

3 Забезпечення захисту інформації в системах зв'язку. Технічні засоби системи захисту інформації

УДК 004.056.5 (076.5)

ДОСЛІДЖЕННЯ КОНТРОЛЮ ПЕРЕДАЧІ ДАНИХ В МЕРЕЖАХ ЗБЕРІГАННЯ FIBRE CHANNEL

Богдан Корнієнко, Семен Сулима

Національний авіаційний університет

Анотація: Мережі зберігання мають дуже високі вимоги до надійності передачі даних. Найменші втрати є неприпустимими й призводять до тяжких наслідків для аплікацій, хост-системи яких працюють із мережею зберігання. Відкидання пакета або кадру при переповненні буферів, як це прийнято в Ethernet та IP мережах, тут зустрічається дуже рідко. В даній статті ми розглянемо механізм контролю передачі даних, що якраз і забезпечує найвищу надійність у мережах зберігання на базі технології Fibre Channel.

Summary: Storage area networks place very high demands on the reliability of data transfer. Minor losses are unacceptable and have serious consequences for applications, host-systems of which are operating with a storage network. Reset of the packet or the frame during the buffer overflow, as is customary in Ethernet and IP networks here is very rare. In this article we will review flow control mechanism, which is precisely provides high reliability in storage area networks based on Fibre Channel.

Ключові слова: Мережі зберігання даних Fibre Channel, контроль передачі даних, методи кредитування.

I Вступ

Механізми гарантованої доставки в мережах передачі даних, такі, наприклад, як Windowing в TCP, PAUSE в Ethernet лише вирішують проблеми, що виникли в процесі передачі даних (виправлення помилок, управління інтенсивністю й т. д.), але ніяк не запобігають їм. У цьому і є принципова відмінність контролю передачі «класичних» мереж від мереж зберігання (як, наприклад, Fibre Channel).

Вибір технології, насамперед, диктується тими задачами, які ті або інші мережі вирішують. Якщо першочерговим завданням глобальних IP мереж, таких як Internet, є обмін інформацією між користувачами, що живуть на величезних відстанях один від одного, то мережі зберігання являють собою просту заміну локальних складових систем вводу-виводу (I/O) комп'ютерів (наприклад, жорстких дисків) [1]. Якщо ж потрібно таку систему «винести» на сотні або навіть тисячі кілометрів, то немає ніяких проблем у використанні гібридних (правда, менш надійних) технологій – певного компромісу між ненадійними мережами передачі даних і дуже надійними мережами зберігання даних.

II Постановка задачі

Метою даної статті є дослідження механізму контролю передачі даних у мережах зберігання на базі технології Fibre Channel, перевірка забезпечення необхідної надійності у мережах зберігання даних та особливостей застосування даної технології.

III Огляд технології Fibre Channel

Модель Fibre Channel складається з п'яти рівнів – FC-0, FC-1, FC-2, FC-3 й FC-4. FC-0 визначає фізичні характеристики з'єднання, FC-1 відповідає за кодування блоків даних, FC-2 займається формуванням і управлінням кадрами, адресацією, контролем передачі даних, виявленням помилок на рівні кадрів. FC-3 містить набір різних сервісів, необхідних для роботи Fibre Channel. FC-4 відповідає за взаємодію із протоколами верхніх рівнів. Технологія Fibre Channel не має точної відповідності еталонній моделі OSI (рис. 1) [2].

Мінімальною одиницею передачі даних в Fibre Channel є слово, що складається з 4 байт (після кодування 8b/10b на рівні FC-1 – з 40 біт). Кадри складаються зі слів й, у свою чергу, формують послідовності (односпрямована зв'язана передача кадрів від однієї ноди до іншої). Послідовності становлять обмін (серія послідовностей між двома нодами). У заголовку кадру знаходяться дані про адреси відправника й отримувача, ідентифікатори послідовності й обміну та інша службова інформація. Крім кадрів існують спеціальні 4-байтні керуючі слова, які називаються впорядкованими множинами

(ordered set). Їх використовують порти для синхронізації й контролю передачі даних. Серед впорядкованих множин виділяють роздільники кадрів, примітиви (заповнювачі й контрольні сигнали) і послідовності примітивів. Надалі нас буде цікавити примітив R_RDY (Receiver Ready) [2, 3].

Прикладний		FC-4	
Презентаційний			
Сеансовий			
Транспортний			
Мережевий		FC-2, FC-3	
Канальний			
Фізичний		FC-1	
		FC-0	

Рисунок 1 - Порівняння моделей OSI та Fibre Channel

Технологія Fibre Channel розрізняє також типи портів пристроїв у мережі: N_Port (порт ноди, звичайно це сервер або пристрій зберігання/резервного копіювання), F_Port (порт комутатора, що з'єднаний з портом ноди), E_Port (порт комутатора, який з'єднаний з іншим комутатором).

В Fibre Channel існує декілька класів обслуговування залежно від типу взаємодії пристроїв у мережі зберігання (табл. 1).

Таблиця 1 – Класи обслуговування в Fibre Channel

Атрибут	Клас 1	Клас 2	Клас 3	Клас 4	Клас 6
Установлення з'єднання	Так	Ні	Ні	Так	Так
Пакетна комутація	Ні	Так	Так	Ні	Ні
Резервування смуги пропускання	100%	Ні	Ні	Частково	100%
Гарантована затримка	Так	Ні	Ні	Так (QoS)	Так
Гарантований порядок доставки	Так	Ні	Ні	Так	Так
Підтвердження про доставку	Так	Так	Ні	Так	Так

Існує також клас обслуговування – F. Він використовується при наявності з'єднань між комутаторами Fibre Channel (ISL).

IV Кредитування

Механізм контролю передачі даних або управління потоком (flow control) актуальний у випадках, коли пристрій приймає даних більше, ніж реально може обробити, через що доводиться їх частину відкидати. Як вже згадувалося, така ситуація вкрай небажана, бо спричиняє серйозні проблеми, що пов'язані з розсинхронізацією, повторними передачами, втратою продуктивності й некоректною роботою аплікацій.

Технологія Fibre Channel має вбудований механізм контролю передачі даних для вирішення описаної проблеми – кредитування. Даний механізм гарантує постійний контроль над портом отримувача: приймаюча сторона має видати кредит для кожного кадру, надісланого передавальною стороною. Якщо вхідні буфери порту отримувача переповнені, то відкидання кадрів не відбудеться, бо просто не будуть видаватися нові кредити. Інакше кажучи, пристрій може передавати кадри іншому пристрою тільки тоді, коли той готовий їх прийняти [4].

Кредити являють собою кількість кадрів, що пристрій може прийняти в даний момент часу. Цю величину пристрої визначають у процесі підключення до фабрики (Login), тому кожен пристрій знає, скільки кадрів може прийняти інший пристрій. Після того, як достатня кількість кадрів була передана, і кредит скінчився, кадри не передаються доти, поки цільовий пристрій не вкаже, що він обробив один або більше кадрів і готовий прийняти нові кадри. Для видачі кредитів отримувач використовує примітив

R_RDY (рис. 2) [3].

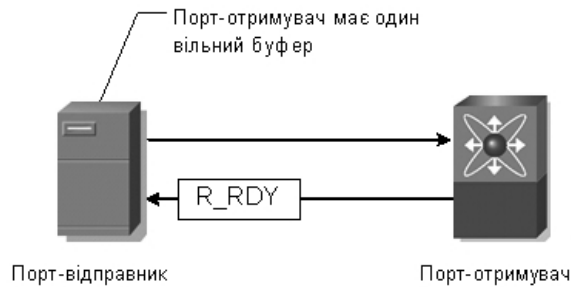


Рисунок 2 – Контроль передачі даних в Fibre Channel

Контроль передачі буває двох типів - buffer-to-buffer й end-to-end (рис. 3). Перший тип використовується між двома безпосередньо підключеними пристроями, інший - між ініціатором і цільовим пристроєм (двома N_Port). Далі будуть детально розглянуті обидва типи контролю передачі даних.

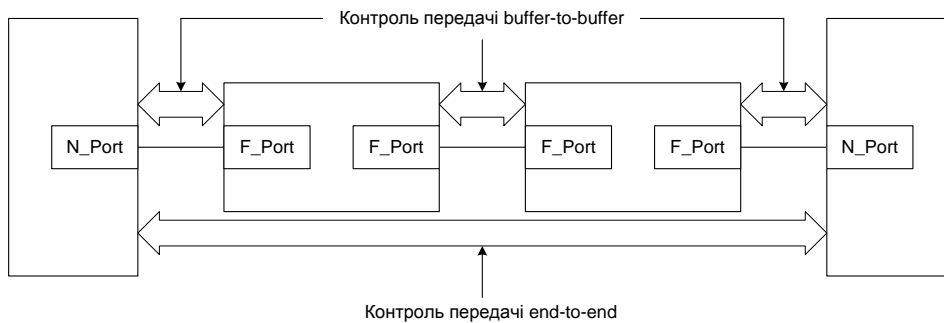


Рисунок 3 – Типи контролю передачі даних в Fibre Channel

V Контроль передачі даних buffer-to-buffer

Контроль передачі даних buffer-to-buffer в основному використовується між N_Port й F_Port і двома E_Port. Він не використовується між двома N_Port та всередині комутаторів у фабриці між вхідним і вихідним портами. Розмір буфера кожного із пристроїв (або кількість кредитів) визначається в процесі FLOGI (Fabric Login). Алгоритм роботи кредитування на основі buffer-to-buffer полягає в наступному:

- N_Port відправника перед тим, як передати кадр, чекає примітива R_RDY від F_Port комутатора, до якого він приєднаний. Цим примітивом комутатор повідомляє, що в нього є вільний буфер для прийому кадру.
- N_Port відправника отримує примітив R_RDY і передає кадр.
- Кадр передається через фабрику в бік порту отримувача з використанням механізму buffer-to-buffer між кожною парою E_Port (якщо на шляху проходження кадру фабрика представлена одним комутатором, то даний пункт опускається).
- F_Port комутатора чекає примітива R_RDY від N_Port одержувача.
- F_Port одержує примітив R_RDY і передає кадр (рис. 4) [3, 5].

VI Контроль передачі даних end-to-end

На відміну від механізму buffer-to-buffer, контроль передачі даних end-to-end працює між двома N_Port, а кількість кредитів визначається в процесі PLOGI (Port Login). Алгоритм роботи схожий із кредитування buffer-to-buffer:

1. N_Port відправника перед тим, як передати кадр, чекає примітива R_RDY від F_Port комутатора, до якого він приєднаний. Цим примітивом комутатор повідомляє, що в нього є вільний буфер для прийому кадру.
2. N_Port відправника отримує примітив R_RDY і передає кадр.

3. Кадр передається через фабрику в бік порту отримувача з використанням механізму buffer-to-buffer між кожною парою E_Port (якщо на шляху проходження кадру фабрика представлена одним комутатором, то даний пункт опускається).

4. F_Port комутатора чекає примітива R_RDY від N_Port одержувача.

5. F_Port отримує примітив R_RDY і передає кадр.

6. N_Port отримувача чекає R_RDY від F_Port після того, як отримав кадр.

7. N_Port отримує R_RDY і передає кадр підтвердження ACK назад відправникові.

8. F_Port з боку відправника чекає R_RDY від N_Port відправника.

9. N_Port посилає кадр R_RDY, і F_Port передає кадр ACK (рис. 5).

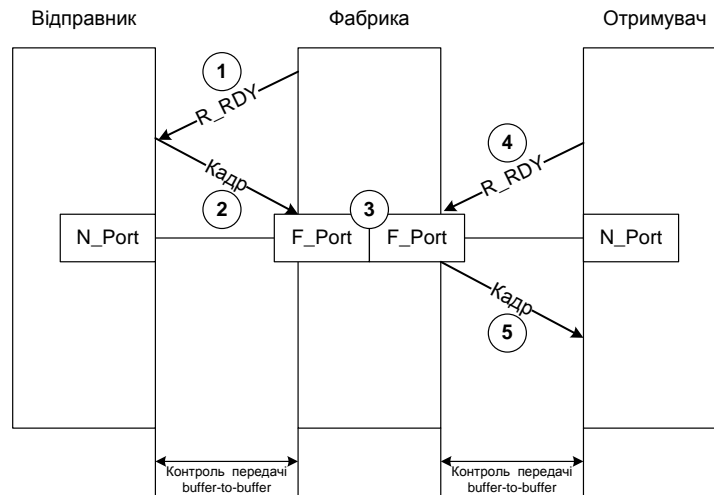


Рисунок 4 - Контроль передачі даних buffer-to-buffer

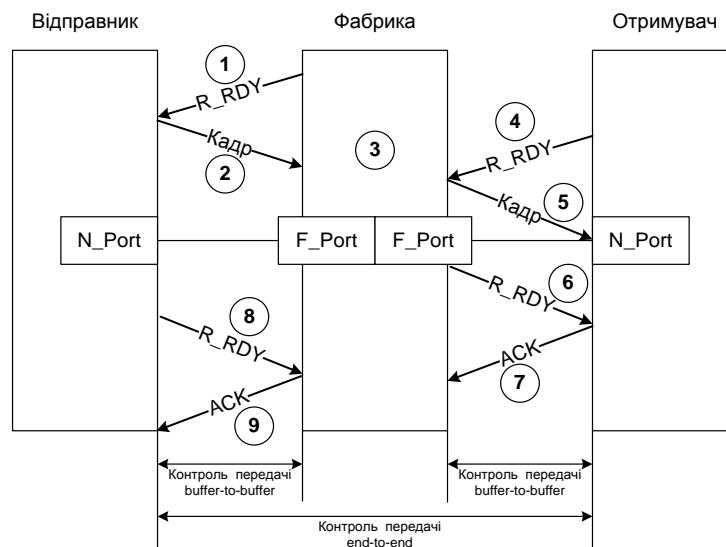


Рисунок 5 - Контроль передачі даних end-to-end

Відповідальність за доставку кадрів несе порт-відправник. Тому очищення буферів протоколів верхніх рівнів відбувається тільки після отримання всіх кадрів ACK [3], [5].

VII Методи кредитування

Основний метод кредитування припускає початок передачі кадрів навіть тоді, якщо порт-приймач не надіслав жодного примітиву R_RDY. Це можливо внаслідок того, що в процесі FLOGI сторони повідомляють одна одну про кількість своїх буферів (*BB_Credit*). При цьому значення *BB_Credit* заноситься до спеціальної таблиці. Також передавальний порт зберігає змінну *BB_Credit_CNT*, що вказує

на кількість використаних буферів. Після завершення процесу підключення до мережі $BB_Credit_CNT = 0$. Приймаючи кадр, одержувач переміщує його в буфер протоколу верхнього рівня, а відправникові надсилає примітив R_RDY , інформуючи про те, що буфер звільнився. Отримавши R_RDY , відправник зменшує значення змінної BB_Credit_CNT . При пересиланні даних виконується умова:

$$BB_Credit_CNT < BB_Credit \quad (1)$$

Аналогічно виглядає основний метод кредитування для контролю передачі даних end-to-end.

$$EE_Credit_CNT < EE_Credit, \quad (2)$$

де EE_Credit_CNT – лічильник буферів, що використовуються; EE_Credit – кількість буферів одержувача, визначена в процесі PLOGI.

Альтернативний метод дозволяє довідатися порту-відправникові лише кількість гарантованих буферів одержувача, але щоб почати передачу, порт-відправник повинен дочекатися примітива R_RDY [3, 7].

VIII Використання контролю передачі даних у різних класах обслуговування Fibre Channel

Залежно від класу обслуговування використовується buffer-to-buffer або end-to-end (або разом) контроль передачі даних (табл. 2) [3].

Таблиця 2 – Використання кредитування в класах обслуговування Fibre Channel

Тип контролю передачі даних	Клас 1	Клас 2	Клас 3	Клас 4	Клас 6	Клас F
Buffer-to-buffer		+	+			+
End-to-end	+	+		+	+	

З таблиці видно, що клас обслуговування 2 використовує одночасно обидва механізми контролю передачі даних. Якщо прийняти $BB_Credit - BB_credit_CNT \neq 0$ рівним 1, а $EE_Credit - EE_credit_CNT \neq 0$ також рівним 1, то для передачі кожного кадру відправник повинен перевіряти умову:

$$(BB_Credit - BB_Credit_CNT) \wedge (EE_Credit - EE_Credit_CNT) = 1, \quad (3)$$

при якій кон'юнкція різниць дорівнює 1.

IX Проблеми контролю передачі даних на великих відстанях

Як вже зазначалось, мережі зберігання даних з самого початку проектувалися як більш швидкісна й масштабована альтернатива локальним підсистемам вводу-виводу (I/O). В рамках концепції безперервності бізнесу (business continuance) з'явилися нові вимоги до мереж зберігання, а саме створення географічно розподілених центрів обробки даних (ЦОД). Контроль передачі даних на основі кредитування в даній ситуації виявився вузьким місцем при побудові таких розподілених ЦОД (рис.6).

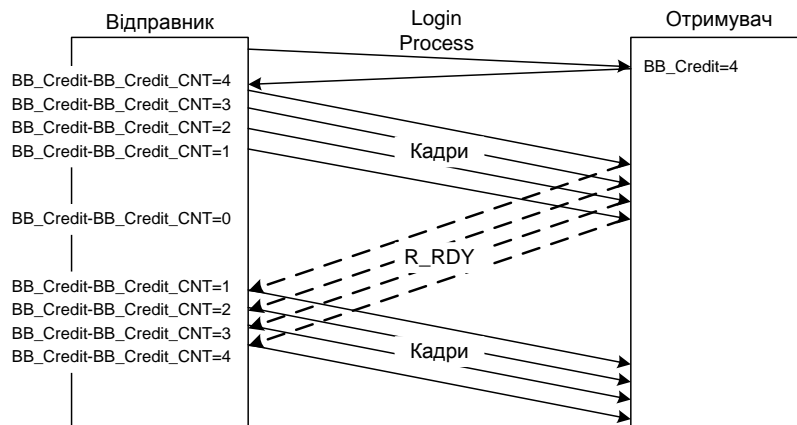


Рисунок 6 - Проблеми контролю передачі даних на великих відстанях

Стандартний розмір буфера призводить до того, що дані передаються фрагментами, без використання всієї пропускної здатності каналу. Зі збільшенням відстані швидкість передачі даних істотно зменшується. Це пов'язано з тим, що передавальна сторона повинна чекати примітивів R_RDY для того, щоб продовжити передачу даних. Спад швидкості передачі даних трапляється тоді, коли відстань досягає точки, де час передачі світлового сигналу туди й назад дорівнює часу на передачу кількості байт, які здатний прийняти буфер одержувача [8], [9]. Математично це можна виразити в такий спосіб:

$$BB_Credit < \frac{RTT}{SF}, \quad (4)$$

де RTT (Round Trip Time) - це час проходження сигналу туди й назад; SF (Serialization delay for a data frame) - затримка серіалізації для кадру даних.

У свою чергу RTT складається з:

$$RTT = SF + PF + SR + PR, \quad (5)$$

де SF (Serialization delay for a data frame) – затримка серіалізації кадру даних; PF (Propagation delay of data frame) – затримка поширення кадру даних; SR (Serialization delay of R_RDY) – затримка серіалізації примітива R_RDY; PR (Propagation delay of R_RDY) – затримка поширення примітива R_RDY.

Для розрахунку оптимальної величини BB_Credit було обрано відстань між двома майданчиками ЦОД у 72 км та пропускна здатність каналу Fibre Channel – 2 Gbps.

$$SF = \frac{(Frame_Size + 24bytes_IDLE) \cdot 8bits \cdot 1,25_8b/10b}{FC_Speed} \cdot 1000000 =$$

$$= \frac{(2148 + 24) \cdot 10}{2125000000} \cdot 1000000 = \frac{21720}{2125000000} \cdot 1000000 = 10.221\mu s.$$

$$PF = PR = 72 \cdot 5 = 360\mu s.$$

$$SR = \frac{(R_RDY_Frame_Size + 8bytes_2IDLE) \cdot 8bits \cdot 1,25_8b/10b}{FC_Speed} \cdot 1000000 =$$

$$= \frac{(4 + 8) \cdot 10}{2125000000} \cdot 1000000 = \frac{120}{2125000000} \cdot 1000000 = 0.056\mu s.$$

$$RTT = SF + SR + PR + PF = 10.221 + 360 + 0.056 + 360 = 730.277\mu s.$$

$$BB_Credit = \frac{RTT}{SF} = \frac{730.277}{10.221} = 71.44 \approx 72.$$

Тобто, канал Fibre Channel з пропускною здатністю в 2 Gbps вимагає 72 кредитів на 72 км без спаду швидкості передачі даних [9].

Сучасні комутатори Fibre Channel дозволяють задавати до 250 та більше кредитів на канал. Зрозуміло, що це накладає істотні обмеження на відстань між майданчиками ЦОД. Щоб не залежати в явному вигляді від механізму контролю передачі даних Fibre Channel, використовують підміну (spoofing) примітивів R_RDY та IDLE. Локальний комутатор для передавальної сторони сам генерує примітиви R_RDY та IDLE, що дозволяє досягти постійного потоку даних та максимальної утилізації каналу [6], [9].

Х Висновки

Мережі зберігання даних дозволяють досягти високої надійності за рахунок спеціального механізму, що використовується для контролю передачі даних. З іншого боку, цей механізм накладає істотні обмеження щодо масштабованості такої мережі на великі відстані. Принцип дії цього механізму простий: система приймає дані тільки тоді, коли вона їх реально може опрацювати. У результаті цього, кадри майже ніколи не відкидаються. Це дає можливість використовувати мережі зберігання даних як альтернативу для підсистем вводу-виводу.

Література: 1. Marc Farley. *Storage Networking Fundamentals: An Introduction to Storage Devices, Subsystems, Applications, Management, and Filing Systems*. – Cisco Press, 2004 – 480 с. 2. James Long. *Storage Networking Protocol Fundamentals*. – Cisco Press, 2006 – 552 с. 3. Василь Пантюхін. *Протоколи SAN – Lynx*, 2005 – 204 с. 4. Gengui Zhou Suresh Muknahallipatna, Timothy Brothers. *Flow Control*. - NagaPrasad, 2003 - 4 с. 5. David Peterson. *FC-FS-2: BB_Credit (Recovery) Cleanup*. – T11, 2005 – 5 с. 6. Руслан Чиняков. *Мережі*

зберігання в ретроспективі й перспективі. - LAN, 2002 – 4 с. 7. Fujitsy Siemens Computers. Основи зберігання даних – чому важливо забезпечити надійність IT-інфраструктури. – Fujitsu Siemens, 2007 – 84 с. 8. [Steve Guendert](#). Buffer-to-Buffer Credits and Their Effect on FICON Performance. - McDATA, 2005 - 5 с. 9. Cisco Systems. Storage Extensions over Optical. – Cisco Systems, 2004 – 70 с.

УДК 681.3

ВАРІАНТИ ЗАХИСТУ ВІД ЗАГРОЗ В КОМУНІКАЦІЯХ РОЗПОДІЛЕНИХ МЕРЕЖ

В'ячеслав Василенко

Національний авіаційний університет

Анотація: Розглядаються питання захисту інформаційних ресурсів комунікаційної мережі зв'язку розподіленої обчислювальної мережі, наводиться варіант організації багаторівневого захисту ресурсів мережі, розглядаються механізми забезпечення функціональних послуг безпеки.

Summary: The questions of defense of informative resources of communication network of the distributed computer network are examined, the variant of organization of multilevel defense of resources of network is pointed, the mechanisms of providing of functional services of safety are examined.

Ключові слова: Загроза, порушник, ресурси, модель, комунікаційна мережа

І Загальний підхід до захисту інформаційних ресурсів розподілених мереж

Для захисту інформаційних ресурсів розподілених обчислювальних мереж (РОМ) пропонується використання корпоративної брандмауер-системи, яка інтегрується в інфраструктуру РОМ і забезпечує виконання встановлених правил доступу до захищеної мережі вузлів РОМ та відслідковування протоколів і послуг із захисту, що використовуються [1].

Така брандмауер-система є єдиною загальною точкою обміну даними кожного вузла РОМ із корпоративною мережею і використовується як бар'єр між захищеною і незахищеною мережами таким чином, що всі дані між мережами проходять безпосередньо через брандмауер-систему. В брандмауер-системі реалізовані механізми безпеки, які роблять цей інтерфейс безпечним і керованим. Механізми безпеки брандмауер-системи дозволяють: аналізувати дані, що проходять через брандмауер-систему; контролювати комунікаційне середовище і партнерів з обміну даними; регламентувати обмін даними відповідно до політики безпеки; реєструвати події, що мають відношення до безпеки.

Використання єдиної загальної точки обміну даними кожного вузла РОМ із корпоративною мережею дає декілька переваг: організація захисту є значно ефективнішою; простіша реалізація корпоративної політики безпеки; використовуються посилені методи автентифікації; забезпечується безпека через розподіл ресурсів; полегшується спостереження за сеансами обміну інформацією.

Основними завданнями брандмауер-системи є: контроль доступу на мережному рівні; контроль доступу на рівні користувачів; контроль доступу на рівні даних; керування правами доступу; контроль доступу на прикладному рівні; ізоляція послуг із захисту; реалізація функцій оповіщення; приховування інфраструктури мережі; конфіденційність комунікацій.

II Варіант організації багаторівневого захисту ресурсів мережі

Для забезпечення захисту інформаційних ресурсів корпоративної мережі РОМ можна реалізувати багаторівневий захист. Необхідність його реалізації обумовлюється, з одного боку, відсутністю універсальних засобів захисту, а з іншого, тим, що жодний окремий компонент не може достатньо міцно захистити мережу. Для ефективного захисту необхідно використовувати множину компонентів, що сумісно працюють таким чином, що здійснення атаки буде неможливим або ускладненим.

Організація багаторівневого захисту пов'язана з визначенням периметра мережі, внутрішньої мережі і політики безпеки системи (фактор персоналу).

Периметр – це посилена границя мережі, яка може включати до свого складу: маршрутизатори (routers); брандмауери (firewalls); систему виявлення вторгнень (СВВ, IDS); пристрої віртуальної приватної мережі (ПВПМ, VPN); програмне забезпечення мережі; демілітаризовану зону (ДМЗ, DMZ) і екрановані підмережі.

Маршрутизатори здійснюють управління вхідним і вихідним трафіком та трафіком в середині мережі. Пограничний маршрутизатор є останнім маршрутизатором перед виходом в незахищену мережу і виконує роль першого і останнього рубежу захисту мережі.