ПРИЛАДОБУДУВАННЯ ТА ІНФОРМАЦІЙНО-ВИМІРЮВАЛЬНІ ТЕХНОЛОГІЇ

INSTRUMENT-MAKING AND INFORMATION-MEASURING SYSTEMS

УДК 681.327.8

М.Карпінський[1], докт.техн.наук; М.Гіжицкі[1]; А.Брандис[1]; Н.Герила[2]; З.Рута[2]

[1]Університет в Бєльску-Бялей (Польща)
[2]Тернопільський державний технічний університет імені Івана Пулюя

СИСТЕМА БЕЗПЕКИ КОМП'ЮТЕРНОЇ МЕРЕЖІ З ВИКОРИСТАННЯМ ПРИСТРОЇВ CISCO IDS І PIX

Комп'ютерна мережа (КМ) є своєрідним носієм інформації, а також її джерелом. Однак можливість приєднання майже кожного до глобальної мережі Internet створює певні проблеми. Деяка інформація повинна бути доступною для виділеної групи осіб, а оскільки всі користувачі мають до неї доступ, то виникає задача забезпечення безпеки цієї інформації.

M.Karpinskyy; M.Gizycki; A.Brandys; N.Heryla; Z.Ruta

APPLIANCE OF CISCO IDS AND PIX DEVICES IN NETWORK SECURITY SYSTEM

A computer network (KM) is an original data carrier and also its source. However possibility of joining almost each to the global network of Internet creates certain problems. Some information must be accessible for the selected group of persons, and as all users have an access to it, there is the task of providing of safety of this information.

Відомо, що інформація може бути настільки потужним знаряддям, використовуючи яке зі зловмисною метою, можна довести фірми до стану банкрутства або процвітання. Для того, щоб оберегти себе від прикрих несподіванок, слід застосовувати систему безпеки КМ. Її впровадження диктується, головним чином, захистом КМ перед різного виду загрозами, а також вимогами певних законодавчих актів. В подальшому пропонується така система на основі пристроїв фірми Cisco, а також описано інші підходи і технології.

Аналіз загроз в КМ

Насамперед слід захистити вразливу та важливу інформацію, яка характеризується тим, що для окремої організаційної одиниці дані можуть бути використані зі зловмисною метою. Інформація володіє такими основними рисами:

– таємність – міра безпеки інформації, яка встановлюється особами, які нею володіють; з цим поняттям пов'язана також довіра або можливість передавання чи приймання інформації іншою особою;

– цілісність – означає, що інформація не була змодифікована;

– доступність – означає можливість використовувати дані для певних користувачів;

Атаки на КМ з погляду здійснюваного місця можна поділити на:

– локальні – зловмисник має фізичний доступ до атакованого об'єкту (є найгрізніші);

– мережеві:

– внутрішні – атака здійснюється з мережі, до якої безпосередньо під'єднаний атакований комп'ютер;

– зовнішні (віддалені) – атакуючий знаходиться в зовнішній мережі відносно атакованого хоста; є найважчі до здійснення і найбільш наочні.

Атаки можна поділити на 3 групи:

– атаки розпізнавальні – зазвичай є першою ознакою спроби взлому; полягають у зборі інформації про задіяні комп'ютери, пристрої та програми, операційну систему та її версії, що можна пізніше використати із зловмисною метою; характерним представником цих атак є сканування портів;

– атаки доступу – це є власне атаки для отримання конкретних даних з метою їх модифікації, або знищення, чи отримання високих привілеїв в операційній системі; до них належать, зокрема, Spyware; серед них можна виділити такі популярні програми: Alexa, Aurete, Cydoor, Gator, Promulgate, SaveNow;

– атаки блокування послуг (DoS – Denial of Service) – мають на меті унеможливити використання послуг або доступ до мережі авторизованих користувачів. Якщо ж ця атака здійснюється з багатьох комп'ютерів одночасно, то тоді має місце розгалужена атака блокування послуг (DDoS - Distributed Denial of Service).

Результатом атаки на КМ можуть бути:

– блокада КМ (атака типу DOS);

– прийняття прав авторизованого користувача КМ; тоді можна змінити налаштування системи або використати систему для подальших атак чи, наприклад, як джерело передачі спаму (тобто open-proxy). КМ з погляду безпеки подано на рис.1.

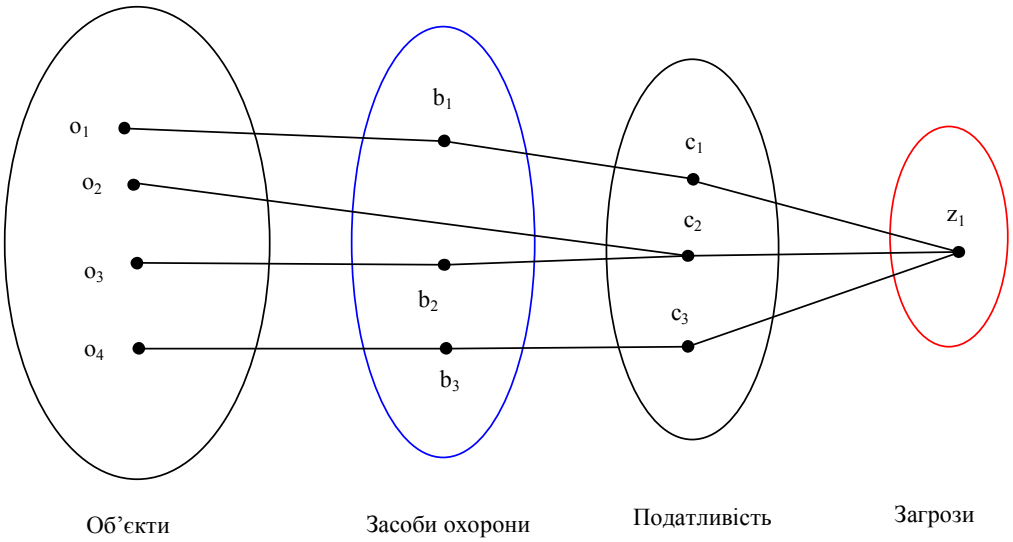

Рисунок 1 - КМ з погляду безпеки:

o1 – файл з наявною інформацією;
o2 – операційна система;
o3 – сервер бази даних;
o4 – мережевий додаток;
b1 – зашифрування;
b2 – актуалізація програмного забезпечення бази даних;
b3 – шифрування з'єднання;
c1 – пароль, який не дає здійснити словникову атаку;
c2 – програми операційної системи;
c3 – недоопрацьований код програми (наприклад: паролі, які пересилаються явним текстом);
z1 – безпосередній доступ зловмисника до інформації.

Порівняння існуючих систем безпеки КМ

Загальними технічними засобами охорони перед загрозами КМ є:

– Firewall;
– сенсори IDS/IPS (Intrusion Detection System/Intrusion Prevention System);
– концентратори VPN (для з'єднання віддалених користувачів з внутрішньою мережею через так званий тунель);
– UPS-и;
– інші пристрої, які мають вбудовані засоби безпеки, такі, наприклад, як списки доступу на маршрутизаторах чи комутаторах 3-го рівня моделі OSI;
– інші пристрої, які приначені для захисту КМ, наприклад, детектор аномалій, акселератори SSL, Data Force-и.

Firewall Cisco PIX

Для цих засобів можна виділити 4 характерні риси щодо розв'язання задачі безпеки КМ:

– забезпечення системи реального часу;
– алгоритм ASA (Adaptive Security Algorithm);
– проксі (cut-throught);
– надмірність.

Принцип роботи алгоритму ASA полягає в наступному (рис.2):

1. Внутрішній хост ініціює з'єднання з зовнішнім джерелом.
2. Firewall записує інформацію про це під'єднання в таблицю станів:

– IP адреса джерела;
– порт джерела;
– IP адреса призначення;
– інформацію про черговість TCP;
– додаткові значення портів TCP/IP;
– присвоєння випадково згенерованого номеру полідовності TCP.

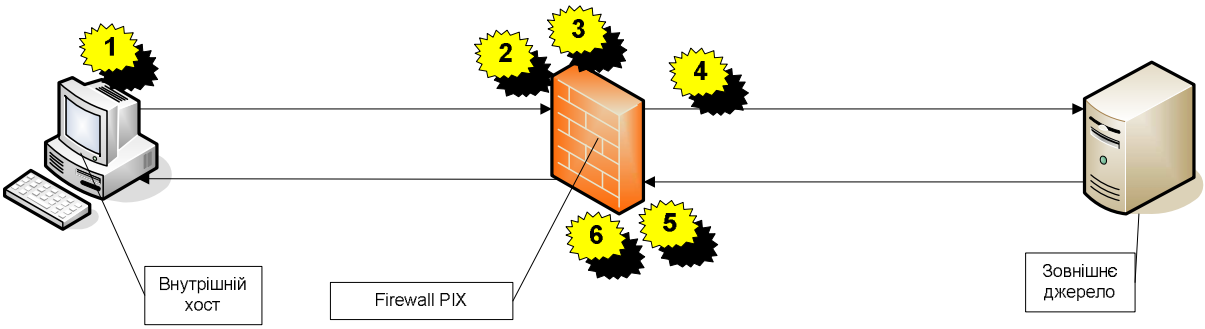

Рисунок 2 - Принцип роботи алгоритму ASA.

3. Отриманий об'єкт сесії порівнюється з вимогами безпеки, і, якщо не відповідає їм, то усувається з таблиці станів, а з'єднання відкидається. Якщо об'єкт відповідає вимогам безпеки, то передається запитання до зовнішнього сервера.

4. Сервер відповідає пакетом на запит. Відповідь досягає Firewall-у, де порівнюється з об'єктом сесії. Якщо результат порівняння є негативним, то переривається з'єднання з цим хостом, інакше сигнал спрямовується до хоста за наданням запиту.

IDS/IPS (Intrusion Detection System/Intrusion Prevention System)

Цей пристрій призначений для моніторингу, наприклад, сегменту КМ і розпізнавання на підставі відповідної бази даних, чи даний рух не належить до певного типу атак.

Мережеві системи IDS (NIDS) можна поділити за способом аналізу подій на:

– викривання сигнатур (signature detection). Система IDS порівнює записані зразки в базі сигнатур атак з актуальним станом журналів, які поточно відслідковуються цим

пристроєм. Якщо якась із сигнатур співпадає, то приймається відповідна дія. Такий підхід найчастіше використовується для комерційних задач;

– викривання аномалій (anomaly detection). Цей метод грунтується на попередньому визначенні правил, які передбачають "нормальне" і "ненормальне" поводження системи. На підставі цих правил отримуємо звіт про появу аномалії, яку пристрій блокує. До таких аномалій можна віднести перевищення заданої кількості з'єднань за визначений час з однієї адреси IP на порти комп'ютера у внутрішній мережі, що інтерпретується як спроба сканування портів;

– профілі користувача. За допомогою них описується нормальна активність користувача, а всі інші дії вважаються підозрілими. Зазвичай, ці профілі формуються за допомогою статистичних методів або алгоритмів нейронних мереж;

– контекстне зіставлення зразків – IDS відслідковує пакети щодо цілісності, тобто в процесі з'єднання пакетів перевіряє, чи вони не піддалися атаці. Для цього цей пристрій може розпізнавати рознесені в часі дії зловмисників або пофрагментовані спроби атак:

– декодування протоколів вищих рівнів. Пристрій декодує протоколи вищих рівнів FTP, HTTP, стараючись вихопити з їх вмісту характерні дані, які свідчать про атаку.

Системи IDS можна охарактеризувати також за способом під'єднання до КМ:

– системи in-line. Такі засоби містять два інтерфейси, завдяки чому є можливість потоку пакетів через ці інтерфейси, і тим самим відслідковування, наприклад, всіх пакетів, якщо IDS є ввімкнений через Firewall на стику внутрішньої та зовнішньої мереж. Система добре відслідковує всі спроби несанкціонованого доступу, але зумовлює невеликі затримки пересилання пакетів в мережі;

– сенсори. Вони містять під'єднаний інтерфейс і їх можна розмістити у вибраному сегменті мережі з метою моніторингу руху. На жаль, вони викривають незначну кількість атак, беручи до уваги те, що вимикаються подібно до кожного хоста. Атака повинна би тоді полягати у розголошенні, або бути спрямованою на конкретний IDS, щоб можна було би її виявити для випадку мережі з комутатором. Позитивним є те, що є комутатори з можливістю спрямування потоку інформації на один порт. Інший спосіб полягає у під'єднанні концентратора замість комутатора до цього сегменту мережі, що, на жаль, зумовлює зниження продуктивності цього сегмента мережі.

Концентратори VPN

Пристрої цього типу забезпечують доступ до технології VPN (Virtual Private Network). Мережу VPN можна порівняти з тунелем, яким здійснюється передача інформації між кінцевими VPN-клієнтами через відкриту мережу, наприклад, Internet, таким чином, що вузли цієї мережі є прозорими для пересилання пакетів інформації. Загалом таке з'єднання передбачає криптування та стиснення інформації, що передається, завдяки чому збільшується перепускна здатність і забезпечується цілісність, таємність і доступність.

Найчастіше використовуються такі VPN протоколи:

– IPsec; PPTP (Point to Point Tunneling Protocol), Open VPN.

Конфігурація системи безпеки КМ навчального закладу з використанням пристроїв Cisco IPS і PIX

Належно спроектована система безпеки повинна передусім бути пристосованою до середовища використання. Тому важливим є детальний аналіз архітектури цієї мережі разом з наявним у ній програмним забезпеченням.

Проект безпечної КМ повинен опиратися на визначену політику безпеки, суть якої для навчального закладу зводиться до такого:

– за замовчуванням користувач не має жодних прав;

– адміністратори мають повні права до дій у всій системі;

– працівники навчального закладу мають право на використання послуг Internet на загальних підставах, можуть теж за дозволом адміністратора користуватися з мережі

VPN як віддалені користувачі, мають доступ до спеціалізованого сервера, на якому знаходяться файли з наукової та навчальної тематики (лише для читання, а право на модифікування має право лише власник), володіють UNIX-вим паролем на сервері з можливістю логування до системи за допомогою ssh, електронною поштовою скринькою, місцем на веб сторінці; на хостах можуть модифікувати лише папку з іменем користувача, а інші об'єкти лише для читання;

– студенти можуть користуватися послугами Internet лише на загальних підставах, мають доступ як анонімні користувачі до одного навчального каталогу сервера FTP, мають електронну поштову скриньку, а також можуть попросити адміністратора про надання UNIX профілю; на виділеному хості можуть модифікувати файли в каталозі "Студент", а інші файли є лише для читання;

– інші користувачі можуть користуватися Internet на загальних підставах;

– використання Internet на загальних підставах означає можливість перегляду сторінок WWW, обслуговування e-mail, серверів FTP, Internet комунікаторів і т.д.

Черговим важливим завданням для проектування системи безпеки КМ є детальне ознайомлення з її схемою та фізичним розміщенням пристроїв і з'єднаннями між ними.

Приклад незахищеної КМ навчального закладу наведено на рис. 3.

Тепер на підставі політики безпеки слід визначитись з запланованими пристроями і місцем їх під'єднання до КМ. Тут основна увага приділена пристроям Cisco IDS/PIX, однак для повнішого використання КМ навчального закладу, з точки зору Internet послуг, які надаються віддаленим користувачам, слід використати також концентратор VPN.

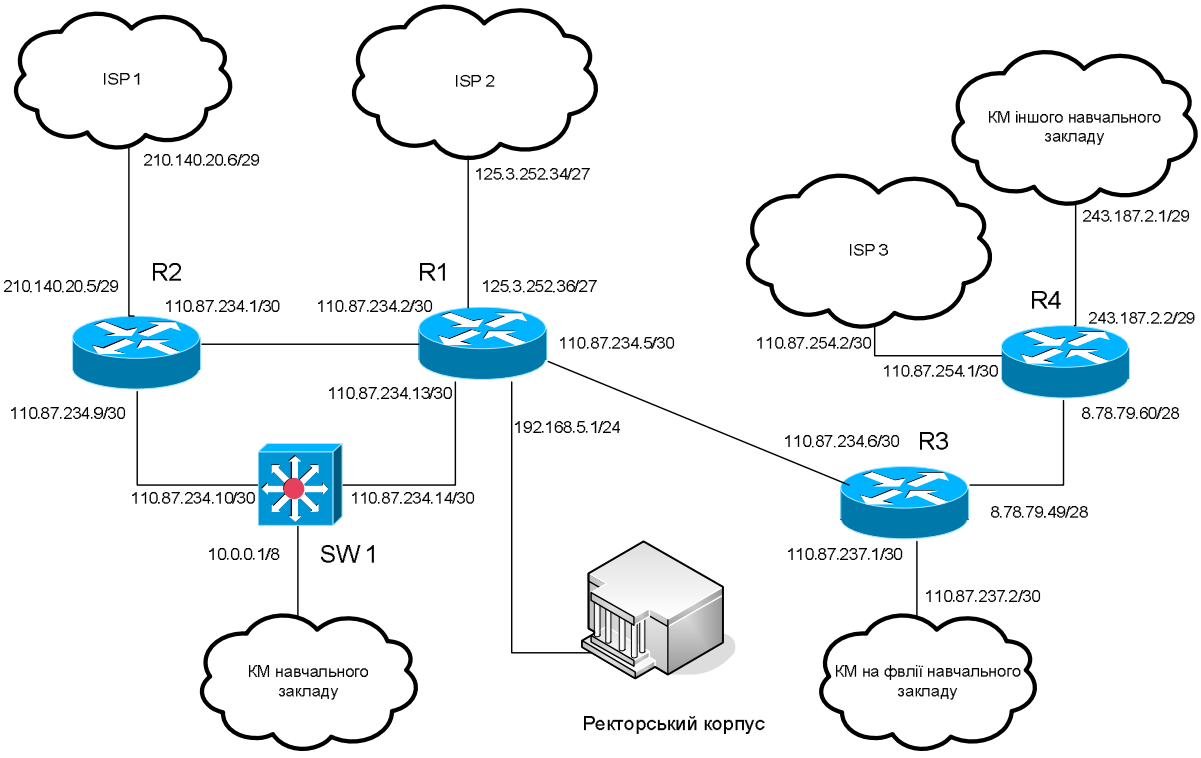

Рисунок 3 - Приклад КМ навчального закладу без системи безпеки.

Проект безпечної КМ навчального закладу завдяки пристроям фірми Cisco показано на рис. 4.

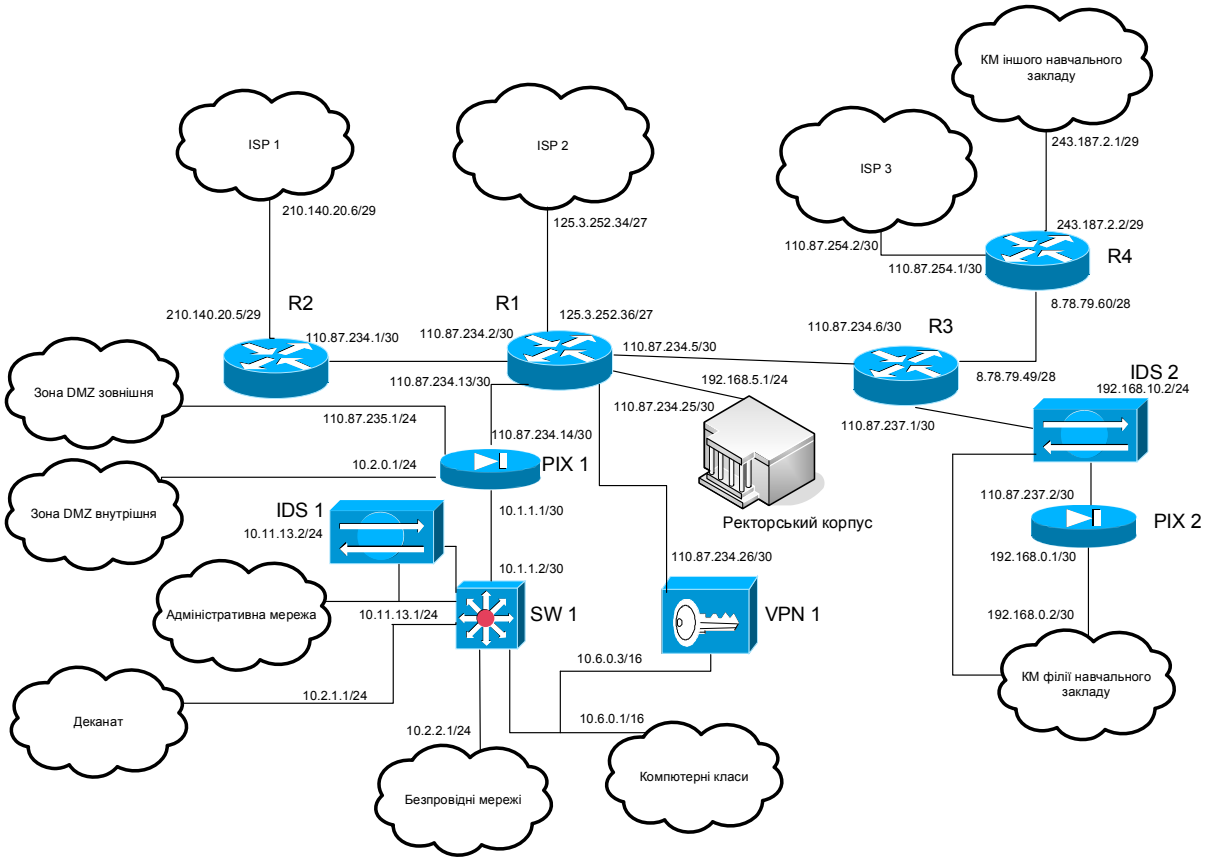

Рисунок 4 - Захищена КМ навчального закладу.

Для застосування пристроїв з метою створення захищеної КМ здійснена модифікація її структури. Тут заслуговує уваги усунення другого резервного шляху з роутера R2 до комутатора, оскільки у випадку його залишення потрібно було би використовувати другий firewall. Тоді можна було б застосувати на обидвох PIX-ах механізм failover чи запобігання аваріям. Такі аварійні ситуації виникають нечасто завдяки випробуваним і стабільним засобам.

Першою лінією захисту є, зазвичай, пограничний маршрутизатор, роль якого тут виконує R1. На ньому повинні бути сконфігуровані попередні положення політики безпеки, зокрема: неможливість логування до PIX-а з Internet. Це здійснюємо завдяки написанню правил в листі доступу:

R1(config)# access-list 101 deny ip any host 110.87.234.14
R1(config)# access-list 101 deny ip any host 110.87.235.1
R1(config)# access-list 101 permit any any
R1(config)# interface FastEthernet0
R1(config-if)# ip access group 101 out

Завдяки цьому забезпечується відкидання всіх пакетів, спрямованих з мережі Internet до firewall-а PIX. На жаль, в даному випадку відсутня можливість віддаленого адміністрування.

Черговим елементом на шляху передавання пакету до КМ навчального закладу є firewall, який виконує функцію головного пристрою захисту КМ від можливих загроз. На ньому знаходяться головні правила доступу. Ось частина з них:

PIX_1(config)# nameif ethernet0 outside security0
PIX_1(config)# nameif ethernet1 inside security100
PIX_1(config)# nameif ethernet2 DMZZ security30
PIX_1(config)# nameif ehernet3 DMZW security60
PIX_1(config)# ip address outside 110.87.234.14 255.255.255.252

```
...
PIX_1(config)# fixup protocol ftp 21
PIX_1(config)# fixup protocol http 80
...
PIX_1(config)# access-list stand_internet permit 10.0.0.0 255.0.0.0  any eq www
...
PIX_1(config)# access-group stand_internet in interface inside
...
PIX_1(config)# access-list dmzz_do_dmzw permit host 110.87.235.2 host 10.2.0.3 eq 3306
...
PIX_1(config)# access-group dmzz_do_dmzw in interface DMZZ
...
PIX_1(config)# logging host DMZW 10.2.0.4
PIX_1(config)# logging trap informational
PIX_1(config)# logging on
...
PIX_1(config)# access-list do_serw_z_internetu permit any  host 110.87.235.2 eq www
...
PIX_1(config)# access-group do_serw_z_internetu in interface outside
...
PIX_1(config)# sysopt security fragguard
PIX_1(config)# fixup protocol smtp 25
PIX_1(config)#  ip audit attack drop
PIX_1(config)# ip audit info alarm
...
PIX_1(config)# enable password skomp3li$ko23*wane__haasl5%o
```

Тут частина конфігурації з PIX-а 1. Спочатку здійснюється конфігурація інтерфейсів, зокрема, найбільш захищеного (security 100) і найменш захищеного (security 0). За замовчуванням пакет може переходити з інтерфейсів з вищим ступенем безпеки до інтерфейсів з меншою мірою захисту, а зворотній шлях є забороненим. У подальшому PIX довідується, що на відповідних портах буде здійснюватися відповідний рух, а тому може результативно аналізувати його під власним кутом зору. Також відає про те, що повинен прослуховувати рух на цих портах. В подальшому кожний хост з внутрішньої КМ отримує доступ до сторінок WWW. Також відбувається доступ в зоні DMZ (внутрішній) хостові, який є сервером WWW і здійснює авторизацію за допомогою бази MySQL. З цією метою застосовано логування до серверу syslog на одному з серверів у внутрішній мережі DMZ. Надається дозвіл на доступ до сервера WWW з Internet. В подальшому визначено правила захисту від таких атак, як: охорона перед атакою фрагментації пакетів (teardrop), нагляд за коректним зв'язком з поштовими серверами та правильністю поштових відомостей, захист від зловмисників при виявленні такої атаки – тоді такий підозрілий пакет відкидається і висилається alert до сервера логів. На практиці важливим є завдання переховування паролю доступу до firewall-у у вигляді зашифрованого тексту.

IDS працює у режимі сенсора і використовується лише один інтерфейс, однак SW1 функціонує на цьому порті таким чином, що весь рух, який проходить через нього, копіюється на порт, на котрому прослуховує IDS. Такий підхід не обтяжує мережі, а навпаки є ефективним щодо навчального закладу, оскільки здійснюється моніторинг КМ з її середини. На жаль, така конфігурація не дає змоги швидкої реакції, наприклад, шляхом переривання зв'язку через IDS. IDS-2 працює в режимі in-line, властиво IDS і є в стані приймати активну участь у відкиданні або дозволі руху пакетів через нього. Головним завданням адміністратора тоді є актуалізація системи і сигнатур атак, а також моніторинг і застосування відповідних кроків в ситуації, що появилася.

Концентратор VPN1 дозволяє віддалене під'єднання до занять, які проводяться в навчальному закладі через визначених користувачів його бази даних. Завдяки цьому можна безпечно використовувати ресурси всієї внутрішньої мережі згідно з привілеями

в локальних мережах комп'ютерних класів. Подібно до IDS, конфігурація опирається на інтерфейсі ssl/web, що є безпечним в даній реалізації.

Висновки.

Запропонована система безпеки КМ дозволяє захиститися перед зловмисниками з Internet, завдяки використанню пристроїв Cisco IDS/PIX. Вона гарантує процес безпеки, який передбачає постійне застосування чотирьох засад, що базуються на політиці безпеки.

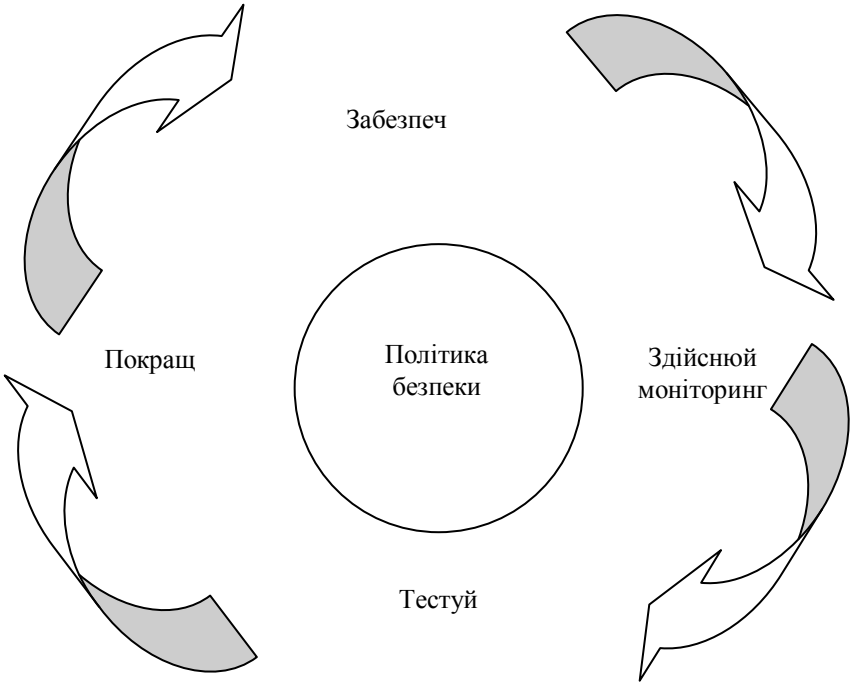

Рисунок 5 - Процес безпеки КМ.

Література

1. „Wielka księga firewalli" R.J. Shimorski, D. Littlejohn Shinder, Dr. T.W. Shinder, A. Carasik-Henmi. Wydawnictwo Helion, 2004, 1376 st.
2. „Akademia sieci Cisco CCNA semestry 1 & 2 semestr" Małgorzata Dąbkowska-Kowalik wydawca: Mikom ISBN: 8372794324 wyd.III. 2004, 784 st.
3. „Akademia sieci Cisco CCNA semestry 3 & 4 semestr" Cisco Press wydawca: Mikom ISBN:8372794286 wyd.III 2004, 934 st.
4. http://pl.wikipedia.org
5. „Podręcznik administratora bezpieczeństwa teleinformatycznego" Krzysztof Liderman wydawnictwo Mikom, ISBN 83-7279-277-8, Warszawa, grudzień 2003, 1023 st.
6. Biuletyn Instytutu Automatyki i Robotyki Wojskowej Akademii Technicznej w Warszawie Nr 17/2002 artykuł: "System bezpieczeństwa teleinformatycznego" K. Liderman
7. „Ściany ogniowe Cisco PIX. Certyfikat CCSP – ZAAWANSOWANA TEMATYKA" G. Bastien, Ch.Abera Degu Wydawnictwo MIKOM grudzień 2004 ISBN 83-7279-452-9. 2004, 1240 st.
8. http://www.cisco.com.

Одержано 01.03.2006 р.