захист усього потоку повідомлень, переданого по окремому каналу зв’язку між двома вузлами, незалежно від джерела і адресату повідомлень. Недолік цих методів у тому, що компрометація одного з вузлів мережі передачі даних може привести до розкриття значної частини потоку повідомлень, тобто потрібен захист усіх вузлів мережі передачі даних.

Абонентські методи захищають повідомлення в процесі передачі між джерелом і адресатом таким чином, що розкриття одного з каналів зв’язку між джерелом і адресатом не приводить до розкриття потоку повідомлень. У загальному випадку говорять, що забезпечується захист між парою користувачів або між ко-

ристувачем і обчислювальним процесом. Основне достоїнство: питання про застосування таких методів може вирішуватися окремими користувачами без порушення інтересів інших учасників. Різновидом абонентських методів є методи, орієнтовані на з'єднання, коли мережа передачі даних розглядається як середовище, надане користувачам для встановлення з'єднання або віртуального каналу від джерела до адресата. При цьому передбачається, що кожне з'єднання буде захищатися окремо. В абонентських методах потрібний захист устаткування тільки в джерелі і адресаті з'єднання.

До основних механізмів захисту повідомлень слід віднести.

1. Розкриття змісту повідомлень. Основний метод захисту від розкриття змісту повідомлень – шифрування, канальне або абонентське.

Канальне шифрування можна виконувати незалежно в кожному каналі зв'язку. Із цією метою, як правило, застосовуються симетричні потокові шифри, і між вузлами підтримується суцільний потік бітів шифротексту. При цьому використовуються довгострокові ключі шифрування. Вузли, у яких проводиться шифрування повинні бути захищені. Слід зазначити, якщо в проміжному вузлі проводиться перешифрування інформації для її подальшої передачі адресатові, це порушує принцип найменшої поінформованості, тобто виникає додаткова загроза розкриття змісту повідомлень на ділянці між джерелом і адресатом. У мережах пакетної комутації в межах одного каналу може зашифровуватися як заголовок, так і інформаційна частина пакета.

Найбільш важливими характеристиками канальних шифраторів є:

– швидкість шифрування;

– алгоритм, що використовується;

– режим роботи (синхронний/асинхронний, дуплекс/напівдуплекс);

– підтримувані протоколи зв'язку;

– протоколи обміну ключовою інформацією;

– спосіб введення ключів (з панелі вручну, із пристроїв введення, дистанційно з робочих станцій);

– реалізація послуг захисту (зворотний виклик, цифровий підпис, діагностика, сигнали тривоги та ін.).

Таким чином, канальне шифрування має наступні особливості:

– розкриття ключа шифрування для одного каналу не приводить до компрометації інформації в інших каналах;

– уся передана інформація, включаючи службові повідомлення, службові поля повідомлень, надійно захищена;

– уся інформація виявляється відкритою на проміжних вузлах (ретрансляторах, шлюзах та ін.);

– користувач не приймає участі в операціях, що виконуються;

– для кожної пари вузлів потрібно мати свій ключ;

– алгоритм шифрування повинен бути досить стійким і забезпечувати швидкість шифрування на рівні пропускної здатності каналу;

– необхідність апаратної реалізації канального шифратора (по вимогах швидкості), що збільшує витрати на створення і обслуговування системи.

При абонентському шифруванні кожне повідомлення, за винятком деяких даних заголовка, які повинні оброблятися в проміжних вузлах маршруту, зашифровується в його джерелі та не розшифровується, поки не досягне місця призначення. Для кожного з'єднання може використовуватися унікальний ключ або застосоване більше дроблення при розподілі ключів (наприклад, один ключ між кожною парою зв'язаних ЕОМ або один ключ усередині всієї захищеної підмережі). У другому випадку спрощується розподіл ключів, але росте обсяг інформації, що компрометується при розкритті ключа. При використанні абонентського шифрування в мережах з пакетною комутацією слід враховувати, що адресні частини пакетів не можуть шифруватися по абонентському (межкінцевому) принципу.

Таким чином, абонентське шифрування має наступні особливості:

– захищеним є тільки зміст повідомлення: уся службова інформація залишається відкритою;

– ніхто крім відправника та одержувача не може відновити інформацію;

– маршрут передачі несуттєвий;

– для кожної пари користувачів потрібен унікальний ключ;

– користувач повинен знати процедури шифрування та розподілу ключів.

На практиці часто використовується комбінація канального й абонентського шифрування.

2. Аналіз потоку. Захист від аналізу потоку повідомлень пов'язаний з маскуванням наступних параметрів:

– частоти передачі повідомлень;

– довжини повідомлень;

– джерела та адресати повідомлень та ін.

Основні заходи захисту полягають у наступному:

а) генерація хибних (надлишкових) повідомлень. При канальному шифруванні між вузлами може бути встановлений безперервний потік біт шифротексту,

що приховує частоту передачі і довжину дійсних повідомлень. При абонентському шифруванні можуть формуватися порожні повідомлення різних довжин, а справжні повідомлені можуть доповнюватися незначущою інформацією. У повідомленнях повинна міститись зашифрована інформація, що вказує на хибний характер повідомлення або його дійсну довжину;

б) доповнення блоку даних до фіксованої довжини. При аналізі потоку не можна виявити точну довжину повідомлень, а тільки число переданих блоків;

в) маскування адреси призначення. Простіше всього реалізується при канальному шифруванні потоку повідомлень. Інші варіанти пов'язані з багаторівневим шифруванням повідомлень (наприклад, між вузлами мережі, між шлюзами мереж і т. ін.), використанням обхідних маршрутів доставки повідомлення;

г) захищені протоколи передачі. Наприклад такі протоколи:

– спеціальна станція збирає повідомлення однакової довжини від відправників, вносить у них зміни та відправляє далі по мережі в іншій послідовності. У результаті здійснюється маскування з'єднання між джерелом і адресатом від усіх суб'єктів автоматизованої системи за винятком цієї спеціальної станції та відправника;

– сегментація пакетів, при якій проводиться їх розподіл і передача паралельно по двом лініям, що знижує ймовірність перехоплення всіх даних. Модифікація цього методу в радіомережах: пакети передаються через різні канали та базові станції.

До основних видів активних загроз інформації можна віднести.

1. Зміна потоку повідомлень. Для виявлення зміни потоку повідомлень необхідно використовувати механізми, що визначають автентичність, цілісність і впорядкованість повідомлень. Дані механізми повинні підтвердити наступні факти:

– повідомлення виходить від санкціонованого відправника;

– зміст повідомлення при передачі не змінився;

– повідомлення доставлене за адресою;

– аналогічне повідомлення раніше не надходило;

– порядок одержання повідомлень відповідає порядку відправлення.

До таких механізмів відносяться:

– контрольні суми повідомлень (імітовставка, геш-результат), передані разом з повідомленням у зашифрованому виді;

– симетричне шифрування: дозволяє виявити зміну шифротексту завдяки розмноженню помилок при розшифруванні (наприклад, при використанні шифрування зі зворотним зв'язком), а також сховати обов'язкові параметри, що підтверджують дійсність повідомлення (адреси, ідентифікатори і т. ін.);

– включення в зашифроване повідомлення додаткових параметрів: тимчасових міток, порядкових номерів, випадкових чисел, криптографічних змінних (наприклад, сеансових ключів);

– цифрові підписи: підтверджують автентичність джерела, цілісність повідомлення, можуть включати в зашифрованому виді всі перераховані типи додаткових параметрів;

– використання механізмів маршрутизації: маршрути можуть вибиратися динамічно або бути заздалегідь задані для того, щоб використовувати фізично безпечні підмережі, ретранслятори, канали. Кінцеві системи при встановленні спроб нав'язування можуть вимагати встановлення з'єднання по іншому маршруту. Може використовуватись вибіркова маршрутизація, тобто частина маршруту задається відправником явно – в обхід небезпечних ділянок;

– паралельна доставка дублікатів повідомлень по інших шляхах: це єдиний захист від загрози знищення, переорієнтації або затримки повідомлення.

2. Переривання передачі повідомлень. Виявлення переривання передачі може забезпечуватися за допомогою протоколу запиту-відповіді. Такий протокол містить у собі періодичний обмін парою повідомлень, що встановлюють тимчасову цілісність і статус з'єднання. У кожне повідомлення повинна включатися інформація, що дозволяє виявити втрату повідомлень у з'єднанні (наприклад, номер повідомлення). Якщо через заданий інтервал часу відповідь від протилежної сторони не надходить, повідомлення вважається загубленим.

3. Ініціювання хибного з'єднання. Для виявлення ініціювання хибного з'єднання необхідно забезпечити перевірку ідентичності сторін, що беруть участь у з'єднанні, і тимчасову цілісність з'єднання (тобто процедура з'єднання не є повтором раніше записаної процедури).

Дані функції реалізуються в протоколах однобічної та взаємної аутентифікації, які розглянуті нами раніше. Підтримка взаємозв'язку між сторонами після первісної перевірки забезпечується за рахунок того, що в даних протоколах, як правило, розподіляються криптографічні ключі. Таким чином, протокол забезпечує і дійсність наступного потоку повідомлень.

Принципи побудови мережевих екранів

Організація захисту технології «клієнт-сервер». Сучасні інформаційні системи звичайно будують за технологією клієнт-сервер. Сервер при цьому відповідає за зберігання та обробку інформації і тільки за його посередництвом клієнти одержують доступ до інформації. Серед послуг, що надаються сервером, можна виділити: електронна пошта, доступ до баз даних, розподілена обробка даних, файл-сервер, сервер печатки та ін.

Програмне забезпечення, побудоване за цією технологією, працює на прикладному рівні, тому системи, побудовані за технологією клієнт-сервер, не залежать від архітектури транспортного середовища передачі даних.

Із усіх протоколів, застосовуваних у клієнт-серверних технологіях, частіше інших використовують:

– протокол HTTP (Hypertext Transfer Protocol), що є основою веб-технологій, що й використовується для доставки гіпертекстових повідомлень;

– протокол Telnet – протокол дистанційного доступу. Дозволяє клієнтові підключитися до сервера й працювати з ним у якості вилученого термінала;

– протокол FTP (File Transfer Protocol) для дистанційного доступу до файлів на FTP-Сервері;

– протокол Gopher для пошуку файлів на серверах Gopher і копіювання файлів на робочу станцію клієнта.

При використанні архітектури клієнт-сервер реалізація політики безпеки включає:

– захист трафіка, переданого між серверною та клієнтською стороною;

– розмежування доступу клієнтів до інформаційних ресурсів сервера;

– забезпечення доступності ресурсів сервера.

Враховуючи специфіку побудови клієнт-серверних систем, типові загрози інформаційної безпеки пов’язані з наступними недоліками:

1) недоліки в системі розмежування доступу клієнтів до ресурсів:

– несанкціонований доступ до даних користувачів у результаті відсутності механізмів захисту;

– несанкціонований доступ до облікових записів;

– доступ до ресурсів з використанням позаштатних засобів;

– виключення законного клієнта із сеансу та використання його імені;

– установлення некоректних атрибутів безпеки в обхід адміністратора;

2) недоліки в системі аудита:

– неповна реєстрація подій;

– недостатня пам’ять під журнал аудита;

– несанкціонований доступ до журналу аудита;

3) недоліки в системі аутентифікації:

– компрометація параметрів аутентифікації (перехоплення, відсутність обмежень на число спроб аутентифікації, використання неунікальних ідентифікаторів і т. ін.);

– вибір некоректних параметрів аутентифікації;

4) слабке пророблення організаційних аспектів політики безпеки:

– дозвіл клієнтам встановлювати неконтрольовану кількість сеансів зв’язку із сервером, що може привести до втрати працездатності сервера;

– некоректні дії користувачів;

5) недоліки системи контролю над роботою засобів захисту:

– відсутність контролю над цілісністю програм захисту або ядра операційної системи;

– відсутність реакції засобів захисту від збоїв системі;

– відсутність механізмів відновлення безпечного стану засобів захисту після збоїв;

6) недоліки системи безпеки в цілому:

– слабкий контроль дистанційного доступу або міжмашинної взаємодії;

– недоліки в організації розподілу доменів безпеки;

– помилкова політика безпеки при обробці інформації різних класів;

– відсутність контролю над експортом і імпортом даних у зовнішні системи;

7) недоліки в реалізації механізмів підтримки засобів захисту:

– погана синхронізація годинників у механізмах, що використовують мітки часу;

– недоліки протоколів віддаленої автентифікації та ін.

Підходи до забезпечення безпеки в клієнт-серверних системах:

1) використання засобів захисту прикладного рівня, що використовуються для встановлення захищеного каналу передачі даних між клієнтом і сервером (наприклад, протокол SSL);

2) використання засобів захисту, що реалізують поряд із встановленням захищеного каналу передачі даних прикладного рівня розмежування доступу до ресурсів сервера (наприклад, протокол Kerberos);

3) застосування засобів захисту більш низьких рівнів (наприклад, тунелювання трафіка за допомогою протоколу SKIP). Розмежування доступу при цьому неефективно).

Протокол міжмережного захисту Kerberos

Протокол Kerberos використовується для аутентифікації та обміну сеансовими ключами, призначеними для встановлення захищеного каналу зв'язку між абонентами, що працюють у локальній або глобальній мережі. Протокол розроблений для мереж TCP/IP і побудований на основі довіри учасників протоколу до третьої сторони, роль якої виконує серверна частина Kerberos.

Основу Kerberos становить протокол Нідхема-Шредера із третьою довіреною стороною. Kerberos виступає в ролі арбітра, якому довіряють усі учасники.

У загальному випадку в ролі клієнта виступає користувач. Сервер Kerberos складається фактично із двох серверів – сервера аутентифікації (AS) і сервера видачі дозволів (TGS). Перш ніж клієнт одержить доступ до ресурсів цільового сервера, він повинен пройти перевірку на сервері Kerberos за визначеним протоколом. У протоколі використовуються дві структури даних – дозволу T та аутентифікатора A.

Дозвіл T зашифровується на ключі сервера, який його сформував, і має структуру: T = (B, net_adr, v, СК), де: B – ідентифікатор клієнта, net_adr – мережна адреса клієнта, v – термін дії дозволу, СК – сеансовий ключ для роботи клієнта з одним із серверів.

Аутентифікатор створюється клієнтом для одержання доступу до цільового сервера, він зашифровується на ключі, що надано клієнтові сервером і має структуру: A = (B, net_adr, t, СК), де B – ідентифікатор клієнта, net_adr – мережна адреса клієнта, t – мітка часу, СК – сеансовий ключ для роботи клієнта з одним із серверів.

1. Клієнт B посилає серверу AS запит на одержання «дозволу на видачу дозволу» T1. B →AS: B, <запит на T1>

2. На сервері AS зберігається база даних з даними про клієнта і його секретні ключі. Сервер по імені знаходить у базі даних секретний ключ клієнта Ka та посилає йому дозвіл. AS →B: (СК1)Kb, (T1)Ktgs, де СК1 – сеансовий ключ для зв'язку із сервером TGS, Ktgs – ключ, загальний для серверів AS і TGS.

3. Клієнт розшифровує сеансовий ключ СК1 і відправляє на сервер TGS запит на дозвіл звернутися до цільового сервера. Він зберігає сеансовий ключ і дозвіл. B →TGS: (A1)СК1, (T1)Ktgs.

4. Сервер TGS розшифровує дозвіл T1 за допомогою свого секретного ключа, витягає з нього сеансовий ключ СК1, розшифровує аутентифікатор A, порівнює мережні адреси та перевіряє мітку часу. Сервер TGS також створює сеансовий ключ СК2 для цільового сервера та клієнта і дозвіл на доступ до цільового

сервера Т2. TGS →В: (СК2) СК1, (Т2)Кцс, де Кцс – ключ, загальний для сервера TGS і цільового сервера.

5. Клієнт, одержавши це повідомлення, розшифровує сеансовий ключ СК2 і посилає на цільовий сервер ЦС наступне повідомлення: В →ЦС: (А2)СК2, (Т2)Кцс.

Цільовий сервер виконує перевірки, аналогічні перевіркам сервера TGS на кроці 4. Якщо клієнтові потрібно автентифіціювати цільовий сервер, ЦС повертає йому мітку часу, зашифровану на їх загальному сеансовому ключі: ЦС→В: (t') СК2.

Протокол Secure Socket Layer (SSL)

Протокол SSL широко використовується в технологіях клієнт-сервер. Його основна мета – забезпечити конфіденційність і достовірність між взаємодіючими додатками. Протокол забезпечує:

– автентифікацію (взаємну, однобічну або без неї) з одночасним узгодженням сеансових ключів на основі несиметричних алгоритмів (RSA, Діффі-Геллмана та ін.);

– перевірку цілісності повідомлень на основі геш-функцій (MD5, SHA);

– шифрування повідомлень на основі симетричних механізмів (DES, RC4).

1. Клієнт (ДО). Повідомлення Clienthello містить:

– випадкове число Client.random, яке потім буде використовуватись для перевірок і формування ключового матеріалу;

– унікальний ідентифікатор сеансу;

– список підтримуваних криптоалгоритмів;

– список алгоритмів стиснення.

2. З – ДО: Serverhello. Повідомлення Serverhello містить:

– випадкове число Server.random, яке потім буде використовуватись для перевірок і формування ключового матеріалу;

– унікальний ідентифікатор сеансу;

– обраний зі списку криптоалгоритм;

– обраний зі списку алгоритм стиснення.

3. З – ДО: Server Certificate. Якщо буде проводитися аутентифікація сервера (що звичайно робиться), сервер також передає сертифікат свого відкритого ключа підписи та, можливо, відкритого ключа шифрування, а також параметри для узгодження ключів (наприклад, параметри ключового Діффі-Геллмана).

4. З – ДО: Server Key Exchange. Якщо у сервера немає сертифіката або в сертифікаті міститься тільки відкритий ключ підпису, то сервер передає дане повідомлення. У ньому перебувають параметри алгоритмів з відкритим ключем і ці ж параметри, але підписані сервером. Дані параметри використовуються для обміну ключами. Наприклад, для RSA – це модуль і відкрита експонента, для Діффі-Геллмана – це простий модуль p, що породжує елемент g і відкритий ключ сервера Yc = gxc mod p. Підпис (RSA, DSA) має вигляд: Sign [hash(Client.random+ Server.random+параметри)]. Гешування hash виконується за допомогою алгоритмів MD5 або SHA.

5. З – ДО: Certificate Request. Сервер запитує в клієнта його сертифікат.

6. З – ДО: Server Hellodone. Сервер припинив передачу.

7. ДО – З: Client Certificate. Якщо сервер відіслав повідомлення Certificate Request, то клієнт передає серверу свій сертифікат.

8. ДО – З: Client Key Exchange. У даним повідомленні втримуються параметри, використовувані для обміну ключами. Вони залежать від обраного алгоритму обміну ключами. Наприклад, для RSA клієнт вибирає випадкове секретне число pre_master_secret і зашифровує його на відкритому ключі сервера, отриманому із сертифіката або з повідомлення Server Key Exchange. Для алгоритму Діффі-Геллмана це відкритий ключ клієнта Yк = gXк, якщо він не був включений у сертифікат клієнта.

9. ДО – З: Certificate Verify. Дане повідомлення клієнт передає, щоб сервер міг перевірити сертифікат. Наприклад, при використанні геш-функції MD5 повідомлення має вигляд:

– MD5 (master_secret + pad2 + MD5(handshake_messages + master_secret + pad1), де master_secret – похідна величина, розрахована і клієнтом, і сервером за допомогою згаданих випадкових чисел, випадкового числа pre_master_secret, що генерованого на кроці 8, і геш-функції;

– handshake_messages – усі повідомлення, починаючи з Clienthello;

– pad1, pad2 – певні константи, в стандарті.

10. ДО – З: Finished. Клієнт завершує протокол. Це перше в сеансі повідомлення з використанням нових криптографічних параметрів, наприклад, MD5 (master_secret + pad2 + MD5(handshake_messages + Sender + master_secret + pad1), де Sender – ідентифікатор клієнта.

Аналогічним повідомленням сервер завершує протокол.

На основі згаданих випадкових чисел клієнта, сервера і значення master_secret генерується ключова послідовність, з якої одержують ключі шиф-

рування та ключі формування коду перевірки цілісності, а також векторів ініціалізації для алгоритму DES.

Клієнт і сервер починають обмін прикладними даними. Перед шифруванням і формуванням коду перевірки цілісності дані стискуються відповідно до обраного алгоритму стиску.

Міжмережеві екрани забезпечують безпеку при здійсненні електронного обміну інформацією між взаємодіючими автоматизованими системами і зовнішніми мережами, розмежування доступу між сегментами корпоративної мережі, а також захист від проникнення та втручання в роботу АС порушників із зовнішніх систем. Розглянуті вище типи міжмережевих екранів, що припускають посередництво при встановленні з'єднання (шлюзах рівня з'єднання та прикладного) реалізована так звана технологія Proxy. Ця технологія широко поширена і застосовується в таких відомих моделях міжмережевих екранів, як Microsoft Proxy Server і Cyberguard Firewall.

Однак для вироблення рішень про дозвіл того або іншого з'єднання для служб TCP/IP (тобто пропустити, заборонити, аутентифіцірувати, зробити запис про це в журналі), міжмережеві екрани повинні вміти одержувати, зберігати, витягати і маніпулювати інформацією із усіх рівнів моделі та з її додатків.

1.4.2. Захист мереж на основі протоколів TCP/IP

Як правило, при спілкуванні з зовнішніми мережами використовується виняткове сімейство протоколів TCP/IP. Тому зовнішній міжмережевий екран повинен враховувати специфіку цих протоколів. При розгляді цього питання, яке стосується мережевих технологій, основою служить семирівнева еталонна модель ISO/OSI.

Відповідно й міжмережеві екрани також класифікуються по тому, на якому рівні виробляється фільтрація – канальному, мережному, транспортному чи прикладному. Відповідно, можна говорити про концентратори, що екранують, (рівень 2), маршрутизатори (рівень 3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.

Природа екранування (фільтрації), як механізму безпеки, дуже глибока. Крім блокування потоків даних, що порушують політику безпеки, міжмережевий екран може ховати інформацію про мережу, що захищається, тим самим ускладнюючи дії потенційних зловмисників. Так, прикладний екран може здійснювати дії від імені суб'єктів внутрішньої мережі, у результаті чого з зовнішньої мережі

здається, що має місце взаємодія виняткова з міжмережевим екраном. При такому підході топологія внутрішньої мережі схована від зовнішніх користувачів, тому задача зловмисника істотно ускладнюється.

Реалізація загроз інформації у мережах на основі протоколів TCP/IP

У мережах (розподілених системах) на основі протоколів TCP/IP можливий широкий спектр загроз, які реалізуюся через атаки, які будемо називати віддаленими, щоб підкреслити міжмережевий характер взаємодії.

Типова віддалена атака це віддалений інформаційний руйнуючий вплив, програмно здійснюваний по каналах зв'язку і характерний для будь-якої розподіленої автоматизованої системи.

Класифікація віддалених атак.

1. По характеру впливу:

– пасивні;

– активні.

2. По меті впливу:

– порушення конфіденційності інформації або ресурсів системи;

– порушення цілісності інформації (приклад: впровадження хибного об'єкта);

– порушення працездатності (доступності) (приклад: відмова в обслуговуванні).

3. За умовою початку здійснення впливу:

– віддалений вплив, також як і будь-який, може здійснюватися тільки за певних умов. У розподілених автоматизованих системах існують три види умов початку здійснення віддаленої атаки:

– напад по запиту від об'єкта, що атакується. У цьому випадку атакуючий очікує передачі від потенційного об'єкта атаки запиту певного типу, який і буде умовою початку здійснення впливу;

– напад по настанню очікуваної події на об'єкті, що атакується. У цьому випадку атакуючий здійснює постійне спостереження за станом операційної системи потенційного об'єкту атаки і при виникненні певної події в цій системі починає вплив;

– безумовний напад. У цьому випадку початок здійснення атаки безумовно стосовно потенційного об'єкту нападу, тобто напад здійснюється негайно і безвідносно до стану системи об'єкту, що атакується.

4. По наявності зворотного зв'язку з об'єктом, що атакується:

– зі зворотним зв'язком;

– без зворотного зв’язку (односпрямована атака).

Віддалена атака, яка здійснюється при наявності зворотного зв’язку з об’єктом, що атакується, характеризується тим, що на деякі запити, передані на об’єкт, що атакується, потрібно одержати відповідь, а, отже, між атакуючим і об’єктом нападу існує зворотний зв’язок, який дозволяє атакуючому адекватно реагувати на всі зміни, що відбуваються на об’єкті, що атакується. Подібні віддалені атаки найбільш характерні для розподілених автоматизованих систем.

На відміну від атак зі зворотним зв’язком віддаленим атакам без зворотного зв’язку не потрібно реагувати на зміни, які відбуваються на об’єкті, що атакується. Атаки даного виду звичайно здійснюються передачею одиночних запитів на об’єкт, що атакується, відповіді на які атакуючому не потрібні (приклад: відмова в обслуговуванні).

5. По розташуванню суб’єкта атаки щодо об’єкта, що атакується:

– внутрішньо-сегментні;

– межсегментні.

З погляду віддаленої атаки надзвичайно важливо, як по відношенню друг до друга розташовуються суб’єкт і об’єкт атаки, тобто в одному або в різних сегментах вони перебувають. Межсегментний віддалений напад представляє набагато більшу небезпеку, ніж внутрішньо-сегментний. Це пов’язане з тим, що у випадку межсегментного нападу об’єкт та безпосередньо атакуючий можуть перебувати на відстані багатьох тисяч кілометрів друг від друга, що може суттєво перешкодити заходам щодо відбиття атаки.

6. За рівнем еталонної моделі ISO/OSI, за яким здійснюється вплив.

Будь-який мережевий протокол обміну, як і будь-яку мережеву програму, можна з тим або іншим ступенем точності проектування еталонної моделі OSI. Віддалена атака також є мережевою програмою. У зв’язку із цим логічно розглядати віддалені атаки на розподілені автоматизовані системи, проектуючи їх на еталонну модель ISO/OSI.

Розглянемо деякі механізми реалізації типових віддалених атак.

Аналіз мережевого трафіка

Аналіз мережевого трафіка дозволяє, по-перше, вивчити логіку роботи розподіленої системи шляхом перехоплення і аналізу пакетів обміну на канальному рівні. Це дозволяє на практиці моделювати та здійснювати типові віддалені атаки.

Аналіз мережевого трафіка дозволяє перехопити потік даних, якими обмінюються об’єкти, наприклад, ім’я та пароль користувача, що пересилаються в

незашифрованому вигляді по мережі.

По характеру впливу аналіз мережевого трафіка є пасивним впливом; без зворотного зв'язку, веде до порушення конфіденційності інформації усередині одного сегмента мережі на канальному рівні OSI. При цьому початок здійснення атаки безумовно стосовно об'єкту атаки.

Однією із проблем безпеки розподіленої автоматизованої системи є недостатня ідентифікація і автентифікація її віддалених один від одного об'єктів. Як відомо, для адресації повідомлень у розподілених автоматизованих систем використовується мережева адреса, яка унікальна для кожного об'єкту системи (на канальному рівні моделі OSI – це апаратна адреса мережного адаптера, на мережному рівні – адреса визначається залежно від використовуваного протоколу мережевого рівня (наприклад, IP-адреса). Однак мережева адреса досить просто підробляється, тому використовувати її як єдиний засіб ідентифікації об'єктів неприпустимо.

При неефективних протоколах автентифікації існують два різновиди нападів:

– напад при встановленому віртуальному каналі;

– напад без встановленого віртуального каналу.

У випадку встановленого віртуального з'єднання атака буде полягати в присвоєнні прав довіреного суб'єкта взаємодії, що легально підключився до об'єкта системи. Це дозволить атакуючому здійснити сеанс роботи з об'єктом розподіленої системи від імені довіреного суб'єкта (маскарад).

Для службових повідомлень у розподілених автоматизованих системах часто використовується передача одиночних повідомлень, що не вимагають підтвердження, тобто не потрібне створення віртуального з'єднання. Напад без встановленого віртуального з'єднання полягає в передачі службових повідомлень від імені мережевих керуючих пристроїв, наприклад, від імені маршрутизаторів. Ідентифікація пакетів без встановленого віртуального каналу можлива лише по мережній адресі відправника, яку легко підробити.

Посилка неправильних керуючих повідомлень може привести до серйозних порушень роботи розподілених автоматизованих систем (наприклад, до зміни конфігурації).

Підміна довіреного об'єкта є активним впливом, з метою порушення конфіденційності і цілісності інформації, по настанню певної події на об'єкті, що атакується. Даний напад може бути як внутрішньо сегментним, так і міжсегментним, як зі зворотним зв'язком, так і без зворотного зв'язку з об'єктом, що атакується, і здійснюється на мережному та транспортному рівнях моделі OSI.

Неправильний об'єкт розподіленої віддаленої системи

У тому випадку, якщо в розподіленій віддаленій системі недостатньо надійно вирішені проблеми ідентифікації мережевих керуючих пристроїв (наприклад, маршрутизаторів), можливий напад, пов'язаний зі зміною маршрутизації та впровадженням у систему хибного об'єкта.

Кожний маршрутизатор має таблицю маршрутизації, у якій для кожного адресата вказується оптимальний маршрут. Для забезпечення ефективної і оптимальної маршрутизації в розподілених віддалених системах застосовуються спеціальні керуючі протоколи, що дозволяють маршрутизаторам обмінюватися інформацією один з одним і віддалено управляти маршрутизаторами (наприклад, протокол SNMP (Simple Network Management Protocol)). Дані протоколи дозволяють віддалено змінювати маршрутизацію в мережі інтернет, що дозволяє змінити вихідну маршрутизацію.

Для зміни маршрутизації атакуючому необхідно послати по мережі спеціальні службові повідомлення від імені мережних керуючих пристроїв (наприклад, маршрутизаторів). У результаті успішної зміни маршруту атакуючий одержить повний контроль над потоком інформації, якою обмінюються два об'єкти розподіленої автоматизованої системи.

Нав'язування хибного маршруту

Така типова віддалена атака може здійснюватися як усередині одного сегменту, так і міжсегментно, як зі зворотним зв'язком, так і без зворотного зв'язку з об'єктом, що атакується, на транспортному та прикладному рівні моделі OSI.

Відмова в обслуговуванні

Одним з основних завдань, покладених на мережеву операційну систему, що функціонує на кожному з об'єктів розподіленої віддаленої системи, є забезпечення надійного дистанційного доступу з будь-якого об'єкта мережі до даного об'єкта. Звичайно в обчислювальних мережах можливість надання дистанційного доступу реалізується в такий спосіб: на об'єкті мережі в мережевій операційній системі запускаються на виконання ряд програм-серверів (наприклад, FTP-сервер, WWW-сервер і т. ін.), що надають дистанційний доступ до ресурсів даного об'єкту. Завдання сервера полягає в тому, щоб постійно очікувати запиту на підключення від віддаленого об'єкта. У випадку одержання подібного запиту сервер повинен по можливості передати на об'єкт, що зробив запит, відповідь у якій або дозволити підключення, або ні.

Мережева операційна система через ряд обмежень здатна мати тільки обмежене число відкритих віртуальних з'єднань і відповідати лише на обмежене число запитів. При нескінченому числі анонімних запитів можливий напад типу «відмова в обслуговуванні». Результатом нападу є порушення на атакованому об'єкті працездатності служби надання дистанційного доступу.

Інший варіант цього нападу – передача такої кількості запитів на об'єкт, що атакується, яке дозволить трафік (спрямований «шторм» запитів). Виникає як переповнення черги запитів і відмови однієї з телекомунікаційних служб, так і повна зупинка комп'ютера через неможливість системи займатися нічим іншим, крім обробки запитів.

Третій варіант – передача на об'єкт, що атакується, некоректного, спеціально підібраного запиту. У цьому випадку при наявності помилок у віддаленій системі можливе зациклення процедури обробки запиту, переповнення буфера з наступним зависанням системи (приклад: «Ping Death»).

Цей напад є активним впливом, здійснюваним з метою порушення працездатності системи, безумовно щодо мети атаки. Цей напад є односпрямованим впливом, як міжсегментним, так і внутрішньо сегментним, здійснюваним на транспортному та прикладному рівнях моделі OSI.

Мережеві екрани у мережах на основі протоколів TCP/IP

Міжмережевий екран (брандмауер) це програмний (апаратний, програмно-апаратний) комплекс, який установлюється на границі мережі і регулює доступ до ресурсів мережі. Міжмережевий екран аналізує та збирає інформацію про зовнішні, стосовно мережі, пакети і сеанси. Відповідно до прийнятих правил Міжмережевий екран пропустить або не пропустить конкретний пакет, дозволить або не дозволить організувати конкретний сеанс.

Міжмережевий екран зазвичай реалізує наступні типи політики:

1. Дозволити будь-яку послугу, якщо вона явно не заборонена.
2. Відмовити в будь-якій послузі, якщо вона явно не дозволена.

Одна з головних функцій міжмережевого екрану – фільтрація пакетів. Фільтрація IP-пакетів зазвичай виконується у фільтруючому маршрутизаторі. Маршрутизатор зазвичай фільтрує IP-пакети на основі наступних атрибутів (усіх або деяких):

– IP-адреса відправника;
– IP-адреса одержувача;
– TCP/UDP-порт відправника;
– TCP/UDP-порт одержувача.

Існує багато способів використання фільтрації для блокування підключень із/до різних хостів або мереж. У системі може знадобитися блокування підключень із певних адрес, наприклад, з недружніх або недовірених хостів або систем. Крім того, може знадобитися блокування всіх зовнішніх для системи адрес (за певним виключенням, наприклад, для SMTP для одержання електронної пошти). Може знадобитися блокування всіх вхідних з'єднань із усіма хостами за винятком декількох пов'язаних із брандмауером підсистем. Цим підсистемам система дозволяються лише певні послуги, наприклад SMTP для однієї з них і TELNET або FTP для іншої. Використовуючи фільтрацію TCP або UDP-портів, маршрутизатор фільтрації пакетів або хост із такою можливістю може безпосередньо реалізувати цю політику.

Фільтруючі маршрутизатори мають ряд недоліків. Для того, щоб протистояти слабкостям маршрутизаторів фільтрації пакетів, у брандмауерах потрібно використовувати програмні додатки для фільтрації таких послуг, як TELNET і FTP. Такі додатки називають proxy-послугою, а хост, що виконує proxy-послугу прикладним шлюзом. Можна комбінувати прикладні шлюзи та маршрутизатори фільтрації пакетів, щоб одержати більш високі рівні безпеки, чим при роздільному використанні.

Розглянемо приклади реалізації міжмережевих екранів:

– з фільтрацією пакетів;

– з подвійним шлюзом;

– з ізольованим хостом;

– з ізольованої підмережею.

Міжмережевий екран з фільтрацією пакетів

Брандмауер з фільтрацією пакетів є найпоширенішим і простим для реалізації в невеликих та простих системах. По суті, установлюється маршрутизатор фільтрації пакетів на інтернет-шлюзі (або будь-який підмережі), і потім конфігуруються правила фільтрації для блокування або фільтрації протоколів і адрес. Звичайно блокуються небезпечні по своїй суті послуги, такі як NIS, NFS і X Windows.

Брандмауер з фільтрацією пакетів має ряд недоліків:

– недостатні або взагалі відсутні реєстраційні можливості, у силу чого адміністраторові складно визначити компрометацію або напад на маршрутизатор;

– правила фільтрації пакетів часто занадто складні для перевірки, що може піддати систему ризику з боку неперевірених слабких місць;

– при занадто складних правилах фільтрації ускладнюється управління ними.

Міжмережевий екран з подвійним шлюзом

Міжмережевий екран з подвійним шлюзом складається з хоста із двома мережевими інтерфейсами з відключеною функцією IP-передачі (тобто, за замовченням хост більше не може направляти пакети між двома підключеними мережами). Крім того, для додаткового захисту на місці підключення до інтернету можна помістити маршрутизатор фільтрації пакетів. Це створює внутрішню ізольовану підмережу, яку можна використовувати для розміщення таких спеціалізованих систем, як інформаційні сервери і групи модемів.

На відміну від міжмережевого екрану з фільтрацією пакетів, подвійний шлюз повністю блокує IP-трафік між інтернетом та системою, що захищається. Послуги та доступ забезпечуються proxy-серверами на прикладному шлюзі.

Здатність хоста ухвалювати маршрутизовні відправником пакети відключається, тому ніякі інші пакети не передаються хостом у захищену підмережу. При цьому може досягатися високий ступінь безпеки, тому що маршрути до захищеної підмережі повинні бути відомі тільки міжмережевому екрані, але не інтернет-системам (інтернет-системи не можуть направляти пакети безпосередньо в захищені системи). Імена та IP-адреси систем будуть сховані від інтернет-систем, тому що брандмауер не передає інформацію DNS.

Міжмережевий екран з подвійним шлюзом так само, як і міжмережевий екран з ізольованої підмережею, описуваний нижче, може відокремлювати трафік, що має відношення до інформаційного сервера, від іншого вхідного і вихідного трафіка. Інформаційний сервер можна розмістити в підмережі між шлюзом і маршрутизатором. Таке розміщення інформаційного сервера підвищує безпеку всієї системи, оскільки, при будь-яких нападах порушників на цей сервер системи, ресурси як і раніше захищені подвійним шлюзом.

Негнучкість подвійного шлюзу може стати недоліком у деяких системах.

Міжмережевий екран з ізольованим хостом

Міжмережевий екран з ізольованим хостом більш гнучкий, ніж міжмережевий екран з подвійним шлюзом, однак це досягається ціною безпеки. Даний міжмережевий екран часто прийнятний для вузлів, де потрібні більш гнучкі засоби, ніж міжмережевий екран з подвійним шлюзом.

Міжмережевий екран з ізольованим хостом поєднує маршрутизатор з фільтрацією пакетів і прикладний шлюз, розміщений стосовно маршрутизатора з

боку захищеної підмережі. Прикладному шлюзу потрібен тільки один мережевий інтерфейс. Proxy-послуги шлюзу будуть пропускати в систему TELNET, FTP і інші послуги. Маршрутизатор фільтрує або ізолює небезпечні по своїй сутності протоколи, не пропускаючи їх на прикладний шлюз і в систему. Він відкидає (або пропускає) прикладний трафік у відповідності з наступними правилами:

– пропускає трафік, спрямований з вузлів інтернету на прикладний шлюз;

– не пропускає інший трафік з вузлів інтернету;

– не пропускає будь-який трафік із системи крім трафіка із прикладного шлюзу.

На відміну від міжмережевого екрану з подвійним шлюзом, прикладному шлюзу потрібен тільки один мережевий інтерфейс і не потрібна окрема підмережа між ним і маршрутизатором. Це забезпечує більшу гнучкість і меншу безпеку, тому що маршрутизатор може пропускати деякі «довірені» послуги в обхід прикладного шлюзу безпосередньо в систему.

Міжмережевий екран з ізольованої підмережею

Це варіант міжмережевого екрану, що поєднує міжмережевий екран з подвійним шлюзом та ізольованим хостом. Два фільтруючі маршрутизатори створюють ізольовану підмережу. Для маршрутизатора, що перебуває з боку інтернету, діють такі правила:

– пропускати трафік із прикладного шлюзу, поштового сервера;

– пропускати з боку інтернет-трафік на прикладний шлюз і поштовий сервер;

– пропускати трафік (FTP, gopher) на інформаційний сервер;

– інший трафік відкидається.

За аналогією працює і внутрішній маршрутизатор.

Маршрутизатори використовуються для напрямку трафіка на певну систему, тому не потрібен подвійний прикладний шлюз. Ізольована підмережа підходить для систем з високим навантаженням і швидкістю трафіка.

На шляху порушника вартують два маршрутизатори.

Для гнучкості можна дозволити проходження між маршрутизаторами трафіка «довірених» служб, але це знижує безпеку. Недолік полягає і у великому навантаженні на маршрутизатор.

Принципи побудови мереж VPN

Одним з варіантів організації міжмережевої взаємодії є створення приватних віртуальних мереж (VPN – Virtual Private Networks). VPN поєднує територіально рознесені локальні мережі однієї або декількох організацій у єдину інформаційно-обчислювальну мережу. У якості транспортного компонента VPN можуть виступати виділені канали, що і комутуються, однак найбільш показовим прикладом на сьогоднішній день є використання транспорту глобальної мережі інтернет.

Використання каналів глобальних мереж передачі даних, що комутуються, забезпечує гнучкість, масштабність і універсальність при побудові VPN. Наприклад, розширення інтернету дозволило підключатися до локальних мереж організацій віддаленим користувачам.

Зазвичай виділяють VPN двох типів:

– VPN, що поєднують територіально рознесені локальні обчислювальні мережі у єдину мережу;

– VPN, що дозволяють підключатися віддаленим робочим станціям до мережі організації.

Найбільш актуальне питання безпеки стало для VPN, де в якості транспортного протоколу використовується стек протоколів TCP/IP. У мережах такого типу захищені дані передаються у вигляді інформаційних пакетів по протоколу IP або IPX.

Для передачі інформації з мереж VPN використовуються спеціальні протоколи, у числі яких слід згадати наступні:

– протокол трансляції канального рівня Layer 2 Forwarding Protocol;

– протокол тунелювання канального рівня Layer 2 Tunneling Protocol;

– протокол тунелювання між вузлами PPTP (Poit-to-Point Tunneling Protocol);

– протокол Ipsec (IP Security);

– протокол SKIP (Simple Key Management for Internet Protocol).

Відповідно до цих протоколів пакети мережного рівня інкапсулюються в пакети протоколу канального рівня PPP (Point-to-Point Protocol) і передаються адресатові.

Для VPN характерні усі раніше розглянуті загрози, характерні для каналів передачі даних і міжмережевої взаємодії. Відповідно, і механізми захисту повинні забезпечити стандартний набір функцій захисту: шифрування трафіка або

пакетів, автентифікацію учасників обміну, цілісність і імітозахист даних, маскування трафіка, а також контроль доступу віддалених користувачів до ресурсів мережі.

Реалізовані засоби захисту не повинні створювати «вузьких» місць у мережі, тобто не повинні суттєво впливати на масштабованість, продуктивність мережі, маршрутизацію, а також повинні забезпечити централізоване адміністрування та аудит, ефективний розподіл ключів.

Серед рішень, що застосовуються для захисту інформації в VPN, можна відзначити міжмережеві екрани і засоби шифрування IP-трафіка. Засоби шифрування IP-трафіка реалізуються у вигляді програмно-апаратних комплексів або програмно.

Міжмережевий екран і програмно-апаратних комплекс доцільно застосовувати для захисту з'єднань типу локальна обчислювальна мережа – локальна обчислювальна мережа, тому що апаратна реалізація забезпечує більш високу продуктивність, ніж лише програмні засоби. Якщо міжмережевий екран здійснює в основному фільтрацію пакетів, то програмно-апаратний комплекс підтримує увесь спектр механізмів захисту, тобто шифрування, вироблення контрольних сум і імітовставок з одночасним вирішенням питань управління ключами.

Як приклад можна привести три схеми включення програмно-апаратних комплексів:

– проста схема з використанням маршрутизатора;

– схема із прямим підключенням;

– ієрархічна схема для великих мереж з різними рівнями безпеки.

Програмні засоби захисту застосовують в основному для захисту з'єднань типу локальна обчислювальна мережа – віддалений користувач.

Основні служби інтернету

Інтернет і TCP/IP надають ряд послуг. Найбільш часто використовується електронна пошта (e-mail), реалізована на основі протоколу SMTP (Simple Mail Transfer Protocol). Широко використовується TELNET (емуляція терміналу) для доступу віддалених терміналів і FTP (протокол передачі файлів, File Transfer Protocol). Крім того, існує ряд служб і протоколів для віддаленої печатки, віддаленого колективного використання файлів і дисків, управління розподіленими базами даних і інформаційних послуг:

– SMPT – простий протокол електронної пошти, використовується для передачі та отримання електронної пошти;

– TELNET – використовується для підключення віддалених систем, підключених через мережу, заснована на емуляції терміналу;

– FTP – протокол передачі файлів, використовується для одержання або передачі і зберігання файлів у мережевій системі;

– DNS (Domain Name Service) – служба найменування доменів, використовується TELNET, FTP і іншими службами для перетворення імен хостів в адреси IP.

Інформаційні послуги:

– gopher – інформаційний браузер і сервер, що забезпечує дружній інтерфейс з іншими інформаційними послугами;

– WAIS (Wide Area Information Service) – глобальна інформаційна служба, використовується для індексування та пошуку у файлових базах даних;

– WWW (World Wide Web) включає FTP, gopher, WAIS і інші інформаційні послуги; популярним клієнтом WWW є Mosaic.

Послуги на основі віддаленого виклику процедури (RPC):

– NFS (Network File System) – мережева файлова система, дозволяє системам колективно використовувати каталоги та диски, дозволяє використовувати віддалений каталог або диск у якості локального;

– NIS (Network Information Services) – мережеві інформаційні послуги, дозволяють декільком системам колективно використовувати бази даних, наприклад, файл паролів, з метою централізованого управління;

– система X Window – графічна віконна система та набір прикладних бібліотек для використання на робочих станціях;

– rlogin, rsh і інші «r»-послуги –концепція віддаленого виконання команд без пароля.

Запитання для самоконтролю

1. Види та властивості інформації, як предмета захисту.

2. Дайте визначення поняттю інформація з обмеженим доступом, конференційна інформація.

3. Які властивості повинна мати інформація?

4. Якими характерними особливостями повинна володіти інформація?

5. Передумови збільшення інформаційних технологій?

6. Яким чином забезпечується безпека нових типів інформаційних ресурсів?

7. Яким чином забезпечується організація довіреної взаємодії сторін в інформаційному просторі?

8. Яким чином забезпечується захист від автоматичних засобів нападу?

9. Які існують принципи організації інформаційної безпеки?

10. Перелічіть організаційні принципи захисту даних?

11. За якими принципами повинна відбуватися побудова системи забезпечення безпеки інформації в АС?

12. Моделі управління мережевими ресурсами? Поняття моделі управління робочою групою та доменна модель управління.

13. Яким чином відбувається реалізація загроз інформації у мережах на основі протоколів TCP/IP?

14. Дайте визначення поняття «віддалена атака»? Яким чином класифікуються атаки на розподілені автоматизовані системи?

15. Тенденції розвитку і застосування методів і засобів захисту інформації в телекомунікаційних системах.

16. Захист інформації в корпоративних мережах.

17. Принципи та методи надання доступу до інформаційних ресурсів.

18. Профіль безпеки стандарту OSI/ISO 15408.

19. Загальні відомості про системи виявлення вторгнень.

20. Визначення типів систем виявлення вторгнень. Визначення цілей застосування та об'єкти моніторингу IDS. Практика застосування політики IDS.

ГЛАВА 2.
МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

2.1. Тенденції розвитку безпекових мережевих технологій

Протягом багатьох років в організаціях переважали локальні обчислювальні мережі (ЛОМ), з функціями спільного використання даних, підключення до мережі додаткових пристроїв, наприклад принтера. Далі ЛОМ об'єднувалися один з одним, в результаті з'явився новий тип – так звані територіальні розподілені мережі (ТРМ). Ці мережі дозволяють здійснювати обмін інформацією усередині географічно розрізнених організацій.

Нині існує велика кількість ТРМ, серед яких найбільш відомі *Internet*, *Relcom* та *Sovintel*, а також спеціалізовані мережі.

Глобальною інформаційною супермагістраллю, покликаною зв'язати розрізнені комп'ютерні системи є інтернет. Спочатку створена як мережа ARPANET, після чого національний науковий фонд США для з'єднання в мережу великого числа науково-дослідних установ і розвитку міжнародної кооперації заснував проект NSFNET. З 1990 року мережа ARPANET припинила своє існування, а мережа інтернет поширилася за межі академічного світу; запропонувавши суспільству одночасно доступ до інформації і швидкий глобальний засіб зв'язку. Комп'ютери, включені в мережу можуть використати одну з наступних операційних систем: Windows – 9X, NT, NetWare, OS/2, Mac OS, UNIX. Швидкість обміну даними залежить від багатьох умов, серед яких конфігурація комп'ютера, мережі, навички користувачів. Обмін даними здійснюється за допомогою веббраузера у клієнта, мережевих протоколів (TCP/IP) і сервера HTTP (Hyper – Text Transfer Protocol).

Тенденції розвитку методів і засобів захисту інформації

Мета заходів в *сфері інформаційної безпеки – захистити інтереси суб'єктів інформаційних стосунків***.** Інтереси ці різноманітні, але усі вони концентруються навколо трьох основних аспектів:

– доступність;

– цілісність;

– конфіденційність.

Перший крок при побудові системи ІБ організації – ранжирування і деталізація цих аспектів.

Важливість проблематики ІБ пояснюється двома головними причинами:

– цінністю накопичених інформаційних ресурсів;

– критичною залежністю від інформаційних технологій.

Руйнування важливої інформації, крадіжка конфіденційних даних, перерва в роботі внаслідок відмови – усе це виливається у великі матеріальні втрати, завдає збитку репутації організації. Проблеми з системами управління або медичними системами погрожують здоров'ю і життю людей.

Сучасні інформаційні системи складні, а значить, і небезпечні вже самі по собі, навіть без урахування активності зловмисників. Постійно виявляються нові вразливі місця в програмному забезпеченні. Доводиться брати до уваги надзвичайно широкий спектр апаратного і програмного забезпечення, численні зв'язки між компонентами.

Змінюються принципи побудови корпоративних ІС. Використовуються численні зовнішні інформаційні сервіси; надаються власне ззовні; отримало широке поширення явище, що визначається словом «аутсорсинг», коли частина функцій корпоративної ІС передається зовнішнім організаціям. Розвивається програмування з активними агентами.

Підтвердженням складності проблематики ІБ є паралельний (і досить швидкий) ріст витрат на захисні заходи і кількості порушень ІБ у поєднанні з ростом середнього збитку від кожного порушення. (Остання обставина – ще один аргумент на користь важливості ІБ.)

Успіх в області інформаційної безпеки може принести тільки комплексний підхід, що поєднує заходи чотирьох рівнів:

– законодавчого;

– адміністративного;

– процедурного;

– програмно-технічного.

Проблема ІБ – не лише і не стільки технічна; без законодавчої бази, без постійної уваги керівництва організації і виділення необхідних ресурсів, без заходів управління персоналом і фізичного захисту вирішити її неможливо. Комплексність також ускладнює проблематику ІБ; потрібна взаємодія фахівців з різних областей.

В якості основного інструменту боротьби зі складністю пропонується об'єктно-орієнтований підхід**.** Інкапсуляція**,** спадкоємство**,** поліморфізм**,** виділення граней об'єктів, варіювання рівня деталізації – усе це універсальні поняття, знання яких потрібне усім фахівцям з інформаційної безпеки.

Законодавчий, адміністративний і процедурний рівні

Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки. Необхідно всіляко підкреслювати важливість проблеми ІБ; сконцентрувати ресурси на найважливіших напрямах досліджень; зорієнтувати освітню діяльність; створити і підтримувати негативне відношення до порушників ІБ – усе це функції законодавчого рівня.

На законодавчому рівні особливої уваги заслуговують правові акти і стандарти. На цьому фоні повчальним є знайомство із законодавством США в області ІБ, яке набагато більше і багатогранніше російського.

Серед стандартів виділяються «Помаранчева книга», рекомендації X.800 і «Критерії оцінки безпеки інформаційних технологій».

«Помаранчева книга» заклала понятійний базис; у ній визначаються найважливіші сервіси безпеки і пропонується метод класифікації інформаційних систем за вимогами безпеки.

Рекомендації X.800 дуже глибоко трактують питання захисту мережевих конфігурацій і пропонують розвинений набір сервісів і механізмів безпеки.

Міжнародний стандарт ISO 15408, відомий як «Загальні критерії», реалізує сучасніший підхід, в нім зафіксований надзвичайно широкий спектр сервісів безпеки (представлених як функціональні вимоги). Його прийняття як національний стандарт важливе не лише з абстрактних міркувань інтеграції у світову спільноту; воно, як можна сподіватися, полегшить життя власникам інформаційних систем, істотно розширивши спектр доступних сертифікованих рішень.

Головне завдання заходів адміністративного рівня – сформувати програму робіт в області інформаційної безпеки і забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ.

Основою програми є політика безпеки, що відбиває підхід організації до захисту своїх інформаційних активів.

Розробка політики і програми безпеки розпочинається з аналізу ризиків, першим етапом якого, у свою чергу, являється ознайомлення з найбільш поширеними загрозами.

Головні загрози – внутрішня складність ІС, неумисні помилки штатних користувачів, операторів, системних адміністраторів і інших осіб, обслуговуючих інформаційні системи.

На другому місці за розміром збитку стоять крадіжки і підлоги.

Реальну небезпеку представляють пожежі і інші аварії підтримувальної інфраструктури.

У загальному числі порушень росте доля зовнішніх атак, але основного збитку як і раніше завдають «свої».

Для переважної більшості організацій досить загального знайомства з ризиками; орієнтація на типові, апробовані рішення дозволить забезпечити базовий рівень безпеки при мінімальних інтелектуальних і розумних матеріальних витратах.

Істотну допомогу в розробці політики безпеки може зробити британський стандарт BS 7799:1995, що пропонує типовий каркас.

Розробка програми і політики безпеки може слугувати прикладом використання поняття рівня деталізації. Вони повинні підрозділятися на декілька рівнів, що трактують питання різної міри специфічності. Важливим елементом програми є розробка і підтримка в актуальному стані карти ІС.

Необхідною умовою для побудови надійного, економічного захисту є розгляд життєвого циклу ІС і синхронізація з ним заходів безпеки. Виділяють наступні етапи життєвого циклу:

– ініціація;
– закупівля;
– установка;
– експлуатація;
– виведення з експлуатації.

Безпеку неможливо додати до системи; її треба закладати із самого початку і підтримувати до кінця.

Заходи процедурного рівня орієнтовані на людей (а не на технічні засоби) і підрозділяються на наступні види:

– управління персоналом;
– фізичний захист;
– підтримка працездатності;
– реагування на порушення режиму безпеки;
– планування відновних робіт.

На цьому рівні застосовні важливі принципи безпеки:

– безперервність захисту у просторі та часі;
– розділення обов’язків;
– мінімізація привілеїв.

Тут також застосовні об’єктний підхід і поняття життєвого циклу. Перший дозволяє розділити контрольовані сутності (територію, апаратуру і так далі) на відносно незалежні підоб’єкти, розглядаючи їх з різною мірою деталізації і контролюючи зв’язки між ними.

Поняття життєвого циклу корисно застосовувати не лише до інформаційних систем, але і до співробітників. На етапі ініціації має бути розроблений опис посади з вимогами до кваліфікації і комп'ютерними привілеями, що виділяються. На етапі установлення необхідно провести навчання, у тому числі з питань безпеки; на етапі виведення з експлуатації слід діяти обережно, не допускаючи нанесення збитку скривдженими співробітниками.

Інформаційна безпека багато в чому залежить від обережного ведення поточної роботи, яка включає:

– підтримку користувачів;

– підтримку програмного забезпечення;

– конфігураційне управління;

– резервне копіювання;

– управління носіями;

– документування;

– регламентні роботи.

Елементом повсякденної діяльності є відстежування інформації в області ІБ; як мінімум, адміністратор безпеки повинен підписатися на список розсилки по нових пропусках в захисті (і своєчасно знайомитися з повідомленнями, що надходять).

Треба, проте, заздалегідь готуватися до подій неординарних, тобто до порушень ІБ. Заздалегідь продумана реакція на порушення режиму безпеки переслідує три головних мети:

– локалізація інциденту і зменшення шкоди, що завдається;

– виявлення порушника;

– попередження повторних порушень.

Виявлення порушника – процес складний, але перший і третій пункти можна і треба ретельно продумати і відпрацювати.

У разі серйозних аварій потрібне проведення відновних робіт. Процес планування таких робіт можна розділити на наступні етапи:

– виявлення критично важливих функцій організації, встановлення пріоритетів;

– ідентифікація ресурсів, необхідних для виконання критично важливих функцій;

– визначення переліку можливих аварій;

– розробка стратегії відновних робіт;

– підготовка до реалізації вибраної стратегії;

– перевірка стратегії.

Програмно-технічні заходи

Програмно-технічні заходи, тобто заходи, спрямовані на контроль комп'ютерних сутностей: устаткування, програм і/або даних, утворюють останній і найважливіший рубіж інформаційної безпеки.

На цьому рубежі стають очевидними не лише позитивні, але і негативні наслідки швидкого прогресу інформаційних технологій. По-перше, додаткові можливості з'являються не лише у фахівців з ІБ, але і у зловмисників. По-друге, інформаційні системи увесь час модернізуються, перебудовуються, до них додаються недостатньо перевірені компоненти (в першу чергу програмні), що ускладнює дотримання режиму безпеки.

Тенденції побудови архітектури безпеки інформації

Заходи безпеки доцільно розділити на наступні види:

– превентивні, перешкоджаючі порушенням ІБ;

– заходи виявлення порушень;

– локалізуючі, звужуючі зону дії порушень;

– заходи по виявленню порушника;

– заходи відновлення режиму безпеки.

У продуманій архітектурі безпеки усі вони мають бути присутніми.

З практичної точки зору важливими також є наступні принципи архітектурної безпеки:

– безперервність захисту у просторі та часі, неможливість минути захисні засоби;

– наслідування визнаних стандартів, використання апробованих рішень;

– ієрархічна організація ІС з невеликим числом сутностей на кожному рівні;

– посилення найслабкішої ланки;

– неможливість переходу в небезпечний стан;

– мінімізація привілеїв;

– розділення обов'язків;

– ешелонування оборони;

– різноманітність захисних засобів;

– простота і керованість інформаційної системи.

Центральним для програмно-технічного рівня є поняття сервісу безпеки. До числа таких сервісів входять:

– ідентифікація та автентифікація;

– управління доступом;
– протоколювання і аудит;
– шифрування;
– контроль цілісності;
– екранування;
– аналіз захищеності;
– забезпечення відмовостійкості;
– забезпечення безпечного відновлення;
– тунелювання;
– управління.

Ці сервіси повинні функціонувати у відкритому мережевому середовищі з різнорідними компонентами, тобто бути стійкими до відповідних загроз, а їх застосування має бути зручним для користувачів і адміністраторів. Наприклад, сучасні засоби ідентифікації/автентифікації мають бути стійкими до пасивного і активного прослуховування мережі і підтримувати концепцію єдиного входу в мережу.

Виділимо найважливіші моменти для кожного з перерахованих сервісів безпеки:

1. Переважними є криптографічні методи автентифікації, що реалізовуються програмним або апаратно-програмним способом. Парольний захист став анахронізмом, біометричні методи потребують подальшої перевірки в мережевому середовищі.

2. В умовах, коли поняття довіреного програмного забезпечення відходить в минуле, стає анахронізмом і найпоширеніша – довільна (дискреційна) – модель управління доступом. У її термінах неможливо навіть пояснити, що таке «троянська» програма. У ідеалі при розмежуванні доступу повинна враховуватися семантика операцій, але доки для цього є тільки теоретична база. Ще один важливий момент – простота адміністрування в умовах великої кількості користувачів і ресурсів і безперервних змін конфігурації. Тут може допомогти ролеве управління.

Протоколювання і аудит мають бути всепроникними і багаторівневими, з фільтрацією даних при переході на більш високий рівень. Це необхідна умова керованості. Бажане застосування засобів активного аудиту, проте треба усвідомлювати обмеженість їх можливостей і розглядати ці засоби як один з рубежів ешелонованої оборони, причому не найнадійніший. Слід конфігурувати їх так, щоб мінімізувати число хибних тривог і не здійснювати небезпечних дій при автоматичному реагуванні.

Усе, що пов’язано з криптографією, складно не стільки з технічної, скільки з юридичної точки зору; для шифрування це вірно удвічі. Цей сервіс є інфраструктурним, його реалізації мають бути присутніми на усіх апаратно-програмних платформах і задовольняти жорстким вимогам не лише до безпеки, але і до продуктивності. Поки ж єдиним можливим виходом є застосування вільно поширюваного ПЗ.

Надійний контроль цілісності також базується на криптографічних методах з аналогічними проблемами і методами їх рішення. Можливо, ухвалення Закону про електронний цифровий підпис змінить ситуацію на краще, буде розширений спектр реалізацій. На щастя, до статичної цілісності є і некриптографічні підходи, засновані на використанні пристроїв, що запам’ятовують, дані на яких доступні тільки для читання. Якщо в системі розділити статичну і динамічну складові і помістити першу в ПЗП або на компакт-диск, можна в корені присікти загрози цілісності. Розумно, наприклад, записувати реєстраційну інформацію на пристрої з одноразовим записом; тоді зловмисник не зможе «замести сліди».

Екранування – ідейно дуже багатий сервіс безпеки. Його реалізації – це не лише міжмережеві екрани, але і обмежуючі інтерфейси, і віртуальні локальні мережі. Екран інкапсулює об’єкт, що захищається, і контролює його зовнішнє представлення. Сучасні міжмережеві екрани досягли дуже високого рівня захищеності, зручності використання і адміністрування; у мережевому середовищі вони є першим і дуже потужним рубежем оборони. Доцільне застосування усіх видів МЕ – від персонального до зовнішнього корпоративного, а контролю підлягають дії як зовнішніх, так і внутрішніх користувачів.

Аналіз захищеності – це інструмент підтримки безпеки життєвого циклу. З активним аудитом його ріднить евристичність, необхідність практично безперервного оновлення бази знань і роль не найнадійнішого, але необхідного захисного рубежу, на якому можна розташувати вільно поширюваний продукт.

Забезпечення відмовостійкості і безпечного відновлення – аспекти високої доступності. При їх реалізації на перший план виходять архітектурні питання, в першу чергу – внесення в конфігурацію (як апаратну, так і програмну) певної надмірності, з урахуванням можливих загроз і відповідних зон ураження. Безпечне відновлення – дійсно останній рубіж, що вимагає особливої уваги, ретельності при проектуванні, реалізації і супроводі.

Тунелювання – скромний, але необхідний елемент в переліку сервісів безпеки. Він важливий не стільки сам по собі, скільки в комбінації з шифруванням і екрануванням для реалізації віртуальних приватних мереж.

Управління – це інфраструктурний сервіс. Безпечна система має бути керованою. Завжди має бути можливість дізнатися, що насправді відбувається в ІС (а в ідеалі – і отримати прогноз розвитку ситуації). Можливо, найбільш практичним рішенням для більшості організацій є використання якого-небудь вільно поширюваного каркаса з поступовим «навішуванням» на нього власних функцій.

2.2. Засади організації захисту інформації в корпоративних мережах

Багато організацій приєднали або хочуть приєднати свої локальні мережі до інтернет, щоб їх користувачі мали легкий доступ до сервісів інтернету. Інтернет в цілому не є безпечним, машини в цих ЛОМ уразливі до неавторизованого використання і зовнішніх атак.

Основи і мета політики безпеки в корпоративних мережах

Інформаційна система типової сучасної організації є дуже складною мережею побудованою у багаторівневій архітектурі клієнт/сервер, яка користується численними зовнішніми сервісами і, у свою чергу, надає власні сервіси зовні. З точки зору безпеки істотними видаються наступні аспекти ІС:

– *корпоративна мережа* має декілька територіально рознесених частин, зв’язки між якими знаходяться у веденні зовнішнього постачальника мережевих послуг, виходячи за межі зони, контрольованої організацією;

– корпоративна мережа має одне або декілька підключень до інтернету;

– на кожній з рознесених частин ІВС можуть знаходитися критично важливі сервери, в доступі до яких мають потребу співробітники, працюючі на віддалених робочих місцях, мобільні користувачі і, можливо, співробітники інших організацій;

– для доступу користувачів можуть застосовуватися не лише комп’ютери, але і споживчі пристрої, що використовують, безпровідний зв’язок;

– впродовж одного сеансу роботи користувачеві доводиться звертатися до декількох інформаційних сервісів, що спираються на різні апаратно-програмні платформи;

– до *доступності* інформаційних сервісів висуваються жорсткі вимоги, які виражаються в необхідності цілодобового функціонування з максимальним часом простою близько декількох хвилин;

– інформаційна система є мережею з *активними агентами*, тобто в процесі роботи програмні компоненти, такі як *аплети* або *сервлети*, передаються з

однієї машини на іншу і виконуються в цільовому середовищі, підтримуючи зв'язок з віддаленими компонентами;

– не усі призначені для користувача системи контролюються мережевими і/або системними адміністраторами організації;

– програмне забезпечення, особливо отримане по мережі, не може вважатися надійним, в нім можуть бути помилки, що створюють проблеми в захисті.

Конфігурація інформаційної системи постійно змінюється на рівнях адміністративних даних, програм і апаратури (міняється склад користувачів, їх привілеї і версії програм, з'являються нові сервіси, нова апаратура і тому подібне).

Архітектурна безпека

Сервіси безпеки, якими б потужними вони не були, самі по собі не можуть гарантувати надійність програмно-технічного рівня захисту. Тільки перевірена архітектура здатна зробити ефективним об'єднання сервісів, забезпечити керованість інформаційної системи, її здатність розвиватися і протистояти новим загрозам при збереженні таких властивостей, як висока продуктивність, простота і зручність використання. Якщо який-небудь (складений) сервіс не має повного набору захисних засобів, потрібне залучення додаткових сервісів, які називаються такими, що екранують. Екрануючі сервіси встановлюються на шляхах доступу до недостатньо захищених елементів; в принципі, один такий сервіс може екранувати (захищати) скільки завгодно велике число елементів.

З практичної точки зору найбільш важливими є наступні принципи архітектурної безпеки:

– *безперервність захисту* у просторі та часі, неможливість минути захисні засоби;

– наслідування визнаних стандартів, використання апробованих рішень;

– ієрархічна організація з невеликим числом сутностей на кожному рівні;

– посилення *найслабкішої ланки*;

– неможливість переходу в *небезпечний стан*;

– мінімізація привілеїв;

– розділення обов'язків;

– *ешелонованість оборони*;

– різноманітність захисних засобів;

– простота і керованість інформаційної системи.

Для забезпечення високої доступності необхідно дотримуватися наступних принципів архітектурної безпеки:

– внесення в конфігурацію тієї або іншої форми *надмірності* (резервне устаткування, запасні канали зв'язку і тому подібне);

– наявність засобів виявлення нештатних ситуацій;

– наявність засобів *реконфігурування* для відновлення, *ізоляції* і заміни компонентів, що відмовили або піддалися атаці на доступність;

– розосередженість мережевого управління;

– відсутність *єдиної точки відмови;*

– виділення підмереж і ізоляція груп користувачів один від одного.

Екранування

Формальна постановка завдання ***екранування*** полягає в наступному. Нехай є дві множини ІС. *Екран* – цей засіб *розмежування доступу* клієнтів з однієї множини до серверів з іншої множини. Екран здійснює свої функції, контролюючи усі інформаційні потоки між двома або безліччю систем (рис. 2.1). Контроль потоків полягає в їх *фільтрації*, можливо, з виконанням деяких перетворень.

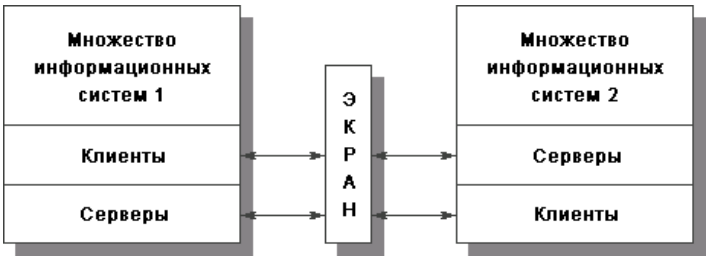


Рис. 2.1. Екран як засіб розмежування доступу

На наступному рівні деталізації екран зручно представляти як послідовність *фільтрів*. Кожен з фільтрів, проаналізувавши дані, може затримати (не пропустити) їх, а може і відразу «перекинути» за екран. Крім того, допускається перетворення даних, передача порції даних на наступний фільтр для продовження аналізу або обробка даних від імені адресата і повернення результату (рис. 2.2).

Рис. 2.2. Екран як послідовність фільтрів

Окрім функцій розмежування доступу, екрани здійснюють *протоколювання* обміну інформацією.

Зазвичай екран не є симетричним, для нього визначені поняття «усередині» і «зовні». При цьому завдання екранування формулюється як захист внутрішньої області від потенційно ворожої зовнішньої. Так, *міжмережеві екрани(*англійський термін firewall) найчастіше встановлюють для захисту корпоративної мережі організації, що має вихід в інтернет.

Екранування допомагає підтримувати *доступність* сервісів внутрішньої області, зменшуючи або взагалі ліквідовуючи навантаження, викликане зовнішньою активністю. Зменшується уразливість внутрішніх сервісів безпеки, оскільки спочатку зловмисник повинен здолати екран, де захисні механізми конфігуровані особливо ретельно.

Екранування дає можливість контролювати також інформаційні потоки, спрямовані в зовнішню область, що сприяє підтримці режиму конфіденційності в ІС організації.

Екранування може бути частковим, захищаючим певні інформаційні сервіси, наприклад екранування електронної пошти системою «Дозор-джет».

МЕ забезпечують декілька типів захисту:

– блокують небажаний трафік;

– направляють вхідний трафік тільки до надійних внутрішніх систем;

– приховують уразливі системи, які не можна узабезпечити від атак з інтернету іншим способом;

– протоколюють трафік в і з внутрішньої мережі;

– приховують інформацію, таку як імена систем, топологія мережі, типи мережевих пристроїв і внутрішні ідентифікатори користувачів, від інтернету;

– забезпечити надійнішу автентифікацію, ніж та, яку представляють стандартні застосування.

Класифікація міжмережевих екранів

При розгляді будь-якого питання, що стосується мережевих технологій, основою служить семирівнева еталонна модель ISO/OSI. Міжмережеві екрани також доцільно класифікувати по рівню фільтрації – канальному, мережевому, транспортному або прикладному. Відповідно, можна говорити про екрануючі *концентратори* (рівень 2), маршрутизатори (рівень 3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.

Фільтрація інформаційних потоків здійснюється міжмережевими екранами на основі *набору правил*, що є вираженням мережевих аспектів політики безпеки організації. У цих правилах, окрім інформації, що міститься у фільтрованих потоках, можуть фігурувати дані, отримані з оточення, наприклад, поточний час, кількість активних з'єднань, *порт*, через який поступив мережевий запит, і так далі. Таким чином, в міжмережевих екранах використовується дуже потужний логічний підхід до розмежування доступу. Чим вище рівень в моделі ISO/OSI, на якому функціонує МЕ, тим більш змістовна інформація йому доступна і, отже, тим точніше надійніше він може бути конфігурований.

Екрануючі маршрутизатори (і концентратори) мають справу з окремими пакетами даних (пакетні фільтри). Рішення про те, пропустити або затримати дані, приймаються для кожного пакету незалежно, на підставі аналізу адрес і інших полів заголовків мережевого (канального) і можливо транспортного рівнів. Ще один важливий компонент аналізованої інформації – порт, через який поступив пакет.

Сучасні маршрутизатори дозволяють зв'язувати з кожним портом декілька десятків правил і фільтрувати пакети як на вході, так і на виході. В принципі, в якості пакетного фільтру може використовуватися і універсальний комп'ютер, забезпечений декількома мережевими картами.

Основні переваги екрануючих маршрутизаторів – доступна ціна і *прозорість* для більш високих рівнів моделі OSI. Основний недолік – обмеженість аналізованої інформації і, як наслідок, відносна слабкість забезпечуваного захисту.

Транспортне екранування дозволяє контролювати процес встановлення віртуальних з'єднань і передачу інформації по них. В порівнянні з пакетними фільтрами, транспортне екранування має більшу інформацію, тому відповідний МЕ може здійснювати точніший контроль за віртуальними з'єднаннями (наприклад, він здатний відстежувати кількість інформації і розривати з'єднання після перевищення певного порогу, перешкоджаючи тим самим несанкціонованому експорту інформації). Аналогічно, можливе накопичення змістовнішої реєстраційної інформації. Головний недолік – звуження сфери застосування, оскільки поза контролем залишаються датаграмні протоколи.

Міжмережевий екран, що функціонує на прикладному рівні, здатний забезпечити найбільш надійний захист. Як правило, подібний МЕ є універсальним комп'ютером, на якому функціонують *екрануючі агенти*, що інтерпретують протоколи прикладного рівня (HTTP, FTP, SMTP, telnet і так далі) в тому ступені, який потрібний для забезпечення безпеки.

При використанні прикладних МЕ, окрім фільтрації, реалізується ще один

найважливіший аспект екранування. Суб'єкти із зовнішньої мережі бачать тільки шлюзовий комп'ютер; відповідно, їм доступна тільки та інформація про внутрішню мережу, яку він вважає потрібним експортувати. Прикладний МЕ насправді екранує, тобто затуляє, внутрішню мережу від зовнішнього світу. В той же час, суб'єктам внутрішньої мережі здається, що вони безпосередньо спілкуються з об'єктами зовнішнього світу. Недолік прикладних МЕ – відсутність повної прозорості, що вимагає спеціальних дій для підтримки кожного прикладного протоколу.

Комплексні міжмережеві екрани, що охоплюють рівні від мережевого до прикладного, поєднують в собі кращі властивості «однорівневих» МЕ різних видів. Захисні функції виконуються комплексними МЕ прозорим для додатків чином, не вимагаючи внесення яких-небудь змін ні в існуюче програмне забезпечення, ні в дії, що стали для користувачів звичними.

Комплексність МЕ може досягатися різними способами: «від низу до верху», від мережевого рівня через накопичення контексту до прикладного рівня, або зверху «вниз», за допомогою доповнення прикладного МЕ механізмами транспортного і мережевого рівнів.

Окрім виразних можливостей і допустимої кількості правил, якість МЕ визначається ще двома важливими характеристиками – *простотою використання* і *власною захищеністю*. У плані простоти використання первинне значення мають наочний інтерфейс при визначенні правил фільтрації і можливість *централізованого адміністрування* складених конфігурацій. У останньому аспекті виділяють кошти централізованого завантаження правил фільтрації і *перевірки набору правил на несуперечність.* Важливий і централізований збір і аналіз реєстраційної інформації, а також отримання сигналів про спроби виконання дій, заборонених політикою безпеки.

Власна захищеність міжмережевого екрану забезпечується тими ж засобами, що і захищеність універсальних систем. Мається на увазі фізичний захист, ідентифікація і автентифікація, розмежування доступу, контроль цілісності, протоколювання і аудит. При виконанні централізованого адміністрування слід також потурбуватися про захист інформації від пасивного і активного прослуховування мережі, тобто забезпечити цілісність і конфіденційність інформації.

Окрім блокування потоків даних, що порушують політику безпеки, МЕ може приховувати інформацію про мережу, що захищається, тим самим ускладнюючи дії потенційних зловмисників. Потужним методом приховування інформації є *трансляція* «внутрішніх» мережевих адрес, яка ще вирішує проблему розширення адресного простору організації.

Багаторівневий захист корпоративних мереж

Міжмережевий екран розташовується між мережею, що захищається (внутрішньою), і зовнішнім середовищем (зовнішніми мережами або іншими сегментами корпоративної мережі). У першому випадку говорять про зовнішній МЕ, в другому – про внутрішній. Залежно від точки зору, зовнішній міжмережевий екран можна вважати першою або останньою (але не єдиною) лінією оборони. Першою – якщо дивитися на світ очима зовнішнього зловмисника. Останньою – якщо прагнути до захищеності усіх компонентів корпоративної мережі і припинення неправомірних дій внутрішніх користувачів.

Міжмережевий екран – ідеальне місце для вбудовування засобів активного аудиту. З одного боку, і на першому, і на останньому захисному рубежі виявлення підозрілої активності по-своєму важливе. З іншого боку, МЕ здатний реалізувати скільки завгодно потужну реакцію на підозрілу активність, аж до розриву зв'язку із зовнішнім середовищем.

На міжмережевий екран доцільно покласти ідентифікацію/автентифікацію зовнішніх користувачів, що потребують доступу до корпоративних ресурсів (з підтримкою концепції єдиного входу в мережу).

В силу принципів *ешелонованості оборони* для захисту зовнішніх підключень зазвичай використовується *двокомпонентне екранування* (рис. 2.3). Первинна фільтрація (наприклад, блокування пакетів протоколу SNMP, що керує, або пакетів з певними IP-адресами, внесеними в «чорний список») здійснюється *граничним маршрутизатором*, за яким розташовується так звана *демілітаризована зона* (мережа з помірною довірою безпеки – веб, електронна пошта і тому подібне) і основний МЕ, що захищає внутрішню частину корпоративної мережі.

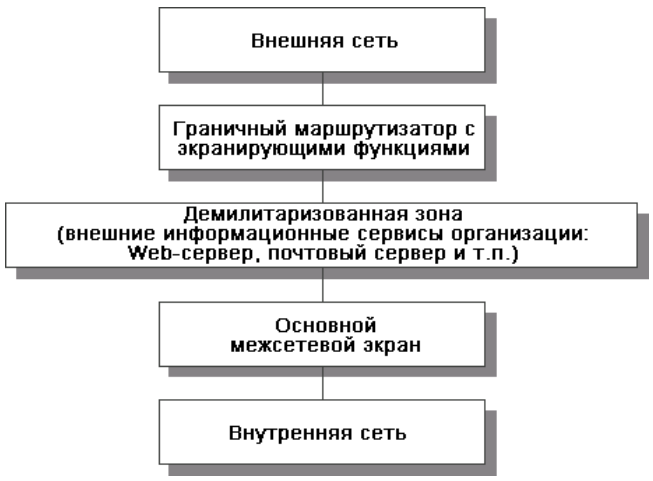


Рис. 2.3. Двокомпонентне екранування з демілітаризованою зоною

Теоретично *міжмережевий екран* (особливо внутрішній) *має бути багатопротокольним.* Проте на практиці при домінуванні сімейства протоколів TCP/IP підтримка інших протоколів уявляється надмірністю, шкідливою для безпеки (чим складніший сервіс, тим він більш уразливий).

І зовнішній, і *внутрішній міжмережевий екран* може стати вузьким місцем за об'ємом мережевого трафіку. Один з підходів до вирішення цієї проблеми передбачає розбиття МЕ на декілька апаратних частин і організацію спеціалізованих *серверів-посередників*. Основний міжмережевий екран може проводити грубу класифікацію трафіку, що входить, за видами і передовіряти фільтрацію відповідним посередникам (наприклад, при аналізі HTTP-трафіка. Витікаючий трафік спочатку обробляється сервером-посередником, який може виконувати і функціонально корисні дії, такі як кешування сторінок зовнішніх веб-серверів (Proxy), що знижує навантаження на мережу взагалі і основний МЕ зокрема).

Ситуації, коли корпоративна мережа утримує лише один зовнішній канал, є швидше виключенням, ніж правилом. Навпаки, типова ситуація, при якій корпоративна мережа складається з декількох територіально рознесених сегментів, кожен з яких підключений до інтернету. В цьому випадку кожне підключення повинне захищатися своїм екраном. Точніше кажучи, можна вважати, що корпоративний зовнішній *міжмережевий екран є складеним*, і вимагається вирішувати задачу погодженого адміністрування (управління і аудиту) усіх компонентів.

Протилежністю складеним корпоративним МЕ є *персональні міжмережеві екрани і персональні екрануючі пристрої*. Перші є програмними продуктами, які встановлюються на ПЕОМ і захищають тільки їх, другі реалізуються на окремих пристроях і захищають невелику локальну мережу, таку як мережу домашнього офісу.

2.3. Принципи надання доступу до IP в корпоративних мережах

Принцип обґрунтованості доступу. Цей принцип полягає в обов'язковому виконанні двох основних умов: користувач повинен мати достатню «форму допуску» для отримання інформації потрібного ним рівня конфіденційності, і ця інформація потрібна йому для виконання його виробничих функцій. Помітимо тут, що у сфері автоматизованої обробки інформації користувачами можуть виступати активні програми і процеси, а також носії інформації різної міри укрупненості. Тоді система доступу припускає визначення для усіх користувачів відповідного програмно-апаратного середовища або інформаційних і програмних ресурсів, які будуть їм доступні для конкретних операцій.

Принцип достатньої глибини контролю доступу. Засоби захисту інформації повинні містити механізми контролю доступу до усіх видів інформаційних і програмних ресурсів АС, які відповідно до принципу обґрунтованості доступу слід розділяти між користувачами.

Принцип розмежування потоків інформації. Для попередження порушення безпеки інформації, яке, наприклад, може мати місце при записі секретної інформації на несекретні носії і в несекретні файли, її передачі програмам і процесам, не призначеним для обробки секретної інформації, а також при передачі секретної інформації по незахищених каналах і лініях зв'язку, необхідно здійснювати відповідне розмежування потоків інформації.

Принцип чистоти повторно використовуваних ресурсів. Цей принцип полягає в очищенні ресурсів, що містять конфіденційну інформацію, при їх видаленні або звільненні користувачем до перерозподілу цих ресурсів іншим користувачам.

Принцип персональної відповідальності. Кожен користувач повинен нести персональну відповідальність за свою діяльність в системі, включаючи будь-які операції з конфіденційною інформацією і можливі порушення її захисту, тобто які-небудь випадкові або умисні дії, які приводять або можуть привести до несанкціонованого ознайомлення з конфіденційною інформацією, її спотворенню або знищенню, або роблять таку інформацію недоступною для законних користувачів.

Принцип цілісності засобів захисту. Цей принцип має на увазі, що засоби захисту інформації в АС повинні точно виконувати свої функції відповідно до перерахованих принципів і бути ізольованими від користувачів, а для свого супроводу повинні включати спеціальний захищений інтерфейс для засобів контролю, сигналізації про спроби порушення захисту інформації і дії на процеси в системі.

Реалізація перерахованих принципів здійснюється за допомогою так званого «монітора звернень», контролюючого будь-які запити до даних або програм з боку користувачів (чи їх програм) по встановлених для них видах доступу до цих даних і програм. Такий монітор представляється у вигляді схеми (рис. 2.4).

Практичне створення монітора звернень, як зрозуміло з приведеного рисунку, припускає розробку конкретних правил розмежування доступу у вигляді так званої моделі захисту інформації. Історично моделі захисту інформації виникли з робіт по теорії захисту операційних систем (ОС). Перша спроба використання такої моделі була зроблена при розробці захищеної ОС за замовленням міністерства оборони США.

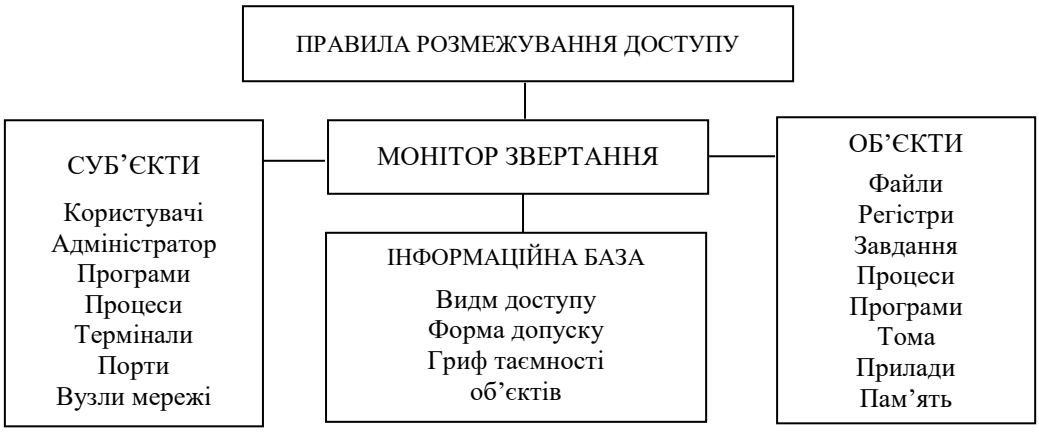


Рис. 2.4. Структура монітора звернень

Поведінка цієї моделі описується наступними простими правилами [1]:

– користувачеві дозволений доступ в систему, якщо він входить в множину відомих системі користувачів;

– користувачеві дозволений доступ до терміналу, якщо він входить в підмножину користувачів, закріплених за цим терміналом;

– користувачеві дозволений доступ до файлу, якщо: рівень конфіденційності користувача не нижчий рівня конфіденційності файлу; прикладна область файлу включається в прикладну область завдання користувача; режим доступу завдання користувача включає режим доступу до файлу; користувач входить в підмножину допущених до файлу користувачів.

У моделі Хартсона [1] як основні характеристики використовується велика кількість так званого п'ятимірного «простору безпеки»:

– встановлених повноважень;

– користувачів;

– операцій;

– ресурсів;

– станів.

Область безпечних станів системи представляється у вигляді декартового добутку перерахованих великих кількостей. Кожен запит на доступ представляється підпростором чотиривимірної проекції простору безпеки. Запити отримують право на доступ у тому випадку, коли вони повністю поміщені у відповідні підпростори.

Одна з перших фундаментальних моделей захисту була розроблена Лемпсоном і потім вдосконалена Грехемом і Деннінгом [10]. Ця модель припускає, що усі спроби доступу до об'єктів перехоплюються і перевіряються спеціальним процесом, що керує. Приведені моделі можуть використовуватися як для захисту

ОС, так і для захисту баз даних (БД). Враховуючи, що такі єдині моделі, як показує практика, значно ускладнюють розгляд питань безпеки, рядом авторів були зроблені спроби розробки спеціальних моделей захисту БД. Прикладом такої моделі є модель Фернандеза, Саммерса і Колмана [11].

Розглянуті вище моделі захисту інформації відносяться до класу матричних і отримали найбільше поширення внаслідок не лише тому, що вони служать не тільки для цілей аналізу логічного функціонування системи, але й успішно піддаються реалізації в конкретних програмах. Оскільки програми в цих моделях виступають в правилах доступу в якості суб'єктів, то вони можуть, при необхідності, розширювати права конкретних користувачів. Наприклад, програма може мати права на сортування файлу, читання якого користувачеві заборонене. У моделі Хартсона і Сяо [1] кожне правило може мати розширення, яке визначає права програм. У інших випадках може знадобитися звуження прав користувачів правами використовуваних ними програм. В той же час програми можуть виступати і в якості об'єктів доступу, типовими операціями для яких є виконання (execute) і використання (use).

Іншим типом моделей є багаторівневі моделі. Вони відрізняються від матричних моделей декількома аспектами. По-перше, ці моделі розглядають управління доступом не у рамках тих, що задаються деяким адміністратором прав, а у рамках представлення усієї системи так, щоб дані однієї категорії або області не були доступні користувачам іншої категорії. По-друге, багаторівневі моделі розглядають не лише сам факт доступу до інформації, але також і потоки інформації усередині системи.

Найбільше поширення отримала багаторівнева модель захисту Белла-ЛаПадула [12, 13]. Основою цієї моделі є поняття рівня конфіденційності (форми допуску) і категорії (прикладній області) суб'єкта і об'єкту доступу. На підставі присвоєних кожному суб'єктові і об'єкту доступу конкретних рівнів і категорій в моделі визначаються їх рівні безпеки, а потім встановлюється їх взаємодія. При цьому в моделі приймається, що один рівень безпеки домінує над іншим тоді і тільки тоді, коли рівень конфіденційності, що відповідає йому, більше або дорівнює рівню конфіденційності іншого, а безліч категорій включає відповідну множину іншого. Рівні конфіденційності є і впорядкованими, тоді як рівні безпеки впорядковані частково, тобто деякі суб'єкти і об'єкти можуть бути незрівняні.

Доступ до об'єкту може розглядатися або як читання (отримання з нього інформації), або як зміну (запис в нього інформації). Тоді види доступу визначаються наступними можливими поєднаннями цих операцій:

– ні читання, ні зміна;

– тільки читання;

– тільки зміна;

– і читання, і зміна.

Головна мета моделі полягає в запобіганні потокам інформації з об'єктів більш високого рівня безпеки в об'єкти нижчого рівня. Ця мета реалізується виконанням наступних правил:

– якщо суб'єкт доступу формує запит на читання, то рівень безпеки суб'єкта повинен домінувати над рівнем безпеки об'єкту;

– якщо формується запит на зміну, то рівень безпеки об'єкту повинен домінувати над рівнем безпеки суб'єкта;

– якщо формується запит на читання-запис, то рівні безпеки суб'єкта і об'єкту мають дорівнювати один одному;

– якщо рівні безпеки суб'єкта і об'єкту доступу незрівняні, то ніякі запити суб'єкта не виконуються.

Підводячи підсумок розгляду двох класів моделей захисту інформації, відмітимо, що перевага матричних моделей полягає в легкості представлення широкого спектру правил забезпечення безпеки інформації. Основний же недолік цих моделей полягає у відсутності контролю за потоками інформації. Зі свого боку, головним недоліком багаторівневих моделей є неможливість управління доступом до конкретних об'єктів на основі обліку індивідуальних особливостей кожного з суб'єктів. Отже, обидва підходи як би припускають пошук різних компромісів між ефективністю, гнучкістю і безпекою. Очевидно, що оптимальне рішення питань безпеки повинне вироблятися із застосуванням обох видів моделей захисту.

Методи ідентифікації і автентифікації користувачів

Реалізація конкретних моделей захисту від несанкціонованого доступу повинна спиратися на відповідні адміністративні (процедурні) заходи і технічні засоби, спрямовані в першу чергу на ідентифікацію і автентифікацію користувачів автоматизованої системи.

Ідентифікація користувачів АС полягає у встановленні, закріпленні за кожним з них унікального ідентифікатора у вигляді номера, шифру, коду і тому подібне. Це пов'язано з тим, що традиційний ідентифікатор вигляду прізвище-ім'я-по батькові не завжди може бути використаний в конкретній АС. Для цілей ідентифікації в різних автоматизованих системах широко, наприклад, застосовуються так званий персональний ідентифікаційний номер (PIN – Personal Identification Number), соціальний безпечний номер (SSN – Social Security

Number), особистий номер, код безпеки і так далі [14]. Такі ідентифікатори використовуються при побудові різних систем розмежування доступу і захисту інформації. Автентифікація полягає в перевірці достовірності користувача по пред'явленому їм ідентифікатору, наприклад, при вході в систему. Така перевірка повинна виключати фальсифікацію користувачів в системі і їх компрометацію. Без перевірки достовірності втрачається сенс в самій ідентифікації користувачів і застосуванні засобів розмежування доступу, побудованих на базі особистих ідентифікаторів. Відсутність грошових коштів перевірки достовірності користувачів може істотно ускладнити реалізацію принципу персональної відповідальності, про який говорилося вище.

Перевірка достовірності (автентифікація) може проводитися різними методами і засобами. Нині в автоматизованих системах використовуються три основні способи автентифікації за:

– паролем або особистим ідентифікуючим номером (користувач «знає»);

– деяким предметом, який є у користувача (користувач «має»);

– якими-небудь фізіологічними ознаками, властивими конкретним особам (користувач «є»).

Перший спосіб реалізують програмні засоби автентифікації, вживані у більшості операційних систем, систем управління базами даних, моніторів телеобробки, мережевих пакетів. Суть цього способу полягає в тому, що кожному зареєстрованому користувачеві видається персональний пароль, який він повинен тримати в таємниці і вводити в автоматизовану систему при кожному зверненні до неї. Спеціальна програма порівнює введений пароль з еталоном, що зберігається в пам'яті, і при збігу паролів запит користувача приймається до виконання.

Простота цього способу очевидна, але очевидні також і його явні недоліки: пароль може бути підібраний перебором можливих комбінацій, а майстерний зловмисник може проникнути в ту область пам'яті, де зберігаються еталонні паролі. Наприклад, в ОС DOS-11, що застосовувалася свого часу у банківській сфері, в стандартній конфігурації були відсутні засоби шифрування паролів у файлі рахунків користувачів. В процесі завантаження цією ОС можна було легко проглянути паролі усіх користувачів. Безпечніші системи здійснюють зберігання списків паролів в зашифрованому вигляді. В той же час перехоплення навіть зашифрованого пароля дозволяє при його використанні отримати несанкціонований доступ до віддаленої ЕОМ.

До заходів підвищення безпеки парольних систем автентифікації, окрім згаданого зберігання списків паролів в зашифрованому вигляді, може бути віднесене скорочення термінів дії паролів аж до застосування паролів одноразового

використання. Останнім часом для цілей автентифікації широко використовується так званий метод «запит-відповідь», яка дозволяє не лише аутентифікувати користувача, але і дає можливість користувачеві здійснювати автентифікацію системи, з якою він працює. Це має принципове значення при роботі в мережі, оскільки використання підставної ЕОМ, ОС або програми є одним з шляхів несанкціонованого отримання повідомлень або паролів законних користувачів. Слід зазначити, що необхідність такої взаємної автентифікації підтверджена міжнародним стандартом по взаємодії відкритих систем.

Різновидом першого способу автентифікації є і так зване упізнання в діалоговому режимі, здійснюване за наступною схемою. У файлах механізмів захисту завчасно створюються записи, що персоніфікують, які містять дані користувача (дата народження, ріст, вага, імена і дати народження рідних і близьких і тому подібне) або досить великий і впорядкований набір паролів. При зверненні користувача програма захисту пропонує йому назвати деякі дані з наявного запису, які порівнюються з тими, що зберігаються у файлі. За результатами порівняння приймається рішення про допуск. Для підвищення надійності упізнання запиту в користувача дані можуть вибиратися кожного разу різні.

В якості предмета, наявного у користувача (другий спосіб автентифікації), застосовуються так звані карти ідентифікації (КІ), на які наносяться дані, що персоніфікують користувача: персональний ідентифікаційний номер, спеціальний шифр або код і т. ін. Ці дані заносяться на картку в зашифрованому вигляді, причому ключ шифрування може бути додатковим ідентифікуючим параметром, оскільки він може бути відомий тільки користувачеві, вводиться ним кожного разу при зверненні до системи і знищується відразу ж після використання.

Інформація, що знаходиться на карті, може бути записана і вирахувана різними способами або комбінацією декількох способів. На приклад, КІ поміщається в зчитуючий пристрій, джерело світла освітлює мікрокристалічну точкову матрицю, встановлену на карті. Оскільки тільки неполяризовані елементи матриці будуть прозорі для світла, то буде прочитаний відповідний код, що містить інформацію про конкретного користувача.

Ще одним типом КІ є інформаційна картка з нанесеними особливим способом із застосуванням фосфору на її поверхню декількома рядами знаків, букв і т. ін. Зчитуючий пристрій в цьому випадку є двома електродами, один з яких прозорий. Картка розташовується між електродами, і при поданні на них напруги електрони, що збуджуються між ізолюючим шаром (основою картки) і шаром фосфору, викликають світіння останнього. Таким чином, інформаційні знаки можуть бути визначеними тільки спеціальним способом, що виключає візуальне

розпізнавання інформації.

Іншим типом КІ є електронна ідентифікуюча карта, побудована на інтегральній мікросхемі. У цієї карти на короткій стороні друкованої плати розташовуються котушки індуктивності, через які передається електроживлення на плату і здійснюється обмін кодованою інформацією з пристроєм, який розпізнається. Інтегральна схема містить арифметичний блок, а також постійний і оперативний пристрої, що запам'ятовують.

На поверхню карти може також наноситися покриття, що дозволяє бачити зображення або текст тільки в інфрачервоному або ультрафіолетовому діапазоні. Над текстом або зображенням можна розмістити рідкокристалічну матрицю, прозору тільки при певній орієнтації кристалів.

Найбільше поширення серед облаштувань автентифікації за типом «користувач має» отримали індивідуальні магнітні карти. Популярність таких пристроїв пояснюється універсальністю їх застосування (не лише в автоматизованих системах), відносно низькою вартістю і високою точністю, вони легко комплексуються з терміналом і персональною ЕОМ. Оскільки зчитувачі цих пристроїв ідентифікують не особу, а магнітну карту, то вони комплектуються спеціальною, часто цифровою клавіатурою для введення власником карти свого шифру, пароля. Для захисту карт від несанкціонованого зчитування і підробки, як і в попередніх випадках, застосовуються спеціальні фізичні і криптографічні методи.

В якості різновидів КІ можна розглядати спеціально помічені дискети, призначені для автентифікації законного власника програмного пакету. Зазвичай поверхня такої дискети штучно ушкоджується за допомогою лазера або тонкої голки. Іноді застосовують нестандартне форматування окремих треків або усієї дискети, а також спеціальну нумерацію секторів.

Для упізнання компонентів обробки даних, тобто програм функціональної обробки, масивів даних (таке упізнання особливо актуальне при роботі в мережі ЕОМ) використовуються спеціальні апаратні блоки-приставки, що є пристроями, що генерують індивідуальні сигнали. В цілях попередження перехоплення цих сигналів і подальшого їх зловмисного використання вони можуть передаватися в зашифрованому виді, причому періодично може мінятися не лише ключ шифрування, але і використовуваний спосіб (алгоритм) криптографічного перетворення.

Всього зростаючого значення останнім часом починають набувати системи упізнання користувачів за фізіологічними ознаками. Тільки при такому підході дійсно встановлюється, що користувач, що претендує на доступ до терміналу,

саме той, за кого себе видає. При використанні цього класу засобів автентифікації виникає проблема «соціальної прийнятності»: процедура автентифікації не повинна принижувати людську гідність, створювати дискомфорт, просто бути занадто морочливою і займати багато часу. Існує досить фізіологічних ознак, що однозначно вказують на конкретну людину. До них відносяться: відбитки ніг і рук, зуби, ферменти, динаміка дихання, риси обличчя і так далі. Для автентифікації термінальних користувачів автоматизованих систем найбільш прийнятними вважаються відбитки пальців, геометрія руки, голос, особистий підпис.

Автентифікація по відбитках пальців. Встановлення особи по відбитках пальців – старий і перевірений прийом. Нині існують два можливі способи використання цього прийому для автентифікації термінального користувача:

– безпосереднє порівняння зображень відбитків пальців, отриманих за допомогою оптичних пристроїв, з відбитками з архіву;

– порівняння характерних деталей відбитку в цифровому виді, які отримують в процесі сканування зображень відбитку.

На сьогодні розроблені спеціальні чутливі матеріали, що забезпечують отримання відбитків без використання фарби, засновані на здатності речовин змінювати свої відбивні характеристики залежно від температури прикладених предметів.

При безпосередньому порівнянні зображень відбитків облаштування автентифікації визначає оптичне співвідношення двох зображень і виробляє сигнал, що визначає міру збігу відбитків. Порівняння відбитків зазвичай виконується безпосередньо на місці установлення пристрою. Передача зображення відбитку по каналах зв’язку не застосовується через її складність, високої вартості і необхідності додаткового захисту цих каналів.

Велике поширення отримав спосіб, побудований на порівнянні деталей відбитків (метод співвідношення борозенок на відбитках). При цьому користувач вводить з клавіатури ідентифікуючу інформацію, по якій облаштування автентифікації проводить пошук необхідного списку деталей відбитку в архіві. Після цього він поміщає палець на оптичне віконце пристрою, і починається процес сканування, в результаті якого обчислюються координати 12 точок, що визначають відносне розташування борозенок відбитку. Об’єм інформації при цьому складає близько 100 байт на відбиток. Порівняння робиться в ЕОМ по спеціальних алгоритмах. Недоліком цього способу, проте, являється те, що практично неможливо забезпечити точне центрування і стабільну пластичність пальця, тому неможливо отримати і точне положення борозенок, внаслідок чого оцінка співвідношення має імовірнісний характер.

Одним з прикладів облаштування автентифікації по відбитках пальців може служити американська система Fingerscan [15]. Ця система складається з центрального облаштування управління і пристроїв для зняття відбитків пальців. Компанія Fingerscan за контрактом з міністерством оборони США розробила інше облаштування автентифікації користувачів по відбитках пальців (облаштування зчитування рельєфу). Користувач вводить свій ідентифікуючий номер, поміщає палець в спеціальну щілину, і пристрій робить оптичне сканування шкіри. До складу пристрою входять лазерна оптична система, апаратура обробки сигналів і мікропроцесор з програмами побудови «образу» відбитку пальця. Рельєф шкіри зчитується пристроєм майже безпомилково. Для занесення еталону відбитку одного пальця вимагається від 3 до 5 хвилин, необхідний об'єм пам'яті 256 байт.

Автентифікація за формою кисті руки. Принцип дії таких облаштувань автентифікації заснований на тому, що на руку випробовуваному направляють яскраве світло і аналізують освітленість чутливих елементів, яка залежить від довжини пальців, закругленості їх кінчиків і прозорості шкіри. Вихідна інформація від кожного фоторезистора перетвориться в цифровий код. Ідентифікуюча інформація може зберігатися централізовано в головній ЕОМ. Перевагою подібних систем є велике число аналізованих параметрів, що зменшує вірогідність помилки.

Автентифікація за допомогою автоматичного аналізу підпису. Відомо, що почерк кожної людини строго індивідуальний, ще більше індивідуальний його підпис. Вона стає надзвичайно стилізованою і з часом набуває характеру умовного рефлексу. Нині існують два принципово різних способів аналізу підпису: візуальне сканування і дослідження динамічних характеристик руху руки при виконанні підпису (прискорення, швидкості, тиски, тривалість пауз). Вважається, що другий спосіб прийнятний, оскільки очевидно, що два підписи однієї і тієї ж людини не можуть бути абсолютно ідентичними. З іншого боку, маючи оригінал підпису, можна навчитися повторювати її практично точно.

При другому способі автентифікації передбачається застосування спеціальних вимірювальних авторучок з датчиками, чутливими до вказаних вище динамічних характеристик руху. Ці параметри унікальні для кожної людини, їх неможливо підробити. У авторучку вбудований двомірний датчик прискорення, що дозволяє вимірювати характеристики на площини, а також датчик тиску, який фіксує параметри вертикальної сили. Існують два способи порівняння результатів вимірів. Перший заснований на порівнянні амплітуд прискорення кожні 5..10 мс. Необхідна пам'ять в цьому випадку – 2 кбайт. Другий спосіб заснований на обчисленні середніх величин повного часу написання, проміжків «мовчання»,

швидкості і прискорення по осях X і Y і середньої сили по осі Z. Необхідна пам'ять для зберігання одного еталонного вектору в цьому випадку складає 200 байт. Фахівці вважають, що система встановлення достовірності підпису при меншій вартості і більшій соціальній прийнятності не поступається по надійності пристроям, що звіряють відбитки пальців.

Автентифікація за характером голосу. На думку ряду фахівців, найдорожчими засобами автентифікації користувачів є засоби верифікації по голосах. Цей напрям дуже перспективний тому, що для автентифікації можуть бути використані телефонні канали зв'язку, а алгоритм упізнання може бути реалізований в центральній ЕОМ. Можна виділити три основні напрями реалізації цього способу аутентифікації:

– аналіз короткочасних сегментів мови (тривалістю до 20 мс) – вибирається серія коротких фрагментів, обробляється, складається статистичний образ, який і порівнюється з еталоном;

– контурний аналіз мови – з фрагмента мови виділяється декілька характеристик, наприклад, висота тону, для них визначається характеристична функція, яка порівнюється з еталонною;

– статистична оцінка голосу – мова повинна звучати достатньо довго (близько 12 секунд), упродовж усього цього періоду збирається інформація про декілька параметрів голосу, на основі якої створюється цифровий образ і порівнюється з еталоном.

Як приклад практичній реалізації останнього підходу можна привести пристрій, розроблений фірмою Philips, включаючи 43-канальний фільтр із смугою пропускання 100..6200 Гц, що практично покриває увесь діапазон частот людського голосу. Кожен канал опитується один раз в 18 мс. В результаті визначаються амплітудно-частотні характеристики усіх каналів і порівнюються з еталоном. Слова, які вимовляє користувач, вибираються за принципом найбільшої різноманітності звуків і заздалегідь виводяться на екран дисплея у випадковій послідовності, що виключає підробки, у тому числі використання магнітофонного запису.

Основними характеристиками облаштувань автентифікації є:

– частота помилкового заперечення законного користувача;

– частота помилкового визнання стороннього;

– середній час напрацювання на відмову;

– число обслуговуваних користувачів;

– вартість;

– об’єм інформації, циркулюючої між зчитуючим пристроєм і блоком порівняння;

– прийнятність з боку користувачів.

Дослідження і випробування облаштувань автентифікації різних типів показали, що частота помилкового заперечення дещо перевищує частоту помилкового визнання і складає величину, що не перевищує, як правило, 1–2%. Так, вітчизняне облаштування автентифікації по підпису має частоту помилкового заперечення, приблизно рівну частоті помилкового визнання і що становить близько 0,5%.

Головним висновком, що виходить з досвіду створення облаштувань автентифікації, є те, що отримання високої точності упізнання користувача можливо тільки при поєднанні різних методів.

Необхідно відмітити, що усі розглянуті методи автентифікації у разі не підтвердження достовірності повинні здійснювати тимчасову затримку перед обслуговуванням наступного запиту. Це необхідно для зниження загрози підбору ідентифікуючих ознак (особливо паролів) в автоматичному режимі. При цьому усі спроби невдач діставання доступу повинні реєструватися в цілях забезпечення ефективного нагляду (контролю) за безпекою системи.

Методи контролю доступу

Наступним кроком в реалізації розглянутих вище моделей захисту інформації є формування конкретних схем розмежування доступу автентифікації користувачів до ресурсів АС. Зазвичай необхідність контролю доступу виникає при розділенні користування яким-небудь ресурсом багатьма суб’єктами. Схеми розмежування доступу зручно розділити на дві групи:

– «спискові» схеми, в яких захисні механізми вбудовуються в кожен об’єкт і здійснюють контроль відповідно до списків доступу цього об’єкту;

– «мандатні» схеми, в яких захисний механізм об’єкту реагує на деякий мандат, і суб’єкт повинен мати набір мандатів для доступу до усіх необхідних йому об’єктів.

При розділенні функцій адресації і захисту зручно розбити пам’ять на області або сегменти, кожен з яких забезпечений своїм ідентифікатором і має той, що не перетинається з іншими сегментами діапазону адрес. При цьому на побудову тієї або іншої конкретної схеми контролю доступу істотний вплив робить механізм захисту пам’яті, використовуваний у відповідній ЕОМ. Різноманітність пропонованих схем і механізмів контролю доступу до інформації в програмній реалізацій дуже велика. Розглянемо тільки деякі з них.

Системи без схем захисту. У деяких системах повністю відсутні механізми, що перешкоджають певному користувачеві отримати доступ до інформації, що зберігається в системі. Хоча на сучасному етапі розвитку засобів захисту інформації ці системи вже не представляють інтересу, про них слід згадати тому, що деякі з них досі широко використовувалися, та ще і продовжують використовуватися. Це, наприклад, DOS для персональних ЕОМ.

Системи, побудовані за принципом віртуальної машини. У таких системах забезпечується взаємна ізоляція користувачів, за винятком тільки деякої кількості загальної інформації. Система з числа доступних їй ресурсів виділяє певний їх об'єм в повне розпорядження користувача, який може вважати, що має у своєму розпорядженні власну ЕОМ. Тут розмежування доступу реалізоване шляхом повного ізолювання користувачів один від одного. Ця схема в чистому вигляді робить складною взаємодію користувачів, тому іноді тут доводиться вводити ще і елементи розмежування доступу, наприклад парольний доступ до деяких ресурсів спільного використання.

Системи з єдиною схемою контролю доступу. Для забезпечення прямого контролю доступу до окремих ресурсів в системі потрібні складніші схеми, ніж розглянуті вище. У таких системах з кожним інформаційним елементом може бути пов'язаний «список авторизованих користувачів», причому власник елементу може наказати різним користувачам різні режими його використання – для читання, для запису або для виконання. Серед функціонально повних систем такого роду можна відмітити систему ADEPT – 50.

Системи з програмованими схемами розмежування доступу. Часто необхідність розмежування доступу може визначатися смисловим змістом інформаційного елементу або контекстом, в якому цей елемент використовується. Складність прямої реалізації подібних механізмів розмежування призводить до методу, заснованого на понятті «довіреного» програмного середовища. При цьому виділяються захищені об'єкти і захищені підсистеми. Захищена підсистема є сукупністю програм і даних, що мають ту властивість, що правом доступу до даних (тобто захищеним об'єктам) наділені програми, що тільки входять в підсистему. У результаті програми підсистеми повністю контролюють доступ до даних і можуть реалізувати будь-який необхідний алгоритм їх обробки і розмежування доступу. Користувач же має можливість діставання тільки опосередкованого доступу до даних, причому тільки через програми захищеної підсистеми, доступ до яких може бути представлений вже традиційними способами. Тут із загальновідомих можна привести систему UNIX.

Системи динамічного розподілу прав. Більшість з представлених вище

схем засновані на статичній моделі розмежування доступу, коли кожен з наявних об’єктів вже внесений в матрицю розмежування перед початком обробки. У момент породження нових об’єктів виникають проблеми: де, на яких носіях їх можна розміщувати, які права давати користувачам на доступ до цих об’єктів, і так далі. У автоматизованих системах реалізація подібних схем в силу своєї складності носить фрагментарний характер. Наприклад, в системі ADEPT – 50 простежується рівень конфіденційності усіх документів, що поміщаються у файл, і при видачі вмісту з файлу йому автоматично привласнюється максимальний рівень конфіденційності з числа використаних.

2.4. Застосування систем виявлення вторгнень до корпоративних мереж

2.4.1. Структуризація сучасних систем виявлення вторгнень

Виявлення вторгнень – це ще одне завдання, що виконується співробітниками, відповідальними за безпеку інформації в організації, при забезпеченні захисту від атак. Виявлення вторгнень – це активний процес, при якому відбувається виявлення хакера при його спробах проникнути в систему. У ідеальному випадку така система лише видає сигнал тривоги при спробі проникнення. Виявлення вторгнень допомагає при превентивній ідентифікації активних загроз за допомогою сповіщень і попереджень про те, що зловмисник здійснює збір інформації, необхідної для проведення атаки. Насправді, як буде показано в матеріалі лекції, це не завжди так. Перед обговоренням подробиць, пов’язаних з виявленням вторгнень, давайте визначимо, що ж це насправді таке.

Загальні відомості про системи виявлення вторгнень

Системи виявлення вторгнень (IDS) з’явилися дуже давно. Першими з них можна рахувати нічний дозор і сторожових собак. Дозорні і сторожові собаки виконували два завдання: вони визначали ініційовані кимось підозрілі дії і обмежували подальше проникнення зловмисника. Як правило, грабіжники уникали зустрічі з собаками і, у більшості випадку, намагалися обходити стороною будівлі, що охороняються собаками. Те ж саме можна сказати і про нічний дозор. Грабіжники не хотіли бути поміченими озброєними дозорцями або охоронцями, які могли викликати поліцію.

Сигналізація у будівлях і в автомобілях також є різновидом системи виявлення вторгнень. Якщо система сповіщення виявляє подію, яка має бути помічена (наприклад, злом вікна або відкриття дверей), то видається сигнал тривоги

із запаленням ламп, включенням звукових сигналів, або сигнал тривоги передається на пульт поліцейського відділка. Функція припинення проникнення виконується за допомогою застережливої наклейки на вікні або знаку, встановленого перед будинком. У автомобілях, як правило, при включеній сигналізації горить червона лампочка, застережлива про активний стан системи сигналізації.

Усі ці приклади ґрунтуються на одному і тому ж принципі: виявлення будь-яких спроб проникнення в захищений периметр об'єкту (офіс, будівля, автомобіль і т. ін.). У випадку з автомобілем або будівлею периметр захисту визначається відносно легко. Стіни будови, обгороджування навколо приватної власності, двері і вікна автомобіля чітко визначають периметр, що захищається. Ще однією характеристикою, загальною для усіх цих випадків, є чіткий критерій того, що саме є спробою проникнення, і що саме утворює периметр, що захищається.

Якщо перенести концепцію системи сигналізації в комп'ютерний світ, то вийде базова концепція системи виявлення вторгнень. Необхідно визначити, чим насправді являється периметр захисту комп'ютерної системи або мережі. Очевидно, що периметр захисту в даному випадку – це не стіна і не обгороджування. Периметр захисту мережі є віртуальним периметром, усередині якого знаходяться комп'ютерні системи. Цей периметр може визначатися міжмережевими екранами, точками розділення з'єднань або настільними комп'ютерами з модемами. Цей периметр може бути розширений для утримання домашніх комп'ютерів співробітників, яким дозволено з'єднуватися один з одним, або партнерів по бізнесу, яким дозволено підключатися до мережі. З появою в діловій взаємодії безпровідних мереж периметр захисту організації розширюється до розміру безпровідної мережі.

Сигналізація, що оповіщає про проникнення грабіжника, призначена для виявлення будь-яких спроб входу в область, що захищається, коли ця область не використовується. Система виявлення вторгнень IDS призначена для розмежування авторизованого входу і несанкціонованого проникнення, що реалізується набагато складніше. Тут можна як приклад привести ювелірний магазин з сигналізацією проти грабіжників. Якщо хто-небудь, навіть власник магазину, відкриє двері, то спрацює сигналізація. Власник повинен після цього повідомити компанію, обслуговуючу сигналізацію, про те, що це він відкрив магазин, і що все гаразд. Систему IDS, навпаки, можна порівняти з охоронцем, що стежить за усім, що відбувається в магазині, і що виявляє несанкціоновані дії (як, наприклад, пронос вогнепальної зброї). На жаль, у віртуальному світі «вогнепальна зброя» дуже часто залишається непомітною.

Другим питанням, яке необхідно враховувати, є визначення того, які події є

порушенням периметра безпеки. Чи є порушенням спроба визначити працюючі комп'ютери? Що робити у разі проведення відомої атаки на систему або мережу? У міру того як задаються ці питання, стає зрозуміло, що знайти відповіді на них не просто. Більше того, вони залежать від інших подій і від стану системи-мети.

Визначення типів систем виявлення вторгнень

Існують два основні типи IDS: вузлові (HIDS) і мережеві (NIDS). Система HIDS розташовується на окремому вузлі і відстежує ознаки атак на цей вузол. Система NIDS знаходиться на окремій системі, що відстежує мережевий трафік на наявність ознак атак, що проводяться в підконтрольному сегменті мережі. На рис. 2.5 показані два типи IDS, які можуть бути присутніми в мережевому середовищі.

Вузлові IDS

Вузлові IDS (HIDS) є системою датчиків, що завантажуються на різні сервера організації і керованих центральним диспетчером. Датчики відстежують різні типи подій (детальніший розгляд цих подій наводиться в наступному розділі) і роблять певні дії на сервері або передають повідомлення. Датчики HIDS відстежують події, пов'язані з сервером, на якому вони завантажені. Сенсор HIDS дозволяє визначити, чи була атака успішною, якщо атака мала місце на тій же платформі, на якій встановлений датчик.

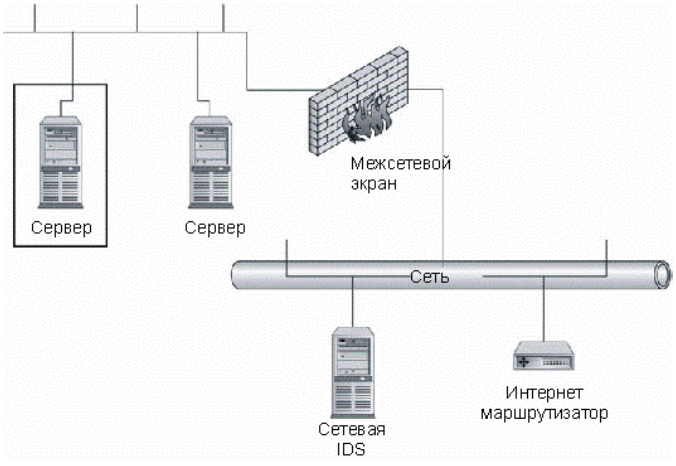


Рис. 2.5. Приклади розміщення IDS в мережевому середовищі

Як буде показано далі, різні типи датчиків HIDS дозволяють виконувати різні типи завдань по виявленню вторгнень. Не кожен тип датчиків може використовуватися в організації, і навіть для різних серверів усередині однієї організації можуть знадобитися різні датчики. Слід зауважити, що система HIDS, як правило, коштує дорожче, ніж мережева система, оскільки в цьому випадку кожен

сервер повинен мати ліцензію на датчик (датчики дешевші для одного сервера, проте загальна вартість датчиків більше в порівнянні з вартістю використання мережевих IDS).

З використанням систем HIDS пов'язано ще одне питання, що полягає в можливостях процесора на сервері. Процес датчика на сервері може займати від 5 до 15 % загального процесорного часу. Якщо датчик працює на активно використовуваній системі, його присутність негативно позначиться на продуктивності і, таким чином, доведеться придбавати продуктивнішу систему.

Вірогідне виникнення розбіжностей, пов'язаних з управлінням і налаштуванням, між адміністраторами безпеки (керівниками роботою IDS) і системними адміністраторами. Оскільки процес повинен постійно знаходитися в активному стані, потрібна хороша координація в їх роботі.

Існує п'ять основних типів датчиків HIDS:

– аналізатори журналів;
– датчики ознак;
– аналізатори системних викликів;
– аналізатори поведінки додатків;
– контролери цілісності файлів.

Слід зауважити, що кількість датчиків HIDS збільшується, і деякі продукти пропонують функціональні можливості, що передбачають використання датчиків більш ніж п'яти основних видів.

Аналізатори журналів

Аналізатор журналу є саме тим, що відбиває саму назву датчика. Процес виконується на сервері і відстежує відповідні файли журналів в системі. Якщо зустрічається запис журналу, що відповідає деякому критерію в процесі датчика HIDS, робиться встановлена дія.

Велика частина аналізаторів журналів налаштована на відстежування записів журналів, які можуть означати подію, пов'язану з безпекою системи. Адміністратор системи, як правило, може визначити інші записи журналу, що представляють певний інтерес.

Аналізатори журналів за своєю природою є реактивними системами. Іншими словами, вони реагують на подію вже після того, як воно сталося. Таким чином, журнал міститиме відомості про те, що проникнення в систему виконане. У більшості випадків аналізатори журналів не здатні запобігти здійснюваній атаці на систему.

Аналізатори журналів, зокрема, добре адаптовані для відстежування активності авторизованих користувачів на внутрішніх системах. Таким чином, якщо в організації приділяється увага контролю за діяльністю системних адміністраторів або інших користувачів системи, можна використати аналізатор журналу для відстежування активності і переміщення запису про цю активність в область, недосяжну для адміністратора або користувача.

Датчики ознак

Датчики цього типу є наборами певних ознак подій безпеки, що зіставляються з трафіком, що входить, або записами журналу. Відмінність між датчиками ознак і аналізаторами журналів полягає в можливості аналізу трафіку, що входить.

Системи, засновані на зіставленні ознак, забезпечують можливість відстежування атак під час їх виконання в системі, тому вони можуть видавати додаткові повідомлення про проведення зловмисних дій. Проте, атака буде успішна або безуспішно завершена перед вступом в дію датчика HIDS, тому датчики цього типу вважаються реактивними. Датчик ознак HIDS є корисним при відстежуванні авторизованих користувачів усередині інформаційних систем.

Аналізатори системних викликів

Аналізатори системних викликів здійснюють аналіз викликів між додатками і операційною системою для ідентифікації подій, пов’язаних з безпекою. Датчики HIDS цього типу розміщують програмну спайку між операційною системою і додатками. Коли додатку вимагається виконати дію, його виклик операційної системи аналізується і зіставляється з базою цих ознак. Ці ознаки є прикладами різних типів поведінка, яка являє собою атакуючі дії, або об’єктом інтересу для адміністратора IDS.

Аналізатори системних викликів відрізняються від аналізаторів журналів і датчиків ознак HIDS тим, що вони можуть запобігати діям. Якщо додаток генерує виклик, що відповідає, наприклад, ознаці атаки на переповнювання буфера, датчик дозволяє запобігти цьому виклику і зберегти систему у безпеці.

Необхідно забезпечувати правильну конфігурацію датчиків цього типу, оскільки їх некоректне налаштування може викликати помилки в додатках або відмови в їх роботі. Такі датчики, як правило, забезпечують можливість функціонування в тестовому режимі. Це означає, що датчик відстежує події, але не робить ніяких блокуючих дій; цей режим можна використати для тестування конфігурації без блокування роботи легітимно використовуваних застосувань.

Аналізатори поведінки додатків

Аналізатори поведінки додатків аналогічні аналізаторам системних викликів, тому що вони застосовуються у вигляді програмної спайки між додатками і операційною системою. У аналізаторах поведінки датчик перевіряє виклик на предмет того, чи дозволено додатку виконувати цю дію, замість визначення відповідність виклику ознакам атак. Наприклад, веб-серверу зазвичай дозволяється приймати мережеві з'єднання через порт 80, прочитувати файли у веб-каталозі і передавати ці файли по з'єднаннях через порт 80. Якщо веб-сервер спробує записати або рахувати файли з іншого місця або відкрити нові мережеві з'єднання, датчик виявить невідповідне нормі поведінка сервера і заблокує дію.

При конфігурації таких датчиків необхідно створювати список дій, дозволених для виконання кожним застосуванням. Постачальники датчиків цього типу надають шаблони для найширше використовуваних застосувань. Будь-які «доморослі» застосування повинні аналізуватися на предмет того, які дії їм дозволяється виконувати, і виконання цього завдання має бути програмно реалізоване в датчику.

Контролери цілісності файлів

Контролери цілісності файлів відстежують зміни у файлах. Це здійснюється за допомогою використання криптографічної контрольної суми або цифрового підпису файлу. Кінцевий цифровий підпис файлу буде змінений, якщо станеться зміна хоч би малої частини початкового файлу (це можуть бути атрибути файлу, такі як час і дата створення). Алгоритми, використовувані для виконання цього процесу, розроблялися з метою максимального зниження можливості для внесення змін до файлу зі збереженням колишнього підпису.

При первинній конфігурації датчика кожен файл, що підлягає моніторингу, піддається обробці алгоритмом для створення початкового підпису. Отримане число зберігається у безпечному місці. Періодично для кожного файлу цей підпис перераховується і зіставляється з оригіналом. Якщо підписи співпадають, це означає, що файл не був змінений. Якщо відповідності немає, значить, у файл були внесені зміни.

Робота датчика цього типу сильно залежить від якості контролю над конфігурацією. Якщо організація не здійснює управління датчиком на належному рівні, то датчик, як правило, виявляє усі типи змін, що вносяться у файл, які, насправді, можуть бути легітимними, але невідомими датчику.

Контролер цілісності файлів не здійснює ідентифікацію атаки, а деталізує

результати проведеної атаки. Таким чином, у разі атаки на веб-сервер сама атака залишиться непоміченою, але буде виявлено ушкодження або зміну домашньої сторінки веб-сайту. Те ж саме відноситься і до інших типів проникнень в систему, оскільки в процесі багатьох з них здійснюється зміна системних файлів.

Мережеві IDS

NIDS є програмним процесом, працюючим на спеціально виділеній системі. NIDS перемикає мережеву карту в системі в нерозбірливий режим роботи, при якому мережевий адаптер пропускає увесь мережевий трафік (а не тільки трафік, спрямований на цю систему) в програмне забезпечення NIDS. Після цього відбувається аналіз трафіку з використанням набору правил і ознак атак для визначення того, чи представляє цей трафік який-небудь інтерес. Якщо це так, то генерується відповідна подія.

На даний момент більшість систем NIDS базуються на ознаках атак. Це означає, що в системи вбудований набір ознак атак, з якими зіставляється трафік в каналі зв'язку. Якщо відбувається атака, ознака якої відсутня в системі виявлення вторгнень, система NIDS не помічає цю атаку. NIDS-системи дозволяють вказувати трафік, що цікавиться, за адресою джерела, кінцевою адресою, портом джерела або кінцевим портом. Це дає можливість відстежування трафіку, що не відповідає ознакам атак. Найчастіше при застосуванні NIDS використовуються дві мережеві карти (рис. 2.6). Одна карта використовується для моніторингу мережі. Ця карта працює в «прихованому» режимі, тому вона не має IP-адреси і, отже, не відповідає на вхідні з'єднання.

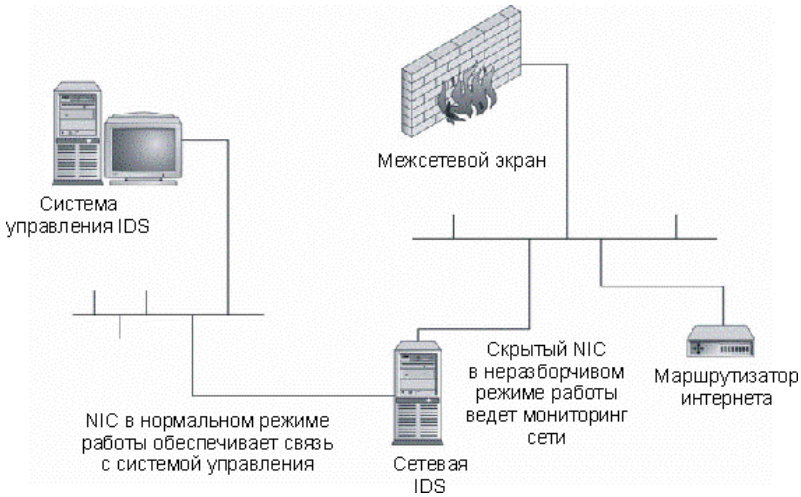


Рис. 2.6. Конфігурація NIDS з двома мережевими картами

У прихованої карти відсутній стек протоколів, тому вона не може відповідати на такі інформаційні пакети, як пинг-запити. Друга мережева карта використовується для з'єднання з системою управління IDS і для відправки сигналів

тривоги. Ця карта приєднується до внутрішньої мережі, невидимої для тієї мережі, відносно якої робиться моніторинг.

Серед переваг використання NIDS можна виділити наступні моменти:

– NIDS можна повністю приховати в мережі таким чином, що зловмисник не знатиме про те, що за ним ведеться спостереження;

– одна система NIDS може використовуватися для моніторингу трафіку з великим числом потенційних систем-цілей;

– NIDS може здійснювати перехоплення вмісту усіх пакетів, що спрямовуються на систему-мету.

Серед недоліків цієї системи необхідно відмітити наступні аспекти:

– система NIDS може тільки видавати сигнал тривоги, якщо трафік відповідає попередньо встановленим правилам або ознакам;

– NIDS може упустити потрібний трафік, що цікавиться, із-за використання широкої смуги пропускання або альтернативних маршрутів;

– система NIDS не може визначити, чи була атака успішною;

– система NIDS не може переглядати зашифрований трафік;

– у комутованих мережах (на відміну від мереж із загальними носіями) потрібно спеціальні конфігурації, без яких NIDS перевірятиме не увесь трафік.

2.4.2. Класифікація політик виявлення вторгнень

При створенні політики IDS необхідно виконати наступні кроки:

1. Визначити цілі створення IDS.
2. Вибрати об’єкти моніторингу.
3. Вибрати дії у відповідь.
4. Встановити пороги.
5. Застосувати політику.

Визначення цілей застосування та об’єкти моніторингу IDS

Цілі використання IDS визначають вимоги для політики IDS. Потенційно цілями застосування IDS є наступні:

– виявлення атак;

– запобігання атакам;

– виявлення порушень політики;

– примус до використання політик;

– примус до наслідування політиків з’єднань;

– збір доказів.

Майте на увазі, що цілі використання пристрою можуть комбінуватися, і конкретні цілі застосування будь-якої IDS залежать від організації. Набір цілей ні в якому разі не обмежується цим списком. IDS дозволяє організації виявляти початок проведення атаки і здійснювати збір доказів або запобігання додатковому ушкодженню за допомогою усунення аварійних ситуацій. Зрозуміло, це не єдина мета, для досягнення якої застосовується IDS. Оскільки IDS здійснює збір деталізованої інформації по багатьох подіях, що відбуваються в мережі і на комп'ютерах організації, вона також може ідентифікувати дії, що порушують політику, і реальний рівень використання мережевих ресурсів.

Розпізнавання атак

Розпізнавання атак є однією з головних цілей використання IDS. Система IDS запрограмована на пошук певних типів подій, які служать ознаками атак. В якості простого прикладу приведемо з'єднання через TCP -порт 80 (HTTP), за яким йде URL, що містить розширення .bat. Це може бути ознакою того, що зловмисник намагається використати уразливість на веб-сервері IIS.

Велику частину атак ідентифікувати не просто. Наприклад, досі в інтернеті широко поширені атаки з вгадуванням пароля. Система HIDS може містити правило, згідно з яким після трьох невдалих спроб входу через короткі проміжки часу вхід в цей обліковий запис блокується. Для цього HIDS повинна відстежувати час і число невдалих спроб входу на кожному обліковому записі, що фіксується в журналі, і скидати лічильник у разі успішного входу або витікання часу.

Ще складнішим прикладом розпізнавання атак є ситуація, коли зловмисник намагається вгадати паролі на декількох облікових записах і системах. Той, що в даному випадку атакує не пробуватиме увійти до одного і того ж облікового запису двічі за короткий проміжок часу, а спробує використати цей пароль в кожному обліковому записі. Якщо час кожної спроби досить великий, лічильники на окремих облікових записах скидатимуться, перш ніж зловмисник тричі здійснить невдалий вхід в систему з використанням цього облікового запису. Єдиним способом виявити таку атаку являється зіставлення інформації з журналів різних систем. Такий аналіз здійснює система HIDS, здатна зіставляти інформацію з декількох комп'ютерів.

Моніторинг політики

Моніторинг політики – це менш помітний аспект діяльності по виявленню атак. Метою системи IDS, налаштованої на відстежування політики, є відстежу-

вання виконання або невиконання політики організації. У найпростішому випадку NIDS можна настроїти на відстежування усього веб-трафіку поза мережею. Така конфігурація дозволяє відстежувати будь-яку невідповідність політикам використання інтернету. Якщо в системі конфігурований список веб-сайтів, що не відповідає веб-стандартам корпоративного використання, NIDS зафіксує будь-які підключення до таких сайтів.

Система NIDS також перевіряє відповідність конфігураціям маршрутизатора або міжмережевого екрану. В цьому випадку NIDS налаштовується на відстежування трафіку, який не повинен проходити через маршрутизатор або міжмережевий екран. При виявленні такого трафіку визначається порушення корпоративної політики міжмережевих екранів.

Використання IDS для моніторингу політики може зайняти дуже багато часу і зажадати великої кількості дій з конфігурації.

Примус до використання політики

Застосування системи IDS в якості засобу примусового використання політики виводить конфігурацію моніторингу політики на більш високий рівень. При відстежуванні політики IDS налаштовується на виконання дій при порушенні політики. У першому прикладі в розділі «Моніторинг політики» IDS з примусом до використання політики не лише визначить спробу з'єднання з недоступним вебсайтом, але і зробить заходи по запобіганню цій дії.

Обробка інциденту

Система IDS може виявитися корисною після виявлення інциденту. В цьому випадку за допомогою IDS можна зібрати докази. NIDS можна настроїти на відстежування певних з'єднань і ведення повноцінного журналу по обліку трафіку. В той же час можна використати і HIDS для фіксації усіх записів журналу для певного облікового запису системи.

Вибір об'єкту моніторингу

Вибір об'єкту моніторингу залежить від цілей, поставлених перед системою IDS, і від середовища, в якій IDS функціонуватиме. Наприклад, якщо мета IDS полягає у виявленні атак, і IDS розташована в інтернеті за межами міжмережевого екрану компанії, то IDS потрібно буде відстежувати увесь трафік, що поступає на міжмережевий екран, для виявлення атак, що входять. В якості альтернативи IDS можна розмістити в межах зони, що захищається міжмережевим екраном, для визначення тільки тих атак, які успішно здолали міжмережевий екран.

Вихідний трафік в даному випадку може ігноруватися (рис. 2.7). У таблиці 2.1 наводяться приклади об'єктів моніторингу при використанні конкретних політик.

Вибір об'єкту моніторингу визначає розташування датчиків. Датчики можуть бути розташовані поза міжмережевим екраном, усередині мережі, на системах з секретною інформацією або на системах, використовуваних спеціально для збору і обробки даних журналу.

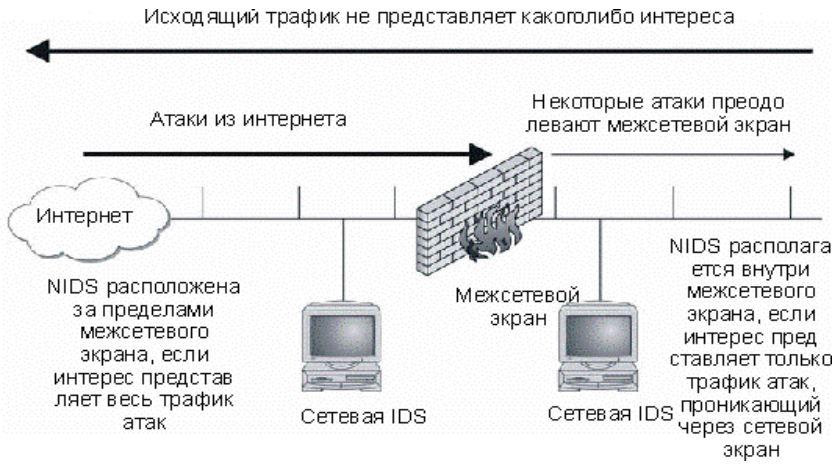


Рис. 2.7. Приклад вибору об'єкту моніторингу

Ключовим моментом, про який необхідно пам'ятати при винесенні рішення з приводу розміщення датчика IDS, є те, що датчик повинен мати можливість перегляду подій, що цікавляться, будь то мережевий трафік або записи журналу. Якщо події, що цікавляться, не долають міжмережевий екран, то не рекомендується розміщувати датчик NIDS в області, що захищається міжмережевим екраном. Аналогічно, якщо події, що цікавляться, фіксуються тільки на головному контролері домена мережі Windows NT, програмне забезпечення HIDS має бути розташоване на головному контролері домена, навіть якщо зловмисник фізично розташовується на робочій станції усередині мережі.

При розміщенні датчиків NIDS необхідно керуватися ще одним ключовим правилом. Якщо в мережі використовуються комутатори замість концентраторів, датчик NIDS правильно не працюватиме, якщо він просто підключений до порту комутатора. Комутатор відправлятиме тільки трафік, спрямований на датчик, до того порту, до якого підключений датчик. У випадку з комутованою мережею існують два варіанти використання датчиків NIDS: застосування порту, що відстежує комутатор, або застосування мережевого розгалужувача. На рис. 2.8 показані конфігурації обох типів.

Таблиця 2.1

Приклади інформації, що відстежується за наявності політики IDS

Політика	**NIDS**	**HIDS**
Виявлення атак	Увесь трафік, що поступає на системи (мережеві екрани, веб-сервери, сервери додатків і так далі), що потенційно атакуються	Невдалі спроби входу. Спроби з'єднання. Вдалий вхід з видалених систем.
Запобігання атакам	Те ж, що і для виявлення атак	Те ж, що і для виявлення атак.
Виявлення порушень політики	Увесь трафік HTTP, що формується на системах клієнтах. Увесь трафік FTP, що формується на системах клієнтах	Успішні HTTP-з'єднання. Успішні FTP-з'єднання. Завантажувані файли.
Примус до використання політик	Те саме, що і для виявлення порушень політики	Те ж, що і для виявлення порушення політики.
Примус до відповідності політикам з'єднань	Увесь трафік, що порушує примусово використовувану політику з'єднання	Успішні з'єднання із заборонених адрес або по заборонених портах.
Збір доказів	Вміст усього трафіку, що формується на системі-меті або атакуючій системі	Усі успішні підключення, витікаючі з атакуючої системи. Усі невдалі з'єднання з атакуючих систем. Усі натиснення клавіш з інтерактивних сеансів на атакуючих системах.

При використанні порту може виникнути конфлікт з персоналом по обслуговуванню мережі через те, що цей порт може використовуватися для дозволу проблем, що виникають в мережі. Окрім цього, багато комутаторів дозволяють вести моніторинг (деякими виробниками замість цього слова використовується термін «зв'язування») тільки одного порту одноразово.

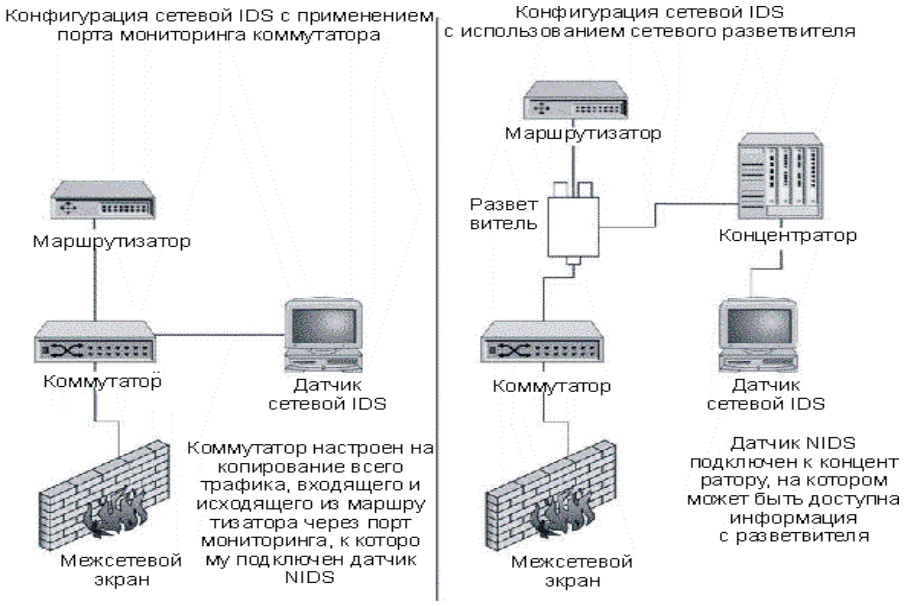


Рис. 2.8. Конфігурації датчика мережевої IDS для комутованої мережі

Порт моніторингу, як правило, не дозволяє здійснювати моніторинг магістралі комутатора. Ця функція не працюватиме у будь-якому випадку, оскільки магістраль комутатора передає дані зі швидкістю в дещо мегабіт в секунду, і датчик

NIDS використовує з'єднання 100BaseT (швидкість 100 мегабіт в секунду). Таке з'єднання не дозволяє здійснювати передачу даних NIDS, тому в цій конфігурації не видається можливим переривання з'єднань.

Розгалужувачі – це пасивні дротяні з'єднання між двома пристроями (наприклад, між маршрутизатором і комутатором). Як правило, розгалужувач підключається до концентратора, до якого також приєднаний датчик NIDS. Це дозволяє датчику відстежувати трафік.

Розгалужувач не дозволяє датчику NIDS здійснювати передачу даних, тому в цій конфігурації переривання з'єднань також неприпустимо.

Види обробки подій, встановлення порогів

Вибір дій у відповідь. Аналогічно вибору об'єкту моніторингу, вибір дій у відповідь залежить від цілей, для яких використовується система IDS. При виникненні події можна вибрати пасивну обробку (дія у відповідь, що не перешкоджає діям того, що атакує) або активну обробку (дія у відповідь, що перешкоджає діям зловмисника). Пасивні дії у відповідь не обов'язково мають на увазі дозвіл продовження події, але не допускають виконання безпосередніх операцій самою системою IDS. Цей момент необхідно мати на увазі. Також слід зважено підійти до вибору автоматичної або ручної обробки подій.

Пасивна обробка подій – це найбільш поширений тип дій, що робляться при виявленні вторгнення. Причина цьому проста – пасивні дії у відповідь забезпечують меншу вірогідність ушкодження легітимного трафіку, являючись, в той же час, найбільш простими для автоматичного застосування. Як правило, пасивні дії у відповідь здійснюють збір більшого числа інформації або передають повідомлення особам, що мають право на вжиття жорсткіших заходів.

Запобігання спробі атаки є сьогодні найширше використовуваним методом обробки події атаки. У більшості випадків такий метод обробки подій залишається встановленим за умовчанням після установки в організації підключення до інтернету і міжмережевого екрану. Надалі, після виконання усіх дій з налаштування, організації довіряють захист від атак з інтернету міжмережевим екранам.

Цей тип дій у відповідь може використовуватися в складніших системах IDS. IDS налаштовується на ігнорування атак через неіснуючі служби або служби, відносно яких міжмережевий екран є невразливим.

Вагомою підставою для ігнорування атаки служить той факт, що системи не чутливі до даного типу атак; наприклад, це відноситься до атаки Microsoft IIS, спрямованої на веб-сервер Unix, і до атаки Sendmail на сервер Microsoft Exchange. Жодна з цих атак не буде успішною, оскільки їх цілі не є уразливими

для цих конкретних атак.

За допомогою інформації, що отримується в результаті сканування уразливостей, можна визначити, які події можна безпечно ігнорувати.

Ведення журналів. При виникненні події будь-якого типу повинна генеруватися максимально можлива кількість інформації для забезпечення детализованного аналізу або для допомоги у вжитті подальших заходів. Занесення події в журнал є пасивною дією у відповідь, у рамках якої більше не здійснюються ніяких операцій. За допомогою збору основних даних (IP -адреса, дата і час, тип події, ідентифікатори процесу, ідентифікатори користувача і так далі) IDS ідентифікує подію як щось, що вимагає подальшої уваги.

Ведення додаткових журналів. Пасивна обробка подій є ефективнішою, якщо здійснюється збір більшої кількості даних про подію, що фіксується в нормальному режимі. Наприклад, якщо звичайний журнал налаштований на збір IP-адрес і номерів портів для усіх з'єднань, то у разі виявлення події може робитися фіксація призначених для користувача ідентифікаторів, ідентифікаторів процесів або фіксація усього трафіку, що проходить через з'єднання.

Ще одним різновидом цього типу обробки події є використання виділеного сервера журналів. У організації може в різних місцях мережі бути присутнім набір систем ведення журналів, які включаються тільки у разі виявлення події. Ці виділені сервери журналів здійснюють збір деталізованої інформації, яка потім використовується для ізолювання джерела трафіку, а також в якості потенційних доказів, якщо подія, що сталася, призведе до судового розгляду.

Повідомлення. На відміну від простої констатації того факту, що подія сталася, повідомлення дозволяють IDS інформувати осіб про подію, що сталася. Повідомлення може мати найрізноманітніші форми, починаючи від мерехтливих вікон і звукових сигналів і закінчуючи поштовими і пейджинговыми повідомленнями. Залежно від обставин той або інший тип прийнятніший за інше. Наприклад, мерехтливі вікна і сирени не дуже корисні, якщо система IDS веде цілодобовий моніторинг. Поштові повідомлення вирушають у видалені місця, але можуть не дійти до одержувача вчасно. Вони також можуть викликати великий об'єм мережевого трафіку, внаслідок чого зловмисник здогадається про присутність системи IDS. Пейджингові повідомлення приходять вчасно (за умови безперебійного функціонування супутника), але можуть не надати досить інформації для вжиття відповідних заходів без попереднього перегляду журналів IDS.

Активна обробка подій

Активна обробка події дозволяє найшвидше зробити можливі заходи для зниження рівня шкідливої дії події. Проте якщо недостатньо серйозно віднестися до логічного програмування дій в різних ситуаціях і не провести належного тестування набору правил, активна обробка подій може викликати ушкодження системи або повну відмову в обслуговуванні легітимних користувачів.

Переривання з'єднань, сеансів або процесів. Ймовірно, найпростішою дією для розуміння є переривання події. Воно може здійснюватися за допомогою переривання з'єднання, використовуваного атакуючим зловмисником (це можливо тільки у тому випадку, якщо подія використовує TCP-з'єднання), із закриттям сеансу користувача або завершенням процесу, що викликав неполадку.

Визначення того, який об'єкт підлягає знищенню, виконується за допомогою вивчення події. Якщо процес використовує надто багато системних ресурсів, краще всього завершити його. Якщо користувач намагається використати конкретну уразливість або здійснити нелегальний доступ до файлів, то рекомендується закрити сеанс цього користувача. Якщо зловмисник використовує мережеве з'єднання в спробах вивчення вразливостей системи, то слід закрити з'єднання.

Дія зі знищення може викликати відмову в обслуговуванні легітимних користувачів. Розберіться в потенційній можливості неправдивих сигналів тривоги, перш ніж виконувати відповідну операцію.

Переналаштування мережі. Припустимо, сталося декілька спроб доступу до комп'ютерів організації з конкретні IP-адреси, отже, є вірогідність того, що з цієї IP-адреси здійснена спроба атаки на інформаційну систему. В даному випадку може знадобитися переналаштування міжмережевого екрану або маршрутизатора. Зміна налаштувань може бути тимчасовою або постійною, залежно від IP-адреси і запрограмованих логічних дій (переривання усього трафіку між партнером по бізнесу може негативно позначитися на продуктивності). Нові фільтри або правила можуть заборонити установку будь-яких з'єднань з видаленим вузлом або заборонити з'єднання лише по конкретних портах.

Обманні дії. Найбільш складним типом активної обробки подій є обманні дії. Відповідь обманом спрямована на введення зловмисника в оману за допомогою створення враження успішного і невиявленого проведення атаки. В той же час система-мета захищається від атаки зловмисника або за допомогою його перенаправлення на іншу систему, або за допомогою переміщення життєво важливих компонентів системи у безпечне місце.

Одним з типів обманних дій є «горщик з медом». Під «горщиком з медом» мається на увазі система або інший об'єкт, що виглядає для зловмисника настільки привабливим, що він не може його пропустити. В той же час за тим, що атакує ведеться спостереження, і усі його дії записуються. Зрозуміло, інформація в «горщику з медом» не є актуальною, але зовні цей об'єкт виглядає як найбільш важливий компонент інформаційної системи.

Автоматична і автоматизована відповідь

Автоматична відповідь – це набір передвстановлених операцій, які виконуються при виникненні певних подій. Такі дії у відповідь, як правило, здійснюються у рамках штатної процедури, що визначає конкретні тригери, що ініціюють набір дій. Ці дії можуть варіюватися від пасивних до активних. Автоматичні дії у відповідь можуть управлятися людьми або комп'ютерами.

У випадку якщо відповідь на інцидент повністю контролюється комп'ютером без участі людини, такі дії у відповідь називаються автоматизованими. Цей тип дій у відповідь повинен контролюватися точно визначеним, ретельно продуманим і добре протестованим набором правил. Оскільки дії у відповідь не вимагають участі користувача, вони виконуватимуться у разі виявлення відповідності встановленому набору правил. Реалізувати автоматизовані дії у відповідь, що примусово знищують мережевий трафік, дуже просто.

У таблиці 2.2 наведені приклади відповідних пасивних і активних дій у відповідь з використанням набору політик, який був визначений вище.

Таблиця 2.2

Приклади дій у відповідь, визначувані політикою IDS

Політика	Пасивні дії у відповідь	Активні дії у відповідь
Виявлення атак	Ведення журналів Ведення додаткових журналів Повідомлення	Немає активної дії у відповідь.
Запобігання атакам	Ведення журналів Повідомлення	Закриття з'єднання. Завершення процесу. Переналаштування міжмережевого екрану.
Виявлення порушень політики	Ведення журналів Повідомлення	Немає активної дії у відповідь.
Примусове використання політик	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштування проксі.
Примусове використання політик з'єднання	Ведення журналів Повідомлення	Закриття з'єднання. Можливо переналаштування маршрутизатора або міжмережевого екрану.
Збір доказів	Ведення журналів Ведення додаткових журналів Повідомлення	Обманні дії. Можливе закриття з'єднання.

Визначення порогів

Порогові значення забезпечують захист від неправдивих спрацьовувань, що підвищує ефективність політики IDS. Порогові значення можуть використовуватися для фільтрації випадкових подій з метою їх відділення від тих подій, які насправді є загрозою безпеки. Наприклад, співробітник може підключитися до веб-сайту, не пов'язаного з діловою активністю, перейшовши по посиланню, наданою пошуковою системою. Співробітник може виконувати легітимний пошук, але через некоректно заданих параметрів пошуку може відобразитися сайт, що не відноситься до роботи. В даному випадку ця окрема подія не викличе генерацію звіту в системі IDS. Такий звіт даремно зайняв би ресурси при вивченні абсолютно нешкідливої дії користувача.

Аналогічно, порогові значення, що виявляють атаки, мають бути налаштовані на ігнорування зондування низького рівня або окремих подій, пов'язаних зі збором інформації. Серед таких подій можна виділити окрему спробу «фінгеринга» (вказівки) співробітника. Програма-покажчик (фінгер), поширена в системах Unix, як правило, використовується для перевірки коректної адреси електронної пошти або для отримання відкритих ключів. Проте, спроби фінгеринга великого числа співробітників за невеликий проміжок часу можуть бути ознакою того, що зловмисник збирає необхідну інформацію для проведення атаки.

Вибір порогових значень для системи IDS безпосередньо залежить від типів подій і потенційних порушень політики. Неможливо ідентифікувати конкретний універсальний набір порогових значень. Проте, можливо визначити параметри, які необхідно враховувати при налаштуванні порогових значень. Нижче приведені ці параметри:

Досвід користувача. Якщо користувач недостатньо досвідчений і допускає безліч помилок, може видаватися надто багато неправдивих сигналів тривоги.

Швидкісні характеристики мережі. У мережах з низькими швидкостями передачі даних можуть видаватися неправдиві сигнали про події, які вимагають отримання певних пакетів впродовж певного проміжку часу.

Очікувані мережеві з'єднання. Якщо система IDS налаштована на видачу сигналу тривоги для певних мережевих з'єднань, і ці з'єднання часто мають місце, то відбуватиметься надто багато неправдивих спрацьовувань.

Навантаження на співробітника по адмініструванню або безпеці. Великий об'єм роботи співробітників, відповідальних за безпеку, може зажадати установку більш високих порогових значень для зниження числа неправдивих спрацьовувань.

Чутливість датчика. Якщо датчик дуже чутливий, може знадобитися установка більш високих порогових значень, щоб понизити число неправдивих спрацьовувань.

Ефективність програми безпеки. Якщо програма безпеки організації дуже ефективна, вона може передбачати пропуск деяких атак, пропущених IDS внаслідок наявності в інформаційному середовищі інших засобів захисту.

Наявні уразливості. Немає причини для видачі сигналу тривоги у разі атак на відсутні в мережі уразливості.

Рівень секретності систем і інформації. Чим вище рівень секретності інформації, використовуваної в організації, тим нижчими мають бути порогові значення для видачі сигналів тривоги.

Наслідки неправдивих спрацьовувань. Якщо наслідки неправдивих спрацьовувань дуже серйозні, може знадобитися установка більш високих порогових значень для видачі сигналів тривоги.

Наслідки неспрацьовування. Навпаки, якщо дуже серйозні наслідки неспрацьовування (чи пропущених подій), може знадобитися установка нижчих порогових значень.

Порогові значення є строго індивідуальними для кожної організації. Можна мати на увазі основні принципи їх визначення, але в кожній організації необхідно в окремому порядку розглядати конкретну ситуацію і задавати порогові значення згідно з приведеними вище параметрами.

2.4.3. Практика застосування політики IDS

Безпосереднє застосування політики IDS повинне ретельно плануватися, як і сама політика. Слід мати на увазі, що до цього моменту політика IDS розроблялася на аркуші паперу з урахуванням (добре, якщо це так) реальних тестів і досвіду використання. Щоб наразити добре організовану мережу на велику небезпеку, в ній досить усього лише встановити неправильно конфігуровану систему IDS. Отже, після розробки політики IDS і визначення первинних порогових значень необхідно встановити IDS згідно з кінцевою політикою, з мінімальним числом яких-небудь активних заходів. Впродовж деякого часу при оцінці порогових значень слід уважно стежити за роботою IDS. Таким чином, політика може бути перевірена на практиці без ушкодження легітимного трафіку або переривання легального доступу користувачів до комп'ютерів.

Не менш важливо під час випробувального або початкового терміну роботи системи ретельно проводити вивчення роботи IDS по дослідженню процесів, що

відбуваються в системі, щоб оцінити міру коректності інформації, видаваною IDS.

Помилкове звинувачення співробітника або зовнішнього користувача внаслідок некоректного визначення факту порушення політики може негативно позначитися на враженні від функціонування системи і поставити в організації питання про ефективність використання програми IDS.

Конфігурація системи виявлення вторгнень

Система виявлення вторгнень може тільки видавати звіти про ті події, на виявлення яких вона налаштована. Конфігурація IDS складається з двох компонентів. Першими з них є ознаки атак, запрограмовані в системі. Другий компонент – будь-які додаткові, визначені адміністратором, події, що також представляють інтерес. Серед цих подій можуть бути певні типи трафіку або повідомлень журналу.

За допомогою включення в кінцевий продукт ознак атак, постачальник або розробник системи по-своєму інтерпретує рівень важливості вказаних подій. Міра важливості, що привласнюється певним подіям в тій або іншій організації, може бути абсолютно іншою, ніж та, яку передбачив розробник. Може знадобитися змінити параметри за умовчанням для деяких ознак або просто відключити ознаки, не застосовані до організації.

Слід мати на увазі, що система IDS видаватиме попередження тільки про ті події, які вона виявить. Якщо на системі, що відстежується датчиком HIDS, не заносяться в журнал певні події, то датчик HIDS їх не розпізнаватиме. Аналогічно, якщо датчик NIDS не може «бачити» певний трафік, він не видасть попередження навіть у тому випадку, якщо подія станеться.

З умовою правильної конфігурації IDS можна привести чотири типи подій, про які повідомлятиме система IDS:

1. Події дослідження.
2. Атаки.
3. Порушення політики.
4. Підозрілі або нез’ясовні події.

Велика частина часу приділятиметься дослідженню підозрілих подій.

Події дослідження

Події дослідження є спробами того, що атакує зібрати дані про систему перед безпосереднім проведенням атаки. Ці події можна розділити на п’ять категорій:

1. «Приховане» сканування.
2. Сканування портів.
3. Сканування «троянських коней».
4. Сканування вразливостей.
5. Відстеження файлів.

Велика частина цих подій відбувається в мережі, в основному, вони виходять з інтернету і спрямовані на системи із зовнішніми адресами.

Події дослідження являють собою спроби збору інформації про системи. Вони не є подіями, що впливають на систему. Деякі комерційні IDS сприймають події дослідження як події високого пріоритету. З урахуванням того, що ці події не завдають збитку системі, такий підхід можна визнати безрозсудним.

Джерелом подібного трафіку може бути і інша система-жертва, захоплена зловмисником, тому цю інформацію слід повідомляти системним адміністраторам цього вузла.

Приховане сканування. Приховане сканування – це спроби ідентифікації систем, присутніх в мережі, з метою запобігти виявленню системи, з якою проводитиметься атака. Цей тип сканування визначатиметься датчиками NIDS як половинчасте сканування IP або приховане сканування IP, і, як правило, таке сканування спрямоване на велику кількість IP-адрес. Реакцією у відповідь є ідентифікація джерела і інформування власника системи-джерела про те, що його система, швидше за все, піддалася дії зловмисника.

Сканування портів. Сканування портів використовується для визначення служб, працюючих на системах мережі. Системи виявлення вторгнень виявляють сканування портів у разі, коли певне число портів (що відповідає пороговому значенню) на одній системі відкривається впродовж невеликого проміжку часу. Датчики NIDS і деякі датчики HIDS забезпечують ідентифікацію цього типу сканування і складають відповідні звіти. Дії у відповідь на сканування цього типу ідентичні діям у відповідь на приховане сканування.

Сканування «троянських коней». Існує безліч шкідливих програм типу «троянський кінь». Датчики NIDS містять ознаки, визначальні багато з цих програм. На жаль, трафік, спрямований на «троянські» програми, як правило, визначається кінцевим портом пакету. Ця обставина викликає велике число неправдивих спрацьовувань системи виявлення вторгнень. У разі виникнення події «Trojan» слід перевіряти початковий порт трафіку. Приміром, трафік, вихідний з порту 80, як правило, поступає з веб-сайту.

Одним з найбільш поширених типів «троянського» сканування є сканування

BackOrifice. Програма BackOrifice використовує порт 31337, і дуже часто зловмисники здійснюють сканування діапазону адрес для цього порту. Консоль BackOrifice також містить функцію «ping host» (відправка пінг-запитів на вузли), яка здійснює сканування автоматично. Турбуватися нема про що, поки не буде зафіксований вихідний трафік з внутрішньої системи. Знову-таки, в даному випадку треба зв'язатися з власником системи-джерела, оскільки вона, ймовірно, піддалася дії зловмисника.

Сканування вразливостей. Сканування вразливостей розпізнається системою IDS при виявленні великого набору різних ознак атак. Як правило, таке сканування спрямоване на декілька систем. Рідкісні випадки, коли сканування вразливостей робиться по відношенню до діапазону адрес без активних систем.

Сканування вразливостей, здійснюване хакерами, неможливо відрізнити від сканування вразливостей, що проводиться компаніями, які перевіряють рівень захищеності інформаційних систем (у багатьох випадках в цих компаніях використовуються ті ж самі засоби!). Так або інакше, саме по собі сканування не заподіює системі якої-небудь шкоди, проте якщо той, хто атакує виконав сканування, в результаті якого виявилися системи з вразливостями до атаки, йому після цього стає відомо, які системи можна атакувати. Для забезпечення відповідності комп'ютерних систем актуальним проблемам безпеки слід контактувати з власником системи-джерела і перевіряти внутрішні системи організації на наявність самих останніх надбудов безпеки і оновлень.

Як правило, складно відрізнити сканування вразливостей від атаки, оскільки IDS в обох випадках ініціює одні і ті ж події. Різниця тут полягає у кількості подій. Сканування вразливостей супроводжується великим числом різних подій за дуже малий відрізок часу, тоді як при проведенні атак відбуваються однотипні події.

Відстеження файлів. Відстеження файлів або перевірка файлових дозволів, як правило, здійснюється внутрішнім користувачем. Користувач намагається визначити, до яких файлів можна здійснити доступ і що ці файли можуть містити. Цей тип розвідки розпізнається тільки датчиком HIDS і тільки у тому випадку, якщо в системі ведеться журнал спроб несанкціонованого доступу. Окремі події подібного роду, як правило, є безневинними помилками, проте якщо простежується певна схема, то слід зв'язатися з користувачем і з'ясувати, що ж сталося.

Атаки

Події атак вимагають найшвидшої реакції у відповідь. У ідеальному випа-

дку IDS має бути налаштована тільки на ідентифікацію подій високого пріоритету у разі використання відомої внутрішньої уразливості. В цьому випадку має бути негайно застосована процедура обробки інциденту.

Майте на увазі, що IDS не розпізнає різницю між безпосередньою атакою і скануванням вразливостей, яке виглядає як атака. Адміністратор системи IDS повинен проводити оцінку інформації, представленої системою IDS, для визначення того, чи є подія атакою. По-перше, необхідно з'ясувати число подій. Якщо впродовж короткого проміжку часу спостерігався набір ознак різних атак, то це, швидше за все, сканування вразливостей, а не безпосередня атака. Якщо ж виявлена одна ознака атаки, спрямованої на одну або декілька систем, то ця подія може бути справжньою атакою.

Порушення політики

Велика частина систем IDS поставляється з ознаками наступних подій.

– загальний доступ до файлів (Gnutella, Kazaa і т. ін.);
– обмін миттєвими повідомленнями;
– сеанси Telnet;
– команди «r» (rlogin, rsh, rexec).

У більшій частині організацій використання такого трафіку є порушенням політики безпеки. На жаль, такі порушення політики можуть представляти для організації велику небезпеку, ніж безпосередні атаки. У більшості випадків подія відбувається насправді. Таким чином, відкривається доступ до файлів, і системи налаштовуються на дозвіл виконання команди rlogin.

Вибір методу обробки різних порушень політики залежить від внутрішніх політик і процедур, що мають місце в організації. Проте, необхідно роз'яснити усі моменти системному адміністраторові або відповідальній особі, щоб йому стала ясна суть політик організації.

Підозрілі події

Події, що не відповідають повністю жодній з інших категорій, заносяться в категорію підозрілих подій. Підозрілою подією називається подія, яку не вдалося розпізнати. Наприклад, ключ реєстру Windows NT був змінений з незрозумілої причини. Це не схоже на атаку, але в той же час не ясно, які причини зміни ключа. В якості іншого прикладу можна привести пакет з прапорами заголовка, що порушують стандарт протоколу. Це може бути спроба розвідувального сканування, результат несправності мережевої карти системи або пакет, при передачі якого виникли помилки. У даних, що видаються системою IDS, не надається досить

відомостей для чіткого визначення конкретної ситуації і з'ясування того, що сталося – нешкідлива помилка або атака.

Анітрохи не менш підозрілим може виявитися несподіваний мережевий трафік, що з'явився у внутрішній мережі. Якщо робоча станція починає просити SNMP-дані з інших систем, то це може бути як наслідком атаки, так і неправильної конфігурації. Підозрілі події необхідно досліджувати настільки, наскільки дозволяють це робити наявні ресурси.

Дослідження підозрілих подій може бути дуже трудомістким завданням. Нерідко представляється розумним пропустити деякі з цих подій або просто передати інформацію мережевому або системному адміністраторові.

Дослідження підозрілих подій та запобігання вторгненням

При виникненні підозрілих дій слід виконати процедуру, що складається з наступних кроків, щоб визначити, чи є ця дія вторгненням, що вдалося, або спробою проникнення, або воно носить нешкідливий характер. Отже, треба виконати наступні кроки:

1. Ідентифікувати системи.
2. Записувати в журнал відомості про додатковий трафік між джерелом і пунктом призначення.
3. Записувати в журнал увесь трафік, що виходить з джерела.
4. Записувати в журнал вміст пакетів з джерела.

При виконанні кожного кроку необхідно визначати, чи досить очевидних ознак для з'ясування того, чи є ця дія атакою. У наступних розділах наводиться опис цих кроків. При дослідженні події необхідно мати на увазі наступний момент. Якщо подія відбувається один раз і більше не повторюється, то дуже важко отримати яку-небудь додаткову інформацію (крім того, звідки поступив трафік). Поодинокі аномалії досліджувати практично неможливо.

Ідентифікація систем

Першим кроком при дослідженні підозрілої активності є ідентифікація систем, що беруть участь у дії. Ця процедура може полягати в перетворенні IP-адрес в імена вузлів. В деяких випадках ім'я вузла знайти не вдається (система не має запису DNS; це клієнт DHCP; видалений DNS-сервер знаходиться в неактивному стані і т. ін.). Якщо пошук DNS закінчується невдачею, то слід спробувати ідентифікувати вузол іншими способами, наприклад, пошуком в реєстрі American Registry of Internet Numbers (ARIN) за адресою http://www.arin.net/, в Internic за

адресою http://www.networksolutions.com/ або в інших каталогах інтернету. Утиліти, такі як Sam Spade (знаходяться за адресою http://samspade.org/), також допоможуть в даному випадку. Неможливість ідентифікації джерела або пункту призначення підозрілих дій не є достатнім доказом того, що подія насправді є атакою. Аналогічно, успішна ідентифікація систем не є достатнім доказом «нешкідливості» виявлених дій.

Джерело підозрілого трафіку може не бути безпосереднім джерелом атаки. Спроби проведення атаки на відмову в обслуговуванні, як правило, проводяться з підміненими початковими адресами, і спроби несанкціонованого доступу або зондування можуть виходити з інших систем, захоплених зловмисником.

Запис в журнал додаткового трафіку

Одна-єдина окрема подія (наприклад, порушення IP-протоколу) може не являти повну інформацію про трафік між двома системами. Іншими словами, необхідно розуміти контекст підозрілих дій. Хорошим прикладом тут служить ознака атаки Sendmail WIZ. Ця ознака ідентифікує спробу використання команди WIZ в програмі Sendmail. Ця подія безпеки ідентифікує будь-яке входження команди WIZ в повідомленні. Якщо команда WIZ є присутньою в тілі повідомлення, то це визначено не спроба вторгнення. Розуміння контексту події допомагає визначати неправдиві спрацьовування.

Налаштуйте IDS на відстежування усього трафіку між джерелом підозрілої активності і пунктом призначення. Як приклад використайте таблицю 2.3.

Тепер поставимо питання, що ж це усе нам дає. По-перше, ми отримуємо уявлення про інший трафік, що має місце між джерелом і пунктом призначення. Якби пакет WIZ був єдиним трафіком між двома системами, з цього можна було зробити висновок про те, що це схоже на спробу проникнення в систему. Навпаки, якщо спостерігається велике число трафіку SMTP (пошта) між двома системами, то, швидше за все, це звичайний легітимний поштовий трафік.

Таблиця 2.3

Приклад конфігурації IDS із записом в журнал усього трафіку між двома системами

Ім’я події	Дія	IP-адреса джерела	IP-адреса пункту призначення	Протокол	Порт джерела	Кінцевий порт
SUS_ACT	Повідомлення, занесення в журнал	Джерело підозрілої активності	Пункт призначення підозрілої активності	TCP, UDP і/або ICMP, залежно від типу виявленої активності	Будь-хто	Будь-хто

Запис в журнал усього трафіку з джерела

Маючи на увазі, що даних, що фіксуються за допомогою запису усього трафіку між двома системами, недостатньо для визначення того, чи є активність легітимною, можна почати збір іншого трафіку, що поступає з джерела. Майте на увазі, що об'єм цього трафіку може бути обмеженим. Якщо джерело підозрілої активності знаходиться в деякій видаленій мережі, то остерігатиметься тільки трафік, що поступає на ваш вузол. Якщо ж джерело локальне, то можливий збір усього трафіку з цього комп'ютера, що дасть набагато ширше уявлення про те, що ж насправді відбувається.

Щоб розпочати збір усього трафіку з джерела, налаштуйте детектор IDS на збір усієї інформації з підозрілого джерела. Приклад такої конфігурації наведений в таблиці 2.4.

Таблиця 2.4

Приклад конфігурації IDS, призначеної для занесення в журнал усього трафіку

Ім'я події	**Дія**	**IP-адреса джерела**	**IP-адреса пункту призначення**	**Протокол**	**Порт джерела**	**Кінцевий порт**
SUS_SRC	Повідомлення, запис в журнал	Джерело підозрілих дій	Будь-хто	TCP, UDP і/або ICMP, залежно від типу виявленої активності	Будь-хто	Будь-хто

Така конфігурація, як правило, генерує деяку інформацію, що не представляє якої-небудь цінності для дослідження. До тих пір, поки можлива об'єктивна оцінка інформації, цей журнал можна використати для складання детальної картини взаємодій, що відбуваються, мають місце між джерелом і пунктом призначення. Спробуйте вникнути в суть спостережуваної активності. Чи є спостережувана активність веб-трафіком? Чи виходить трафік з підозрілого джерела, або ж його джерелом є ваш вузол?

На цьому етапі дослідження має бути відома наступна інформація.

– ім'я системи-джерела;

– тип і частота трафіку, обмін яким відбувається між джерелом і пунктом призначення;

– тип і частота трафіку, обмін яким відбувається між джерелом і будь-якими іншими системами вашого вузла.

Ця інформація забезпечує досить детальне уявлення про природу підозрілого трафіку. Проте, міра очевидності того, що відбувається може не сказати про те, чи є спостережувана активність спробою атаки.

Запис в журнал вмісту пакетів з джерела

Кінцевим кроком дослідження, що проводиться, є запис в журнал вмісту пакетів, що виходять з джерела. Слід зауважити, що цей підхід корисний тільки при роботі з текстовими протоколами, такими як telnet, FTP, SMTP і HTTP (в деякій мірі). Якщо використовуються двійкові протоколи або протоколи з шифруванням, цей підхід абсолютно даремний. Для реалізації описаного методу необхідно змінити конфігурацію IDS, як показано в таблиці 2.5.

За допомогою занесення в журнал вмісту пакетів можна скласти повний запис сеансу, а також зафіксувати команди, що безпосередньо відправляються в пункт призначення.

Таблиця 2.5

Приклад конфігурації IDS, що здійснює перехоплення вмісту пакетів

Ім'я події	**Дія**	**IP-адреса джерела**	**IP-адреса пункту призначення**	**Протокол**	**Порт джерела**	**Кінцевий порт**
SUS_ACT	Повідомлення, запис в журнал утримуваного пакету	Джерело п дозрілої а тивності	Пункт призначення підозрілої активності	TCP або UDP	Будь-хто	Порт, на який спрямований підозрілий трафік
SUS_ACT	Повідомлення, запис в журнал утримуваного пакету	Пункт при начення під зрілої акти ності	Джерело підозр лої активності	TCP або UDP	Порт, на який спрямований підозрілий трафік	Будь-хто

Після фіксації деяких даних необхідно проглянути знайдену інформацію. Чи означає сеанс потенційну атаку, або ж усе виглядає в межах допустимого? Скомбінувавши ці дані з іншою знайденою інформацією, можна знайти відповідь на це питання. Якщо цього зробити не вдалося, спробуйте знайти людину, у якої є досвід роботи з досліджуваним протоколом.

Запобігання вторгненням

Запобігання вторгненням стало основним завданням продуктів, що розроблялися останнім часом, в області виявлення вторгнень. Нові концепції спрямовані на зміну природи IDS за допомогою додавання функцій по запобіганню вторгненням замість тільки виявлення. Багато продуктів, що відповідають цій концепції, є абсолютно новими на ринку. Проте, вказана функціональність реалізована у ряді продуктів, що вже зарекомендували себе.

Способи запобігання вторгненням за допомогою системи IDS

Щоб запобігти вторгненню, необхідно або зупинити здійснювану атаку перед її досягненням системи-жертви, або зупинити дію атаки перед виконанням на системі-жертві коду, що використовує уразливість.

Механізм запобігання атаці найлегше розглядати на вузлі, використовуючому HIDS. Наприклад, можна використати аналізатори системних викликів або поведінки додатка. Якщо виклик додатка схожий на атаку, аналізатор системних викликів запобіжить виконанню виклику операційною системою. Якщо додаток намагається виконати неавторизовану операцію, аналізатор поведінки додатка запобіжить її виконанню. У обох випадках HIDS запобігає атаці.

Процес запобігання атаці за допомогою NIDS є складнішим. У стандартній конфігурації NIDS датчик розташовується в тому місці, з якого він може відстежувати трафік (рис. 2.6). При вступі через канал зв'язку даних атаки датчик перехоплює пакет і починає його аналізувати. У деякий момент датчик визначає, що пакет є атакою, і робить дію. Ця дія, як правило, полягає в закритті з'єднання (тільки якщо атака проводиться через з'єднання TCP) або в переналаштуванні міжмережевого екрану для блокування подальшого трафіку з джерела. На жаль, у випадку з NIDS час працює не на користь досягнення мети. Під час аналізу пакету датчиком пакет продовжує свій рух по мережі. У більшості випадків пакет досягає мети ще перед закриттям з'єднання або виконанням дій з переналаштування міжмережевого екрану. Найчастіше атака випереджає дії датчика з її запобігання.

Закриття з'єднання або блокування трафіку з атакуючої системи може понизити рівень ушкодження системи, але не запобіжить дії на неї зловмисника.

Для запобігання за допомогою NIDS успішного проведення атак на систему рішення по пакету повинне прийматися до того, як пакет досягне системи-мети. Це означає, що архітектуру системи NIDS треба змінити так, щоб датчик NIDS був розташований на одному каналі зв'язку з трафіком (як міжмережевий екран), а не просто стежив за трафіком (рис. 2.9), що проходить мимо.

Розглянута архітектура не є єдино можливою. Також можливо розташувати датчик NIDS на міжмережевому екрані або реалізувати його тісний взаємозв'язок з міжмережевим екраном, щоб останній не пропускав трафік без дозволу датчика NIDS.

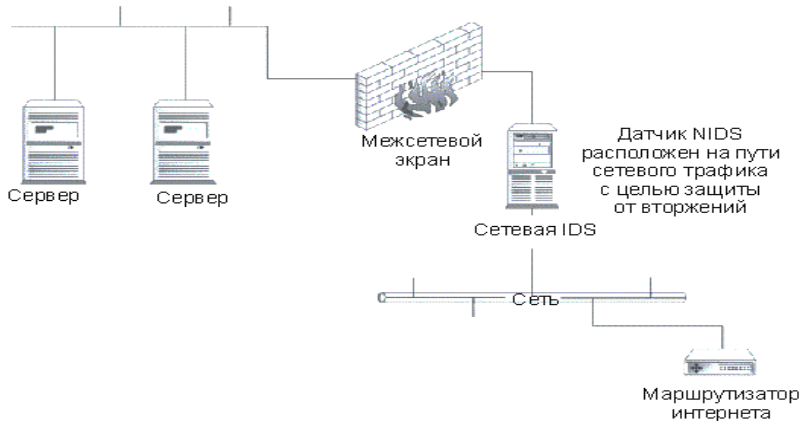


Рис. 2.9. Конфігурація, необхідна для запобігання атакам датчиком NIDS

Проблеми, пов'язані з виявленням вторгнень

Заміна реактивної природи IDS на превентивну створює деякі проблеми. Дійсно, після цієї зміни виникають два серйозні питання: потенційна можливість відмови в обслуговуванні і недостатній середній рівень доступності.

Відмова в обслуговуванні

При запобіганні вторгненням головним механізмом обробки більше не являється повідомлення системи, мережі і системних адміністраторів. Тепер «ядром» системи є блокування спроби виконання дії. Коли IDS блокує атаку, вона запобігає виконанню дії, будь то системний виклик, операція додатка або мережеве з'єднання. Це блокування запобігає атаці. Очевидно, при цьому мається на увазі коректна ідентифікація системою IDS дії як атаки.

Якщо дія, спроба якої була здійснена, насправді не була атакою, а IDS заблокувала його, то, можливо, IDS заблокувала законну дію, що виконується в інформаційному середовищі. Внаслідок цього IDS може викликати відмову в обслуговуванні. Якщо дія, що викликала проблему, була деякою аномалією (наприклад, пакет з помилками), то повторна передача пакету або повторна установка з'єднання, як правило, здійснюються успішно. Проте, якщо IDS некоректно ідентифікує легітимні дії або трафік, приймаючи їх за атаки, то, швидше за все, відмова в обслуговуванні відбуватиметься і надалі.

Датчики IDS видають безліч неправдивих сигналів тривоги. Вжиття превентивних заходів без повного розуміння характеристик неправдивих спрацьовувань і характеристик легітимних дій є причиною виникнення проблем.

Доступність

Доступність мереж і систем є важливою властивістю багатьох комп'ютерних систем. Організації витрачають величезну кількість часу і грошей на налаштування своїх мереж і систем на зниження числа поодиноких неполадок. Якщо датчик IDS встановлений так, що через нього повинен проходити увесь мережевий трафік, датчик NIDS повинен відповідати високому рівню вимог до доступності інших компонентів мережі. Те ж саме відноситься і до датчиків HIDS, розташованих на вузлі. Чи буде вузол продовжувати функціонувати у разі збою програмного забезпечення датчика, або ж він також буде відключений? У інформаційному середовищі, в якому дуже важливий чинник доступності, необхідно вирішити вказані питання перед установкою таких систем.

2.4.4. Методи і засоби аналізу безпеки програмного забезпечення

Широко відомі різні засоби програмного забезпечення виявлення елементів – від простих антивірусних програм-сканерів до складних відладчиків і дизасемблерів – аналізаторів і саме на базі цих засобів і виробився набір методів, якими здійснюється аналіз безпеки ПЗ.

У такій класифікації тип використовуваних для аналізу засобів не береться до уваги – в цьому її перевагу по порівнянню, наприклад, з розділенням на статичний і динамічний аналіз.

Комплексна система дослідження безпеки ПЗ повинна включати як контрольно-випробні, так і логіко-аналітичні методи аналізу, використовуючи переваги кожного з них. З методичної точки зору логіко-аналітичні методи виглядають прийнятнішими, оскільки дозволяють оцінити надійність отриманих результатів і простежити послідовність (шляхом зворотних міркувань) їх отримання. Проте ці методи доки ще мало розвинені і, поза сумнівом, більше трудомісткі, ніж контрольно-випробні.

Контрольно-випробні методи аналізу безпеки програмного забезпечення

Контрольно-випробні методи – це методи, в яких критерієм безпеки програми служить факт реєстрації в ході тестування програми порушення вимог по безпеці, що пред'являються в системі передбачуваного застосування досліджуваної програми. Тестування може проводитися за допомогою тестових запусків, виконання у віртуальному програмному середовищі, за допомогою символічного виконання програми, її інтерпретації і іншими методами.

Контрольно-випробні методи діляться на ті, в яких контролюється процес

виконання програми і ті, в яких відстежуються зміни в операційному середовищі, до яких призводить запуск програми. Ці методи найбільш поширені, оскільки вони не вимагають формального аналізу, дозволяють використати наявні технічні і програмні засоби і швидко ведуть до створення готових методик. Як приклад, можна привести методику пробного запуску в спеціальному середовищі з фіксацією спроб порушення систем захисту і розмежування доступу. Розглянемо формальну постановку завдання аналізу безпеки ПЗ для вирішення її за допомогою контрольно-випробних методів.

Нехай задана безліч обмежень на функціонування програми, що визначають її відповідність вимогам по безпеці в системі передбачуваної експлуатації. Ці обмеження задаються у вигляді безлічі предикатів.

Ця множина складається з двох підмножин:

– підмножини обмежень на використання ресурсів апаратури і операційної системи, наприклад оперативної пам'яті, процесорного часу, ресурсів ОС, можливостей інтерфейсу і інших ресурсів;

– підмножини обмежень, що регламентують доступ до об'єктів, що містять дані (інформацію), тобто областям пам'яті, файлам і так далі.

Для доказу того, що досліджувана програма задовольняє вимогам по безпеці, що пред'являються на передбачуваному об'єкті експлуатації, необхідно довести, що програма не порушує жодної з умов, що входять в *C.* Для цього необхідно визначити безліч параметрів $P=\{pi|i=1,...,K\}$, контрольованих при тестових запусках програми. Параметри, що входять в цю множину визначаються використовуваними системами тестування. Безліч контрольованих параметрів має бути вибрана таким чином, що по безлічі виміряних значень параметрів P можна було отримати безліч значень аргументів A. Після проведення *T* випробувань по вектору отриманих значень параметрів Pi, $i=1,...,T$ можна побудувати вектор значень аргументів Ai, $i=1,...,T$.

Тоді завдання аналізу безпеки формалізується таким чином.

Програма не містить РПЗ, якщо для будь-якого її випробування $i=1,...,T$ безліч предикатів $C=\{cj(a1i, a2i...aMi)|j=1,...,N\}_{\text{істинно}}$.

Очевидно, що результат виконання програми залежить від вхідних даних, оточення і так далі, тому при обмеженні ресурсів, необхідних для проведення випробувань, контрольно-випробні методи не обмежуються тестовими запусками і застосовують механізми екстраполяції результатів випробувань, включають методи символічного тестування і інші методи, запозичені з теорії верифікації (тестування правильності) програми, що досить пропрацювала.

Контрольно-випробні методи аналізу безпеки розпочинаються з визначення

набору контрольованих параметрів середовища або програми. Необхідно відмітити, що цей набір параметрів залежатиме від використовуваного апаратного і програмного забезпечення (від операційної системи) і досліджуваної програми. Потім необхідно скласти програму випробувань, здійснити їх і перевірити вимоги до безпеки, що пред'являються до цієї програми в передбачуваному середовищі експлуатації, на запротокольованих діях програми і змінах в операційному середовищі, а також використовуючи методи екстраполяції результатів і стохастичні методи.

Очевидно, що найбільшу трудність тут представляє визначення набору критичних з точки зору безпеки параметрів програми і операційного середовища. Вони дуже сильно залежать від специфіки операційної системи і визначаються шляхом експертних оцінок. Крім того в умовах обмежених об'ємів випробувань, укладення про виконання або невиконання вимог безпеки як правило носитиме імовірнісний характер.

Логіко-аналітичні методи контролю безпеки програм

При проведенні аналізу безпеки за допомогою логіко-аналітичних методів будується модель програми і формально доводиться еквівалентність моделі досліджуваної програми і моделі РПЗ. У простому випадку моделлю програми може виступати її бітовий образ, в якості моделей вірусів безліч їх сигнатур, а доказ еквівалентності полягає в пошуку сигнатур вірусів в програмі. Складніші методи використовують формальні моделі, засновані на сукупності ознак, властивих тій або іншій групі РПЗ.

Формальна постановка завдання аналізу безпеки логіко-аналітичними методами може бути сформульована таким чином.

Вибирається деяка система моделювання програм, представлена безліччю моделей усіх програм, – *Z*. У вибраній системі досліджувана програма представляється своєю моделлю *M*, що належить безлічі *Z*. Має бути задана безліч моделей РПЗ$V=\{vi|i=1,...,N\}$, отримане або шляхом побудови моделей усіх відомих РПЗ, або шляхом породження безлічі моделей усіх можливих (у рамках цієї моделі) РПЗ. Безліч V є підмножиною безлічі Z. Крім того, має бути задане відношення еквівалентності визначальна наявність РПЗ в моделі програми, позначимо його E(x, y). Це відношення виражає тотожність програми x і РПЗ y, де x – модель програми, y – модель РПЗ, і y належить безлічі V.

Тоді завдання аналізу безпеки зводиться до доказу того, що модель досліджуваної програми *M* належить відношенню $E(M, v)$, де *v* належить безлічі *V*.

Для проведення логіко-аналітичного аналізу безпеки програми необхідно,

по-перше, вибрати спосіб представлення і отримання моделей програми і РПЗ. Після цього необхідно побудувати модель досліджуваної програми і спробувати довести її приналежність до відношення еквівалентності, задаючого безліч РПЗ.

На підставі отриманих результатів можна зробити укладення про міру безпеки програми. Ключовими поняттями тут є «спосіб представлення» і «модель програми». Річ у тому, що на комп'ютерну програму можна дивитися з дуже багатьох точок зору – це і алгоритм, який вона реалізує, і послідовність команд процесора, і файл, що містить послідовність байтів і так далі. Усі ці поняття утворюють ієрархію моделей комп'ютерних програм. Можна вибрати модель будь-якого рівня моделі і спосіб її представлення, необхідно тільки щоб модель РПЗ і програми були задані одним і тим же способом, з використанням понять одного рівня. Іншою серйозною проблемою є створення формальних моделей програм, або хоч би певних класів РПЗ. Механізм завдання відношення між програмою і РПЗ визначається способом представлення моделі. Найбільш перспективним тут видається використання семантичних графів і об'єктно-орієнтованих моделей.

В цілому повний процес аналізу ПЗ включає три види аналізу:

– лексичний аналіз верифікації;

– синтаксичний аналіз верифікації;

– семантичний аналіз програм.

Кожен з видів аналізу є закінченим дослідженням програм згідно своєї спеціалізації.

Результати дослідження можуть мати як самостійне значення, так і корелюватися з результатами повного процесу аналізу.

Лексичний аналіз верифікації припускає пошук розпізнавання і класифікацію різних лексем об'єкту дослідження (програма), представленого у виконуваних кодах. При цьому лексемами є сигнатури. В даному випадку здійснюється пошук сигнатур наступних класів:

– вірусів;

– елементів РПЗ;

– «підозрілих функцій» (лексеми);

– штатних процедур для системних ресурсів і зовнішніх пристроїв.

Пошук лексем (сигнатур) реалізується за допомогою спецпрограм-сканерів.

Синтаксичний аналіз верифікації припускає пошук, розпізнавання і класифікацію синтаксичних структур РПЗ, а також побудову структурно-алгоритмічної моделі самої програми.

Рішення завдань пошуку і розпізнавання синтаксичних структур РПЗ має

самостійне значення для аналізу верифікації програм, оскільки дозволяє здійснювати пошук елементів РПЗ, що не мають сигнатури. Структурно-алгоритмічна модель програми потрібна для реалізації семантичного аналізу.

Семантичний аналіз припускає дослідження програми вивчення сенсу складових її функцій (процедур) в аспекті операційного середовища комп'ютерної системи. На відміну від попередніх видів аналізу, заснованих на статичному дослідженні, семантичний аналіз націлений на вивчення динаміки програми – її взаємодії з довкіллям. Процес дослідження здійснюється у віртуальній операційній середовищу з повним контролем дій програми і відстежуванням алгоритму її роботи по структурно-алгоритмічній моделі.

Семантичний аналіз є найбільш ефективним видом аналізу, але і самим трудомістким. З цієї причини методика поєднує в собі три перелічених вище за аналіз. Вироблені критерії дозволяють розумно поєднувати різні види аналізу, істотно скорочуючи час дослідження, не знижуючи його якості.

Запитання для самоконтролю

1. Методи і засоби аналізу безпеки програмного забезпечення.
2. Контрольно-випробні методи аналізу безпеки програмного забезпечення.
3. Логіко-аналітичні методи контролю безпеки програм.
4. Інформаційні технології та принципи організації інформаційної безпеки.
5. Види та властивості інформації як предмета захисту.
6. Інформаційні технології та проблеми їхньої безпеки.
7. Принципи організації інформаційної безпеки.
8. Моделі управління мережевими ресурсами.
9. Програмні та апаратні засоби захисту в інформаційних системах.
10. Технології захисту інформації при міжмережевій взаємодії.
11. Захист повідомлень при передачі каналами та лініями зв'язку.
12. Принципи побудови мережевих екранів.
13. Технології захисту у мережах на основі протоколів TCP/IP.
14. Реалізація загроз інформації у мережах на основі протоколів TCP/IP.
15. Принципи побудови мереж VPN.
16. Виявлення мережевих атак шляхом аналізу трафіка.
17. Основи захвату та аналізу мережевого трафіка.
18. Виявлення мережевих атак шляхом аналізу трафіка.
19. Надійність та стійкість програмного забезпечення.
20. Методи забезпечення стійкості програмного забезпечення.

ГЛАВА 3.
СУЧАСНІ ТЕХНОЛОГІЇ БЕЗПЕКИ КОРПОРАТИВНИХ МЕРЕЖ

3.1. Забезпечення безпеки корпоративної мережі за OSI моделлю

3.1.1. Безпека на фізичному рівні

Фізичний рівень (physical layer) має справу з передачею бітів по фізичних каналах зв'язку, таких, наприклад, як коаксіальний кабель, вита пара, оптоволоконний кабель або цифровий територіальний канал. До цього рівня мають відношення характеристики фізичних серед передачі даних, такі як смуга пропущення, прешкодозахищеність, хвильовий опір і інші. На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію, наприклад, крутість фронтів імпульсів, рівні напруження або струму сигналу, що передається, тип кодування, швидкість передачі сигналів. Крім цього, тут стандартизуються типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня реалізовуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом.

Прикладом протоколу фізичного рівня може служити специфікація 10Base-T технології Ethernet, яка визначає як кабель, що використовується неекрановану пару категорії з хвильовим опором 100 Ом, роз'єм RJ-45, максимальну довжину фізичного сегмента 100 метрів, манчестерський код для представлення даних в кабелі, а також деякі інші характеристики середи і електричних сигналів.

Найбільш поширених специфікацій фізичного рівня належать:

– EIA-RS-232-C, CCITT V.24/V.28 – механічні/електричні характеристики незбалансованого послідовного інтерфейсу;

– EIA-RS-422/449, CCITT V.10 – механічні, електричні і оптичні характеристики збалансованого послідовного інтерфейсу;

– IEEE 802.3 – Ethernet;

– IEEE 802.5 – Token ring.

Фізичний рівень надає засіб транспортування бітів кадра по мережевому середовищі. Фізичний рівень одержує кадра від канального рівня та кодує його в середовище за допомогою імпульсів (електричних, світлових, мікрохвильових).

Середовище не передає кадри цілком. Середовище передає сигнали, що представляють біти кадра по одному за раз.

Фізичний рівень може так само додавати власні набори сигналів для вказівки початку й кінця кадра.

Стандарти для фізичного рівня пишуть ті ж організації, що й для канального – ITU, IEEE, ISO, ANSI, EIA/TIA, FCC. Вони реалізуються в мережних адаптерах пристроїв. Технології певні цими організаціями включають 4 області стандартів фізичного рівня:

– фізичні й електричні властивості середовища;

– механічні властивості конекторів;

– вистава бітів у вигляді сигналів;

– визначення службових сигналів.

Три основні функції фізичного рівня:

– фізичні компоненти;

– кодування (encding) даних – приведення бітів кадра до визначеного виду;

– сигналізація (signaling) у середовище за допомогою сигналів;

– час біта (bit time) – час приміщення біта в середовище передачі.

Біти можуть представлятися за допомогою зміни амплітуди, частоти, фази сигналу.

NRZ – для вистави 0 і 1 використовує різні рівні напруги. Уразливий до електромагнітної інтерференції й довгим послідовностям 1 і 0. Забезпечує дуже низьку швидкість передачі.

Манчестерське кодування – для вистави 0 і 1 використовує перехід від високої напруги до низького й навпаки. Перехід відбувається в середині часу біта (такту). Застосовується в 10Base-T.

Перед тем як сигналізувати біти кадра в середовище, їх попередньо кодують за допомогою кодових груп. Це дозволяє захиститися від помилок у процесі передачі бітів, збільшити ефективність методів сигналізації, відрізнити біти даних від службових.

Надлишковий код 4B/5B – кодує чотири біти кадра, п’ятьома бітами коду. Це дає 32 комбінації, причому для кодування даних використовується тільки 16 з них. Інші використовуються в службових цілях.

Передача даних може бути обмірювана як:

– смуга пропущення (bandwidth) – кількість інформації, яка може бути передане по середовищу за певний проміжок часу;

– пропускна здатність (throughput) – кількість біт, передане по середовищу за певний проміжок часу;

– корисне навантаження (goodput) – кількість даних користувача, передане по середовищу за певний проміжок часу.

Для побудови мереж застосовують різні види середовищ передачі даних.

Мідний кабель чутливий до електромагнітної інтерференції. Для захисту від неї використовують екрановані типи мідного кабелю.

Неекранована вита пари (unshielded twisted-pair) представляє із себе 4х або 2х парний кабель. Пари перекручуються між собою для зменшення перешкод (crosstalk), що наводяться провідниками один на одного. Усі пари маркуються по кольорах, щоб точно визначити обрану пару на різних кінцях кабелю. У якості конектора застосовується RJ-45. Стандарти розподілу пінів по кольорах у конекторі 586A (застарілий) і 586B.

Прямий кабель (straight-through) – обоє кінці кабелю обжимаються одним стандартом. Застосовується для з'єднання різних пристроїв (ПК – комутатор, роутер – комутатор).

Скретний кабель (crossover) – кінці кабелю обжимаються за різними стандартами. Застосовується для з'єднання однакових пристроїв (комутатор – комутатор, роутер – роутер, ПК – ПК).

Перевернений кабель (rollover) – RJ45 на COM/USB, використовується для підключення до консольних портів мережного встаткування Cisco.

Коаксіальний кабель – складається із двох провідників, центральна жила й обплетення. Раніше застосовувався для побудови локальних мереж, сьогодні застосовується в мережах кабельного телебачення.

Екранована вита пара (shielded twisted-pair cable) – пари екрануються окремо й усі разом. Раніше застосовувався для мереж Token Ring, зараз застосовується для мереж 10G Ethernet.

Мідний кабель може являти загрозу поразки електричним струмом, якщо він підключений до несправного встаткування, або під час грози.

Оболонка кабелю горить і виділяє токсичні речовини.

Оптичний кабель (Fiber-optic) – складається із центральної скляної жили по якій поширюється світло. Використовуються на більших дистанціях, не піддані електромагнітної інтерференції й забезпечують високу швидкість передачі даних. Для дуплексної передачі може використовуватися як кабель із двома жилами так і з однієї.

Одномодове волокно – тонка центральна жила (8–10 мікрон), більші відстані до 100 км, для створення імпульсів використовуються лазери.

Багатомодове волокно – товста центральна жила (50 мікрон), не більші відстані до 2 км, для створення імпульсів використовуються світлодіоди (LED).

Фізичний рівень відповідає за підтримку зв'язку (link), тобто здійснює інтерфейс між мережевим носієм та мережевим пристроєм. На цьому рівні регламентуються напруги, частоти, довжини хвиль, типи конекторів, число й функціональність контактів, схеми кодування сигналів тощо.

Можна виділити два основні середовища передачі даних:

– проводове (за участю кабелів);

– безпроводове (без участі кабелів).

Забезпечення безпеки на фізичному рівні полягає у забезпеченні структурної цілісності мережі. Структурна цілісність мережі – здатність зберігати неподільність системи. Основними загрозами структурної цілісності мережі є:

– проникнення в систему (отримання несанкціонованого доступу до ресурсів мережі);

– фізичне пошкодження мережі;

– створення завад у безпроводових каналах передачі даних.

Для реалізація цих загроз необхідно володіти апріорними знаннями про будову мережі. Проникнення у систему здійснюється з метою вводу хибної інформації, модифікації інформації, що передається в мережі, несанкціонованого користування ресурсами мережі (частотним, часовим, апаратним). Для проникнення в мережі необхідно, щоб порушник:

– мав устаткування сумісне з устаткуванням мережі;

– був здатний розпізнавати структуру і параметри сигналу;

– знав параметри мережі (ідентифікатор мережі, що закриває інфраструктуру мережі; був занесеним в таблицю дозволених адрес в точці доступу, і т. ін.);

– мав ключ шифру (у разі шифрування інформації в мережі) тощо.

Як окремий вид загрози фізичного впливу слід виділити створення завад у мережі. Дана атака може бути реалізована при наявності інформації про засобів безпроводового зв'язку, параметрах сигналу, режиму роботи тощо. Це досягається засобами радіотехнічного моніторингу, після чого, за отриманими даними, робиться висновок про порядок створення завад. Слід зауважити, що найбільш вразливими елементами системи є вузлові об'єкти: ретранслятори, репітери, базові станції, центри комутації, тощо. При їх враженні, виходить з ладу мережа безпроводового зв'язку, окрема зона обслуговування стільникового радіозв'язку чи безпроводового доступу, що збільшує вразливість системи в цілому.

Адміністративними (організаційними) методами з джерелами завад бореться служба радіоконтролю частотних ресурсів, яка повинна розробляти заходи по припиненню випромінювань джерел завад, що заважають зареєстрованим радіозасобам. Згідно рекомендаціям МСЕ такими заходами можуть бути:

– зміна частоти;

– використання направлених антен;

– коректування розкладів або експлуатаційні угоди (розділення за часом);

– зміна класу випромінювання;

– переміщення окремих каналів в багатоканальній системі передачі;

– перенесення навантаження на інші наявні частоти;

– припинення роботи однієї із станцій, що є джерелом завад для інших.

Проте повністю виключити можливість дії завад тільки організаційними методами не можливо, тому необхідно приймати заходи технічного характеру по підвищенню завадостійкості радіозасобів. До їх числа входить використання методів, які основані на просторовій, частотній або поляризаційній селекції сигналів або використання сигналів, структура яких забезпечує підвищену завадостійкість.

3.1.2. Безпека на канальному рівні

Канальний рівень:

– надає доступ до середовища й фреймування для протоколів вищих рівнів;

– контролює як дані містяться в середовище, а так само відслідковує помилки передачі.

Кадр (frame) – протокольний блок даних канального рівня.

Вузол (node) – пристрій підключене до загального середовища передачі даних.

Середовище (media) – середовище передачі даних (кабель, радіохвилі).

Мережа – вузли з’єднані між собою середовищем передачі даних.

Завдяки канальному рівню, протоколам мережного рівня не потрібно турбується про той яка технологія використовується на конкретному відрізку мережі. Що дозволяє протоколам мережного рівня працювати поверх зовсім різних мереж. Протоколи канального рівня визначають інкапсуляцію пакетів у кадри й техніки приміщення бітів у середовище.

Методи контролю доступу до середовища (media access control) описані протоколами канального рівня визначають процеси, за допомогою яких пристрої можуть взаємодіяти із середовищем і передавати кадри в різних мережних середовищах. Фреймуванням і доступом до середовища управляють мережні адаптери пристроїв.

На відміну від інших рівнів, PDU канального рівня на додаток до заголовка

й даних, містить кінцевик (trailer). Так само на початку й наприкінці кадру втримується спеціальна послідовність бітів, по якій приймач розуміє де кадр починається й де закінчується.

Канальний рівень розділяється на два підрівня:

– LLC – фреймуючий пакет і визначальний протокол мережного рівня. (реалізується в драйверах);

– MAC – додає адреси канального рівня й маркірує початок і кінець кадру. (реалізується в мережному адаптері).

Протоколи й стандарти канального рівня пишуться такими організаціями як ISO, IEEE, ITU, ANSI.

Контроль доступу до середовища регулює переміщення кадрів у середовище передачі даних.

Контрольований (controlled) – кожному вузлу виділяється час на передачу даних – Token Ring, FDDI. При цьому:

– тільки одна станція одноразово може передавати дані;

– кожна станція чекає своєї черги;

– немає колізій;

– дані передає тільки станція, що одержала маркер.

Асоціативний (contention-based) – будь-який вузол може передати дані в будь-який момент (Ethernet, Wireless)

– станції можуть передавати в будь-який момент;

– присутні колізії;

– механізми боротьби з колізіями CSMA/CD Ethernet, CSMA/CA Wi-Fi.

Типи передачі даних:

– half duplex – поки одна станція передає, інші чекають своєї черги;

– full duplex – станція може одночасно передавати і ухвалювати дані.

Типи топології:

– логічна – описує як дані передаються по мережі;

– фізична – описує як вузли з’єднані між собою.

Логічна й фізична топології мережі можуть не збігатися.

Точка-точка (Point-to-Point) – тільки два вузли з’єднано один з одним фізично або логічно.

Множинний доступ (multi access) – більш 3 пристроїв з’єднаних загальним середовищем передачі даних.

Кільце (ring) – пристрої з’єднані в кільце або зірку, дані передаються від одного до іншого у вигляді кільця.

Доступ до середовища та фреймування

Одним із завдань канального рівня є перевірка доступності середовища передачі. Інше завдання канального рівня – реалізація механізмів виявлення та корекції помилок. Для цього на канальному рівні біти групуються в набори, звані кадрами (frames). Канальний рівень забезпечує коректність передачі кожного кадру.

Структура кадру може відрізнятися залежно від протоколу канального рівня. Чим складніше умови середовища передачі, тем складніше структура кадру.

Основні поля заголовка кадру для будь-якого протоколу:

– початок кадру;

– адреси;

– довжина кадру або тип протоколу 3 рівня.

Якщо кадр передається в з'єднаннях типу точка-точка (Point-to-Point), необхідність в адресації практично відпадає. Такі кадри можуть використовувати тільки одна адреса призначення, широкомовний. Якщо кадр передається з використання множинного доступу до середовища, у ньому для успішної доставки повинні втримуються обоє адреси й джерела й призначення. У кінцевик (trailer) кадру записується контрольна сума наприклад CRC для перевірки цілісності у вузлі приймання. Так само кінцевик містить біти закінчення кадру.

З погляду інформаційної безпеки канальний рівень є достатньо дослідженим і відповідає за формування та доставку кадру без помилок. На цьому рівні використовується апаратна MAC-адресація та здійснюється обчислення контрольної суми. Широко застосовуються зловмисниками атаки на підміну MAC-адреси, атаки на ARP і Spanning-Tree протоколи, кінцевою метою яких є перехоплення трафіку та одержання доступу до більш важливої конфіденційної інформації. Можливості побудови віртуальних мереж VLAN, які реалізовані на базі комутаторів, створюють загрозу захоплення зловмисником усіх портів VLAN. Активне впровадження безпроводових мереж IEEE 802.11 створило загрозу безконтрольного підключення зловмисників до них.

Небезпека уразливості протоколів канального рівня моделі OSI полягає в тому, що, зламавши мережу на канальному рівні, атакуючий може переступити через засоби захисту на вищих рівнях.

Типи атак на канальному рівні локальних обчислювальних мереж

1. Пасивні:

– підслуховування (sniffing) і аналіз мережного трафіку, використовують недоліки в протоколах і мережному устаткуванні. За допомогою сніфера можна отримати корисну, а інколи і конфіденційну інформацію (наприклад, імена користувачів і паролі);

– підміна довіреного суб'єкта. Велика частина мереж і операційних систем (ОС) використовують IP-адресу комп'ютера, для того, щоб визначати, чи той це адресат, який потрібний. В деяких випадках можливе некоректне привласнення IP (або MAC) – адреси або підміна цих адрес відправника іншою адресою. Такий спосіб атаки називають фальсифікацією адреси.

2. Активні:

– відмова в обслуговуванні (Denial of Service, DOS). Цей тип атак не націлений на діставання доступу до мережі або на здобуття з цієї мережі якої-небудь інформації. Атака DOS робить мережу організації недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування якого-небудь ресурсу мережі, ОС або застосування. Вона паралізує роботу мережі і позбавляє звичайних користувачів доступу до загальних ресурсів організації. При цьому використовуються протоколи TCP і ICMP. Найбільш відомі: TCP SYN Flood; Ping of Death;

– порушення роботи мережі або її ділянок – деякі недоліки протоколів канального рівню не можуть використовуватися передбаченим чином. Тобто, не можна навмисно вплинути на їх поведінку, але є можливість порушити їх нормальну роботу і таким чином розхитати відмовостійкість ділянки мережі або всієї мережі. Приклад: Переповнення таблиці комутації.

Протидіяти наведеним загрозам на канальному рівні можна шляхом застосування MAC- фільтрації, використання брандмауерів для ізоляції різних зон у мережі та відмови від VLAN, а для безпроводових мереж необхідно застосовувати шифрування, автентифікацію та фільтрацію MAC-адрес.

3.1.3. Безпека на мережному рівні

Мережевий рівень – найбільш вразливий рівень з погляду захисту. На ньому формується вся маршрутизована інформація, відправник і одержувач фігурують явно, здійснюється управління потоком. Крім того, протоколами мережевого рівня пакети обробляються на всіх маршрутизаторах, шлюзах та інших проміжних

вузлах. Майже всі специфічні мережеві порушення здійснюються з використанням протоколів цього рівня (читання, модифікація, знищення, дублювання, переорієнтація окремих повідомлень або потоку в цілому, маскування під інший вузол тощо). Захист від таких загроз здійснюється протоколами мережевого і транспортного рівнів і за допомогою засобів криптографічного захисту. На цьому рівні може бути реалізована вибіркова маршрутизація.

Протоколи канального рівня локальних мереж забезпечують доставку даних між вузлами тільки в мережі з відповідною топологією. Це обмеження не дозволяє створювати мережі з розвинутою структурою. Тому для того, щоб з одного боку зберегти простоту процедур передачі даних для типових топологій, а з другого – допустити використання довільних топологій, вводиться додатковий мережний рівень. На мережному рівні сам термін «мережа» наділяють специфічним значенням. В даному випадку під мережею розуміється сукупність комп'ютерів, з'єднаних між собою відповідно до одної з типових топологій, які використовують для передачі даних один із протоколів канального рівня, визначений для даної топології. Всередині мережі доставка даних забезпечується канальним рівнем, тоді як передачу даних між мережами забезпечує мережний рівень, який забезпечує можливість правильного вибору маршруту передачі. Для передачі повідомлення від відправника, що знаходиться в одній мережі, отримувачу в іншій мережі, потрібно здійснити певну кількість транзитних передач між мережами (хоп – hop – стрибок), щоразу вибираючи найкращий маршрут. Для виконання функцій по передачі даних між вузлами по мережі, мережний рівень використовує:

– адресацію;

– інкапсуляцію/декапсуляцию;

– маршрутизацію.

Протоколи мережного рівня: Ipv4, Ipv6, IPX, Appletalk, CLNS/Decnet.

Характеристики Ipv4:

– без установлення сеансу (connectionless);

– ненадійний (unreliable) – не гарантує доставку (best effort), пакети можуть губитися, функції по забезпеченню надійності покладають на протоколи транспортного рівня;

– не залежить від середовища передачі (media independent), крім MTU, канальний рівень повідомляє розмір максимального блоку передачі (MTU) мережному рівню. При перевищенні розміру MTU пакет може бути фрагментований перед передачею.

Розподіл вузлів на групи

Замість того, щоб тримати всі пристрої в одній мережі, більш практично ділити їх на групи.

Групувати пристрої можна по:

– місцю знаходження – групувати вузли, що перебувають поруч (на одному поверсі, в одному будинку);

– цілям – групувати вузли по виконуваних завданнях і типах трафіку;

– приналежності – групувати вузли по приналежності до тієї або іншої компанії, відділу.

Проблеми великих мереж:

– зниження продуктивності – велика кількість вузлів в одному сегменті створює багато широкомовного трафіка, що навантажує мережу;

– погрози безпеки – у точку переходу з однієї мережі в іншу можна налаштувати обмеження за типом трафіку й адрес;

– управління адресацією – вузлам немає необхідності зберігати багато маршрутів, досить знати адреса свого шлюзу.

IP-Адреса є 32-бітною, ієрархічною та складається з 2 частин:

– мережна частина – указує на мережу, у якій перебуває вузол;

– вузлова частина – указує на вузол у мережі.

Розмір мережної частини визначається маскою мережі або довжиною префікса.

Маршрутизація на мережному рівні моделі OSI

Проблема вибору найкращого шляху називається ***маршрутизацією***, і її вирішення є однією з головних задач мережного рівня. Ця проблема ускладнюється ще й тим, що найкоротший шлях не завжди є й найкращим. Деякі алгоритми маршрутизації стараються пристосуватися до зміни навантаження, тоді як інші приймають рішення на основі середніх показників за тривалий час. Вибір маршруту може здійснюватися і за іншими критеріями, наприклад, надійності передачі. Мережний рівень розв’язує також задачі узгодження різних технологій, спрощення адресації у великих мережах та створення надійних і гнучких бар’єрів на шляху небажаного трафіку між мережами.

Повідомлення мережного рівня прийнято називати *пакетами* (packets). При організації доставки пакетів на мережному рівні використовують поняття «номер мережі». В цьому випадку адреса отримувача складається із старшої частини – номера мережі та молодшої – номера вузла в цій мережі. Усі вузли однієї

мережі повинні мати одну й ту ж старшу частину адреси, у зв'язку з чим терміну «мережа» на мережному рівні можна дати й інше, більш формальне визначення: мережа – це сукупність вузлів, мережна адреса яких містить один і той же номер мережі.

На мережному рівні визначаються два види протоколів. Перший вид – мережні протоколи (routedprotocols) – реалізують переміщення пакетів в мережі (саме ці протоколи зазвичай мають на увазі, коли говорять про протоколи мережного рівня). Проте часто до мережного рівня відносять і інший вид протоколів, що називаються протоколами обміну маршрутною інформацією або протоколами маршрутизації (routing protocols). Протоколи мережного рівня реалізуються програмними модулями операційної системи, а також програмними і апаратними засобами маршрутизаторів. На мережному рівні працюють протоколи ще одного типу, які відповідають за відображення адреси вузла, що використовується на мережному рівні, в локальну адресу мережі. Прикладами протоколів мережного рівня є протокол міжмережної взаємодії IP та протокол міжмережного обміну пакетами IPX.

Для передачі інформації між вузлами, що перебувають у різних мережах, необхідні маршрутизатори. Вони є прикордонними пристроями, що з'єднують мережі один з одним. Для маршрутизатора мережі в яких перебувають його порти є підключеними (directly connected). А ті мережі до яких підключені його сусіди – вилученими (remote). Якщо ПК потрібно відправити інформацію вузлу не з його мережі, то він направляє її своєму шлюзу. Шлюз (він же маршрутизатор) вибирає шлях передачі інформації ґрунтуючись на своїй таблиці маршрутів.

При цьому:

– *ipconfig* – показує поточні мережні налаштування;

– *route print (netstat -r)* – показує таблицю маршрутизації Windows/Linux (маршрут у таблиці містить: адресу мережі; адресу сусіда; метрику);

– *show ip route* – показує таблицю маршрутизаторів CISCO.

Маршрут за замовчуванням (default route) застосовується для всіх пакетів адреси призначення яких не значаться в таблиці. Має вигляд 0.0.0.0/0

Route ADD | DELETE | CHANGE – команда для роботи з таблицею маршрутів в Windows/Linux. Порядок обробки таблиці маршрутизатором.

– рівняються адреси мереж і адреса призначення побітно. Вибирається адреса з найбільшим збігом біт;

– якщо немає жодного підходящого, тоді маршрут за замовчуванням;

– якщо немає ні першого, ні другого – пакет викидається, а на адресу джерела висилається повідомлення про помилку.

Якщо в таблиці найшовся збіг, визначається сусід із цією мережею й інтерфейс маршрутизатора на якім він доступний. Пакет пересилається сусідові.

Маршрутизатор змінює заголовок кадра при передачі його з одного інтерфейсу на інший, тому що інтерфейси можуть працювати на різних протоколах(MAC адреси не містять інформації про мережу).

3.1.4. Безпека на транспортному рівні

Ролі транспортного рівня:

– відстеження індивідуальних сеансів і мультиплексування сеансів;

– сегментування даних;

– складання сегментів у вихідний блок даних;

– ідентифікація додатків за номерами портів.

Так як різні типи додатків надають різні вимоги для передачі трафіка на транспортному рівні використовується кілька протоколів.

Протоколи транспортного рівня можуть надавати:

– сеанси орієнтовані на з’єднання (connection-oriented conversations);

– надійність доставки (reliable delivery);

– реконструкцію даних по номерах сегментів (ordered data reconstruction);

– контроль потоку (flow control).

Для забезпечення надійності доставки протоколи транспортного рівня застосовують:

– облік переданих даних;

– підтвердження про приймання сегментів;

– повторне пересилання загублених сегментів.

Це вносить додаткове навантаження на мережу (overhead) за рахунок службових повідомлень протоколу.

Два основні протоколи транспортного рівня:

– TCP використовується протоколами потребуючими надійність доставки;

– UDP використовується протоколами не потребуючими надійності доставки.

Для того щоб відрізняти сеанси різних додатків один від одного, використовуються номери портів. Сокет – дозволяє унікально ідентифікувати сеанс зв’язку <IP адреса:Номер порту>.

За призначення портів протоколу відповідає організація IANA.

– добре відомі (well known), 0–1023, закріплені за самими популярними протоколами;

– зареєстровані (registered), 1024–49151, можуть бути видані протоколу самим розроблювачем без обігу в IANA;

– динамічні або приватні (dynamic or private), 49152–65535, використовуються тимчасово в момент установлення сеансу зв'язки.

Команда netstat видає список сеансів TCP відкритих в ОС. Так само показує порти, що прослуховуються службами.

Керування сеансами TCP

TCP (Transmission Control Protocol) – це один з самих широко поширених протоколів транспортного рівня. Головна функція TCP полягає в доставці повідомлень без втрат, чого не може гарантувати протокол нижчого рівня IP (Internet Protocol). Для доставки повідомлень заздалегідь встановлюється з'єднання між процесом-відправником і процесом-одержувачем. Це з'єднання здійснює надійну доставку дейтаграм. Протокол TCP проводить повторну передачу спотвореного або загубленого пакету.

Виділення усіх функцій, необхідних для надійної доставки повідомлень, в окремий рівень звільняє розробників застосовних програм і утиліт від рішення завдань управління потоком дейтаграм. Протокол забезпечує наскрізну передачу даних від відправника до одержувача. Оскільки TCP орієнтований на встановлення з'єднання, то адресат, що отримав дейтаграму, повинен повідомити відправника про це. Мається на увазі, що між відправником і одержувачем встановлюється віртуальний канал, де вони обмінюються повідомленнями, частина з яких є підтвердження про отримання даних або коди помилок. Віртуальний канал насправді може мати на увазі декілька реальних фізичних каналів передачі даних, оскільки повідомлення може проходити через один або декілька шлюзів.

Коли деяке застосування (процес) прикладного рівня відправляє повідомлення іншого застосування за допомогою TCP, передбачається, що повідомлення є потоком, тобто є потоком байтів, що передаються асинхронно. TCP отримує потік байтів і збирає його в пакети (сегменти), додаючи заголовки в початок сегментів. Довжина сегменту зазвичай визначається протоколом або вибирається адміністратором системи.

Процес обміну даними розпочинається з передачі запиту на встановлення з'єднання від машини-відправника до машини-одержувача. У запиті міститься спеціальне ціле число, що називається номером сокета (socket). У відповідь одержувач посилає номер свого сокета. Номери сокетів відправника і одержувача

однозначно визначають з'єднання (звичайно, з'єднання також не можливо без вказівки IP-адреси відправника і одержувача, але це завдання вирішується протоколами нижчого рівня – IP).

Після встановлення з'єднання TCP починає передавати сегменти повідомлення. На нижчому IP-рівні відправника сегменти розбиваються на одну або декілька дейтаграм. Пройшовши через мережу, дейтаграми поступають до одержувача, де IP-рівень знову збирає з них сегменти і передає їх TCP. TCP збирає усі сегменти в повідомлення. Від TCP повідомлення поступає до процесу-одержувача, де обробляється протоколом прикладного рівня. TCP на машині-одержувачі збирає ціле повідомлення з сегментів, керуючись порядковими номерами сегментів, які записані в їх заголовку. Якщо якийсь сегмент повідомлення втрачений або пошкоджений (що перевіряється по контрольній сумі в заголовку сегменту), то відправнику посилається повідомлення, що містить номер помилкового сегменту. В цьому випадку відправник повторно передає сегмент. Якщо сегмент успішно прийнятий, то одержувач посилає відправнику підтвердження-квитанцію (ACK – acknowledgement).

У TCP застосовується засіб обмеження потоку даних, що називається ковзаючим вікном. Воно є фрагментом повідомлення, якого адресат готовий прийняти. При встановленні з'єднання відправнику повідомляється розмір вікна (розмір вікна кратний розміру сегменту). Після того, як відправник передав кількість байтів, що відповідає розміру вікна, він повинен чекати квитанції. Як тільки буде отримана квитанція на передані сегменти, вікно зрушується вправо на відповідне число байтів, і нові сегменти можуть бути передані. Відправник може передати без отримання квитанцій в мережу максимально стільки сегментів, скільки їх укладається в ковзаючому вікні. В процесі обміну даними одержувач може присилати квитанції, в яких буде вказаний новий розмір ковзаючого вікна. Важливу роль в протоколі TCP грають таймери. Сегмент вважається втраченим, якщо квитанція на нього не поступила впродовж заданого часу очікування. При цьому проводиться повторна передача сегменту. При отриманні квитанції таймер зупиняється. Якщо одержувач виявляє декілька правильних копій одного і того ж сегменту, то усі зайві копії просто відкидаються і відправнику передається тільки одна квитанція.

Заголовок TCP має розмір в 20 байт, розмір заголовка не фіксований і може змінюватися. використовується протоколами потребуючими надійність доставки даних, електронна пошта, HTTP, telnet, SSH, FTP і т. ін.

У форматі повідомлення протоколу TCP під номер порту відводиться 16 біт, тому максимально можливим номером порту є число 65535. Номери портів від 0

до 255 строго зарезервовані під системні потреби, їх не допускається використати в застосовних програмах. У інтервалі від 256 до 1023 багато портів також використовується мережевими службами, тому і їх не рекомендується застосовувати для прикладних потреб. Як правило, більшість прикладних застосувань, побудованих на основі TCP/IP використовують номери портів в діапазоні від 1024 до 5000. Рекомендується використати номери від 3000 до 5000, номери вище 5000 використовуються найчастіше для короткострокового застосування.

Сервер не може мати кілька служб, що слухають один той самий порт.

У якості порту джерела клієнт вибирає будь-який порт із динамічного й зареєстрованого діапазону.

Тристороннє рукостискання (three-way handshake) – процес установлення сеансу TCP. Клієнт відправляє сегмент TCP із прапором SYN. Сервер відповідає сегментом із прапорами SYN і ACK. Клієнт відсилає сегмент із прапором ACK. Після чого вони можуть почати передавати дані. Цей процес дозволяє визначити наявність пристрою, що ухвалює, у мережі, його готовність до приймання й сповістити сам пристрій приймання про відкриття сеансу зв'язки.

Закриття сенсу проходить в 4 етапи з використанням сегментів із прапорами FIN і ACK, тому що сеанс TCP є дуплексним.

Так само, прапорець URG указує на терміновість сегмента, PSH – проштовхує накопичені в буфері приймача сегменти далі, RST – скидає процес установлення сеансу зв'язки. При встановленні сеансу TCP задається номер послідовності (sequence number), він використовується для обліку скільки байт передається в сегменті й для виявлення втрат. Для підтвердження отриманих даних використовується номер підтвердження (acknowledgment number).

Кількість байт переданих без підтвердження називається розміром вікна (window size). Первісний розмір вікна визначається джерелом і приймачем при тристоронньому рукостисканні.

Вузол зберігає копії відправлених сегментів поки не одержить підтвердження про їхнє успішне одержання. Якщо один із сегментів губиться, пересилаються всі сегменти вікна до якого він належав.

Вибіркове підтвердження (selective acknowledgements) дозволяє вузлам у випадку втрати сегмента, переслати повторно тільки один сегмент.

TCP має механізми керування потоком переданих даних (flow control). Одним з таких механізмів є – метод ковзного вікна. Він дозволяє динамічно змінювати розмір вікна в процесі передачі даних, підбудовуючись під стан мережі.

Протокол UDP

Протокол UDP (User Datagram Protocol) є простішим транспортним протоколом, ніж протокол TCP. Він надає прикладним процесам послуги транспортного рівня, які мало чим відрізняються від послуг нижчого рівня, що надаються протоколом IP.

Розмір заголовка 8 байт. Протокол не встановлює попереднього з'єднання й забезпечує не гарантовану доставку даних. Використовується для потокового відео, голосу й онлайн ігор. UDP не нумерує сегменти, і у вузлі-приймачі передає їхньому додатку в тому порядку, у якому він їх одержав з мережі (а не в тому, у якім вони були відправлені).

Протокол UDP забезпечує доставку дейтаграм, але не вимагає підтвердження їх отримання. Тому він не вимагає встановлення з'єднання між передавальним і приймаючим процесами. Протокол UDP використовується в тих випадках, коли вимагається передати дані без встановлення з'єднання. Такий зв'язок в принципі не надійний, оскільки відправнику не повідомляється, чи правильно прийнято його повідомлення і чи отримано воно взагалі. Для перевірки виникнення помилок може використовуватися контрольна сума пакету, але помилки ніяк не обробляються – вони або ігноруються, або їх обробка виконується вже на більш високому, прикладному рівні. Дані, що відправляються прикладним процесом через UDP, досягають місця призначення як єдине ціле, не дробившись на частини. Наприклад, якщо процес-відправник передав п'ять повідомлень через порт, то і процес одержувач повинен рахувати з порту п'ять повідомлень. Розмір кожного записаного повідомлення повинен співпадати з розміром кожного прочитаного. Протокол UDP використовується тоді, коли потрібно простий механізм передачі даних. Тоді контроль помилок або не виконується (наприклад, в прикладному протоколі TFTP – Trivial File Transfer Protocol – простий протокол передачі файлів), або виконується на прикладному рівні (наприклад, в управляючому протоколі SNMP – Simple Network Management Protocol або у файловій системі NFS – Network File System).

3.1.5. Безпека на сеансовому рівні

Сеансовий рівень (рівень сесії). На даному рівні встановлюються, обслуговуються і припиняються сесії між представницькими об'єктами додатків (прикладними процесами). В якості прикладу протоколи сеансового рівня можна розглянути протокол RPC (Remote Procedure Call). Як випливає з назви, даний про-

токол призначений для відображення результатів виконання процедури на віддаленому хості. У процесі виконання цієї процедури між додатками встановлюється сеанс на з'єднання. Призначенням даного з'єднання є обслуговування запитів, які виникають, наприклад, при взаємодії програми-сервера з додатком-клієнтом.

Шлюз сеансового рівня (Session Level Gateway – SLG). Це активний транслятор TCP-з'єднання. Шлюз приймає запит авторизованого клієнта на надання послуг, перевіряє допустимість запитаного сеансу (handshaking), встановлює потрібне з'єднання з адресою призначення зовнішньої мережі і формує статистику з даного сеансу зв'язку. Після встановлення факту, що довірений клієнт і зовнішній хост є «законними» (авторизованими) учасниками сеансу, шлюз транслює пакети в обох напрямках без фільтрації. При цьому часто пункт призначення обмовляється заздалегідь, а джерел інформації може бути багато (з'єднання «один-до-багатьох») – це, наприклад, типовий випадок використання зовнішнього вебресурса. Використовуючи різні порти, можна створювати різні конфігурації сполук, обслуговуючи одночасно всіх користувачів, що мають право на доступ до ресурсів мережі. Істотним недоліком SLG є те, що після встановлення зв'язку пакети фільтруються тільки на сеансовому рівні моделі OSI без перевірки їх вмісту на рівні прикладних програм. Авторизований зловмисник може спокійно транслювати шкідливі програми через такий шлюз. Таким чином, реалізація захисту здійснюється в основному на рівні квитування (Handshaking).

Протоколи сеансового рівня OSI/ISO забезпечують механізми управління сеансами управління сеансом, включаючи реєстрацію, управління діалогом і обмін параметрами сеансу. Ці протоколи описані в стандартах ISO 8326/CCITT X.215 (визначення і основні характеристики сеансової служби) і стандартах ISO 8327/CCITT X.225, визначальних специфікації протоколів:

– BCS – базової комбінованої підмножини;

– BSS – базової підмножини синхронізації;

– BAS – базової підмножини функціонування.

Управління діалогом під час сеансу реалізується в OSI/ISO за допомогою мітки, володіння якої надає право на зв'язок. Мітку можна запросити, причому для ES може бути заданий пріоритет на використання мітки.

Протоколи рівня представлення OSI/ISO забезпечують прозорий для прикладних процесів зв'язок ES, реалізованих на різних комп'ютерних платформах і різному операційному середовищі. Ці протоколи описані в стандартах ISO 8822/CCITT X.216 (визначення служби) і ISO 8823/CCITT X.226, визначальній специфікації протоколу:

– базові процедури встановлення/закінчення з'єднання;

– контекстне управління (вибірка/видалення контексту);

– контекстне представлення при повторній синхронізації або відновленні активності.

Синтаксис структур даних для ASN – абстрактній нотації даних (Abstract Syntax Notation) визначений в стандартах ISO 8824/CCITT X.208 (специфікації ASN.1) і ISO 8825/CCITT X.209 (основні правила кодування для ASN.1). До рівня представлення відносяться також і стандарти представлення кодів символів. Найбільш поширеними стандартами є 7-бітовий код ASCII його 8-бітове розширення, що містить символи псевдографіки і букви інших алфавітів (наприклад, кирилиця). Для великих машин IBM використовується двійковий розширений код EBCDIC. Стандартами ISO визначені 8-бітовий код ISO 8859 і 16-бітовий код 6937 (для представлення символів найбільш поширених алфавітів, включаючи ієрогліфи).

На протоколи сеансового рівня і рівня представлення даних лягає основне навантаження по забезпеченню безпеки мережі. На сеансовому рівні безпека забезпечується за допомогою ідентифікаторів і паролів користувачів. ISO рекомендує при реалізації моделі OSI забезпечувати безпеку мережі за допомогою шифрування на рівні представлення даних. Для шифрування даних запропонований стандарт ISO 9797, визначальний механізм цілісності даних за допомогою криптографічної функції перевірки з використанням алгоритму блокового шифрування.

Формування захищених віртуальних каналів

Сеансовий рівень є максимально високим рівнем моделі OSI, на якому можливе формування захищених віртуальних каналів. При побудові захищених віртуальних мереж на даному рівні досягаються найкращі показники по функціональної повноті захисту інформаційного обміну, надійності контролю доступу, а також простоті конфігурування системи безпеки. Протоколи формування захищених віртуальних каналів на сеансовому рівні прозорі для прикладних протоколів захисту, а також високорівневих протоколів надання різних сервісів (протоколів HTTP, FTP, POP3, SMTP, NNTP та ін.). Однак на сеансовому рівні починається безпосередня залежність від додатків, що реалізують високорівневі протоколи. Тому реалізація протоколів захисту інформаційного обміну, відповідних цьому рівню, в більшості випадків вимагає внесення змін до високорівневі мережеві додатки.

Так як сеансовий рівень моделі OSI відповідає за установку логічних з'єднань і управління цими сполуками, то на даному рівні з'являється можливість використання програм-посередників, перевіряючих допустимість запитаних з'єднань і забезпечують виконання інших функцій захисту міжмережевої взаємодії. У загальному випадку програми-посередники, які традиційно використовуються в міжмережевих екранах, можуть виконувати такі функції:

– ідентифікація та автентифікація користувачів;

– криптозазист переданих даних;

– розмежування доступу до ресурсів внутрішньої мережі та розмежування доступу до ресурсів зовнішньої мережі;

– фільтрація і перетворення потоку повідомлень, наприклад, динамічний пошук вірусів і прозоре шифрування інформації;

– трансляція внутрішніх мережевих адрес для вихідних пакетів повідомлень;

– реєстрація подій та реагування на поставлені події;

– кешування даних, запитуваних із зовнішньої мережі.

Таким чином, при побудові захищених віртуальних мереж на сеансовому рівні з'являється можливість не тільки криптографічного захисту інформаційного обміну, включаючи аутентифікацію, а й можливість реалізації ряду функцій посередництва між взаємодіючими сторонами.

Для криптографічного захисту інформаційного обміну на сеансовому Рівні найбільшу популярність отримав протокол SSL/TLS (Secure Sockets Layer/Transport Layer Security), розроблений компанією Netscape Communications.

Протокол SSL

Протокол Secure Sockets Layer (SSL), споконвічно орієнтований на захист інформаційного обміну між клієнтом і сервером комп'ютерної мережі, є промисловим протоколом сеансового рівня моделі OSI використовують для забезпечення безпеки інформаційного обміну криптографічні методи захисту інформації. Конфіденційність переданих даних забезпечується за рахунок їх криптографічного закриття, а аутентифікація взаємодіючих сторін, а також достовірність і цілісність циркулюючої інформації – за рахунок формування та перевірки цифрового підпису.

Ядром протоколу SSL є технологія комплексного використання асиметричних і симетричних криптосистем. В якості алгоритмів асиметричного шифрування використовуються такі алгоритми, як RSA (розробки RSA Data Security

Inc.), а також алгоритм Діффі-геллмана. Для обчислення геш-функцій можуть застосовуватися стандарти MD5 і SHA-1. Припустимими алгоритмами симетричного шифрування є RC2, RC4, DES, а також потрійний DES. У протоколі SSL третьої версії набір криптографічних алгоритмів є розширюваним. Для аутентифікації взаємодіючих сторін і криптозахисту ключа симетричного шифрування застосовуються цифрові сертифікати відкритих ключів користувачів (клієнта і сервера), завірені цифровим підписом спеціальних сертифікаційних центрів. Підтримуються цифрові сертифікати, відповідні загальноприйнятому стандарту X.509 [11].

Протокол SSL розроблений корпорацією Netscape, а потім підтриман ий низкою провідних виробників програмного забезпечення. Через своїх позитивних якостей SSL практично витіснив конкуруючі високорівневі протоколи щодо захисту інформаційного обміну, наприклад, такі як SHTTP (Secure HTTP), і став загальновизнаним неофіційними стандартом захисту в інтернеті і у внітрішній мережі. Специфікації SSL були свого часу запропоновані в якості офіційних стандартів інтернету, але не отримуючи цього статусу за формальними обставинами. Не виключено, що SSL все ж таки почне просуватися по щаблях формального прийняття IETF як стандарт, так як він вже став промисловим протоколом, розвиватися і просуваються поза ієрархією технічних координуючих інститутів інтернету. Останньою версією SSL є версія 3.0, про яку і йтиметься.

Клієнтська частина SSL реалізована у всіх популярних веб-навігаторах, до яких відносяться Netscape Navigator компанії Netscape і Internet Explorer від Microsoft а серверна – в більшості як комерційних, так і поширюваних на некомерційних умовах WWW-серверів наприклад, в серверних додатках компаній IBM, Netscape, Microsoft, Spyglass, Open Market.

Відповідно до протоколу SSL криптозахищені тунелі створюються між кінцевими точками віртуальної мережі. Протокол SSL передбачає два етапи взаємодії клієнта і сервера при формуванні та підтримці захищається з’єднання:

– встановлення SSL-сесії;

– захищене взаємодія.

Процедура встановлення SSL-сесії, звана також процедурою рукостискання raquo, відпрацьовується перед безпосереднім захистом інформаційного обміну і виконується по протоколу початкового привітання (handshake protocol), що входить до складу протоколу SSL. У процесі становлення SSL-сесії вирішуються наступні завдання:

– аутентифікація сторін;

– узгодження криптографічних алгоритмів і алгоритмів стиснення, які будуть використовуватися при захищеному інформаційному обміні;

– формування спільного секретного майстер-ключа;

– генерація на основі сформованого майстер-ключа загальних секретних сеансових ключів для криптозахисту інформаційного обміну.

У реалізаціях протоколу SSL для аутентифікації взаємодіючих сторін і формування загальних секретних ключів найчастіше використовують алгоритм RSA розробки RSA Data Security Inc.

Однозначне і достовірне відповідність між відкритими ключами і їх власниками встановлюється за допомогою цифрових сертифікатів, які видаються спеціальними Центрами Сертифікації. Сертифікат являє собою блок даних, що містить наступну інформацію:

– ім’я центру сертифікації;

– ім’я власника сертифіката;

– відкритий ключ власника сертифіката;

– період дії сертифіката;

– ідентифікатор і параметри криптоалгоритму, який повинен використовуватися при обробці сертифіката;

– цифровий підпис центру сертифікації, завіряє всі дані у складі сертифіката.

Цифровий підпис центру сертифікації у складі сертифіката забезпечує достовірність і однозначність відповідності відкритого ключа й його власника. Центр сертифікації виконує роль нотаріуса, що посвідчує справжність відкритих ключів, що дозволяє їх власникам користуватися послугами захищеної взаємодії без попередньої особистої зустрічі. Необхідність безумовної довіри до центру сертифікації з боку всіх учасників захищеного обміну пред’являє до нього досить високі вимоги з перевірки автентичності завіряються відкритих ключів. Одним з таких центрів в інтернеті є компанія VeriSign, заснована RSA Data Security Inc., за участю компаній Visa, IBM, Netscape, Microsoft і Oracle.

Третя версія протоколу SSL підтримує три режими аутентифікації:

– взаємна аутентифікація сторін;

– одностороння аутентифікація сервера без аутентифікації клієнта;

– повна анонімність.

При використанні останнього варіанту взаємодіючі сторони незахищені від атак, пов’язаних з підміною учасників взаємодії, даному режимі забезпечується захист інформаційного обміну без будь-яких гарантій щодо достовірності взаємодіючих сторін.

У режимі односторонньої аутентифікації сервера без аутентифікації клієнта процедура встановлення SSL-сесії між клієнтом і сервером включає наступні кроки.

Клієнт посилає серверу запит на встановлення захищеного з'єднання, в якому передає деякі формальні параметри цього з'єднання:

– поточний час і дату;

– випадкову послідовність (RAND_CL);

– набір підтримуваних клієнтом алгоритмів симетричного шифрування і алгоритмів обчислення геш-функції;

– набір підтримуваних алгоритмів стиснення та ін.

Сервер обробляє запит від клієнта і передає йому узгоджений набір параметрів:

– ідентифікатор SSL-сесії;

– конкретні криптографічні алгоритми з числа запропонованих клієнтом (якщо з якої-небудь причини запропоновані алгоритми або їх параметри не задовольняють вимогам сервера, сесія закривається);

– сертифікат сервера, завірений цифровим підписом центру сертифікації;

– випадкову послідовність (RAND_SERV).

Клієнт перевіряє отриманий сертифікат сервера за допомогою відкритого ключа центру сертифікації, який йому відомий. При негативному результаті перевірки сесія закривається, а при позитивному – клієнт виконує наступні дії:

– генерує випадкову 48-байтну послідовність Pre_MasterSecret, призначену для генерації загального секретного майстер-ключа; шифрує Pre_MasterSecret з відкритого ключа сервера, отриманому в сертифікаті сервера, і посилає серверу;

– за допомогою узгоджених геш-алгоритмів формує загальний секретний майстер-ключ (MasterSecret), використовуючи в якості параметрів послідовність Pre_MasterSecret, послану сервера випадкову послідовність RAND_CL і одержану від нього випадкову послідовність RAND_SERV;

– використовуючи MasterSecret, обчислює криптографічні параметри SSL-сесії: формує спільні з сервером сеансові секретні ключі для симетричного шифрування й обчислення геш-функцій;

– переходить в режим захищеної взаємодії.

Сервер розшифровує отриману послідовність Pre_MasterSecret за своїм закритим клюему і виконує на її основі ті ж операції, що і клієнт:

– за допомогою узгоджених геш-алгоритмів формує загальний секретний майстер-ключ (MasterSecret), використовуючи в якості параметрів

Pre_MasterSecret, а також послану клієнту випадкову послідовність RAND_SERV і одержану від нього випадкову послідовність RAND_CL;

– використовуючи MasterSecret, обчислює криптографічні параметри SSL-сесії: формує загальні з клієнтом сеансові секретні ключі для симетричного шифрування й обчислення геш-функцій;

– переходить в режим захищеної взаємодії.

Так як при формуванні параметрів SSL-сесії і клієнт, і сервер користувалися одними і тими ж вихідними даними (узгодженими алгоритмами, спільної секретної послідовності Pre_MasterSecret і випадковими послідовностями RAND_CL і RAND_SERV), то очевидно що в результаті описаних вище дій вони виробили однакові сеансові секретні ключі. Для перевірки ідентичності параметрів SSL-сесії клієнт і сервер посилають один одному тестові повідомлення, зміст яких відомо кожної зі сторін:

– клієнт формує повідомлення з власних посилок на адресу сервера на кроці 1 та посилок, отриманих від сервера на кроці 2, вносячи елемент випадковості у вигляді послідовності MasterSecret, унікальною для даної сесії; формує код для перевірки цілісності повідомлення (MAC), шифрує повідомлення за загальним сеансовому секретному ключу й відправляє серверу;

– сервер, у свою чергу, формує повідомлення з власних посилок на адресу клієнта на кроці 2, посилок, отриманих від клієнта на кроці 1, і послідовності MasterSecret; формує код для перевірки цілісності повідомлення (MAC), шифрує повідомлення на загальному сеансовому секретному ключі і відправляє клієнту;

– у разі успішного розшифрування і перевірки цілісності кожної зі сторін отриманих тестових повідомлень, SSL-сесія вважається встановленої і сторони переходять в штатний режим захищеної взаємодії.

У процесі захищеної взаємодії із встановленими криптографічними параметрами SSL-сесії виконуються наступні дії:

– кожна сторона при передачі повідомлення формує MAC-код для подальшої перевірки цілісності повідомлення і потім зашифровує вихідне повідомлення разом з MAC-кодом по сеансовому секретному ключу;

– кожна сторона при прийомі повідомлення розшифровує його і перевіряє на цілісність (обчислюється поточний MAC-код і звіряється з MAC-кодом перевірки цілісності, отриманим разом з повідомленням);

– у разі виявлення порушення цілісності повідомлення, SSL-сесія закривається.

Незважаючи на те, що протокол SSL підтримується програмним забезпеченням серверів і клієнтів, що випускаються провідними західними компаніями, у

нашій країні є обставини, що перешкоджають поширенню даного протоколу та прийняття його в якості базового для реалізації програм, що вимагають захищеного інформаційного взаємодії беруть участь.

Практично всі існуючі продукти, що підтримують протокол SSL, реалізовані в США і через експортних обмежень доступні тільки в усіченому варіанті (з довжиною сеансового ключа 40 біт для алгоритмів симетричного шифрування і 512 біт для алгоритму RSA, використовуваного на етапі встановлення SSL-сесії), що на сьогоднішній день явно недостатньо.

3.2. Створення списків управління доступом (ACL)

На сьогодні для будь-якого системного адміністратора однієї з найгостріших проблем залишається забезпечення безпеки комп'ютерної мережі. Здавалося б, такі завдання покликані вирішувати міжмережеві екрани, проте часом перший удар переймають на себе саме комутатори. Хоча це і не основне їх завдання, проте, на даний момент комутатори мають широкий функціонал для успішного вирішення подібного роду завдань. Йдеться не лише про захист мереж від атак ззовні, але і про всілякі атаки усередині мережі, таких як підміна DHCP-сервера, атаки типу DoS, ARP Spoofing, неавторизований доступ і так далі. В деяких випадках комутатори не здатні повністю захистити мережу від подібного роду атак, але здатні значно ослабити загрози їх виникнення. Ця тема буде присвячена принципам забезпечення мережевої безпеки на базі устаткування D-Link.

Призначення і зміст списків управління доступом. Типи профілів доступу

Списки управління доступом (Access Control List, ACL) є потужним засобом фільтрації потоків даних без втрати продуктивності, оскільки перевірка вмісту пакетів виконується на апаратному рівні (рис. 3.1). Фільтруючи потоки даних, адміністратор може обмежити типи додатків, дозволених для використання в мережі, контролювати доступ користувачів до мережі і визначати пристрої, до яких вони можуть підключатися. Також ACL можуть використовуватися для визначення політики QoS шляхом класифікації трафіку і перевизначення його пріоритету.

ACL є послідовністю умов перевірки параметрів пакетів даних. Коли повідомлення поступають на вхідний порт, комутатор перевіряє параметри пакетів даних на збіг з крите-риями фільтрації, визначеними в ACL, і виконує над пакетами одну з дій: *permit* («дозволити») або *deny* («заборонити»).

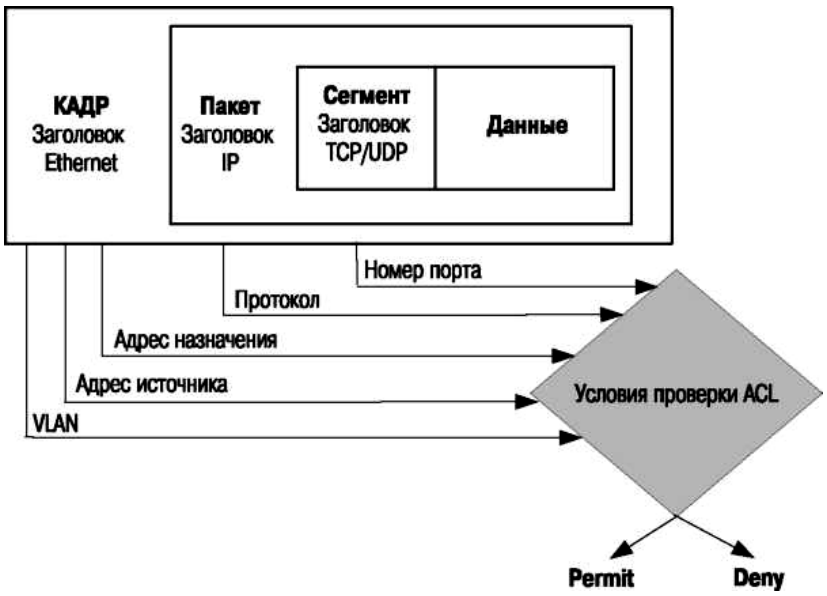
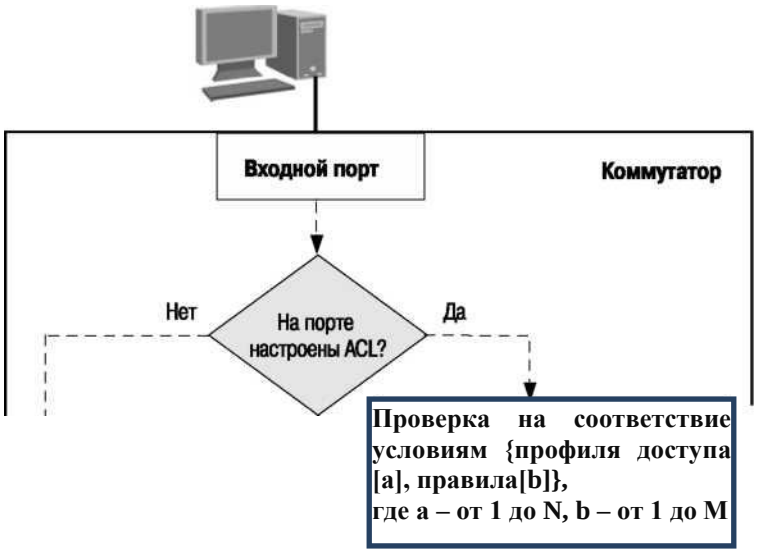


Рис. 3.1. Списки управління доступом (ACL)

Критерії фільтрації можуть бути визначені на основі наступної информації, що міститься в пакеті:

– порт комутатора;
– MAC/IP-адрес;
– тип Ethernet/ тип протоколу;
– VLAN;
– 802.1p/DSCP;
– порт TCP/UDP (тип додатка);
– перші 80 байт пакету, включаючи поле даних.

Списки управління доступом складаються з профілів доступу (Access Profile) і правил (Rule). Профілі доступу визначають типи критеріїв фільтрації, які повинні перевірятися в пакеті даних (MAC-адреса, IP-адреса, номер порту,



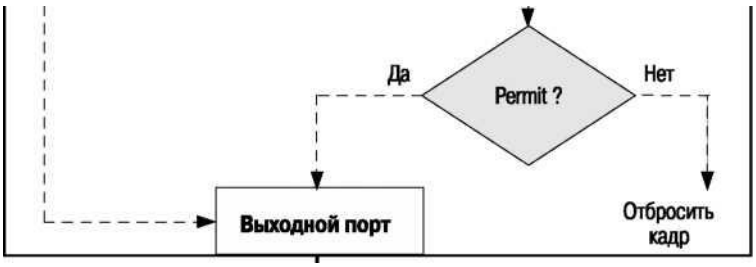


Рис. 3.2. Принцип роботи ACL

VLAN і так далі), а в правилах безпосередньо вказуються їх значення. Коли комутатор отримує кадр, він перевіряє його поля на збіг з типами критеріїв фільтрації і їх параметрами, заданими в профілях і правилах. Послідовність, в якій комутатор перевіряє кадр на збіг з параметрами фільтрації (рис. 3.2), визначається порядковим номером профілю (Profile ID) і порядковим номером правила (Rule ID). Профілі доступу і правила усередині них працюють послідовно, в порядку зростання їх номерів. Тобто кадр перевіряється на відповідність умовам фільтрації, починаючи з першого профілю і першого правила в нім. Так, кадр спочатку перевірятиметься на відповідність умовам, визначеним в правилі 1 профілю 1. Якщо параметри кадру не підходять під умови перевірки, то далі кадр перевірятиметься на збіг з умовами, визначеними в правилі 2 профілі 1 і так далі.

Якщо жодне з правил поточного профілю не співпало з параметрами кадру, то комутатор продовжить перевірку на збіг параметрів кадру з умовами правила 1 наступного профілю. При першому збігу параметрів кадру з правилом до кадру буде застосовано одна з дій, визначених в правилі: «Заборонити», «Дозволити» або «Змінити вміст поля пакету» (пріоритет 802.1p/ DSCP). Далі кадр перевірятися не буде. Якщо жодне з правил не підходить, застосовується політика за умовчанням, що дозволяє проходження усього трафіку.

У комутаторах D-Link існує три типи профілів доступу: Ethernet, IP і Packet Content Filtering (фільтрація по вмісту пакету).

Профіль Ethernet (Ethernet Profile) дозволять фільтрувати кадри по наступних типах критеріїв:

– VLAN;

– MAC -адрес джерела;

– MAC -адрес призначення;

– 802.1p;

– тип Ethernet.

Профіль IP (IP Profile) підтримує наступні типи критеріїв фільтрації:

– VLAN;

– маска IP-джерела;

– маска IP-призначення;

– DSCP;

– протокол (ICMP, IGMP, TCP, UDP);

– номер порту TCP/UDP.

Профіль фільтрації по вмісту пакету (PacketContentFilteringProfile) використовується для ідентифікації пакетів, шляхом побайтного дослідження їх заголовків Ethernet. Слід зазначити, що не усі моделі комутаторів підтримують Packet.ContentFilteringProfile. За інформацією про підтримку функції необхідно звернутися до документації на використовуваний комутатор.

Процес створення профілю доступу. Приклади налаштування ACL

Процес створення профілю доступу можна розділити на такі основні кроки:

– аналіз завдання фільтрації і визначення типу профілю доступу – Ethernet, IP або Packet Content Filtering;

– визначення стратегії фільтрації. Наприклад: відкидати кадри деяких вузлів і приймати кадри від усіх інших вузлів – ця стратегія застосовна для мережевого середовища з декількома вузлами/протоколами портів/підмережами, для яких необхідно виконувати фільтрацію; приймати кадри від деяких вузлів і відкидати кадри усіх інших вузлів – ця стратегія застосовна для мережевого середовища з декількома вузлами/протоколами портів/підмережами, кадри від которых дозволені в мережі. Трафік інших вузлів відкидатиметься;

– визначення, маски профілю доступу (Access Profile Mask) і створення її (команда create access_profile). Маска профілю доступу використовується для вказівки, які біти значень полів IP -адрес, MAC-адреса, порт TCP/UDP і так далі повинні перевірятися в пакеті даних, а які ігноруватися;

– додавання правила профілю доступу (Access Profile Rule), пов’язане з цією маскою (команда config access_profile). Правила профілю доступу перевіряються відповідно до номера access_id. Чим менший номер, тим раніше перевіряється правило. Якщо жодне правило не спрацювало, кадр пропускається.

У середовищі QoS, після того, як спрацьовує правило, перед відправкою пакету даних біти 802.1p/DSCP можуть бути замінені на нові низько- і високопріоритетні значення.

Маска профілю доступу визначає, які біти в значеннях полів «IP-адрес», «MAC-адреса», «порт TCP/UDP» і так далі що приходять на комутатор кадрів повинні перевірятися, а які ігноруватися (рис. 3.3). Биті маски мають наступні значення:

– «0» – означає ігнорування значення відповідного біта поля пакету даних;

– «1» – означає перевірку значення відповідного біта поля пакету даних.

Припустимо, адміністраторові мережі необхідно заборонити проходження трафіку від вузла з MAC-адресою 01-00-00-00-AC-11. Маска профілю доступу для цієї адреси буде рівна FF-FF-FF-FF-FF-FF. Якщо необхідно заборонити або дозволити проходження через комутатор трафіку будь-якого вузла з підмереж 192.168.16.0/24–192.168.31.0/24, то маска профілю доступу обчислюватиметься, як показано на рис. 3.3.

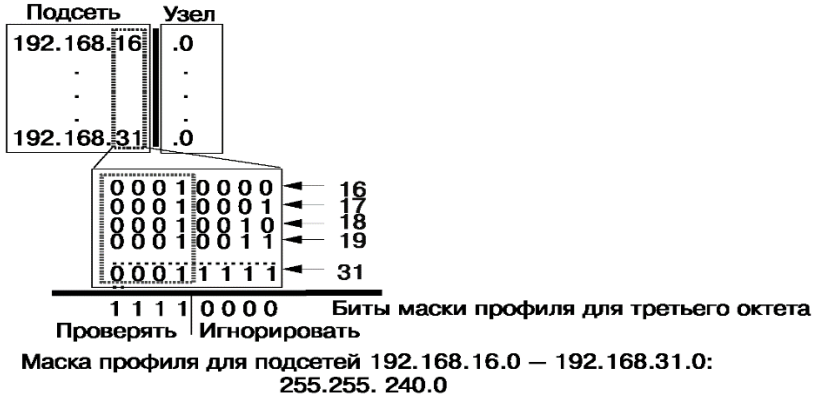


Рис. 3.3. Обчислення маски профілю

Перші два октети IP -адрес з діапазону, що перевіряється, мають однакове значення – «192.168». Вони використовуватимуться при перевірці пакету, тому відповідні біти маски містять усе 1. Останній октет IP-адреси ігноруватиметься, оскільки немає зацікавленості в перевірці індивідуальних адрес вузлів підмереж. Тому останній октет маски профілю містить всі 0. У третьому октеті значення маски дорівнюватиме 240 (11110000), тому що воно охоплює усі номери з 16 (00010000) до 31 (0001111), що мають однакові значення (0001) перших чотирьох бітів. Останні чотири біти третього октету IP -адреси маска профілю ігноруватиме, як малозначні.

Припустимо, що адміністраторові мережі необхідно дозволити доступ в інтернет тільки деяким користувачам, а іншим користувачам заборонити. Користувачі ідентифікуються по MAC-адресах їх комп'ютерів.

У прикладі, показаному на рис. 3.4, користувачі ПК 1 і ПК 2 отримають доступ в інтернет, оскільки їх MAC-адреси вказані в дозволяючому правилі 1. Як тільки користувачі інших комп'ютерів спробують вийти в інтернет, спрацює правило 2, яке забороняє проходження через комутатор кадрів з MAC-адресою призначення, рівною MAC-адресі інтернет-шлюзу.

Правило 1: якщо MAC-адреса джерела SourceMAC рівна MAC-адресам ПК 1 або ПК 2 – дозволити (permit):

create access_proflle ethernet source_mac FF-FF-FF-FF-FF-FF
proflle_ld 1 proflle_name Permlt_Internet
conflg access_proflle proflle_ld 1 add access_ld 1 ethernet
source_mac 00-50-BA-11-11-11 port 1 permlt
conflg access_proflle proflle_ld 1 add access_ld 2 ethernet
source_mac 00-50-BA-22-22-22 port 10 permlt

Рис. 3.4. Приклад ACL для профілю Ethernet Налаштування комутатора для профілю Ethernet

Правило 2: якщо MAC-адреса призначення Dest MAC рівна MAC – адресі інтернет-шлюзу – заборонити (deny).

create access_profile ethernet destination_mac FF-FF-FF-FF-FF-FF profile_id 2 profile_name Deny_Internet

config access_profile profile_id 2 add access_id 1 ethernet destination_mac 00-50-BA-99-99-99 port 11 deny

Інакше – за умовчанням дозволити доступ усім вузлам.

В якості другого прикладу приведемо налаштування ACL з профілем IP (рис. 3.5). Припустимо, що адміністраторові необхідно дозволити доступ в Интернет тільки користувачам з IP-адресами з 192.168.0.1/24 по 192.168.0.63/24. Іншим користувачем мережі 192.168.0.0/24 з адресами, що не входять в дозволений діапазон, доступ в інтернет заборонений.

Правила записуються зверху вниз:

Правило 1. Якщо SourcelP рівний IP -адресам з 192.168.0.1 по 192.168.0.63 Permit.

Правило 2. Якщо SourcelP з мережі 192.168.0.0/24 і не належить дозволеному діапазону (192.168.0.1/24–192.168.0.63/24) – deny.

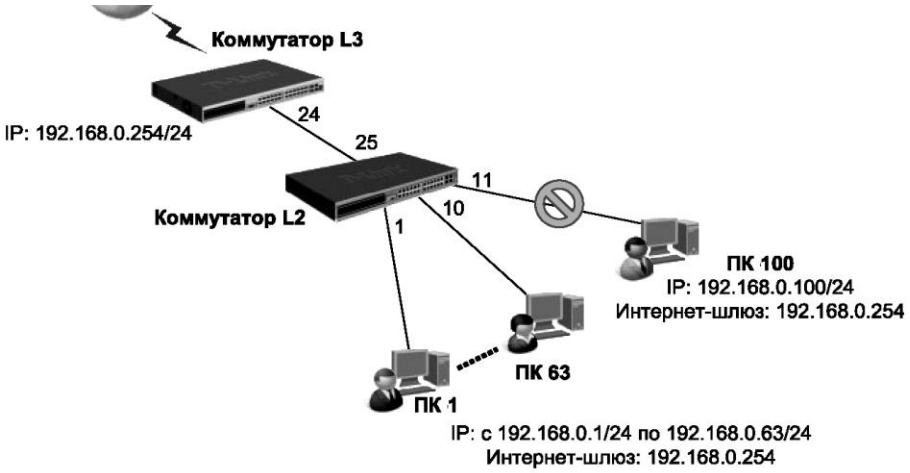


Рис. 3.5. Приклад ACL для профілю IP

Налаштування в комутаторі L3 профілю IP

Правило 1. Якщо IP -адрес джерела Source IP рівний IP -адресам з діапазону з 192.168.0.1 по 192.168.0.63 – дозволити (permit).

create access_profile ip source_ip_mask 255.255.255.192 profile_id 1 config access_profile profile_id 1 add access_id 1 ip source_ip 192.168.0.0 port 24 permit

Правило 2. Якщо IP -адрес джерела Source IP належить мережі 192.168.0.0/24, але не входить в дозволений діапазон адрес – заборонити (deny).

create access_profile ip source_ip_mask 255.255.255.0 profile_id 2 config access_profile profile_id 2 add access_id 1 ip source_ip192.168.0.0 port 24 deny

Інакше – за умовчанням дозволити доступ усім вузлам.

3.3. Функції контролю підключення вузлів до портів комутатора

У тому випадку, якщо який-небудь порт на комутаторі активний, до нього може підключитися будь-який користувач і отримати несанкціонований доступ до мережі. Цей користувач може почати генерувати шкідливий трафік, який потрапить в мережу і створить проблеми усередині неї. Для захисту від подібних ситуацій, а також для контролю підключення вузлів до портів комутатори D-Link надають функції безпеки, які дозволяють вказувати MAC- і/або IP-адреси пристроїв, яким дозволено підключатися до цього порту, і блокувати доступ до мережі вузлам з невідомими комутатору адресами.

Функція налаштування портів комутатора Port Security

Функція Port Security (рис. 3.6) дозволяє настроїти який-небудь порт комутатора так, щоб доступ до мережі через нього міг здійснюватися тільки певними

пристроями. Пристрої, яким дозволено підключатися до порту, визначаються за MAC-адресами. MAC-адреси можуть бути вивчені динамічно або вручну налагоджені адміністратором мережі. Окрім цього, функція Port Security дозволяє обмежувати кількість MAC-адрес, що вивчаються портом, тим самим обмежуючи кількість вузлів, що підключаються до нього.

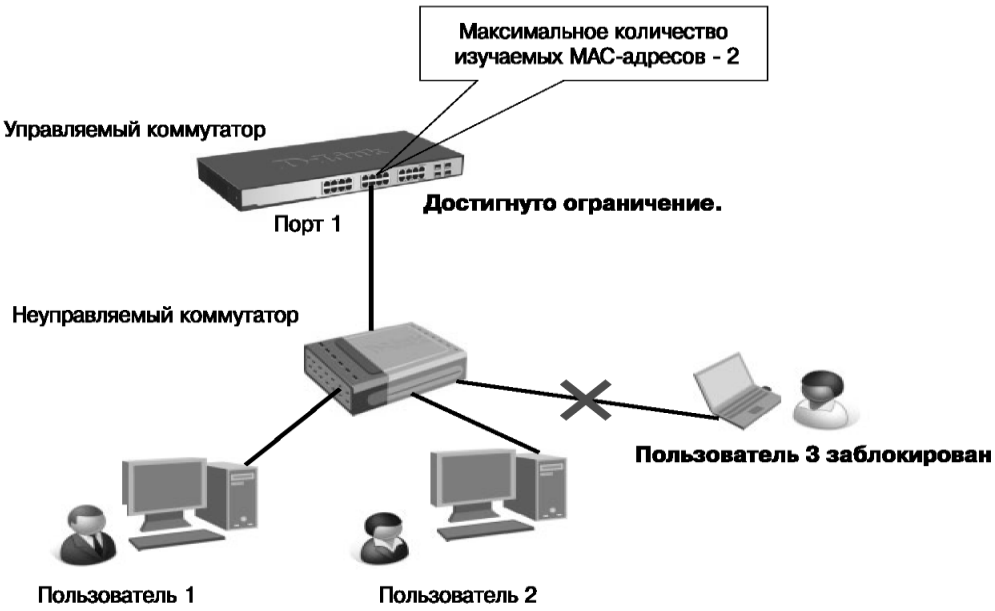


Рис. 3.6. Функція Port Security

Необхідно відмітити, що для функції Port Security існують обмеження по кількості MAC-адрес, які може обслуговувати кожен порт. Ці обмеження різні для різних моделей комутаторів. Для отримання інформації про максимальну кількість обслуговуваних портом MAC-адрес необхідно звернутися до специфікації на використовуваний пристрій.

Існує три режими роботи функції Port Security:

– permanent («постійний») – занесені в таблицю комутації MAC-адреси ніколи не застарівають, навіть якщо витік час, встановлений таймером FDB Aging Time, або комутатор був перезавантажений;

– delete on timeout («видалити після закінчення часу») – занесені в таблицю комутації MAC-адреси застаріють після витікання часу, встановленого таймером FDB Aging Time, і будуть видалені. Якщо стан каналу зв'язку на підключеному порту змінюється, MAC-адреси, вивчені на ньому, видаляються з таблиці комутації, що аналогічно виконанню дій при витіканні часу, встановленого таймером FDB Aging Time;

– delete on reset («видалити при скиданні налаштувань») – занесені в таблицю комутації MAC-адреси будуть видалені після перезавантаження комутатора (цей режим використовується за умовчанням).

При підключенні неавторизованого користувача до порту комутатора він буде заблокований, а комутатор відправить повідомлення SNMP Trap або створить запис в log-файлі, якщо адміністратор настроїв виконання цих дій. Порт комутатора відкидатиме трафік, що поступає з невідомої MAC-адреси.

Як приклад розглянемо ситуацію, показану на рис.3.6. На портах 1-3 керовані комутатори налагоджені обмеження по кількості користувачів (до кожного порту може підключитися не більше двох користувачів), що підключаються. MAC-адреси користувачів, що підключаються, вивчаються портами 1-3 динамічно.

Налаштування комутатора:

config port_security ports 1-3 admin_state enabled

max_learning_addr 2 lock_address_mode DeleteOnTimeout

У наведеному прикладі конфігурації використовується режим Delete on Timeout. Це означає, що вивчені на порту MAC-адреси будуть видалені з таблиці комутації після закінчення часу, встановленого таймером Aging Time, якщо по них не було звернень (наприклад, робоча станція відключилася від мережі). В цьому випадку до мережі зможуть підключиться нові користувачі, MAC-адреси, яких будуть динамічно вивчені портом (рис. 3.7).

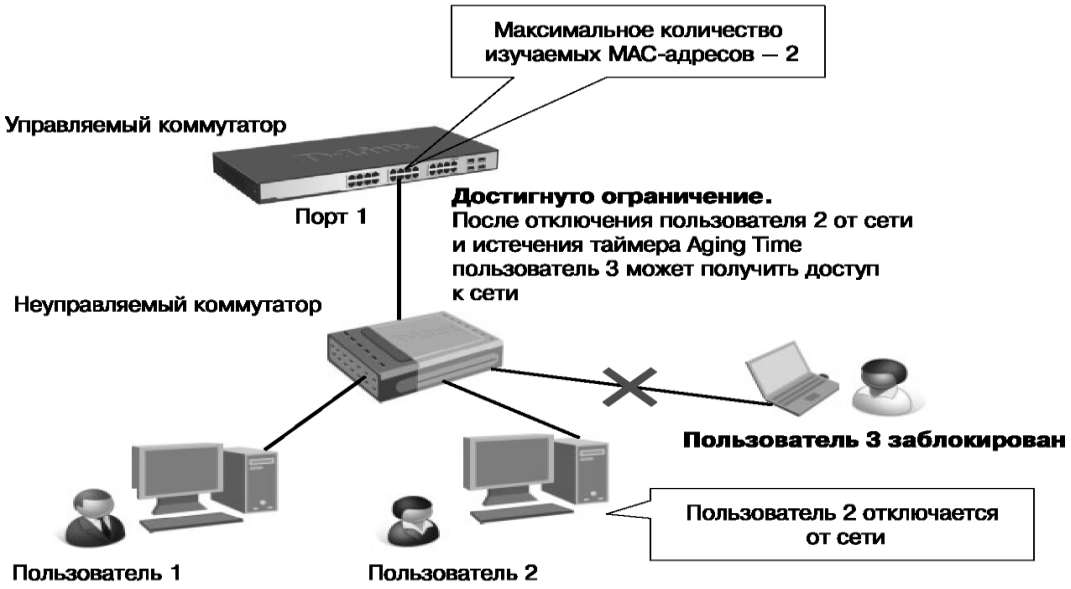


Рис. 3.7. Функція Port Security в режимі Delete on Timeout

При використанні режиму роботи Permanent адреси, вивчені портом, будуть додані в статичну таблицю MAC-адрес і зберігатимуться в ній навіть після включення/виключення живлення і перезавантаження комутатора.

Функція Port Security виявляється дуже корисною при побудові будинкових мереж, мереж провайдерів інтернету і локальних мереж з підвищеною вимогою

по безпеці, де вимагається виключити доступ незареєстрованих робочих станцій до послуг мережі. Використовуючи функцію Port Security, можна повністю заборонити динамічне вивчення MAC-адрес вказаними або усіма портами комутатора. В цьому випадку доступ до мережі отримають тільки ті користувачі, MAC-адреси яких вказані в статичній таблиці комутації.

Налаштування комутатора здійснюється таким чином:

– активізувати функцію Port Security на відповідних портах і заборонити вивчення MAC-адрес (параметр maxlearningaddr встановити рівним 0).

config port_security ports 1-24 admin_state enabled max_learning_addr 0

– створити записи в статичній таблиці MAC-адрес (ім'я VLAN в прикладі «default»).

create fdb default 00-50-BA-00-00-01 port 2
create fdb default 00-50-BA-00-00-02 port 2
create fdb default 00-50-BA-00-00-03 port 2
create fdb default 00-50-BA-00-00-04 port 2
create fdb default 00-50-BA-00-00-05 port 8

Функція контролю доступу комп'ютерів в мережу IP-MAC-Port Binding

Функція IP-MAC-Port Binding (IMPB), реалізована в комутаторах D-Link, дозволяє контролювати доступ комп'ютерів в мережу на основі їх IP- та MAC-адрес, а також порту підключення (рис. 3.8). Адміністратор мережі може створити записи («білий лист»), зв'язуючі MAC- та IP-адреси комп'ютерів з портами підключення комутатора. На основі цих записів, у разі збігу усіх складових, клієнти діставатимуть доступ до мережі зі своїх комп'ютерів. У тому випадку, якщо при підключенні клієнта зв'язка MAC-IP-порт відрізнятиметься від параметрів заздалегідь зконфігурованого запису, комутатор заблокує MAC-адресу відповідного вузла із занесенням його в «чорний лист».

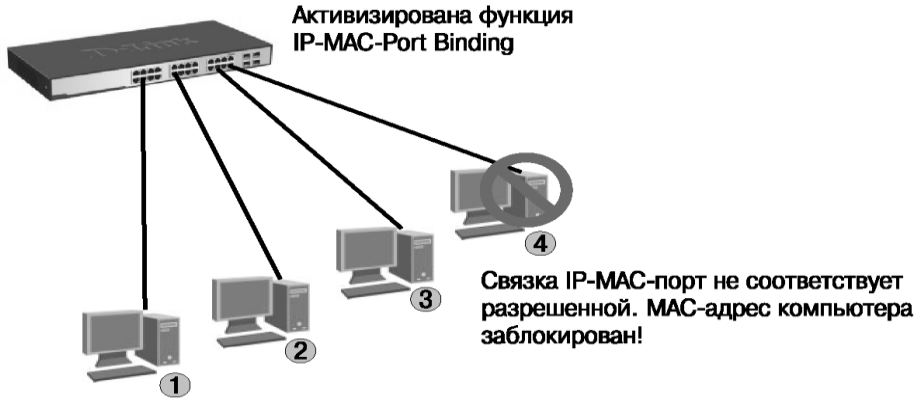


Рис. 3.8. Функція IP – MAC – Port Binding

Функція IP-MAC-Port Binding спеціально розроблена для управління підключенням вузлів в мережах ETTH (Ethernet-to-the-Home) і офісних мережах. Окрім цього функція IMPB дозволяє боротися з атаками типу ARPSpoofing, під час яких зловмисні користувачі перехоплюють трафік або переривають з'єднання, маніпулюючи пакетами ARP.

Функція IP-MAC-Port Binding включає три режими роботи: ARPmode (за умовчанням), ACLmode і DHCPSnoopingmode.

ARPmode є режимом, використовуваним за умовчанням при налаштуванні функції IP-MAC-Port Binding на портах. При роботі в режимі ARP комутатор аналізує ARP-пакети і зіставляє параметри IP-MAC-ARP-пакета з передвстановленою адміністратором зв'язкою IP-MAC. Якщо хоч би один параметр не співпадає, то MAC-адреса вузла буде занесена в таблицю комутації з відміткою «drop» («відкидати»). Якщо усі параметри співпадають, MAC-адреса вузла буде занесена в таблицю комутації з відміткою «allow» («дозволений»).

При функціонуванні в ACL mode комутатор на основі передвстановленого адміністратором «білого листа» IMPB створює правила ACL. Будь-який пакет, зв'язка IP-MAC якого відсутній в «білому листі», блокуватиметься ACL. Якщо режим ACL відключений, правила для записів IMPB будуть видалені з таблиці ACL. Слід зазначити, що цей режим не підтримується комутаторами, в яких відсутні апаратні таблиці ACL (інформацію про підтримку або відсутність режиму ACL можна знайти в специфікації на відповідну модель комутатора).

Режим DHCP Snooping використовується комутатором для динамічного створення записів IP-MAC на основі аналізу DHCP-пакетів і прив'язки їх до портів з включеною функцією IMPB (адміністраторові не вимагається створювати записи вручну). Таким чином, комутатор автоматично створює «білий лист» IMPB в таблиці комутації або апаратній таблиці ACL (якщо режим ACL включений). При цьому для забезпечення коректної роботи сервер DHCP має бути підключений до довіреного порту з вимкненою функцією IMPB. Адміністратор може обмежити максимальну кількість створюваних в процесі автоматичного вивчення записів IP – MAC на порт, тобто обмежити для кожного порту з активізованою функцією IMPB кількість вузлів, які можуть отримати IP-адресу з DHCP-сервера. При роботі в режимі DHCP Snooping комутатор не створюватиме записи IP-MAC для вузлів з IP-адресою встановленою вручну. Режим DHCP Snooping окремо від режимів ARP або ACL не використовується.

При активізації функції IMPB на порту адміністратор повинен вказати режим його роботи:

– strict mode – в цьому режимі порт за умовчанням заблокований. Перш ніж передавати пакети, він відправлятиме їх на ЦП для перевірки збігу їх параметрів IP-MAC із записами в «білому листі». Таким чином, порт не передаватиме пакети до тих пір, поки не переконається в їх достовірності. Порт перевіряє усе IP і ARP-пакети;

– loose mode – в цьому режимі порт за умовчанням відкритий. Порт буде заблокований, як тільки через нього пройде перший недостовірний пакет. Порт перевіряє тільки пакети ARP і IP Broadcast.

На рис. 3.9 показано приклад роботи функції IP-MAC-Port Binding в режимі ARP.

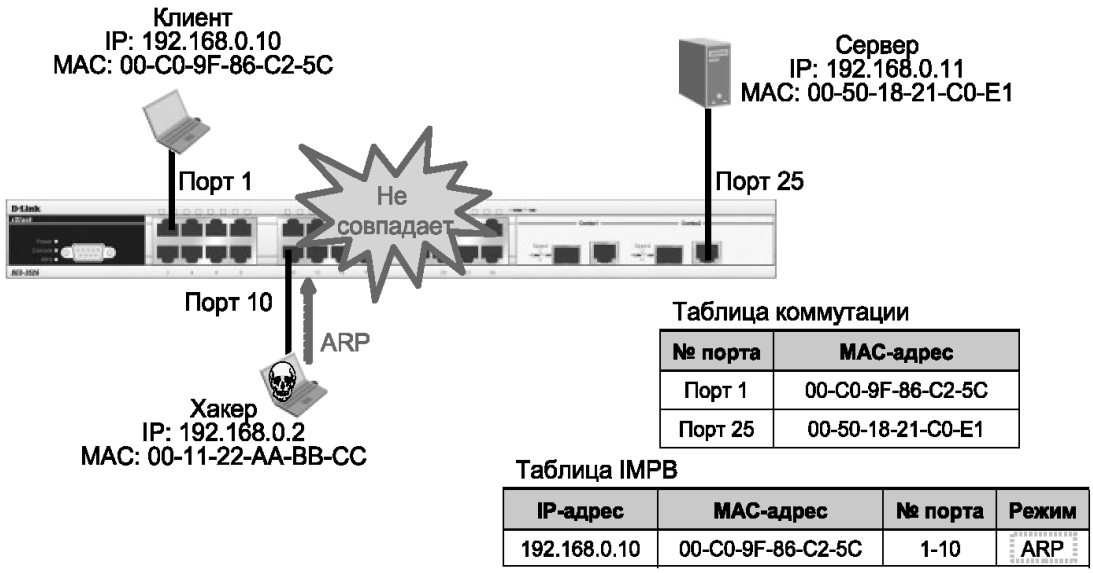


Рис. 3.9. Приклад роботи функції IP-MAC-Port Binding в режимі ARP

Хакер ініціював атаку типу ARPSpoofing. Комутатор виявляє, що на порт 10 приходять пакети ARP, зв'язка IP-MAC для яких відсутній в «білому листі» IMPB, і блокує MAC-адресу вузла.

Налаштування комутатора:

– створити запис IP – MAC – PortBinding, зв'язуючу IP – MAC – адреса вузла з портами підключення, і вказати режим роботи функції:

create address_binding ip_mac ipaddress 192.168.0.10 mac_address 00-C0-9F-86-C2-5C ports 1-10 mode arp

– активізувати функцію на необхідних портах і вказати режим роботи портів:

config address_binding ip_mac ports 1-10 state enable loose

На рис. 3.10 показаний приклад роботи функції IP – MAC – PortBinding в режимі DHCP Snooping. Комутатор динамічно створює запис IMPB після того,

як клієнт отримає IP-адрес від DHCP-сервера.

Налаштування комутатора:

– активізувати функцію IP-MAC-Port Binding в режимі DHCP Snooping глобально на комутаторі:

enable address_binding dhcp_snoop

– вказати максимальну кількість створюваних в процесі автовивчення записів IP-MAC на порт:

config address_binding dhcp_snoop max_entry ports 1-10 limit 10

– активізувати функцію IP-MAC-Port Binding в режимі DHCP Snooping на відповідних портах:

config address_binding ip_mac ports 1-10 state enable

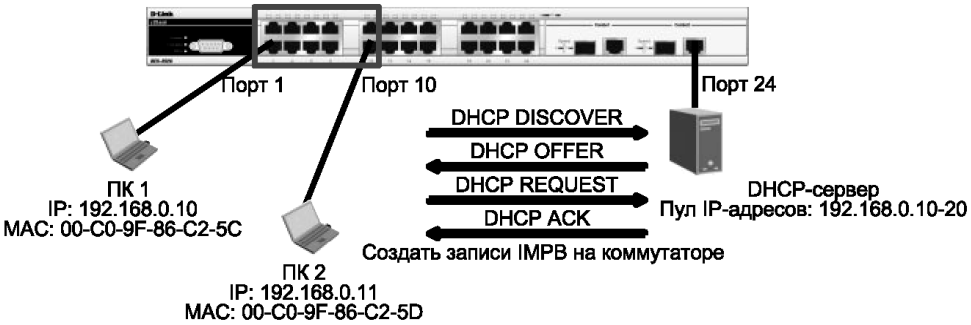


Таблица записей DHCP Snooping				
IP Address	MAC Address	Lease Time	Ports	Status
192.168.0.10	00-C0-9F-86-C2-5C	86390	1	Active
192.168.0.11	00-C0-9F-86-C2-5D	86395	10	Active

Таблица IP-MAC-Port Binding			
IP Address	MAC Address	Ports	Mode
192.168.0.10	00-C0-9F-86-C2-5C	1	AUTO
192.168.0.11	00-C0-9F-86-C2-5D	10	AUTO

Коммутатор автоматически создает записи IP-MAC-Port Binding, когда получает пакет DHCP.

Рис. 3.10. Приклад роботи функції IP – MAC – PortBinding в режимі DHCPSnooping

Необхідно відмітити, що для функції PortSecurity існують обмеження по кількості MAC-адрес, які може обслуговувати кожен порт. Ці обмеження різні для різних моделей комутаторів. Для отримання інформації про максимальну кількість обслуговуваних портом MAC-адрес необхідно звернутися до специфікації на використовуваний пристрій. Якщо стан каналу зв’язку на підключеному порту змінюється, MAC-адреси, вивчені на нім, видаляються з таблиці комутації, що аналогічно виконанню дій при витіканні часу, встановленого таймером FDB Aging Time При підключенні неавторизованого користувача до порту комутатора він буде заблокований, а комутатор відправить повідомлення SNMP Trap або створить запис в log-файлі, якщо адміністратор настроїв виконання цих дій.

3.4. Проведення аутентифікації користувачів за стандартом IEEE 802.1X

Стандарт IEEE 802.1X (IEEE 802.1X-2010) описує використання протоколу

EAP (Extensible Authentication Protocol) для підтримки аутентифікації за допомогою сервера аутентифікації і визначає процес інкапсуляції даних EAP, що передаються між клієнтами (запитуючими пристроями) і серверами аутентифікації. Стандарт IEEE 802.1X здійснює контроль доступу і не дозволяє неавторизованим пристроям підключатися до локальної мережі через порти комутатора.

Ролі пристроїв в стандарті 802.1X

У стандарті IEEE 802.1X визначені наступні три ролі, які можуть виконувати пристрої (рис. 3.11):

– клієнт (client/supplicant);

– аутентифікатор (authenticator);

– сервер аутентифікації (authentication server).

Рис. 3.11. Мережа з аутентифікацією 802.1X

Клієнт (client/supplicant) – це робоча станція, яка просить доступ до локальної мережі і сервісів комутатора і відповідає на запити від коммутатора (рис. 3.12). На робочій станції повинно бути встановлено клієнтське ПЗ для 802.1X, наприклад, то, яке вбудоване в ОС Microsoft Windows XP.

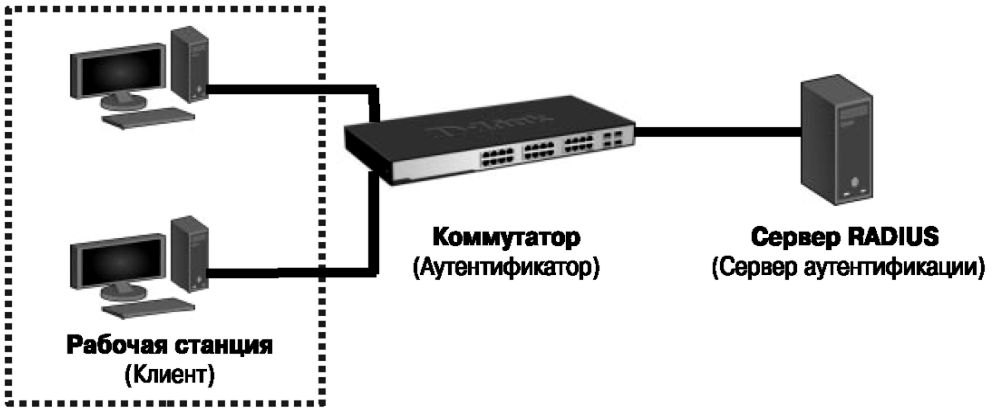


Рис. 3.12. Клієнт 802.1X

Сервер аутентифікації (authentication server) виконує фактичну аутентифікацію клієнта (рис. 3.13). Він перевіряє достовірність клієнта і інформує комутатор, надавати або ні клієнтові доступ до локальної мережі. RADIUS (Remote Authentication Dial – In User Service) працює в моделі «клієнт-сервер», в якій інформація про аутентифікацію передається між сервером RADIUS і клієнтами RADIUS.

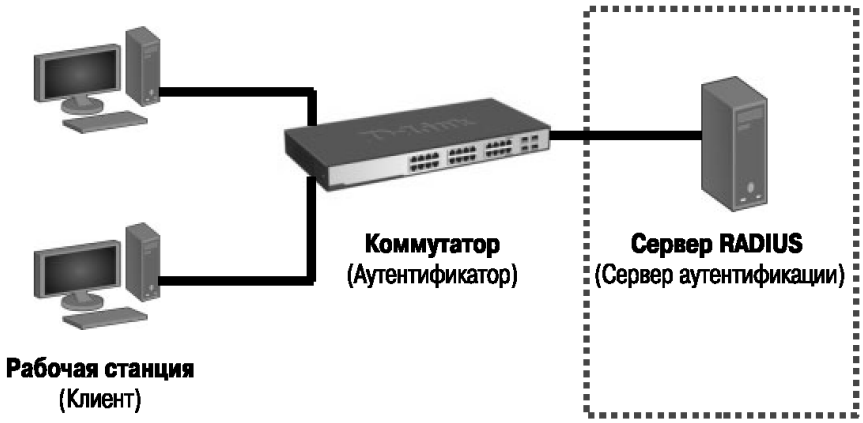


Рис. 3.13. Сервер аутентифікації

Аутентифікатор (authenticator) управляє фізичним доступом до мережі, ґрунтуючись на статусі аутентифікації клієнта (рис. 3.14). Цю роль виконує комутатор. Він працює як посередник (proxy) між клієнтом і сервером аутентифікації: отримує запит на перевірку достовірності від клієнта, перевіряє цю інформацію за допомогою сервера аутентифікації і пересилає відповідь клієнтові. Комутатор підтримує клієнт RADIUS, який відповідає за інкапсуляцію і деинкапсуляцию кадрів EAP і взаємодія з сервером аутентифікації.

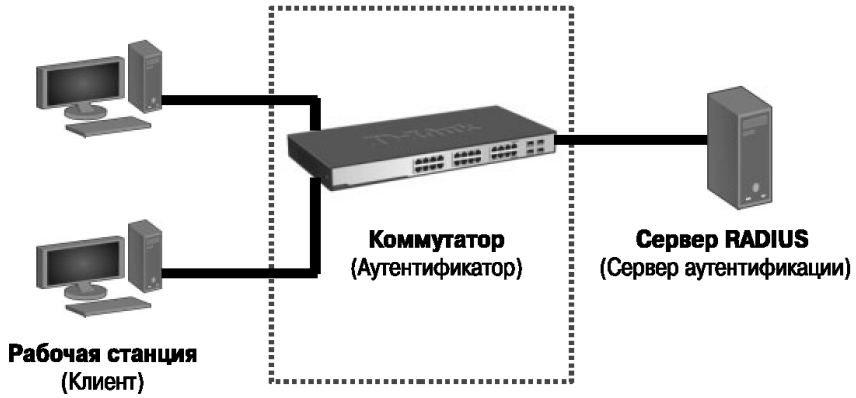


Рис. 3.14. Аутентифікатор

Ініціювати процес аутентифікації можуть або комутатор, або клієнт.

Клієнт ініціює аутентифікацію, посилаючи кадр EAPOL – start, який змушує

комутатор відправити йому запит на ідентифікацію. Клієнт відправляє EAP-відповідь зі своєю ідентифікацією, з комутатором-клієнтом і сервером аутентифікації до успішної або неуспішної аутентифікації. Якщо аутентифікація завершилася успішно, то порт комутатора стає авторизованим.

Схема обміну EAP-кадрами залежить від використовуваного аутентифікації. На рис. 3.15 показана схема обміну, що ініціюється клієнтом, де сервером RADIUS використовується метод аутентифікації One – Time – Password (OTP).

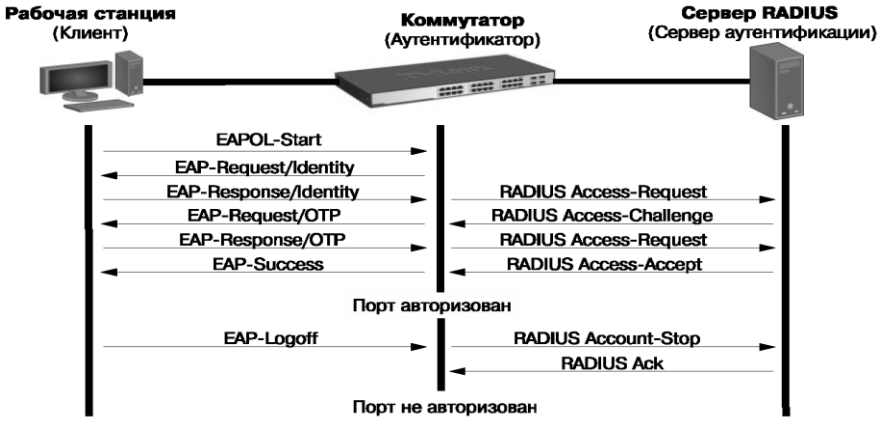


Рис. 3.15. Процес аутентифікації 802.1X

Реалізації аутентифікації 802.1X в комутаторах D-Link

У комутаторах D-Link підтримуються дві реалізації аутентифікації 802.1X:

– port-based 802.1X (802.1X на основі портів);

– MAC-based 802.1X (802.1X на основі MAC-адрес).

При аутентифікації 802.1X на основі портів (port-based 802.1X), після того, як порт був авторизований, будь-який користувач, підключений до нього, може отримати доступ до мережі. Розглянемо приклад налаштування функції port-based 802.1X для схеми, показаної на рис. 3.16.

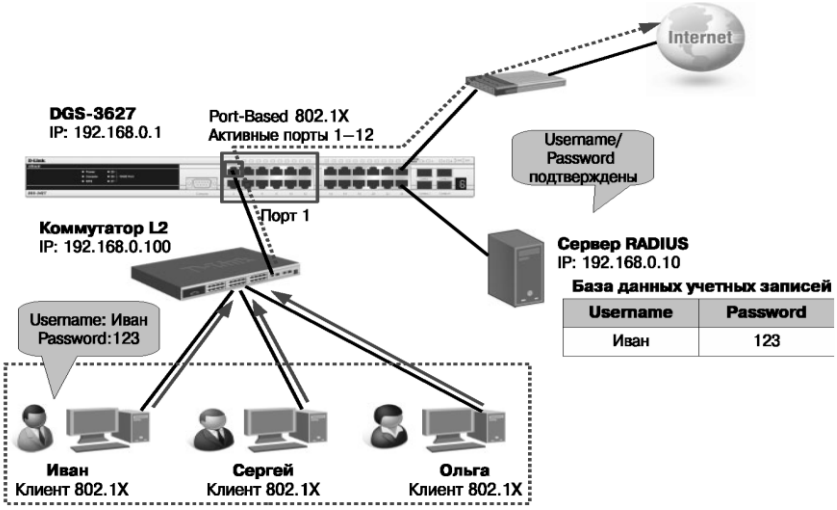


Рис. 3.16. Аутентифікація 802.1X на основі портів

Налаштування комутатора DGS -3627:

– налаштувати перевірку достовірності користувачів на сервері RADIUS:

config 802.1x auth_protocol radius_eap

– налаштувати аутентифікації 802.1X: port-based:

config 802.1x auth_mode port_based

– налаштувати порти, до яких підключаються клієнти в якості аутентифікатора (на uplink-портах до комутаторів вищого рівня не слід настроювати режим «authenticator»):

config 802.1x capability ports 1-12 authenticator

– активізувати функцію 802.1X:

enable 802.1x

– настроїти параметри сервера RADIUS:

config radius add 1 192.168.0.10 key 123456 default

На відміну від аутентифікації 802.1X на основі портів, де один порт, авторизований клієнтом, залишається відкритим для усіх клієнтів, аутентифікація 802.1X на основі MAC-адрес – це аутентифікація безлічі клієнтів на одному фізичному порті комутатора (рис. 3.17). При аутентифікації 802.1X на основі MAC-адрес (MAC–based 802.1X) перевіряються не лише ім’я користувача/пароль підключених до порту комутатора клієнтів, але і їх кількість. Кількість клієнтів, що підключаються, обмежена максимальною кількістю MAC-адрес, яке може вивчити кожен порт комутатора. Для функції MAC-based 802.1X кількість MAC-адрес, що вивчаються, вказується в специфікації на пристрій. Сервер аутентифікації перевіряє ім’я користувача/пароль, і якщо інформація достовірна, аутентифікатор (комутатор) відкриває логічне з’єднання на основі MAC-адреси клієнта. При цьому, якщо досягнута межа вивчених портом комутатора MAC-адрес, новий клієнт буде заблокований.

Розглянемо приклад налаштування функції MAC-based 802.1X для схеми, показаної на рис. 3.17.

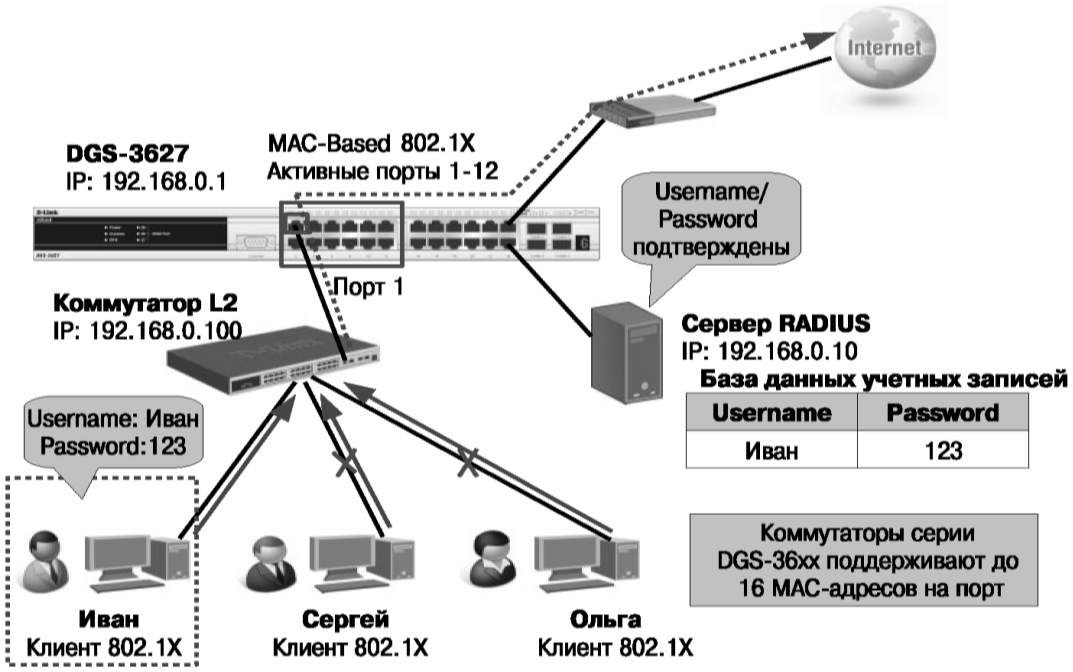


Рис. 3.17. Аутентифікація 802.1X на основі MAC-адрес

Налаштування комутатора DGS-3627. Комутатори серії DGS-36xx підтримують до 16 MAC-адрес на порт:

– налаштувати перевірку достовірності користувачів на сервері RADIUS:

config 802.1x auth_protocol radius_eap

– налаштуватитипаутентифікації 802.1X: MAC-based:

conflg 802.1x auth_mode mac_based

– налаштувати порти, до яких підключаються клієнти в якості аутентифікатора:

conflg 802.1x capablllty ports 1-12 authentlcator

– активізувати функцію 802.1X:

enable 802.1x

– налаштувати параметри сервера RADIUS:

conflg radlus add 1 192.168.0.10 key 123456 default

На рис. 3.18. показана локальна аутентифікація 802.1X на основі MAC-адрес.

Слід зазначити, що комутатор може виконувати роль сервера аутентифікації. В цьому випадку база цих облікових записів користувачів зберігатиметься локально на самому комутаторі.

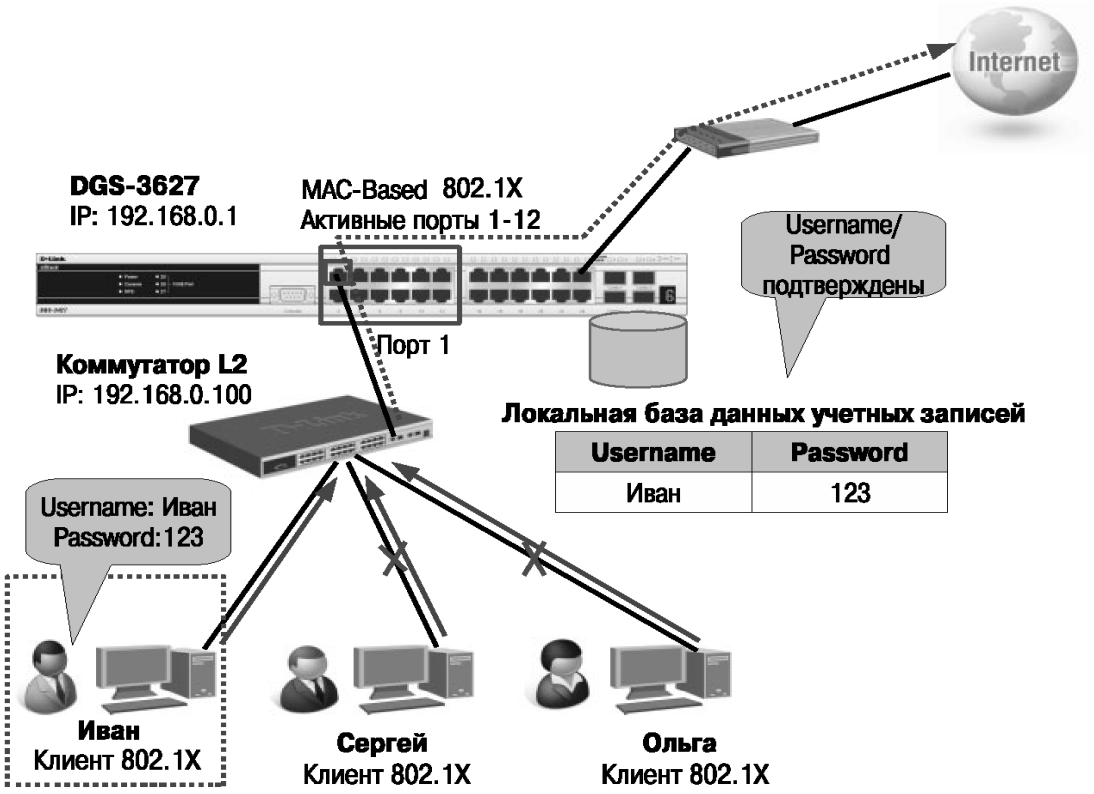


Рис. 3.18. Аутентифікація 802.1X на основі MAC-адрес з використанням локальної бази цих облікових записів користувачів

Стан порту комутатора визначається тим, що отримав або не отримав клієнт право доступу до мережі. Спочатку порт знаходиться у неавторизованому стані. У цьому стані він забороняє проходження усього трафіку, що входить і витікаючого, за винятком пакетів EAPOL. Коли клієнт автентифікований, порт переходить в авторизований стан, дозволяючи передачу крізь нього будь-якого трафіку.

Можливі наступні варіанти, коли клієнт або комутатор не підтримують 802.1X. Якщо клієнт, який не підтримує 802.1X, підключається до неавторизованого порту 802.1X, комутатор посилає клієнтові запит на авторизацію. Оскільки в цьому випадку клієнт не відповість на запит, порт залишиться в неавторизованому стані і клієнт не отримає доступ до мережі.

Коли клієнт з підтримкою 802.1X підключається до порту, на якому не підтримується протокол 802.1X, він починає процес аутентифікації, посилаючи кадр EAPOL – start. Не отримавши відповіді, клієнт посилає запит певну кількість разів. Якщо після цього відповідь не отримана, клієнт, вважаючи, що порт знаходиться в авторизованому стані, починає передавати дані.

У разі, коли і клієнт, і комутатор підтримують 802.1X, при успішній аутентифікації клієнта порт переходить в авторизований стан і починає передавати усі кадри клієнта. Якщо в процесі аутентифікації виникли помилки, порт залишається в неавторизованому стані, але аутентифікація може бути відновлена. Якщо

сервер аутентифікації не може бути досягнутий, комутатор може повторно передати запит. Якщо від сервера не отримана відповідь після певної кількості спроб, клієнтові буде відмовлено в доступі до мережі через помилок аутентифікації. Щоб вірогідність такої ситуації була мінімальною, на комутаторі можна налаштувати параметри декількох серверів RADIUS.

Коли клієнт завершує сеанс роботи, він посилає повідомлення EAPOL-logoff, що переводить порт комутатора в неавторизований стан. Якщо стан каналу зв'язку порту переходить з активного (up) в не-активне (down) або отриманий кадр EAPOL-logoff, порт повертається в неавторизований стан.

3.5. Створення гостьової VLAN з обмеженими правами

Функція 802.1X Guest VLAN використовується для створення гостьової VLAN з обмеженими правами для користувачів, що не пройшли аутентифікацію. Коли клієнт підключається до порту комутатора з активізованою аутентифікацією 802.1X і функцією Guest VLAN, відбувається процес аутентифікації (локально або віддалено з використанням сервера RADIUS). У разі успішної аутентифікації клієнт буде поміщений в VLAN призначення (Target VLAN) у відповідності с передвстановленим на сервері RADIUS параметром VLAN. Якщо цей параметр не визначений, то клієнт буде повернений в первинну VLAN (відповідно до налаштувань порту підключення).

У тому випадку, якщо клієнт не пройшов аутентифікацію, він поміщається в Guest VLAN з обмеженими правами і доступом.

Процес аутентифікації з використанням Guest VLAN

Функція Guest VLAN підтримується тільки для аутентифікації 802.1X на базі портів. Слід зазначити, що, використовуючи функцію 802.1X Guest VLAN, клієнтам можна надавати ряд обмежених сервісів до проходження процесу аутентифікації 802.1X.

Члени Guest VLAN можуть взаємодіяти один з одним в межах цієї VLAN, навіть якщо вони не пройшли аутентифікацію 802.1X. Після успішного проходження аутентифікації член Guest VLAN може бути переміщений в VLAN призначення (Target VLAN) відповідно до атрибуту VLAN, вказаному на сервері RADIUS. Клієнт може завантажити з сервера і встановити необхідне програмне забезпечення 802.1X. Наочніше цей процес приведений на блок-схемі (рис. 3.19).

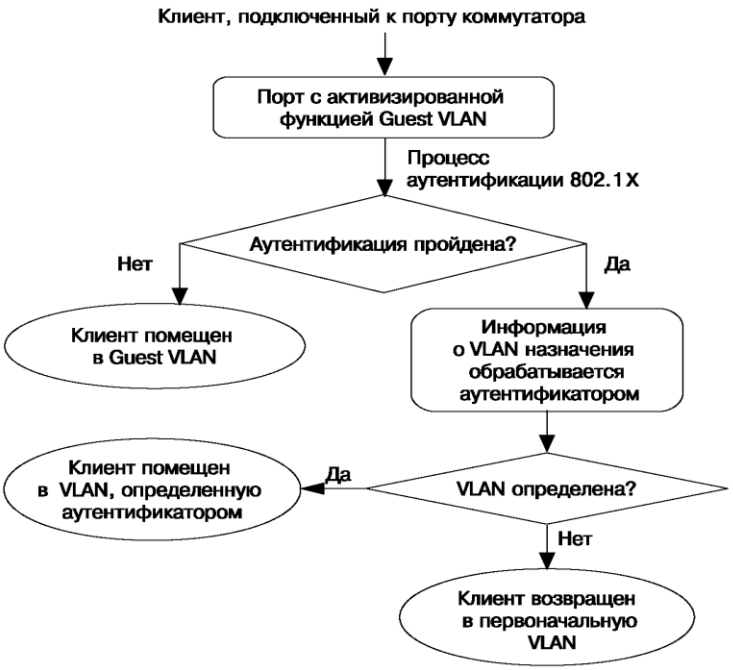


Рис. 3.19. Процес аутентифікації з використанням Guest VLAN

Розглянемо приклад, показаний на рис. 3.20. До аутентифікації клієнт 1 знаходиться в Guest VLAN і має доступ до робочих станцій, розташованих в ній, і загальнодоступному web/FTP-серверу. Після успішної аутентифікації клієнта 1 порт комутатора, до якого він підключений, буде додано в VLAN 10 і клієнт 1 зможе отримати доступ до конфіденційної інформації, що зберігається на FTP-сервері VLAN 10. Якщо клієнт не пройшов аутентифікацію 802.1X, він залишиться в Guest VLAN з обмеженими правами.

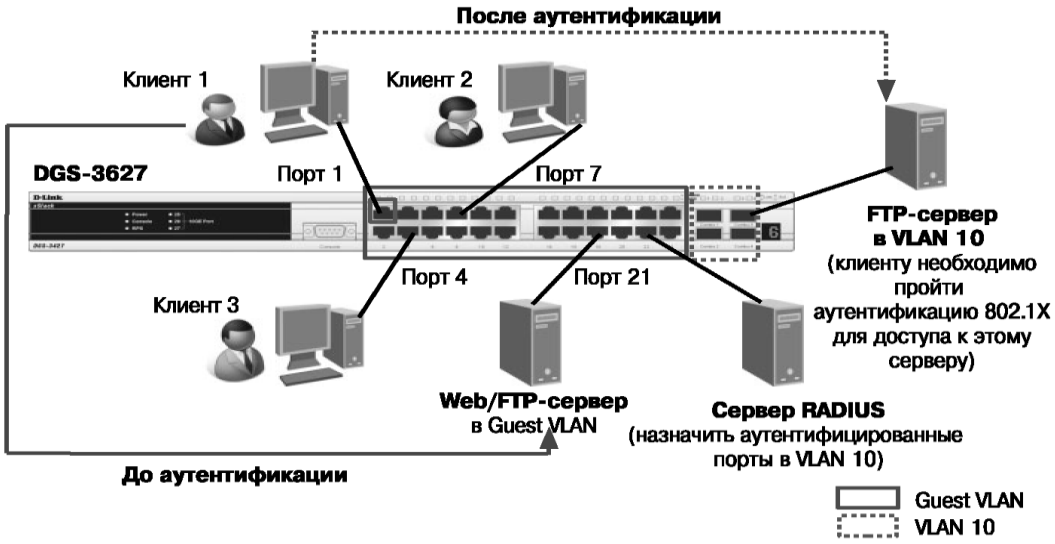


Рис. 3.20. Ресурси, доступні клієнтові до і після аутентифікації 802.1X при використанні Guest VLAN

Як приклад використання і налаштування функції 802.1X Guest VLAN розглянемо схему мережі компанії (рис. 3.21), в якій користувачам неминувшим аутентифицію, що знаходиться в VLAN 10, дозволений доступ в інтернет. Після успішної аутентифікації користувачів, порти, до яких вони підключені, будуть додані в VLAN 20.

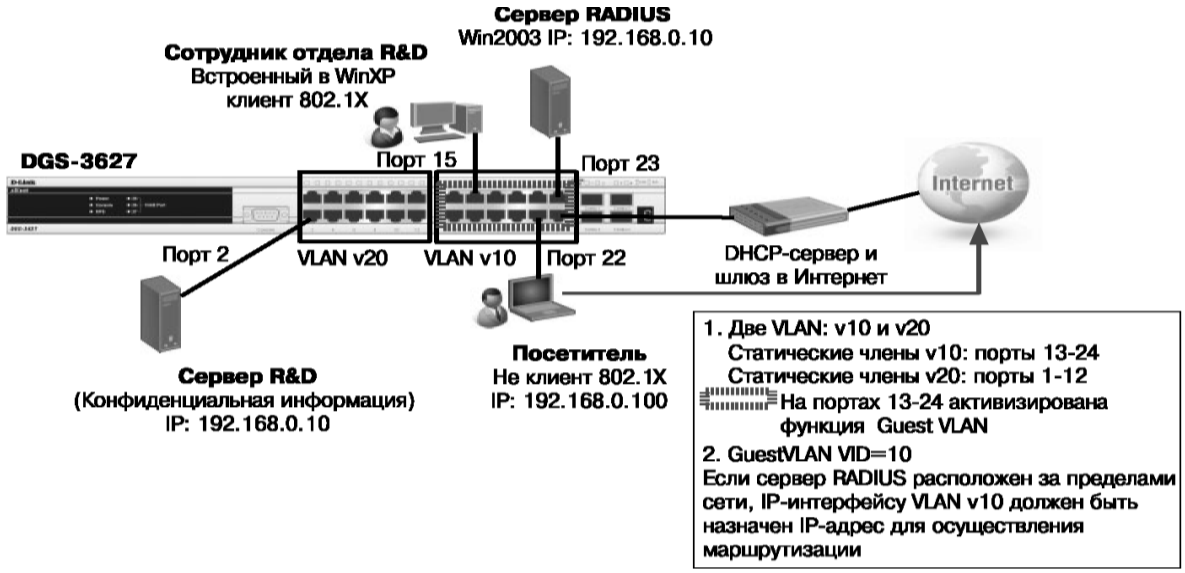


Рис. 3.21. Приклад використання 802.1X Guest VLAN

Налаштування комутатора DGS-3627

– створити на комутаторі VLAN v10 і v20:

conflgvlandefaultdelete 1-24

createvlanv10 tag 10

conflg vlan v10 add untagged 13-24

create vlan v20 tag 20

conflg vlan v20 add untagged 1-12

conflg lplf System lpaddress 192.168.0.1/24 vlan v10

– активізувати функції 802.1Xi Guest VLAN:

enable 802.1x

create 802.1x guest_vlan v10

conflg 802.1x guest_vlan ports 13-24 state enable

– налаштувати комутатор в якості аутентифікатора і задати параметри сервера RADIUS:

conflg 802.1x capablllty ports 13-24 authentlcator conflg radlus add 1 192.168.0.10 key 123456 default

Налаштування параметрів на сервері RADIUS включає установку наступних призначених для користувача атрибутів (рис. 3.22).

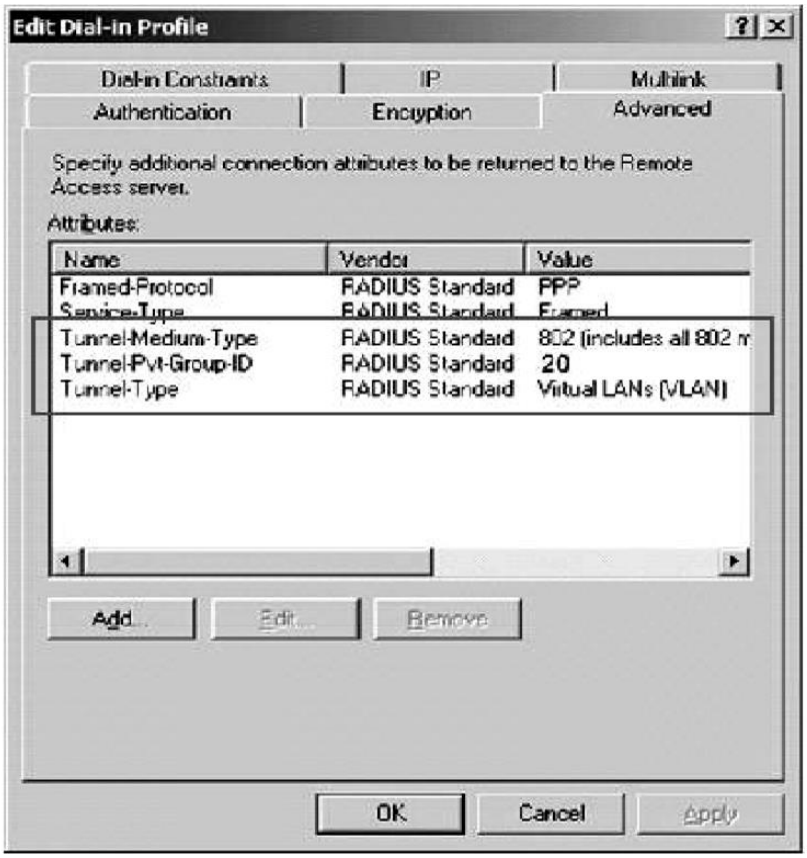


Рис. 3.22. Призначені для користувача атрибути на сервері RADIUS

Tunnel – Medium – Type (65) = 802

Tunnel – Pvt – Group – ID (81) = 20←VID

Tunnel – Type (64) = VLAN

Перевірити конфігурацію комутатора можна за допомогою наступних команд:

```
DGS-3627#show 802.1x auth_configuration
Command: show 802.1x auth_configuration

802.1X                      : Enabled
Authentication Mode         : Port_based
Authentication Protocol     : RADIUS_EAP

Port number         : 1
Capability          : None
AdminCrlDir         : Both
OpenCrlDir          : Both
Port Control        : Auto
QuietPeriod         : 60 sec
TxPeriod            : 30 sec
Supp Timeout        : 30 sec
Server Timeout      : 30 sec
MaxReq              : 2 times
ReAuthPeriod        : 3600 sec
ReAuthenticate      : Disabled

DGS-3627#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
---------------------------------

Guest VLAN : v10
Enable Guest VLAN Ports : 13-24

DGS-3627#show radius
Command: show radius

Idx   IP Address      Auth-Port   Acct-Port   Status   Key
---   ----------      ---------   ---------   -------  ------
 1    192.168.0.10    1812        1813        Active   123456

Total Entries: 1
```

Поки клієнт, підключений до порту 22, не пройшов аутентифікацію, поточна конфігурація VLAN і стан аутентифікації 802.1X на комутаторі будуть наступними:

```
DGS-3627#show vlan
VID: 1   VLAN Name    : default
VLAN Type: Static Advertisement : Enabled
Member Ports             : 25-27
Static Ports             : 25-27
Current Tagged Ports     :
Current Untagged Ports   : 25-27
Static Tagged Ports      :
Static Untagged Ports:  25-27
Forbidden Ports          :

VID: 10  VLAN Name       : v10
VLAN Type: Static Advertisement : Disabled
Member Ports             : 13-24
Static Ports             : 13-24
Current Tagged Ports     :
Current Untagged Ports   : 13-24
Static Tagged Ports      :
Static Untagged Ports    : 13-24
Forbidden Ports          :

VID: 20  VLAN Name       : v20
VLAN Type: Static Advertisement : Disabled
Member Ports             : 1-12
Static Ports             : 1-12
Current Tagged Ports     :
Current Untagged Ports   : 1-12
Static Tagged Ports      :
Static Untagged Ports    : 1-12
Forbidden Ports          :

Total Entries        : 3

DGS-3627#show 802.1x auth_state
Command: show 802.1x auth_state

Port      Auth PAE State        Backend State     Port State
---       --------------        -------------     ----------
1         ForceAuth             Success           Authorized
2         ForceAuth             Success           Authorized
3         ForceAuth             Success           Authorized
4         ForceAuth             Success           Authorized
5         ForceAuth             Success           Authorized
6         ForceAuth             Success           Authorized
7         ForceAuth             Success           Authorized
8         ForceAuth             Success           Authorized
9         ForceAuth             Success           Authorized
10        ForceAuth             Success           Authorized
11        ForceAuth             Success           Authorized
12        ForceAuth             Success           Authorized
13        Disconnected          Idle              Unauthorized
14        Disconnected          Idle              Unauthorized

.............

22        Connecting            Idle              Unauthorized
```

Після аутентифікації клієнта, поточні налаштування VLAN і стан аутентифікації 802.1X зміняться таким чином:

```
DGS-3627#show vlan
VID: 1   VLAN Name       : default
VLAN Type: Static Advertisement : Enabled
Member Ports             : 25-27
Static Ports             : 25-27
Current Tagged Ports     :
Current Untagged Ports   : 25-27
Static Tagged Ports      :
Static Untagged Ports    : 25-27
Forbidden Ports          :

VID: 10  VLAN Name       : v10
VLAN Type: Static Advertisement : Disabled
Member Ports             : 13-21,23-24
Static Ports             : 13-21,23-24
Current Tagged Ports     :
Current Untagged Ports   : 13-21,23-24
Static Tagged Ports      :
Static Untagged Ports    : 13-21,23-24
Forbidden Ports          :

VID: 20  VLAN Name       : v20
VLAN Type: Static Advertisement : Disabled
Member Ports             : 1-12,22
Static Ports             : 1-12,22
Current Tagged Ports     :
Current Untagged Ports   : 1-12,22
Static Tagged Ports      :
Static Untagged Ports    : 1-12,22
Forbidden Ports          :

Total Entries : 3

DGS-3627#show 802.1x auth_state
Command: show 802.1x auth_state

Port  Auth PAE State    Backend State    Port State
---   --------------    -------------    ----------
1     ForceAuth         Success          Authorized
2     ForceAuth         Success          Authorized
3     ForceAuth         Success          Authorized
4     ForceAuth         Success          Authorized
5     ForceAuth         Success          Authorized
6     ForceAuth         Success          Authorized
7     ForceAuth         Success          Authorized
8     ForceAuth         Success          Authorized
9     ForceAuth         Success          Authorized
10    ForceAuth         Success          Authorized
11    ForceAuth         Success          Authorized
12    ForceAuth         Success          Authorized
13    Disconnected      Idle             Unauthorized
14    Disconnected      Idle             Unauthorized
.....
22    Authenticated     Idle             Authorized
```

Функції захисту ЦП комутатора

Функція Safeguard Engine спеціально розроблена для забезпечення доступності комутатора в ситуаціях, коли в результаті заповнення мережі шкідливим трафіком його ЦП сильно завантажений. В результаті цього, ЦП комутатора не може належним чином обробляти пакети протоколів STP/RSTP/MSTP, IGMP, надавати адміністративний доступ через веб-інтерфейс, CLI, SNMP і виконувати інші завдання, що вимагають обробки на ЦП. Функція Safeguard Engine дозволяє ідентифікувати і приорітезувати трафік (наприклад, ARP-широко мовлення, пакети з невідомою IP-адресою при значення і так далі), що направляється для обробки на ЦП, з метою відкидання небажаних пакетів для збереження функціональності комутатора. Коли комутатор з включеною функцією Safeguard Engine отримує велику кількість пакетів, призначених для обробки на ЦП і встановлене верхнє порогове значення Rising Threshold, що перевищує, він переходить в режим високого завантаження (exhausted mode). Знаходячись в цьому режимі, комутатор може виконувати одну з наступних дій для зменшення завантаження ЦП:

– припинення отримання усіх ARP-пакетів і широкомовних IP-пакетів (при роботі функції в строгому режимі, strict mode);

– обмеження смуги пропускання для отримуваних ARP-пакетів і широкомовних IP-пакетів шляхом її динамічної зміни (при роботі функції в нестрогому режимі, fuzzy mode).

При нормалізації роботи мережі і зниженні кількості небажаних пакетів до встановленого нижнього порогового значення Falling Threshold комутатор вийде з режиму високого завантаження і механізм Safeguard Engine перестане функціонувати. Слід зазначити, що при перемиканні комутатора в режим Exhausted можуть виникати наступні побічні ефекти:

– при роботі функції Safeguard Engine в строгому режимі неможливо здійснювати адміністративний доступ до комутатора рівня 2, оскільки цей режим передбачає відкидання усіх ARP-запитів, ЦП, що поступають на інтерфейс. Для вирішення цієї проблеми в статичній ARP-таблиці робочої станції, що управляє, можна створити запис, зв’язуючий MAC-адресу комутатора з IP-адресою його інтерфейсу управління. В цьому випадку робочій станції не потрібно буде відправляти ARP-запит комутатору;

– при роботі функції Safeguard Engine в строгому режимі на комутаторі рівня 3, окрім неможливості адміністративного доступу, також може бути пору-

шена маршрутизація між підключеними до нього підмережами, оскільки відкидатимуться ARP-запити, які поступають не лише на інтерфейс ЦП, але і на IP-інтерфейси комутатора.

Перевагою нестрогого режиму роботи функції Safeguard Engine є те, що в ньому не просто відкидаються усі ARP-пакети або широкомовні IP-пакети, а динамічно змінюється смуга пропускання для них. Таким чином, навіть при серйозній вірусній епідемії, комутатор рівня 2/3 буде доступний по управлінню, а комутатор рівня 3, у тому числі, зможе забезпечувати маршрутизацію між підмережами. Як приклад використання функції Safeguard Engine розглянемо ситуацію, коли одна з робочих станцій, підключених до комутатора, постійно розсилає ARP-пакети з дуже високою швидкістю. Завантаження ЦП комутатора при цьому міняється від нормальної до 90%. При усуненні причини, що викликала лавинну генерацію ARP-пакетів на робочій станції, завантаження ЦП знизиться до норми. Для захисту ЦП від подібних ситуацій і зниження його завантаження на комутаторі можна настроїти функцію Safeguard Engine.

Налаштування комутатора:

– активізуйте функцію Safeguard Engine:

config safeguard_engine state enable

– задайте нижнє і верхнє порогові значення (вказуються значення у відсотках від завантаження ЦП), при яких відбуватиметься перемикання між нормальним режимом роботи і режимом Exhausted. Вкажіть режим роботи функції:

config safeguard_engine utilization rising 40 falling 25 mode strict

– активізуйте функцію Safeguard Engine:

config safeguard_engine state enable

– задайте нижнє і верхнє порогові значення (вказуються значення у відсотках від завантаження ЦП), при яких відбуватиметься перемикання між нормальним режимом роботи і режимом Exhausted. Вкажіть режим роботи функції:

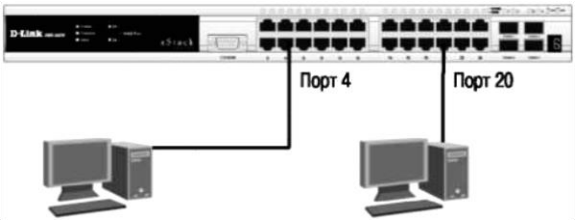
config safeguard_engine utilization rising 40 falling 25 mode strict

Стандартні списки управління доступом виконують фільтрацію трафіку на апаратному рівні і не можуть фільтрувати потоки даних, призначені для обробки на ЦП, наприклад, повідомлення ICMP, що відправляються на IP-адресу управління комутатором. У разі виникнення великої кількості таких пакетів продуктивність комутатора може сильно знизитися через високе завантаження ЦП.

Функція CPU Interface Filtering, підтримувана на старших моделях комутаторів D-Link, є ще одним рішенням, що дозволяє обмежувати пакети, що поступають для обробки на ЦП, шляхом фільтрації небажаного трафіку на апаратному

рівні. За своєю суттю функція CPU Interface Filtering є списками управління доступом до інтерфейсу ЦП і має аналогічні стандартним ACL принципами роботи і конфігурації.

Як приклад розглянемо завдання, в якому необхідно настроїти комутатор так, щоб пакети ICMP, що передаються комп'ютером ПК 2, не вирушали на обробку на ЦП, але при цьому ПК 2 міг передавати дані іншим пристроям, наприклад ПК 1.



ПК 1 IP: 10.31.3.2/8

ПК2 IP : 10.31.3.2/8

Рис. 3.23. Схема мережі для налаштування комутатора

– активізуйте функцію CPU Interface Filtering глобально на комутаторі:

enable cpu_interface_filtering

– створіть профіль доступу для інтерфейсу ЦП:

create cpu access_profile ip source_ip_mask 255.255.255.128 icmp profile_id 1

– створіть правило для профілю доступу:

config cpu access_profile profile_id 1 add access_id 1 ip source_ip 10.31.3.2 icmp deny

Запитання для самоконтролю

1. Методи забезпечення надійності програмного забезпечення.

2. Формування інструментально-технологічних комплексів.

3. Ієрархічна декомпозиція в моделі OSI/ISO.

4. Загрози в архітектурі відкритих мереж в моделі OSI/ISO.

5. Процедури захисту в моделі OSI/ISO.

6. Сервісні служби захисту в моделі OSI/ISO.

7. Адміністрування засобів захисту в моделі OSI/ISO.

8. Реалізація захисту в моделі OSI/ISO.

9. Основні положення загальних критеріїв безпеки інформаційних технологій стандарту ISO 15408.

10. Функціональні вимоги до засобів захисту стандарту ISO 15408.

11. Вимоги гарантій засобів захисту стандарту ISO 15408.

12. Рівні гарантій безпеки стандарту ISO 15408.

13. Мета розробки, основні положення та склад загальних критеріїв стандарту ISO 15408.

14. Потенційні загрози безпеці та типові завдання захисту стандарту ISO 15408.

15. Продукт інформаційних технологій стандарту ISO 15408.

16. Профіль захисту стандарту ISO 15408.

17. Проект захисту стандарту ISO 15408.

18. Забезпечення безпеки на фізичному рівні моделі OSI.

19. Комунікаційні сигнали та кодування.

20. Забезпечення безпеки на транспортному рівні моделі OSI.

ГЛАВА 4.
ТЕХНОЛОГІЯ ПОБУДОВИ ЗАХИЩЕНОЇ КОРПОРАТИВНОЇ МЕРЕЖІ

4.1. Передача потоку даних. Багатоадресна розсилка

У сучасних IP –мережах існує три способи відправки пакетів від джерела до приймача:

– одноадресна передача (unicast);

– широкомовна передача (broadcast);

– багатоадресна розсилка (multicast).

При одноадресній передачі потік даних передається від вузла відправника на індивідуальну IP-адресу конкретного вузла одержувача. Широкомовна передача передбачає доставку потоку даних від вузла відправника безлічі вузлів одержувачів, підключених до мережі, з використанням широкомовної IP-адреси.

Багатоадресна розсилка забезпечує доставку потоку даних групі вузлів на IP-адресу групи багатоадресної розсилки. У цієї групи немає фізичних або географічних обмежень: вузли можуть знаходитися у будь-якій точці світу. Вузли, які зацікавлені в отриманні даних для певної групи, повинні приєднатися до цієї групи (підписатися на розсилку) за допомогою протоколу IGMP (Internet Group Management Protocol, міжмережевий протокол управління групами). Після цього пакети багатоадресної розсилки IP, що містять в полі призначення заголовка групову адресу, поступатимуть на цей вузол і оброблятися.

Адресація багатоадресної IP-розсилки

Джерело багатоадресного трафіку направляє пакети багатоадресної розсилки не на індивідуальні IP-адреси кожного з вузлів-одержувачів, а на групову IP-адресу. Групові адреси визначають довільну групу IP-вузлів, що приєдналися до цієї групи і бажаючих по-лучать адресований їй трафік.

Агентство IANA (Internet Assigned Numbers Authority ‘Агентство по виділенню імен і унікальних параметрів протоколів інтернету’), яке управляє призначенням групових адрес, виділило для багатоадресної розсилки адреси IPv4 класу D в діапазоні від 224.0.0.0 до 239.255.255.255. Використання групових IP-адрес з блоку із адміністративним обмеженням найзручніше при організації багатоадресної розсилки в локальній мережі підприємства або організації. Відповідно до RFC 2365 «Administratively Scoped IP Multicast» підмережа 239.192.0.0/14 виділена для приватного використання і визначена як локальна область організації IPv4.

Формат IP-адреси класу D показаний на рис. 4.1. Перші 4 біта адреси завжди рівні 1110, інші 28 біт використовуються для ідентифікації конкретної групи одержувачів багатоадресного трафіку.

1	1	1	0	Multicast ID
Перші 4 біта				28 біт

Рис. 4.1. Формат IP-адреси класу D

Як правило, робочі станції локальної мережі отримують і обробляють кадри тільки у разі збігу MAC-адреси призначення кадру з їх власною MAC-адресою або якщо MAC-адреса широкомовна. При використанні багатоадресної розсилки необхідно, щоб декілька вузлів могли отримувати потік даних із загальною MAC-адресою. Одним із способів, що дозволяють досягти цього, є перетворення групової IP-адреси в MAC-адресу.

У специфікації IEEE 802.3 визначена можливість вказівки типу MAC-адреси призначення: індивідуальний або груповий (широкомовний або багатоадресний). Для цього використовується перший біт поля адреси призначення (Destination Address) кадру Ethernet. Якщо значення біта дорівнює 1, це вказує на те, що кадр призначений для групи або для усіх вузлів мережі (широкомовна адреса має вигляд 0xFF-FF-FF-FF-FF-FF).

MAC-адреса групової розсилки розпочинається з префікса, що складається з 24 бітів, – 0x01-00-5E. Наступний, 25-й біт (чи біт високого порядку) прирівнюється до 0. Останні 23 біта MAC-адреси формуються з 23 молодших бітів групового IP-адреса. Це проілюстровано на рис. 4.2.

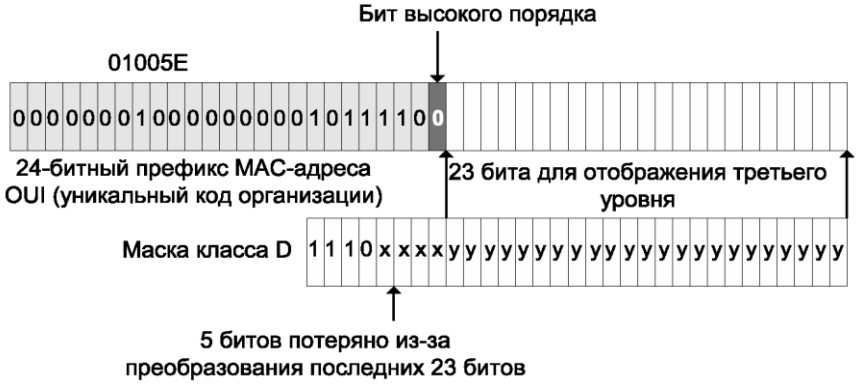


Рис. 4.2. Перетворення групової IP -адреси в адресу MAC-адреса групової розсилки

Оскільки, при перетворенні втрачаються 5 бітів 1-го октету IP-адреси, адреса, що вийшла, не є унікальною. Кожній MAC-адресі відповідає 32 IP-адреса групової розсилки. Це необхідно враховувати при призначенні IP-адрес багатоадресної розсилки.

Сам по собі багатоадресний трафік не знає нічого про те, де знаходяться його адресати. Як і для будь-якого застосування, для цього потрібні протоколи.

Протокол IGMP використовується для динамічної реєстрації окремих вузлів у багатоадресній групі локальної мережі. Вузли мережі визначають приналежність до групи, посилаючи IGMP-повідомлення на свій локальний багатоадресний маршрутизатор. По протоколу IGMP маршрутизатори (комутатори L3) отримують IGMP -повідомлення і періодично посилають запити, щоб визначити, які групи активні або не активні в цій мережі.

У загальному випадку протокол IGMP визначає наступні типи повідомлень:

– запит про приналежність до групи (membership query);

– відповідь про приналежність до групи (membership report);

– повідомлення про вихід з групи (leave group message).

Нині існують три версії протоколу IGMP:

– IGMP версії 1 (IGMP v1, описаний в RFC 1112);

– IGMP версії 2 (IGMP v2, описаний в RFC 2236);

– IGMP версії 3 (IGMP v3, описаний в RFC 3376).

Протокол IGMP використовується тільки в мережах з адресацією IPv4, оскільки в мережах з адресацією IPv6 групова передача пакетів реалізована інакше.

Управління багатоадресною розсилкою на 2-му рівні OSI (IGMP Snooping)

Коли комутатор 2-го рівня отримує багатоадресний трафік, він починає передавати кадри через усі порти, оскільки не знаходить запису про MAC-адресу у своїй таблиці комутації. Це суперечить основному призначенню комутатора, яке полягає в обмеженні трафіку і передачі його тільки тим портам, до яких підключені одержувачі.

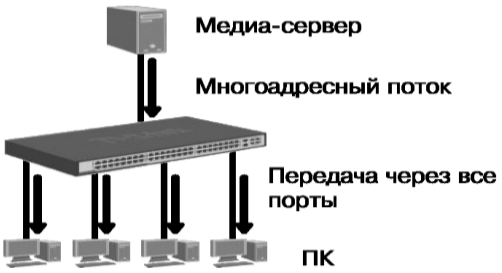


Рис. 4.3. Передача багатоадресного трафіку без підтримки управління ним на комутаторі

Управління багатоадресною розсилкою на комутаторі 2-го рівня може бути виконано двома способами.

Перший спосіб полягає в створенні статичних таблиць комутації для портів,

до яких не підключені передплатники багатоадресних груп. Це дозволяє обмежити багатоадресний трафік і передавати його тільки через ті порти, до яких підключені вузли-передплатники. Проте цей спосіб не дозволяє динамічно відстежувати додавання або виключення членів з багатоадресної групи.

Другим способом, що дозволяє розв'язати проблему лавинної передачі (flooding) багатоадресних пакетів і динамічно відстежувати стан підписки вузлів, являється функція IGMP Snooping (IGMP-прослуховування).

IGMP Snooping – це функція другого рівня моделі OSI, яка дозволяє комутаторам вивчати членів багатоадресних груп, підключених до його портів, прослуховуючи IGMP-повідомлення (запити і відповіді), передані між вузлами-передплатниками і маршрутизаторами (комутаторами рівня 3) мережі.

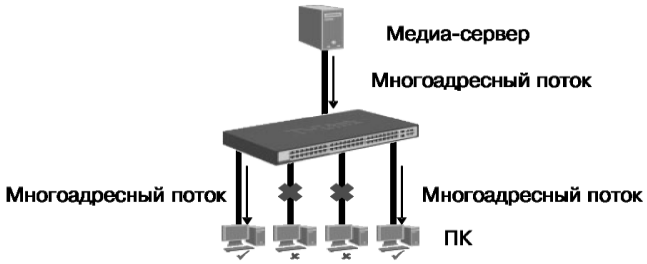


Рис. 4.4. Передача багатоадресного трафіку з підтримкою IGMP Snooping

Коли вузол, підключений до комутатора, хоче вступати до багатоадресного гурту або відповідає на IGMP-запит, отриманий від маршрутизатора (комутатора рівня 3) багатоадресної розсилки, він відправляє IGMP-відповідь, у якій вказана адреса багатоадресної групи. Комутатор переглядає інформацію в IGMP-відповіді і створює у своїй асоціативній таблиці комутації IGMP Snooping запис для цієї групи (якщо вона не існує). Цей запис зв'язує порт, до якого підключений вузол-передплатник – порт, до якого підключений маршрутизатор (комутатор рівня 3) багатоадресної розсилки, і MAC-адреса багатоадресної групи.

Якщо комутатор отримує IGMP-відповідь для цієї ж групи від іншого вузла цієї VLAN, то він додає номер порту у вже існуючий запис асоціативної таблиці комутації IGMP Snooping. Формуючи таблицю комутації багатоадресної розсилки, комутатор здійснює передачу багатоадресного трафіку тільки тим вузлам, які в ньому зацікавлені.

Розглянемо приклад роботи функції IGMP Snooping для мережі, показаної на рис. 4.5. Комутатор L3 відправляє IGMP-запит про приналежність до групи комутатору L2, який розсилає його через усі порти, за винятком порту-одержувача. ПК 1 хоче вступати до багатоадресного гурту 239.192.1.10 і відправляє IGMP-відповідь на адресу групи, вказуючи в якості багатоадресної MAC-адреси

призначення 0x01-00-5E-40-01-0A. Процесор комутатора L2 аналізує IGMP-відповідь і створює в асоціативній таблиці комутації IGMP Snooping (у первинний момент часу вона порожня) запис для MAC-адреси 0x01-00-5E-40-01-0A, еквівалентного груповій адресі 239.192.1.10. Також в цей запис заноситься інформація про порти, до яких підключені ПК 1 і комутатор L3.

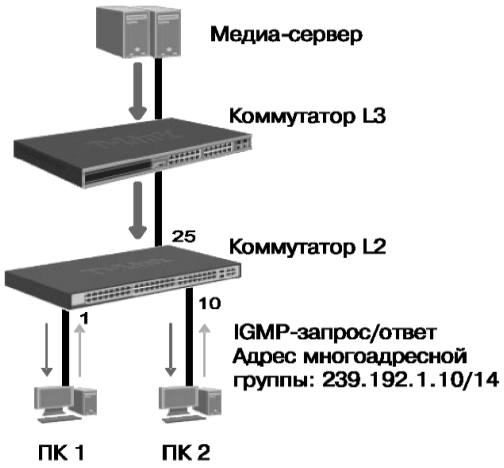


Рис. 4.5. Процес створення таблиці комутації IGMP Snooping

ПК 2 хоче вступати до багатоадресної групи 239.192.1.10 і відправляє IGMP-відповідь на адресу групи, не чекаючи отримання чергового IGMP-запита. Комутатор L2 аналізує IGMP-відповідь і додає порт 10, до якого підключений ПК 2, у вже існуючий запис для MAC-адреси 0x01-00-5E-40-01-0A. В результаті порти 1, 10 і 25 асоційовані з багатоадресною MAC-адресою 0x01-00-5E-40-01-0A.

Коли комутатор отримує IGMP-повідомлення про вихід вузла з групи, він видаляє номер порту, до якого підключений цей вузол, з відповідного запису таблиці комутації IGMP Snooping.

Таблиця 4.1

Таблиця комутації IGMP Snooping

Номер порту	Багатоадресна група	MAC-адреса багатоадресної групи
1,10,25	**238.192.1.10**	**01-00-5E-40-01-0A**

Функція IGMP Snooping сильно завантажує центральний процесор і може понизити продуктивність комутатора. Тому в комутаторах зазвичай використовуються спеціалізовані мікросхеми ASIC, які перевіряють IGMP-повідомлення на апаратному рівні.

Налаштування багатоадресної розсилки IGMP Snooping

Розглянемо приклад налаштування функції IGMP Snooping на комутаторах

D-Link. На рис. 4.6 показана схема мережі, в якій реалізований сервіс багатоадресної розсилки. Клієнти, серед яких є передплатники багатоадресної розсилки, підключені до комутаторів другого рівня.

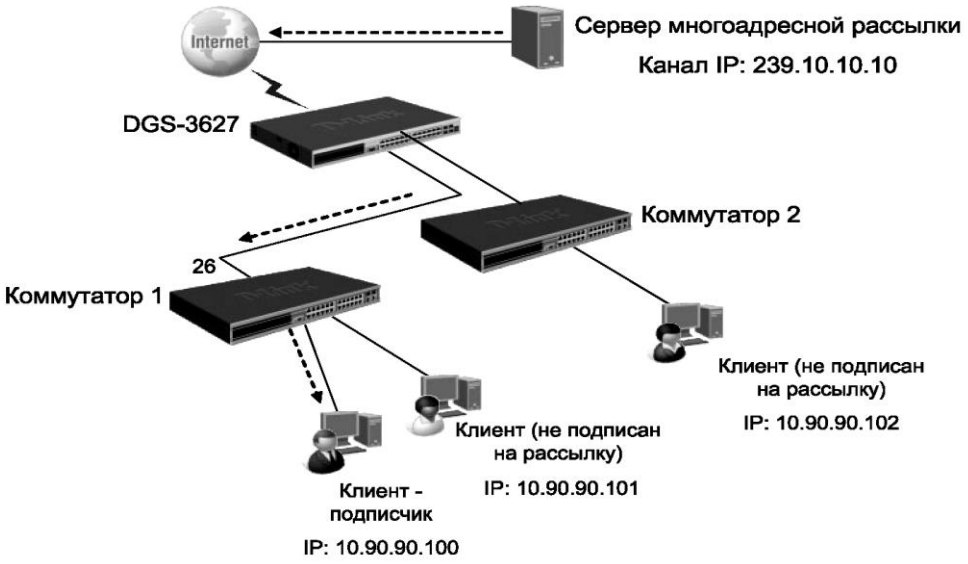


Рис. 4.6. Схема мережі з багатоадресною розсилкою

Налаштування комутатора 1

– активізувати функцію IGMP Snooping глобально на комутаторі:

enable igmp_snooping

– активізувати функцію IGMP Snooping у вказаній VLAN (у цьому прикладі VLAN за умовчанням):

config igmp_snooping vlan default state enable

– включити фільтрацію багатоадресного трафіку, щоб уникнути його передачі вузлам, що не є передплатниками багатоадресної розсилки:

config multicast vlan_filtering_mode vlan default filter_unregitered_groups

Функція IGMP Snooping Fast Leave, активізована на комутаторі, дозволяє миттєво виключити порт з таблиці комутації IGMP Snooping при отриманні ним повідомлення про вихід з групи. Це дозволяє припинити передачу по мережі непотрібних потоків даних і ефективніше використати смугу пропускання.

На рис. 4.7 приведена схема мережі, в якій на комутаторі 2 активізована функція IGMP Snooping Fast Leave. Усі порти комутатора 2 знаходяться в VLAN за замовчуванням (Default VLAN). До одного з портів комутатора підключений вузол-передплатник багатоадресної розсилки. Функція IGMP Snooping Fast Leave корисна в додатках IPTV, оскільки завдяки ній можна зменшити час відгуку, коли користувачі перемикаються між телевізійними каналами. Слід зазначити, що порт буде видалений з таблиці комутації IGMP Snooping тільки у тому випадку, якщо до нього більше не підключено жодного вузла-передплатника.

Рис. 4.7. Приведена схема мережі з функцією IGMP Snooping Fast Leave

Налаштування комутатора 2:

– активізувати функцію IGMP Snooping глобально на комутаторі і у вказаній VLAN (у цьому прикладі VLAN за замовчуванням). Включити фільтрацію багатоадресного трафіку:

enable igmp_snooping

config igmp_snooping vlan default state enable

config multicast vlan_filtering_mode vlan default filter_unregistered_groups

– активізувати функцію IGMP Snooping Fast Leave у вказаній VLAN:

config igmp_snooping vlan default fast_leave enable

4.2. Технології побудови віртуальних локальних мереж (VLAN)

Оскільки комутатор Ethernet є облаштуванням канального рівня, то відповідно до логіки роботи він розсилатиме широкомовні кадри через усі порти. Хоча трафік з конкретними адресами (з'єднання «точка-точка») ізольований парою портів, широкомовні кадри передаються в усю мережу (на кожен порт). Широкомовні кадри – це кадри, що передаються на усі вузли мережі. Вони потрібні для роботи багатьох мережевих протоколів, таких як ARP, BOOTP або DHCP. З їх допомогою робоча станція сповіщує інші комп'ютери про свою появу в мережі. Так само розсилка широкомовних кадрів може виникати через некоректно працюючого мережевого адаптера. Широкомовні кадри можуть привести до нераціонального використання смуги пропускання, особливо у великих мережах. Для того, щоб цього не відбувалося, важливо обмежити область поширення широкомовного трафіку (ця область називається широкомовним доменом) – організувати не-великі широкомовні домени, або віртуальні локальні мережі (Virtual LAN, VLAN).

Логічна сегментація мереж за допомогою технології VLAN

Віртуальною локальною мережею називається логічна група вузлів мережі, трафік якої, у тому числі і широкомовний, на канальному рівні повністю ізольований від інших вузлів мережі. Це означає, що передача кадрів між різними віртуальними мережами на підставі MAC-адреси неможлива незалежно від типу адреси – унікальної, групової або широкомовної. В той же час усередині віртуальної мережі кадри передаються за технологією комутації, тобто тільки на той порт, який пов'язаний з адресою призначення кадру. Таким чином за допомогою віртуальних мереж вирішується проблема поширення широкомовних кадрів і наслідків, що викликаються ними, які можуть розвинутися в широкомовні шторми і істотно понизити продуктивність мережі.

VLAN мають наступні переваги:

– гнучкість впровадження. VLAN є ефективним способом угрупування мережевих користувачів у віртуальні робочі групи, незважаючи на їх фізичне розміщення в мережі;

– забезпечують можливість контролю широкомовних повідомлень, що збільшує смугу пропускання, доступну для користувача;

– дозволяють підвищити безпеку мережі, визначивши за допомогою фільтрів, налагоджених на комутаторі або маршрутизаторі, політику взаємодії користувачів з різних віртуальних мереж.

Розглянемо приклад, що показує ефективність використання логічної сегментації мереж за допомогою технології VLAN при рішенні типової задачі організації доступу в інтернет співробітникам офісу. При цьому трафік кожного відділу має бути ізольований.

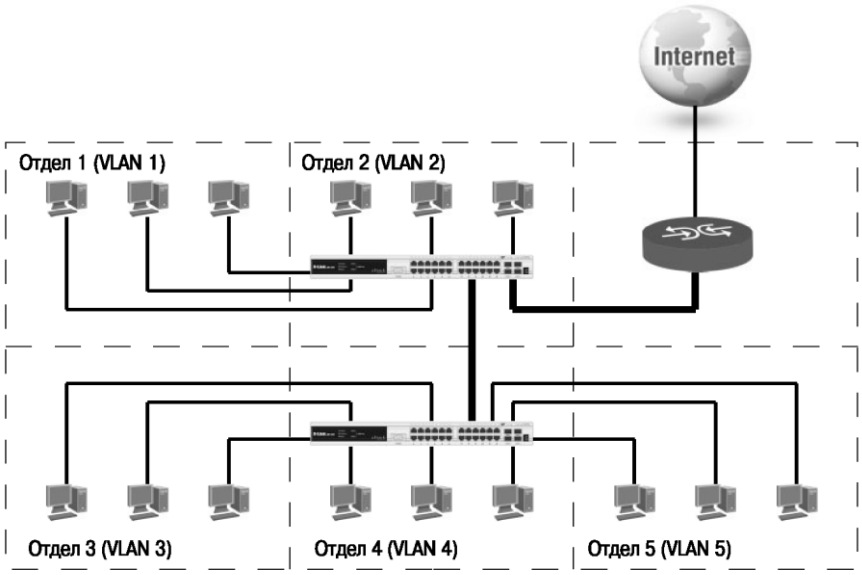


Рис. 4.8. Логічне угрупування мережевих користувачів в VLAN

Припустимо, що в офісі є декілька кімнат, в кожній з яких розташовується невелика кількість співробітників. Кожна кімната є окремою робочою групою.

При стандартному підході до рішення задачі за допомогою фізичної сегментації трафіку кожного відділу потрібно було б у кожну кімнату встановлювати окремий комутатор, який би підключався до маршрутизатора, що надає доступ в інтернет. При цьому маршрутизатор повинен мати достатню кількість портів, що забезпечує можливість підключення усіх фізичних сегментів (кімнат) мережі. Це рішення погано масштабоване і є дорогим, оскільки при збільшенні кількості відділів збільшується кількість необхідних комутаторів, інтерфейсів маршрутизатора і магістральних кабелів.

При використанні віртуальних локальних мереж вже не вимагається підключати користувачів одного відділу до окремого комутатора, що дозволяє скоротити кількість використовуваних пристроїв і магістральних кабелів. Комутатор, програмне забезпечення якого підтримує функцію віртуальних локальних мереж, дозволяє виконувати логічну сегментацію мережі шляхом відповідного програмного налаштування. Це дає можливість підключати користувачів, що знаходяться в різних сегментах, до одного комутатора, а також скорочує кількість необхідних фізичних інтерфейсів на маршрутизаторі.

Типи побудови віртуальних локальних мереж (VLAN)

У комутаторах можуть бути реалізовані наступні типи VLAN:

– на основі портів;
– на основі стандарту IEEE 802.1Q;
– на основі стандарту IEEE 802.1ad (Q-in-Q VLAN);
– на основі портів і протоколів IEEE 802.1v;
– на основі MAC-адрес;
– асиметричні.

Також для сегментації мережі на канальному рівні моделі OSI в комутаторах можуть використовуватися інші функції, наприклад функція Traffic Segmentation.

При використанні VLAN на основі портів (port-based VLAN) кожен порт призначається в певну VLAN, незалежно від того, який користувач або комп’ютер підключений до цього порту (рис. 4.9 і 4.10). Це означає, що усі користувачі, підключені до цього порту, будуть членами однієї VLAN. Конфігурація портів статична і може бути змінена тільки вручну.

Основні характеристики VLAN на основі портів:

– застосовуються в межах одного комутатора. Якщо необхідно організувати декілька робочих груп в межах невеликої мережі на основі одного комутатора, наприклад, необхідно рознести технічний відділ і відділ продажів, то рішення VLAN на базі портів оптимально підходить для цього завдання;

– простота налаштування. Створення віртуальних мереж на основі групування портів не вимагає від адміністратора великого об'єму ручної роботи – досить усім портам, що поміщаються в одну VLAN, присвоїти однаковий ідентифікатор VLAN (VLAN ID);

– можливість зміни логічної топології мережі без фізичного переміщення станцій. Досить усього лише змінити налаштування порту з однією VLAN (наприклад, VLAN технічного відділу) на іншу (VLAN відділу продажів), і робоча станція відразу ж дістає можливість спільно використати ресурси з членами нової VLAN Таким чином, VLAN забезпечують гнучкість при переміщеннях, змінах і нарощуванні мережі;

– кожен порт може входити тільки в одну VLAN. Для об'єднання віртуальних підмереж як усередині одного комутатора, так і між двома комутаторами, треба використати мережевий рівень OSI-моделі. Один з портів кожної VLAN підключається до інтерфейсу маршрутизатора, який створює таблицю маршрутизації для пересилки кадрів з однієї підмережі (VLAN) в іншу (IP-адреса підмереж мають бути різними).

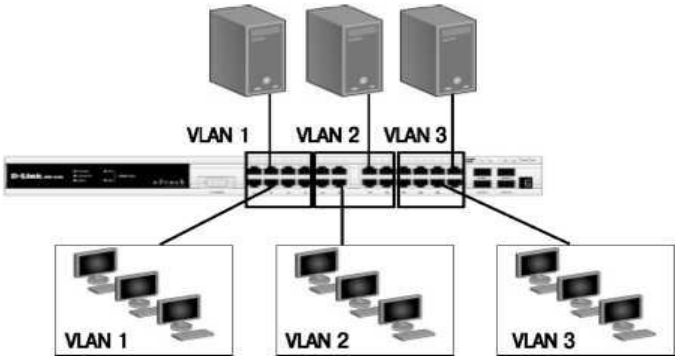


Рис. 4.9. VLAN на основі портів

Недоліком такого рішення є те, що один порт кожної VLAN необхідно підключати до маршрутизатора. Це призводить до додаткових витрат на купівлю кабелів і маршрутизаторів, а також порти комутатора використовуються дуже марнотратно. Розв'язати цю проблему можна двома способами: використати комутатори, які на основі фірмового рішення дозволяють включати порт декілька VLAN, або використати комутатори рівня 3 (рис. 4.11).

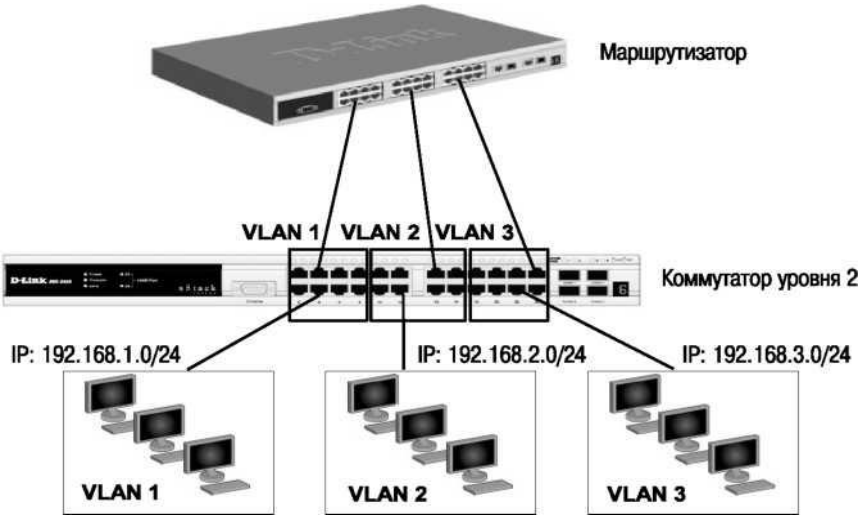


Рис. 4.10. Об’єднання VLAN за допомогою маршрутизуючого пристрою

З точки зору зручності і гнучкості налаштувань, VLAN стандарту IEEE 802.1Q є кращим рішенням в порівнянні з VLAN на основі портів.

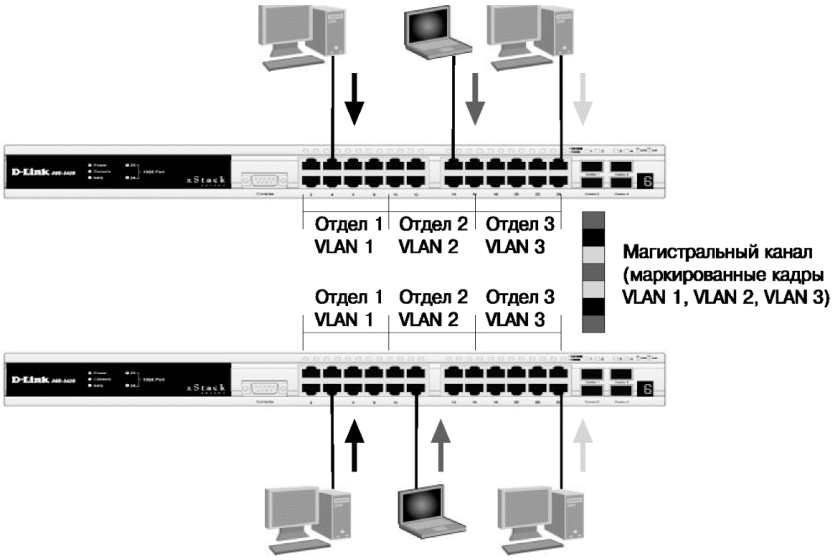


Рис. 4.11. Передача кадрів різних VLAN по магістральному каналу зв’язку

Переваги VLAN стандарту IEEE 802.1Q:

– гнучкість і зручність в налаштуванні і зміні – можна створювати необхідні комбінації VLAN як в межах одного комутатора, так і в усій мережі, побудованій на комутаторах з підтримкою стандарту IEEE 802.1Q. Здатність додавання тегів дозволяє інформації про VLAN поширюватися через безліч 802.1Q-сумісних комутаторів по одному фізичному з’єднанню (магістральному каналу, Trunk Link);

– дозволяє активізувати алгоритм єднального дерева (Spanning Tree) на усіх портах і працювати в звичайному режимі. Протокол Spanning Tree виявля-

ється дуже корисним для застосування у великих мережах, побудованих на декількох комутаторах, і дозволяє комутаторам автоматично визначати деревовидну конфігурацію зв'язків в мережі при довільному з'єднанні портів між собою. Для нормальної роботи комутатора потрібна відсутність замкнутих маршрутів у мережі. Ці маршрути можуть створюватися адміністратором спеціально для утворення резервних зв'язків або ж виникати випадковим чином, що цілком можливо, якщо мережа має численні зв'язки, а кабельна система погано структурована або документована. За допомогою протоколу Spanning Tree комутатори після побудови схеми мережі блокують надмірні маршрути. Таким чином, автоматично запобігає виникнення петель в мережі;

– здатність VLAN IEEE 802.1Q додавати і витягати теги із заголовків кадрів дозволяє використати в мережі комутатори і мережеві пристрої, які не підтримують стандарт IEEE 802.1Q;

– облаштування різних виробників, що підтримують стандарт, можуть працювати разом, незалежно від якого-небудь фірмового рішення;

– зв'язати підмережі на мережевому рівні, потрібний маршрутизатор або комутатор L3. Проте для простіших випадків, наприклад, для організації доступу до сервера з різних VLAN, маршрутизатор не знадобиться. Треба включити порт комутатора, до якого підключений сервер, в усі підмережі, а мережевий адаптер сервера повинен підтримувати стандарт IEEE 802.1Q.

Функція Q-in-Q, також відома як Double VLAN, відповідає стандарту IEEE 802.1ad, який є розширенням стандарту IEEE 802.1Q. Вона дозволяє додавати в маркіровані кадри Ethernet другий тег IEEE 802.1Q.

Завдяки функції Q-in-Q провайдери можуть використати їх власні унікальні ідентифікатори VLAN (звані Service Provider VLAN ID або SP-VLAN ID) при наданні послуг користувачам, в мережах яких налагоджено декілька VLAN. Це дозволяє зберегти використовувані користувачами ідентифікатори VLAN (Customer VLAN ID або CVLAN ID), уникнути їх збігу і ізолювати трафік різних клієнтів у внутрішній мережі провайдера.

Стандарт IEEE 802.1v є розширенням стандарту IEEE 802.1Q. Він дозволяє об'єднувати вузли мережі у віртуальні локальні мережі на основі підтримуваних ними протоколів. При визначенні членства в VLAN стандарт класифікує немарковані кадри за типом протоколу і портом. Формат тегу 802.1v аналогічний формату тегу 802.1Q.

Для забезпечення можливості використання ресурсів (серверів, інтернет-шлюзів і так далі), що розділяються, користувачами з різних мереж VLAN в про-

грамному забезпеченні комутаторів 2-го рівня D-Link реалізована підтримка функції Asymmetric VLAN(асиметричні VLAN). Ця функція дозволяє клієнтам з різних VLAN взаємодіяти з пристроями (наприклад, серверами), що розділяються, не підтримувальним ітерування 802.1Q, через один фізичний канал зв'язку з комутатором, не вимагаючи використання зовнішнього маршрутизатора. Активація функції Asymmetric VLAN на комутаторі 2-го рівня дозволяє зробити його немарковані порти членами декількох віртуальних локальних мереж. При цьому робочі станції залишаються повністю ізольованими один від одного. Наприклад, асиметричні VLAN можуть бути налагоджені так, щоб забезпечити доступ до поштового сервера усім поштовим клієнтам. Клієнти зможуть відправляти і отримувати дані через порт комутатора, підключеного до поштового серверу, але прийом і передача даних через інші порти буде для них заборонений.

4.3. Особливості реалізації VLAN стандарту 802.1Q

Визначення IEEE 802.1Q

Tagging («маркування кадру») – процес додавання інформації про приналежність до 802.1Q VLAN в заголовок кадру.

Untagging («витягання тегу з кадру») – процес витягання інформації про приналежність до 802.1Q VLAN із заголовка кадру.

VLAN ID (VID) – ідентифікатор VLAN.

Port VLAN ID (PVID) – ідентифікатор порту VLAN.

Ingress port («вхідний порт») – порт комутатора, на якого поступають кадри, і при цьому приймається рішення про приналежність до VLAN.

Egress port («вихідний порт») – порт комутатора, з якого кадри передаються на інші мережеві пристрої, комутатори або робочі станції, і, відповідно, на нім повинне прийматися рішення про маркування.

Правила функціонування віртуальних локальних мереж стандарту 802.1Q

Будь-який порт комутатора може бути налагоджений як tagged (маркований) або як untagged (немаркований). Функція untagging дозволяє працювати з тими мережевими облаштуваннями віртуальної мережі, які не розуміють тегів в заголовку кадру Ethernet. Функція tagging дозволяє настроювати VLAN між декількома комутаторами, що підтримують стандарт IEEE 802.1Q.

Стандарт IEEE 802.1Q визначає зміни в структурі кадру Ethernet, що дозволяють передавати інформацію про VLAN по мережі. На рис. 4.12 зображені маркіровані і немаркіровані порти VLAN і формат тегу 802.1Q VLAN.

До кадру Ethernet додані 32 біта (4 байти), які збільшують його розмір до 1522 байт. Перші 2 байти (поле Tag Protocol Identifier, TPID) з фіксованим значенням 0x8100 визначають, що кадр містить тег протоколу 802.1Q. Інші 2 байти містять наступну інформацію:

– Priority («пріоритет») – 3 біта поля пріоритету передачі кодують до восьми рівнів пріоритету (від 0 до 7, де 7 – найвищий пріоритет), які використовуються в стандарті 802.1p;

– Canonical Format Indicator (CFI) – 1 біт індикатора канонічного формату зарезервований для позначення кадрів мереж інших типів (Token Ring, FDDI), що передаються по магістралі Ethernet;

– VID (VLAN ID) – 12-бітовий ідентифікатор VLAN визначає, який VLAN належить трафік. Оскільки під поле VID відведене 12 біт, то можна задати 4094 унікальних VLAN (VID 0 і VID 4095 зарезервовані).

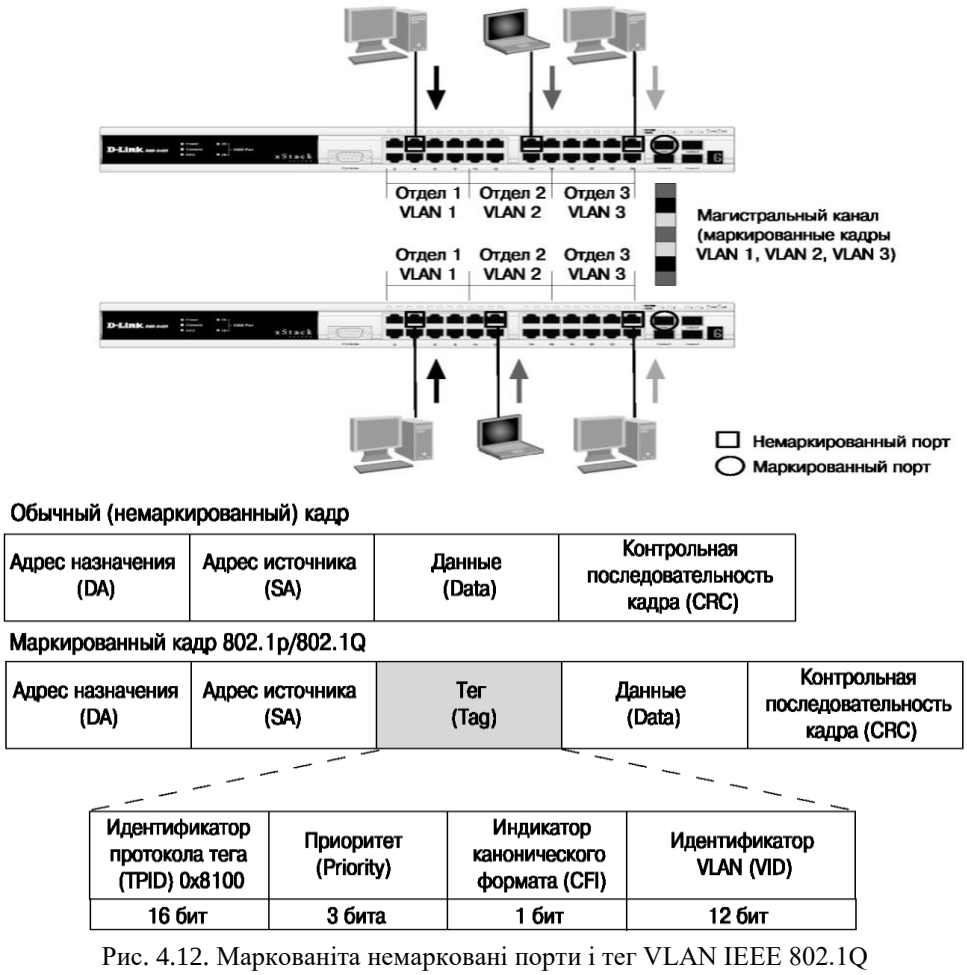


Рис. 4.12. Маркованіта немарковані порти і тег VLAN IEEE 802.1Q

Кожен фізичний порт комутатора має параметр, що називається ідентифікатор порту VLAN (PVID). Цей параметр використовується для того, щоб визна-

чити, в яку VLAN комутатор направить немаркований кадр, що входить, з підключеного до порту сегменту, коли кадр треба передати на інший порт (усередині комутатора в заголовки усіх немаркованих кадрів додається ідентифікатор VID, рівний PVID порту, на який вони були прийняті). Цей механізм дозволяє одночасно існувати в одній мережі пристроям з підтримкою і без підтримки стандарту IEEE 802.1Q.

Комутатори, що підтримують протокол IEEE 802.1Q, повинні зберігати таблицю, що зв'язує ідентифікатори портів PVID з ідентифікаторами VID мережі. При цьому кожен порт такого комутатора може мати тільки один PVID і стільки ідентифікаторів VID, скільки підтримує ця модель комутатора. Якщо на комутаторі не налагоджені VLAN, то усі порти за умовчанням входять в одну VLAN з PVID = 1.

Рішення про просування кадру усередині віртуальної локальної мережі приймається на основі трьох наступних видів правил.

– правила вхідного трафіку (ingress rules) – класифікація отримуваних кадрів відносно приналежності до VLAN;

– правила просування між портами (forwarding rules) – ухвалення рішення про просування або відкидання кадру;

– правила вихідного трафіку (egress rules) – ухвалення рішення про збереження або видалення в заголовку кадру тега 802.1Q перед його передачею.

Правила вхідного трафіку (рис. 4.13) виконують класифікацію кожного отримуваного кадру відносно приналежності до певній VLAN, а також можуть служити для ухвалення рішення про прийом кадру для подальшої обробки або його відкидання на основі формату прийнятого кадру.

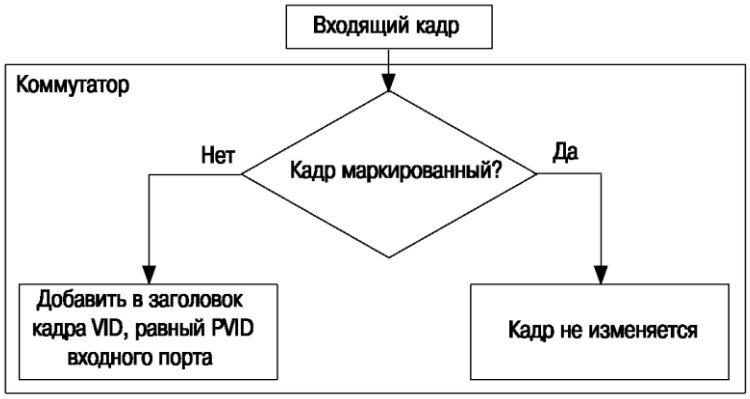


Рис.4.13. Правила вхідного трафіку

Класифікація кадру за приналежністю VLAN здійснюється таким чином:

– якщо кадр не містить інформацію про VLAN (немаркірований кадр), то в його заголовок комутатор додає тег з ідентифікатором VID, рівним ідентифікатору PVID порту, через який цей кадр був прийнятий;

– якщо кадр містить інформацію про VLAN (маркірований кадр), то його приналежність до конкретній VLAN визначається по ідентифікатору VID в заголовку кадру. Значення тегу в нім не змінюється.

Активізувавши функцію перевірки формату кадру на вході, адміністратор мережі може вказати, кадри яких форматів прийматимуться комутатором для подальшої обробки. Керовані комутатори D-Link дозволяють настроювати прийом портами або тільки маркованих кадрів (taggedonly), або обох типів кадрів – маркованих і немаркованих (admit_all).

Правила просування між портами здійснюють ухвалення рішення про відкидання або передачу кадру на порт призначення на основі його інформації про приналежність конкретної VLAN і MAC-адреси вузла-приймача.

Якщо вхідний кадр маркований, то комутатор визначає, чи є вхідний порт членом тій же VLAN, шляхом порівняння ідентифікатора VID в заголовку кадру і набору ідентифікаторів VID, що асоціюються з портом, включаючи його PVID. Якщо ні, то кадр відкидається. Цей процес називається ingress filtering (вхідною фільтрацією) і використовується для збереження пропускної спроможності усередині комутатора шляхом відкидання кадрів, що не належать тій же VLAN, що і вхідний порт, на стадії їх прийому. Якщо кадр немаркірований, вхідна фільтрація не виконується.

Далі визначається, чи являється порт призначення членом тій же VLAN. Якщо ні, то кадр відкидається. Якщо ж вихідний порт входить в цю VLAN, то комутатор передає кадр в підключений до нього сегмент мережі.

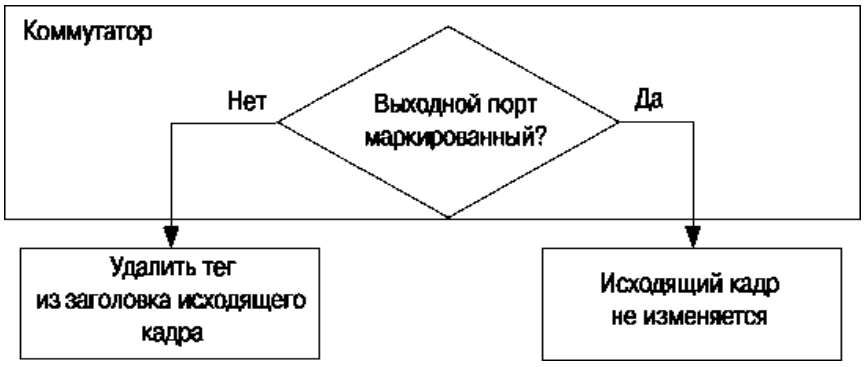


Рис. 4.14. Правила вихідного трафіку

Правила вихідного трафіку (рис. 4.14) визначають формат витікаючого кадру – маркований або немаркований. Якщо вихідний порт є немаркованим

(untagged), то він витягатиме тег 802.1Q із заголовків усіх маркірованих кадрів, що виходять через нього. Якщо вихідний порт налагоджений як маркований (tagged), то він зберігатиме тег 802.1Q в заголовках усіх маркірованих кадрів, що виходять через нього.

На рис. 4.15–4.18 наведений приклад передачі немаркованого і маркованого кадру через маркований і немаркований порти комутатора.

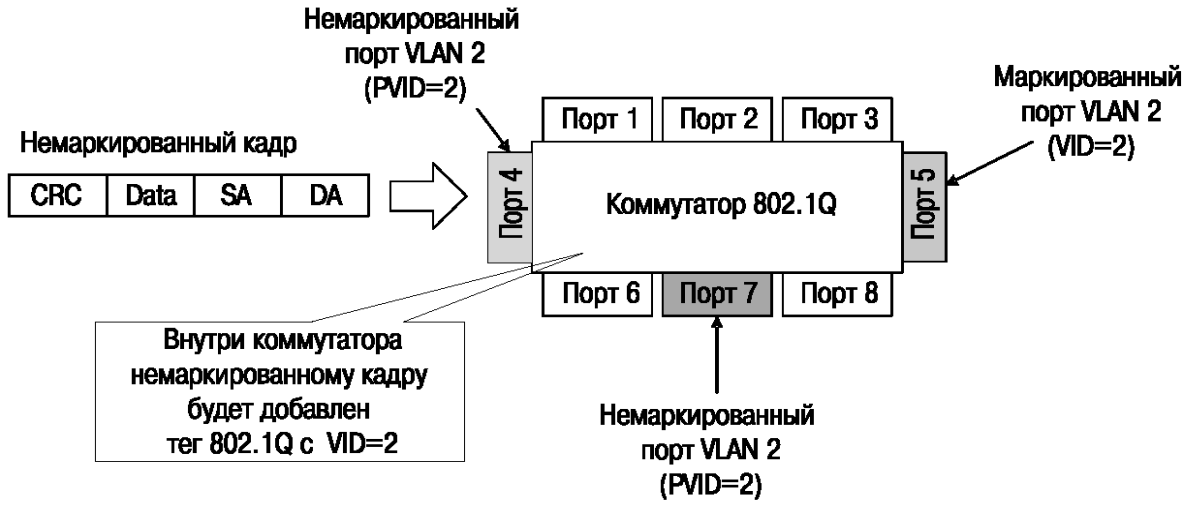


Рис. 4.15. Немаркований вхідний кадр

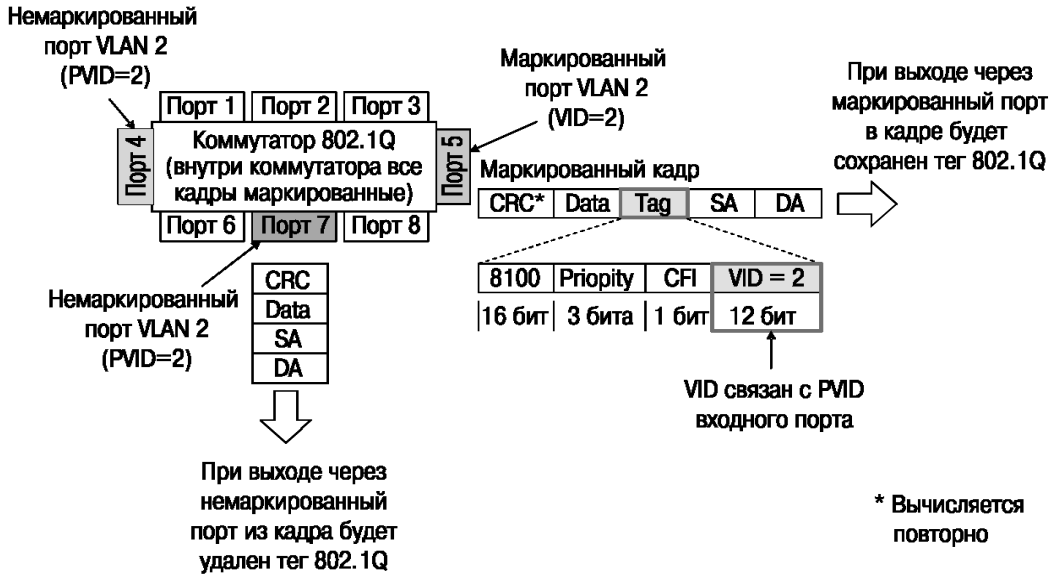


Рис. 4.16. Немаркований кадр, що передається через маркований і немаркований порти

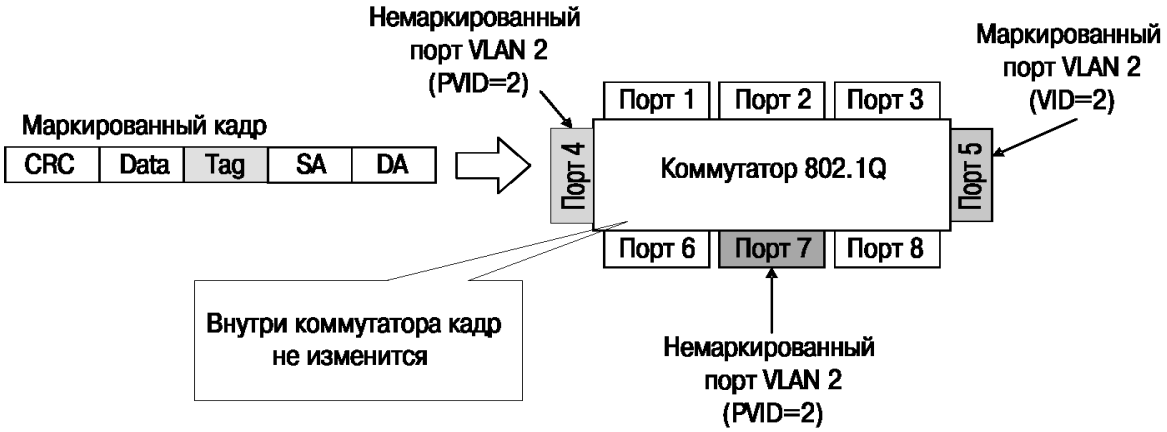


Рис. 4.17.Маркований вхідний кадр

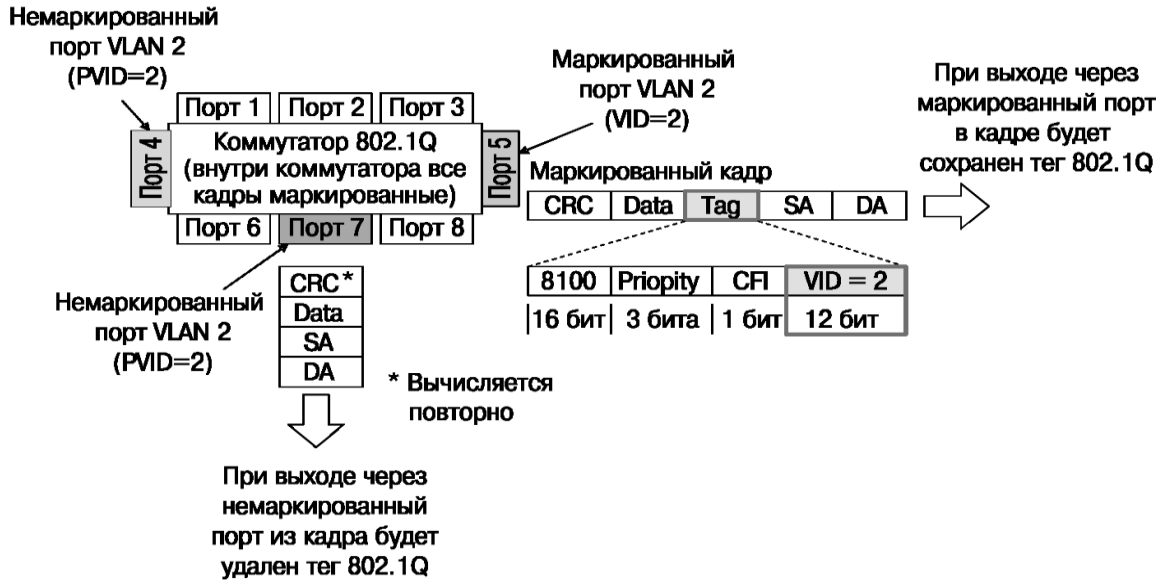


Рис. 4.18.Маркований кадр, що передається через Маркований і немаркований порти

Налаштування віртуальних локальних мереж стандарту 802.1Q

На рис. 4.19 показано схему мережі, VLAN, що складається з двох груп. Як приклад передачі даних між облаштуваннями однієї VLAN, побудованої на декількох комутаторах, розглянемо пересилку кадру з порту 5 комутатора 1 на порт 6 комутатора 3.

Порт 5 комутатора 1 є немаркірованим портом VLAN v2 (PVID=2). Тому, коли будь-який немаркірований кадр поступає на порт 5, комутатор забезпечує його тегом 802.1Q зі значенням VID, рівним 2.

Далі комутатор 1 перевіряє у своїй таблиці комутації, через який порт необхідно передати кадр і чи належить цей порт VLAN v2. Кадр може бути переданий через порт 1, оскільки він є маркірованим членом VLAN v2. Після передачі кадру через порт 1 тег 802.1Q в нім буде збережений.

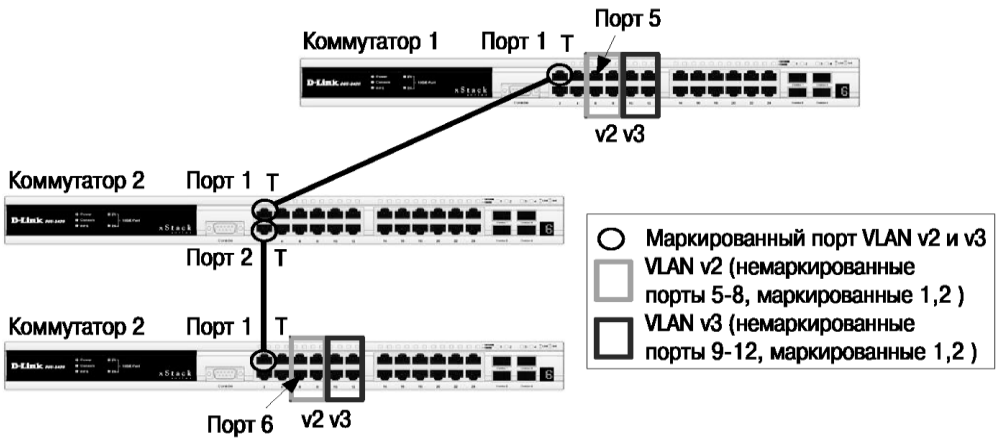


Рис. 4.19. Схема мережі VLAN

Після цього маркірований кадр поступить на порт 1 комутатора 2. Перш ніж передати кадр далі, порт 1 перевірить, чи є він сам членом VLAN v2. Оскільки порт 1 комутатора 2 є маркірованим членом VLAN v2, він прийме кадр і передасть його на порт 2, згідно з таблицею комутації. Після передачі кадру через порт 2 комутатори 2 тег 802.1Q в нім буде збережений, оскільки порт 2 є маркірованим портом VLAN v2.

Порт 1 комутатора 3 прийме кадр, що поступив. Після перевірки на приналежність до VLAN порт 1 передасть кадр на порт 6, знайдений звичайним способом в таблиці комутації комутатора 3. Порт 6 є немаркованим портом VLAN y2, тому при виході кадру через цей порт тег 802.1P з нього буде видалений.

Нижче наведений приклад налаштування комутаторів, що дозволяє реалізувати задану схему мережі VLAN.

Налаштування комутатора 1:

– видалити відповідні порти з VLAN за замовчуванням (default VLAN) і створити нові VLAN:

config vlan default delete 1-12 create vlan v2 tag 2 create vlan vS tag S

– у створені VLAN додати порти, для яких необхідно вказати, які з них є маркованими і немаркованими:

config vlan v2 add untagged 5-8 config vlan v2 add tagged 1-2 config vlan vS add untagged 9-12 config vlan vS add tagged 1-2

– налаштування комутатора 2:

config vlan default delete 1-2 create vlan v2 tag 2 create vlan vS tag S config vlan v2 add tagged 1-2 config vlan vS add tagged 1-2

– налаштування комутаторів 3:

config vlan default delete 1-12 create vlan v2 tag 2 create vlan vS tag S config vlan v2 add untagged 5-8 config vlan v2 add tagged 1 config vlan vS add untagged 9-12 config vlan vS add tagged 1

Заводські установки за замовчуванням призначають усі порти комутатора в default VLAN з VID = 1. Перед створенням нової VLAN необхідно видалити з default VLAN усі порти, які вимагається зробити немаркованими членами нової VLAN.

4.4. Реалізації VLAN з розширеннями стандарту IEEE 802.1Q

Функція Q-in-Q, також відома як DoubleVLAN, відповідає стандарту IEEE 802.1ad, який є розширенням стандарту IEEE 802.1Q. Вона дозволяє додавати в маркіровані кадри Ethernet другий тег IEEE 802.1Q.

Завдяки функції Q-in-Q провайдери можуть використати їх власні унікальні ідентифікатори VLAN (звані Service Provider VLANID або SP-VLANID) при наданні послуг користувачам, в мережах яких налагоджено декілька VLAN. Це дозволяє зберегти використовувані користувачами ідентифікатори VLAN (Customer VLANID або CVLANID), уникнути їх збігу і ізолювати трафік різних клієнтів у внутрішній мережі провайдера.

Особливості реалізації VLAN з розширенням Q-in-Q

На рис. 4.20 зображені формати звичайного кадру Ethernet, кадру Ethernet з тегом 802.1Q, кадру Ethernet з двома тегами 802.1Q.

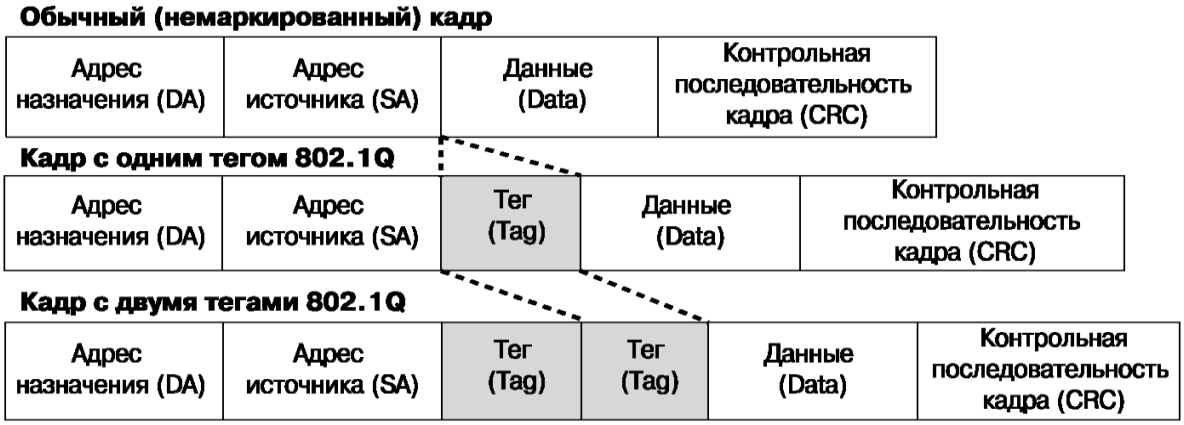


Рис. 4.20. Формату кадру Ethernet з двома тегами 802.1Q

Інкапсуляція кадру Ethernet другим тегом відбувається таким чином: тег, що містить ідентифікатор VLAN мережі провайдера (зовнішній тег), вставляється перед внутрішнім тегом, що містить клієнтський ідентифікатор VLAN. Передача кадрів в мережі провайдера здійснюється тільки на основі зовнішнього тега SP-

VLAN ID, внутрішній тег користувацької мережі CVLAN ID при цьому прихований.

Функція Q-in-Q дозволяє розширити доступний простір ідентифікаторів і використати до 4094 x 4094 = 16 760 836 унікальних віртуальних локальних мереж.

Існує дві реалізації функції Q-in-Q: port-based Q-in-Q і selective Q-in-Q. Функція port-based Q-in-Q за замовчуванням привласнює будь-якому кадру, що поступив на порт доступу граничного комутатора провайдера, ідентифікатор SP-VLAN, рівний ідентифікатору PVID порту. Порт маркірує кадр незалежно від того, є він маркірованим або немаркірованим. При вступі маркірованого кадру в нього додається другий тег з ідентифікатором, рівним SP-VLAN. Якщо на порт прийшов немаркірований кадр, в нього добавляється тільки тег з SP-VLAN порту.

Функція selective Q-in-Q є гнучкішою в порівнянні з port-based Q-in-Q. Вона дозволяє:

– маркірувати кадри зовнішніми тегами з різними ідентифікаторами SP-VLAN залежно від значень внутрішніх ідентифікаторів CVLAN;

– задавати пріоритети обробки кадрів зовнішніх SP-VLAN на основі значень пріоритетів внутрішніх призначених для користувача CVLAN;

– додавати до немаркірованих призначених для користувача кадрів окрім зовнішнього тега SP-VLAN внутрішній тег CVLAN.

У тегу VLAN є поле ідентифікатора протоколу тегу (TPID, Tag Protocol IDentifier), який визначає тип протоколу тегу. За умовчанням значення цього поля для стандарту IEEE 802.1Q дорівнює 0x8100.

На облаштуваннях різних виробників TPID зовнішнього тегу VLAN кадрів Q-in-Q може мати різні значення за умовчанням. Для того, щоб кадри Q-in-Q могли передаватися по загальнодоступних мережах через облаштування різних виробників, рекомендується використати значення TPID зовнішнього тегу рівне 0x8 8A8, згідно із стандартом IEEE 802.1ad.

Усі порти граничного комутатора, на якому використовуються функції port-based Q-in-Q або selective Q-in-Q, мають бути налагоджені як порти доступу (UNI) або Uplink-порти (NNI); UNI (User-to-Network Interface) – ця роль призначається портам, через які здійснюватиметься взаємодія граничного комутатора провайдера з клієнтськими мережами; NNI (Network-to-Network Interface) – ця роль призначається портам, які підключаються до внутрішньої мережі провайдера або інших граничних комутаторів.

Функція selective Q-in-Q дозволяє додавати в кадри різні зовнішні теги

VLAN, ґрунтуючись на значеннях внутрішніх тегів. Для цього на портах UNI граничного комутатора необхідно задати правила відповідності ідентифікаторів CVLAN ідентифікаторам SP-VLAN (vlan translation).

Окрім цього, на комутаторах D-Link з підтримкою функції Q-in-Q, можна активізувати режим Missdrop. При налаштуванні selective Q-in-Q, включення цього режиму дозволить відкидати кадри, що не підходять ні під одне з правил відповідності ідентифікаторів. При налаштуванні port-based Q-in-Q, режим Missdrop потрібно відключати, щоб порт комутатора міг приймати кадри що не підходять ні під одне з правил vlan translation. Кадрам, що в цьому випадку входять, привласнюватиметься зовнішній тег рівний PVID відповідного порту UNI.

Значення пріоритету зовнішнього тегу за замовчуванням дорівнює значенню пріоритету внутрішнього тегу, якщо кадр є маркованим. Якщо пріоритет в отриманому кадрі відсутній, то як пріоритет зовнішнього тегу використовуватиметься пріоритет відповідного вхідного порту UNI.

Приклади налаштування функції протоколу Q-in-Q

На рис. 4.21 показана базова архітектура мережі провайдера послуг з функцією port-based Q-in-Q.

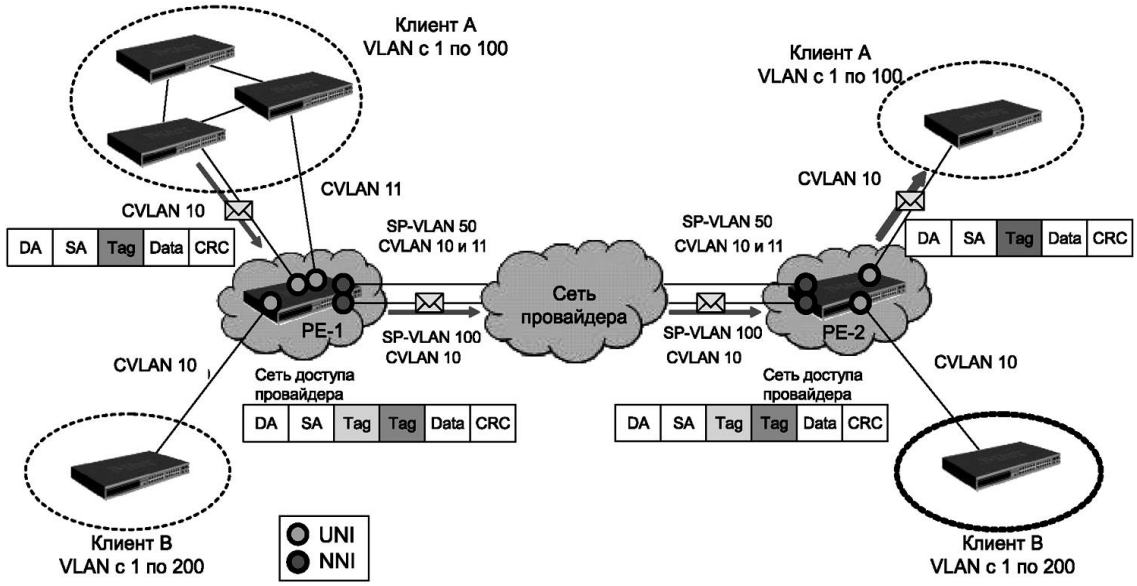


Рис. 4.21. Базова архітектура мережі провайдера із застосуванням функції port-based Q-in-Q

Граничні комутатори мережі провайдера послуг PE-1 і PE-2 дозволяють обробляти трафік віртуальних локальних мереж двох підключених до них клієнтських мереж. Кожному клієнтові провайдером присвоєний унікальний ідентифі-

катор VLAN: SP-VLAN 50 для клієнта A і SP-VLAN 100 для клієнта B. При передачі кадру з клієнтської мережі в мережу провайдера, в його заголовок додаватиметься другий тег 802.1Q: для мережі A-SP-VLAN 50, для мережі B-SP-VLAN 100. При передачі кадру з мережі провайдера в клієнтську мережу другий тег віддалятиметься граничним комутатором.

Розглянемо приклад налаштування функції port-based Q-in-Q на комутаторах D-Link. На рис. 4.22 приведена схема підключення двох клієнтських VLAN до мережі провайдера послуг. Граничними комутаторами є комутатори Gigabit Ethernet 3-го рівня. У мережі клієнта використовуються комутатори Fast Ethernet 2-го рівня.

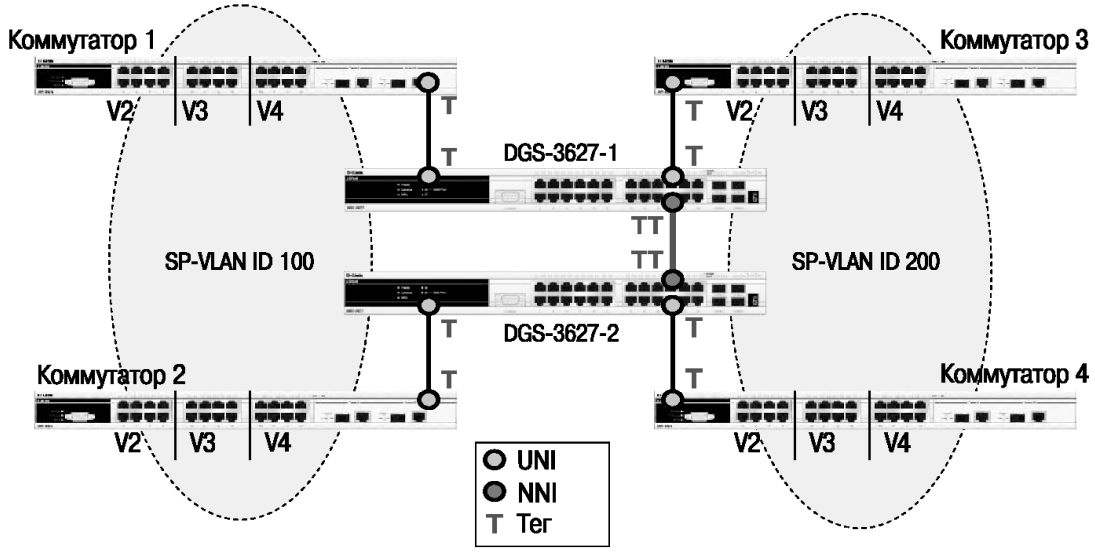


Рис. 4.22. Схема підключення клієнтських VLAN до мережі провайдера послуг

Налаштування комутатора DGS-3627 включає:

– активізувати функцію Q-in-Q VLAN на комутаторі:

enable qinq

– видалити відповідні порти з Q-in-Q VLAN за замовчуванням і створити нові VLAN:

config vlan default delete 1-24

create vlan d100 tag 100

create vlan d200 tag 200

– призначити порти доступу в створених Q-in-Q VLAN:

config vlan d100 add untagged 1-12

config vlan d200 add untagged 1S-24

– призначити Uplink-порти в створених Q-in-Q VLAN:

config vlan d100 add tagged 25-27

config vlan d200 add tagged 25-27

– налаштувати ролі портів доступу в Q-in-Q і відключити режим Missdrop на них:

config qinq ports 1-24 role uni missdrop disable

Налаштування комутаторів 1, 2, 3, 4:

– видалити відповідні порти з VLAN за умовчанням (defaultVLAN) і створити нові VLAN:

config vlan default delete 1-26
create vlan v2 tag 2
create vlan v3 tag 3
create vlan v4 tag 4

– у створені VLAN додати порти, для яких необхідно вказати, які з них є маркованими і немаркованими:

config vlan v2 add untagged 1-8
config vlan v2 add tagged 25-26
config vlan v3 add untagged 9-16
config vlan v3 add tagged 25-26
config vlan v4 add untagged 17-24
config vlan v4 add tagged 25-26

Приклад налаштування функції selective Q-in-Q

Кожному клієнтові провайдером призначений унікальний ідентифікатор: SP-VLAN 1000 для клієнта CVLAN 200 і SP-VLAN 1001 для клієнта CVLAN 300. Як граничні комутатори використовуються комутатори Fast Ethernet 2-го рівня. Порти 9 обох граничних комутаторів служать для підключення до користувацьких мереж (UNI-порти), передача даних в мережу провайдера здійснюється через порти 11 (NNI-порти). Для того, щоб граничні комутатори могли здійснювати передачу призначених для користувача кадрів з використанням функції selective Q-in-Q, на них необхідно виконати наступні налаштування.

Налаштування комутаторів 1, 2:

– створити необхідні VLAN і додати порти, для яких необхідно вказати, які з них є маркованими і немаркованими:

create vlan v1000 tag 1000
create vlan v1001 tag 1001

– комутаторам мережі провайдера послуг:

config vlan v1000 add tag 9,11 c
onfig vlan v1001 add tag 9,11

– активізувати функцію Q-in-Q VLAN, вказати значення TPID внутрішнього і зовнішнього тегу, ролі портів і задати правила відповідності ідентифікаторів CVLAN ідентифікаторам SP-VLAN:

enable qinq
config qinq ports all 0x8100
config qinq ports 9 role uni
create vlan_translation ports 9 cvid 200 add svid 1000
create vlan_translation ports 9 cvid 300 add svid 1001

Особливості реалізації VLAN на основі стандарту IEEE 802.1v

Стандарт IEEE 802.1v є розширенням стандарту IEEE 802.1Q. Він дозволяє об'єднувати вузли мережі у віртуальні локальні мережі на основі підтримуваних ними протоколів. При визначенні членства в VLAN стандарт класифікує немарковані кадри за типом протоколу і портом. Формат тегу 802.1v аналогічний формату тегу 802.1p. У стандарті IEEE 802.1v визначені наступні правила класифікації кадрів, що входять (рис. 4.23):

– при вступі на порт немаркірованого кадру, комутатором здійснюється перевірка заголовка канального рівня і типу протоколу вищерозміщеного рівня. Якщо тип протоколу відповідає типу VLAN 802.1v на цьому порту, то в заголовок кадру додається тег з ідентифікатором УТО, рівним ідентифікатору VLAN 802.1v. Якщо збіги не знайдені, то в заголовок кадру додається тег з ідентифікатором УТО, рівним ідентифікатору вхідного порту PVID;

– при вступі на порт маркованого кадру значення тегу VLAN в ньому не змінюється.

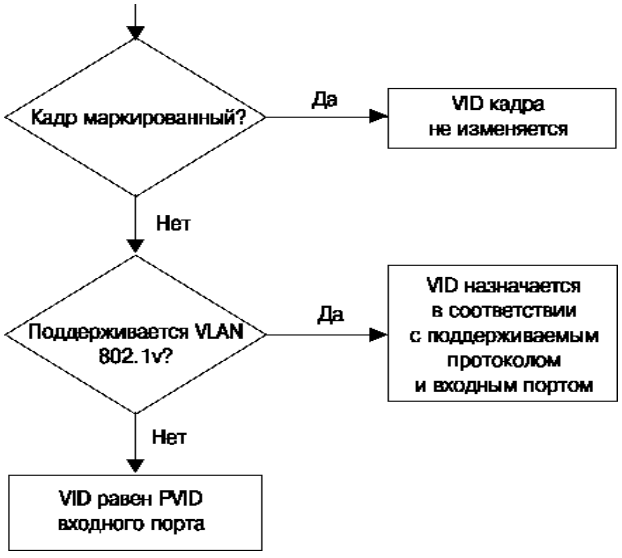


Рис. 4.23. Правила класифікації кадрів, що входять

Усередині комутатора усі кадри є маркованими. Передача кадрів здійснюється на основі таблиці VLAN шляхом порівняння значень ідентифікаторів VID. Якщо порт призначення є членом тій же VLAN, що і вхідний порт, то він передає кадр в підключений до нього сегмент мережі. Інакше кадр відкидається.

Для вихідних портів діють такі ж правила, як для стандарту IEEE 802.1Q.

На рис. 4.24 показано типове підключення клієнтів до мережі провайдера послуг. Користувачі локальної мережі знаходяться у виділеній VLAN (VLAN 20). Їх підключення в інтернет здійснюється через PPPoE- сервер (VLAN 10). Для того, щоб трафік локальної мережі був відокремлений від трафіку PPPoE, на комутаторі для протоколу PPPoE створена VLAN 802.1v з ідентифікатором VID=10.

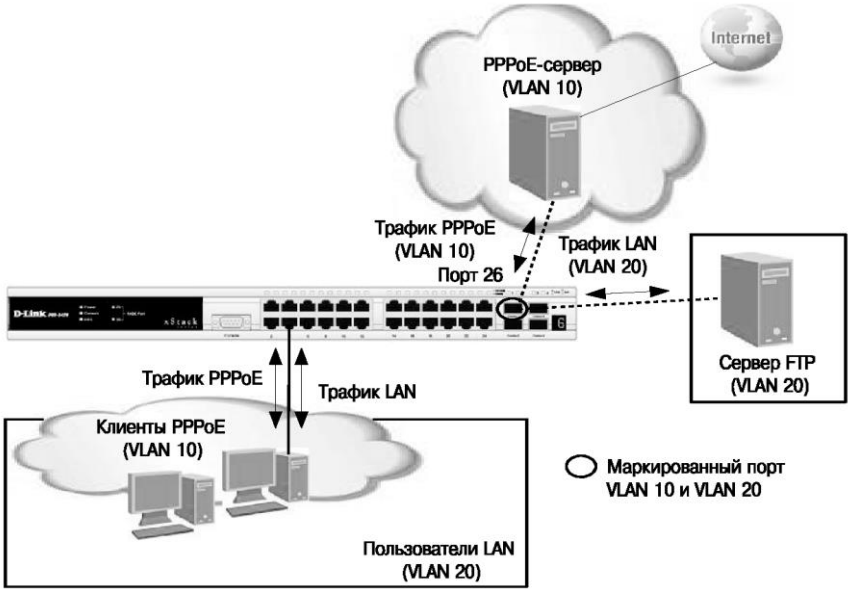


Рис. 4.24. Схема мережі VLAN

Налаштування комутатора:

– створення нових VLAN 802.1Q:

config vlan default delete 1-28

create vlan pppoe tag 10

config vlan pppoe add untagged 1-24

config vlan pppoe add tagged 26

create vlan base tag 20

config vlan base add tagged 26

config vlan base add untagged 1-24

– налаштування PVID портів, до яких підключені користувачі:

config port_vlan 1-24 pvid 20

– створення VLAN 802.1v для протоколу PPPoE (перша група протоколів налагоджена для кадрів PPPoE, що передаються на стадії дослідження, друга – для кадрів PPPoE встановленої сесії):

create dot1v_protocol_group group_id 1 group_name pppoe_disc
config dot1v_protocol_group group_id 1 add protocol ethernet_2 8863 c
reate dot1v_protocol_group group_id 2 group_name pppoe_session
config dot1v_protocol_group group_id 2 add protocol ethernet_2 8864
config port dot1v ports 1-24 add protocol_group group_id 1 vlan pppoe
config port dot1v ports 1-24 add protocol_group group_id 2 vlan pppoe

4.5. Особливості реалізації статичних і динамічних VLAN

Для коректної роботи віртуальної локальної мережі вимагається, щоб у базі даних фільтрації (FilteringDatabase) містилася інформація про членство в VLAN. Ця інформація потрібна для ухвалення правильного рішення (переслати або відкинути) при передачі кадрів між портами комутатора.

Існують два основні способи, що дозволяють встановлювати членство в VLAN: статичні VLAN і динамічні VLAN.

У статичних VLAN встановлення членства здійснюється вручну адміністратором мережі. При зміні топології мережі або переміщенні користувача на інше робоче місце адміністраторові вимагається вручну виконувати прив’язку VLAN-порт для кожного нового з’єднання.

Членство в динамічних VLAN може встановлюватися динамічно на магістральних інтерфейсах комутаторів на основі протоколу GVRP (GARP VLAN Registration Protocol). Протокол GARP (Generic Attribute Registration Protocol) використовується для реєстрації і відміни рєстрації атрибутів, таких як VID.

Використання протоколу GVRP в статичних і динамічних VLAN

Статичні записи про реєстрацію в VLAN (Static VLAN Registration Entries) використовуються для уявлення інформації про статичних VLAN у базі даних фільтрації. Ці записи дозволяють задавати точні налаштування для кожного порту VLAN: ідентифікатор VLAN, тип порту (маркований або немаркований), один з елементів протоколу GVRP, що управляють:

– fixed (порт завжди є членом цією VLAN);

– forbidden (порту заборонено реєструватися як членові цією VLAN);

– normal (звичайна реєстрація за допомогою протоколу GVRP).

Елементи GVRP, що управляють, використовуються для активізації роботи

протоколу на портах комутатора, а також для вказівки тієї, чи може ця VLAN бути зареєстрована на порту.

Динамічні записи про реєстрацію в VLAN (Dynamic VLAN Registration Entries) використовуються для уявлення у базі даних фільтрації інформації про порти, членство в VLAN яких встановлено динамічно. Ці записи створюються, оновлюються і віддаляються в процесі роботи протоколу GVRP.

Протокол GVRP визначає спосіб, за допомогою якого комутатори обмінюються інформацією про мережу VLAN, щоб автоматично зареєструвати членів VLAN на портах в усій мережі. Він дозволяє дина-мически створювати і видаляти VLAN стандарту IEEE 802.1Q на магістральних портах, автоматично реєструвати і виключати атрибути VLAN (під реєстрацією VLAN мається на увазі включення порту в VLAN, під виключенням – видалення порту з VLAN).

Протокол GVRP використовує повідомлення GVRP BPDU (GVRP Bridge Protocol Data Units), що розсилаються на багатоадресну MAC-адресу 01-80-C2-00-00-21 для сповіщення пристроїв-передплатників про події. Сповіщення (advertisement) можуть містити інформацію про виконання наступних дій:

– Join message – реєстрація порту в VLAN.

– JoinEmpty: VLAN на локальному передплатнику не налагоджена;

– JoinIn: VLAN на локальному передплатнику зареєстрована;

– Leave message – видалення VLAN з конкретного порту.

– LeaveEmpty: VLAN на локальному передплатнику не налагоджена;

– LeaveIn: VLAN на локальному передплатнику видалена;

– Leave message – видалення усіх, зареєстрованих на порту VLAN. Це повідомлення вирушає після того, як пройде час, заданий таймером LeaveAll Timer;

– Empty message – вимога повторного динамічного сповіщення і статичного налаштування VLAN.

Таймери GVRP

Join Timer – час в мілісекундах (100–100000), через який вирушають повідомлення JoinIn або JoinEmpty. Визначає проміжок часу між моментом отримання комутатором інформації про вступ в VLAN і фактичним моментом вступу в VLAN. За умовчанням встановлено значення 200 мс.

Коли комутатор отримує повідомлення про виключення порту з VLAN (Leave message) від іншого передплатника GVRP, він чекає заданий період часу (від 100 до 100000 мілісекунд), визначуваний таймером Leave Timer, щоб переконатися, що інформація про цій VLAN більше не існує в мережі. Наприклад,

коли комутатор отримує повідомлення Leave, він не видаляє миттєво інформацію про відповідній VLAN, а запускає Leave Timer і чекає, коли його час витече. Якщо за цей час не буде отримано сполучення JoinIn з інформацією про VLAN, що видаляється, то вона буде комутатором видалена. Звичайне значення таймера Leave Timer встановлюють в два рази більше значення таймера Join Timer. За умовчанням значення таймера дорівнює 600 мс.

LeaveAll Timer – інтервал часу в мілісекундах (100–100000), через який вирушає повідомлення LeaveAll. Коли комутатор – передплатник GVRP отримує це повідомлення, він перезапускає усі таймери, включаючи LeaveAll Timer. Зазвичай значення тайме-ра LeaveAll встановлюють в два рази більше значення таймера Leave Timer. За умовчанням значення таймера дорівнює 10000 мс.

На рис. 4.25 показано процес поширення інформації про VLAN по мережі з використанням протоколу GVRP. На комутаторі 1 створені статичні віртуальні мережі VLAN v10, v20 і v30. Порт 25 є маркованим членом усіх VLAN. Комутатор 1 відправляє сповіщення про VLAN v30 через порт 25 комутатору 2 (повідомлення JoinEmpty). Комутатор 2 отримує це сповіщення, динамічно створює VLAN v30 і включає в неї порт 25. Порт 26 комутатора 2 відправляє сповіщення про VLAN v30 комутатору 3 (повідомлення JoinEmpty), але сам не стає членом цій VLAN.

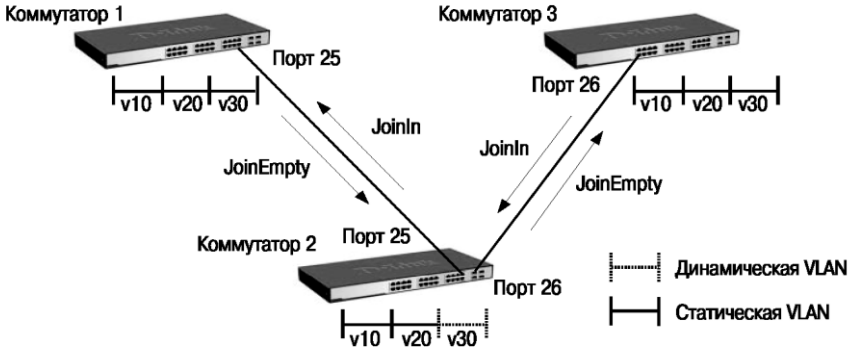


Рис. 4.25. Процес поширення інформації про реєстрацію VLAN по мережі

Комутатор 3 отримує сповіщення, динамічно створює VLAN v30 і включає в нього порт 26. Далі комутатор 3 змінює стан VLAN v30 з динамічного на статичний і відправляє через порт 26 повідомлення JoinIn про реєстрацію віртуальної мережі. Комутатор 2 отримує це сповіщення і реєструє порт 26 в VLAN v30, який вже був створеним раніше. Повідомлення про реєстрацію VLAN v30 вирушає через порт 25 комутатору 1. Отримавши це повідомлення, комутатор 1 перестає розсилати сповіщення про VLAN v30.

Порт з підтримкою протоколу GVRP підключається до мережі VLAN тільки у тому випадку, якщо він безпосередньо отримує сповіщення про нього. Якщо

порт з підтримкою протоколу GVPR передає сповіщення, отримане від іншого порту комутатора, він не підключається до цієї мережі VLAN.

Рис. 4.26 показує процес поширення інформації про видалення VLAN по мережі.

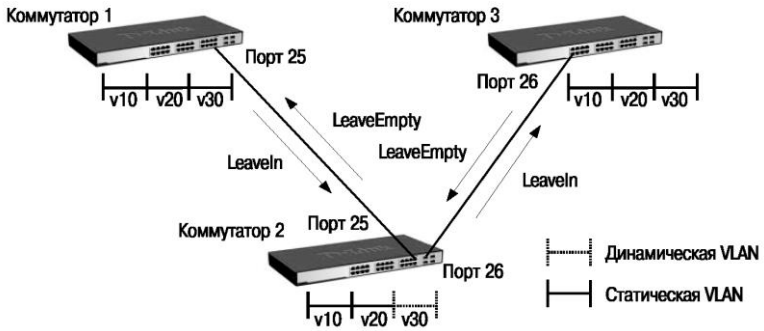


Рис. 4.26. Процес поширення інформації про видалення VLAN по мережі

На комутаторі 1 видалена статична VLAN v30, і він відправляє повідомлення LeaveIn через порт 25 комутатору 2. Коли комутатор 2 отримає сповіщення про видалення VLAN v30, він виключить порт 25 з цієї VLAN і відправить повідомлення LeaveIn комутатору 3 через порт 26. Комутатор 3 отримає сповіщення про видалення VLAN v30, але видалить її не відразу, а після закінчення періоду, встановленого таймером Leave Timer. Після видалення VLAN v30 комутатор 3 відправить через порт 26 повідомлення LeaveEmpty. Після отримання цього повідомлення комутатор 2 виключить порт 26 з VLAN v30 і видалить її після закінчення періоду, встановленого таймером Leave Timer. Через порт 25 буде передано повідомлення LeaveEmpty комутатору 1. Комутатор 1 виключить свій порт 25 з динамічної VLAN v30.

Порядок налаштування протоколу GVRP

У прикладі, показаному на рис. 4.26, вимагається настроїти можливість динамічного поширення по мережі інформації про VLAN v30 з використанням протоколу GVRP. Нижче приведені налаштування комутаторів.

Налаштування комутаторів 1, 3:

– видалити відповідні порти з VLAN за умовчанням (default VLAN) і створити нові VLAN:

configvlandefault delete 1-24

create vlan v10 tag 10

create vlan v20 tag 20

create vlan vS0 tag S0

– у створені VLAN додати порти, для яких необхідно вказати, які з них є маркованими і немаркованими:

config vlan v10 add untagged 1-8

config vlan v20 add untagged 9-16

config vlan vS0 add untagged 17-24

config vlan v10 add tag 25-26

config vlan v20 add tag 25-26

– активізувати протокол GVRP і функцію сповіщення проводовій VLAN (у цьому прикладі VLAN v30) по мережі:

config vlan vS0 advertisement enable

enable gvrp

config port_vlan 25-26 gvrp_state enable

Налаштування комутатора 2:

configvlandefaultdelete 1-24

create vlan v10 tag 10

create vlan v20 tag 20

config vlan v10 add untagged 1-12

config vlan v20 add untagged 1S-24

config vlan v10 add tagged 25-26

config vlan v20 add tagged 25-26

enable gvrp

config port_vlan 25-26 gvrp_state enable

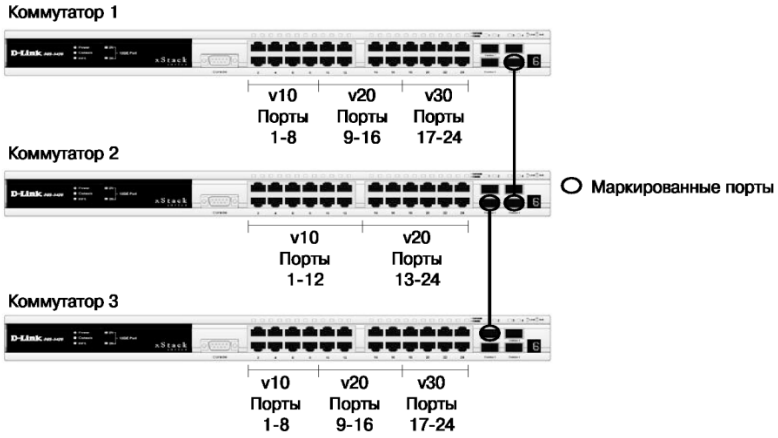


Рис. 4.26. Схема мережі VLAN

Запитання для самоконтролю

1. Керування сеансами TCP. Протокол UDP.

2. Варіанти застосування функції контролю підключення вузлів до портів комутатора.

3. Забезпечення безпеки на канальному рівні моделі OSI.

4. Механізми доступу до середовища та фреймування.

5. Забезпечення безпеки на рівні додатків моделі OSI.

6. Служби рівня додатків моделі OSI.

7. Забезпечення безпеки на мережному рівні моделі OSI.

8. Протоколи мережного рівня IPVN.

9. Маршрутизація на мережному рівні моделі OSI.

10. Особливості управління багатоадресною розсилкою на 2-му рівні моделі OSI (IGMP Snooping).

11. Планування захищеної мережі.

12. Організація захищеного підключення.

13. Особливості реалізації статичних і динамічних VLAN.

14. Методика створення списків управління доступом (ACL).

15. Призначення і зміст списків управління доступом.

16. Типи профілів доступу.

17. Процес створення профілю доступу.

18. Приклади налаштування ACL.

19. Варіанти списків реалізації управління доступом (ACL).

20. Основні команди комутаторів.

ПІСЛЯМОВА

Формування безпечної мережевої інфраструктури починається, як відомо, процесу з планування. На цьому етапі особлива увага приділяється:

– сервісам, які будуть використовуватися в мережі;

– ризикам, що пов'язані з використовуваними сервісами;

– механізмам, необхідним для зниження цих ризиків.

На підставі даних, отриманих на етапі планування, розробляється відповідний дизайн мережевої інфраструктури і створюється набір політик безпеки.

Наступним є етап безпосереднього впровадження, в ході якого відбувається як первісне налаштуванням системи захисту, так і постійне відстеження подій безпеки, їх аналіз та оптимізація відповідних політик безпеки. Слід відмітити, що саме від написання ефективних політик безпеки та їх суворого дотримання залежить робота всієї системи захисту. Правильні політики повинні бути зафіксовані документально й не мати великої кількості винятків. На все обладнання повинно регулярно встановлюватися поновлення.

Суттєву небезпеку при цьому відіграє використання простих паролів, помилок в конфігурації пристроїв, налаштувань за замовчуванням, незахищених протоколів і технологій.

Для забезпечення повної безпеки всієї IT інфраструктури слід впроваджувати механізми захисту на всіх рівнях мережі від кордону до комутаторів доступу. При цьому доцільно використовувати керовані комутатори з підтримкою функціонала захисту протоколів ARP, DHCP та STP, авторизувати користувачів при підключенні за допомогою технології 802.1x, підключати співробітників в різних VLAN залежно від їх функціональних обов'язків, задавати правила взаємодії і доступу до різних ресурсів на рівні розподілу.

При підключенні до мережі WAN та інтернет важливо крім брандмауера мати можливість сканувати трафік на рівні додатків, перевіряти наявність загроз за допомогою IPS систем. Використовуване обладнання повинно бути стійким до DoS і DDoS-атак. Для виходу користувачів в інтернеті доцільно використовувати проксі сервера з додатковою перевіркою на віруси, небажане, шкідливе і шпигунське ПЗ, а також організацією веб та контент фільтрації. Також важлива наявність рішення для перевірки пошти на предмет спаму і вірусів. Всі корпоративні ресурси, до яких потрібно забезпечити доступ ззовні з метою безпеки повинні бути винесені в окрему демілітаризовану зону DMZ.

Для віддаленого доступу слід використовувати технологію VPN з шифру-

ванням переданих даних. Для управління всім мережевим обладнанням – захищені протоколи SSH, HTTPS та SNMPv3. Для можливості аналізу логів час на пристроях повинен бути синхронізованим. Для розуміння, який трафік ходить в мережі, наскільки завантажено обладнання та які події на ньому відбуваються необхідно використовувати протоколи Syslog, RMON, Sflow, NetFlow.

Надзвичайно важливим є ведення обліку того, хто, коли і які зміни вносить в конфігурації обладнання. Повний перелік технологій, які використовуються для забезпечення безпеки мережевої інфраструктури, вказані на схемі, що наведена на рис. 5.

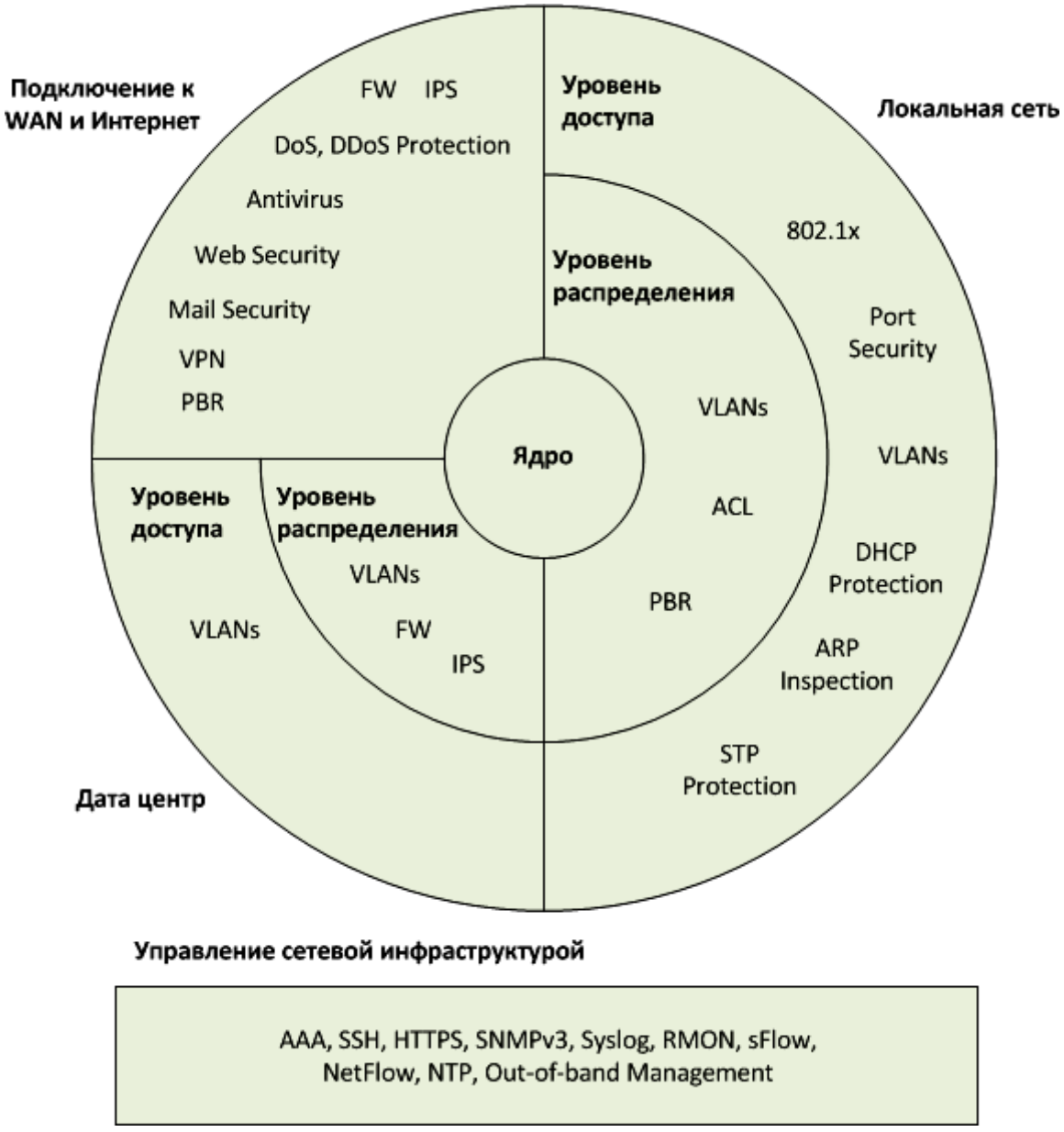


Рис. 5. Перелік технологій для забезпечення безпеки мережевої інфраструктури

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бурячок В. Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби / В. Л. Бурячок, Г. М. Гулак, В. Б. Толубко. – К.: ДУТ, 2015. – 449 с.
2. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В. Г. Олифер, Н. А. Олифер. – СПб: Питер, 2000. – 992 с.
3. Руководство по технологиям объединенных сетей. 3-е издание. Пер. с англ. М.: Вильямс, 2002. – 1040 с.
4. Шринивас В. Качество обслуживания в сетях IP / В. Шринивас. – М.: Вильямс, 2003. – 851 с.
5. Mueller S. Upgrading and Repairing Networks / S. Mueller. – Que, 2002.
6. Lekkas P. C. Network Processors / P. C. Lekkas. – The McGraw-Hill Companies, 2003.
7. Богуш В. М. Основи інформаційної безпеки держави / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005 – 432 с.
8. Богуш В. М. Інформаційна безпека від А до Я: 3000 термінів і понять / В. М. Богуш, А. М. Кудін. – К.: МОУ, 1999. – 456 с.
9. Галатенко В. А. Информационная безопасность. – Открытые системы, NN4-6, 1995.
10. Домарев В. В. Безопасность информационных технологий. Системный подход / В. В. Домарев. – К.: ООО «ТИД ДС», 2004. – 992 с.
11. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 120 с.
12. Уфимцев Ю. С. Методика информационной безопасности / Ю. С. Уфимцев, В. П. Буянов, Е. А. Ерофеев и др. – М.: Экзамен, 2004. – 544 с.
13. Безопасность сетевой инфраструктуры. Примеры решений. http://netwave.ua/ru/bezopasnost-setevoj-infrastruktury-primery-reshenij/

НАВЧАЛЬНЕ ВИДАННЯ

Володимир Леонідович Бурячок
Андрій Олександрович Аносов
Віктор Володимирович Семко
Володимир Юрійович Соколов
Павло Миколайович Складанний

ТЕХНОЛОГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ МЕРЕЖЕВОЇ ІНФРАСТРУКТУРИ

(українською мовою)

Видається у авторській редакції

художник-дизайнер Б. В. Вовкотруб
комп’ютерна верстка Б. В. Вовкотруб

Підписано до друку 28.04.2019 р.
Формат 60×84/16. Друк офсет. Папір офсет. Гарнітура Таймс.
Ум. друк. аркушів 11.2. Наклад 350 прим.