УДК 004.7.056.5

Остапук О. І. ORCID: 0000-0001-6557-9525 (ВІТІ)
Плугова О. Б. ORCID: 0000-0001-7848-7806 (ВІТІ)
Лазута Р. Р. ORCID: 0000-0003-3254-9690 (ВІТІ)
д-р техн. наук Міночкін А. І. ORCID: 0000-0001-5723-5052 (ВІТІ)

ВАРІАНТ АРХІТЕКТУРИ ТА ФУНКЦІОНУВАННЯ ПІДСИСТЕМИ УПРАВЛІННЯ МЕРЕЖЕВОЮ БЕЗПЕКОЮ

В останні роки спостерігається стрімке зростання інформаційних та особливо телекомунікаційних технологій, що базуються на порівняно простих, зрозумілих та доступних алгоритмічних, технічних рішеннях, реалізованих в стандартних протоколах мережі Internet (електронна пошта, SMTP, IMAP, файловий обмін FTP, маршрутизація RIP, OSPIF та ін.). Все це призвело до їх виключного застосування практично в усіх створюваних мережах зв'язку як загального користування, так і, на жаль, в телекомунікаційних мережах системи зв'язку спеціального призначення, для яких відкритість, практична незахищеність, а не рідко й недостатня ефективність застосування протоколів обов'язково передбачає використання ресурсоємних системотехнічних рішень, що забезпечить задану ефективність та інформаційну безпеку функціонування таких мереж.

Функціонування мультисервісних мереж з високими показниками за ефективністю в умовах інформаційної протидії та досить жорстоких вимог до них з боку користувачів (посадових осіб органів управління) можливе тільки при вирішенні цілого комплексу задач із забезпечення інформаційної безпеки.

Вирішальну роль в цьому процесі відводиться автоматизованій системі управління мережею.

У статті розглянуто варіант архітектури та функціонування підсистеми управління мережевою безпекою за стандартами ISO.

Ключові слова: *мультисервісні мережі, інформаційна безпека, управління мережевою безпекою.*

A. Ostapuk, O. Pluhova, R. Lazuta, A. Minochkin. **Version of architecture and functioning of the network security management subsystem.**

In recent years, there has been a rapid growth of information and especially telecommunications technologies based on relatively simple, clear and accessible algorithmic, technical solutions implemented in standard Internet protocols (e-mail, SMTP, IMAP, FTP file sharing, RIP routing, OSPIF and others) all This has led to the exclusive use of almost all existing communication networks, both public and, unfortunately, in telecommunications networks of special purpose communication systems, for which openness, practical insecurity, and often insufficient efficiency of protocols necessarily involves the use of resource-intensive system solutions. will provide the set efficiency and information security of functioning of such networks.

Operation of multiservice networks with high efficiency in the conditions of information counteraction and rather rigid requirements to them from users (officials of bodies of Management), is possible only at the decision of the whole complex of tasks on maintenance of information security.

The automated network management system plays a crucial role in this process.

The article considers the variant of architecture and functioning of the network security management subsystem according to ISO standards.

Keywords: *multiservice networks, information security, network security management.*

Постановка завдання. Достатня складність мереж, що входять до складу мультисервісних мереж зв'язку (абонентські мережі, мережі доступу, транспортна мережа, мережі послуг прикладного рівня) та впроваджуваних в них механізмів захисту інформації, збільшення кількості вразливостей, пов'язаних з використанням стандартних протоколів, наявність потенційних помилок чи «закладок» в програмному забезпеченні засобів телекомунікацій, засобів надання послуг зв'язку та управління, можливості супротивника в кібератаках обумовлює необхідність розробки достатньо складних автоматизованих комплексів управління мережевою безпекою. До складу цих комплексів, як правило, повинні входити потужні адаптивні засоби виявлення та аналізу загроз.

Такі комплекси здатні не тільки контролювати працездатність засобів захисту інформації в кожній мережі, а й суттєво підвищити захищеність елементів мультисервісної мережі зв'язку від інформаційного впливу, існуючих помилок в конфігурації кожної мережі, сприяти виявленню можливих шляхів атакуючих дій різних категорій супротивника, визначенню критичних мережевих ресурсів, а також здатність підготовки даних з коригування або вибору нової політики безпеки, адекватній існуючій загрозі. Стаття направлена на пошук шляхів реалізації головних задач управління мережевою безпекою в рамках системи управління.

Мета статті: пошук шляхів реалізації головних задач управління мережевою безпекою в рамках системи управління.

Викладення основного матеріалу. Стандарти ISO з управління мережевою безпекою (ISO 7498-2, ISO 10164-7, 10164-8, 10164-9, ISO/IEC 17799:2000 та інші), а також рекомендації МСЕ – Т (Х.800, М.3016.0-М.3016.4, Y.2701 та ін.) висувають ряд вимог до архітектури безпеки, механізмів її забезпечення.

Управління мережевою безпекою передбачає включення до складу 8 прикладних процесів «механізмів безпеки» (рис. 1) [1; 2].

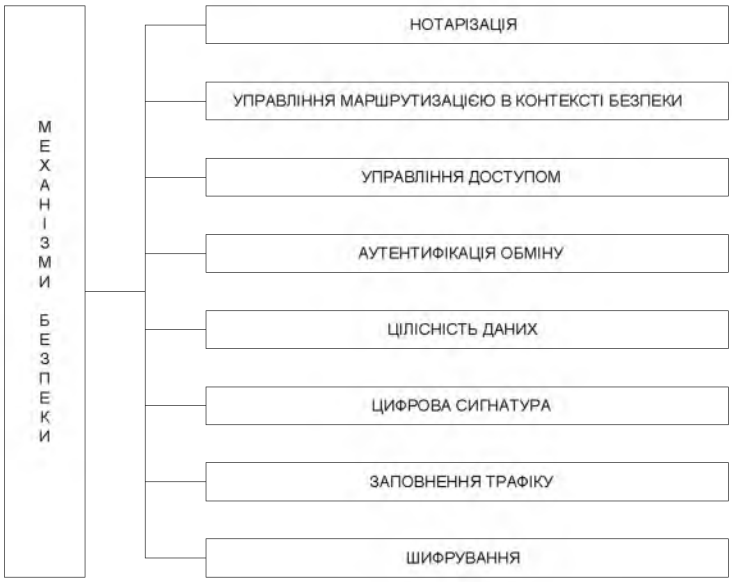

Рис. 1. Вбудовані механізми безпеки

Механізм «Нотарізація» гарантує, що третя особа для гарантії правильності інформації використовує не тільки її зміст, а також відомості про джерело інформації, хронометраж та доставку адресату.

Механізм «Управління маршрутизацією в контексті безпеки» містить правила, які дозволяють при передачі пакетів (повідомлень) уникати певних підмереж, направлень чи трактів передачі інформації з метою забезпечення заданого рівня безпеки.

Механізм «Управління доступом» використовується для запобігання несанкціонованому доступу до ресурсу мережі (якщо доступ заборонено) або запобігти використанню його несанкціонованим способом.

Механізм «Аутентифікація обміну» використовується тоді, коли ідентичність особи чи прикладного процесу повинна бути перевіреною раніше, ніж наданий доступ до певного ресурсу мережі.

Механізм «Цілісність даних» використовується, щоб гарантувати, що дані про обмін, взаємодію чи просто змінені несанкціонованим способом.

Механізм «Цифрова сигнатура» (або унікальний набір байтів) використовується для гарантії того, що отримувач даних – саме та особа, кому адресовані ці дані, і що пакет даних не був змінений чи пошкоджений. Для цього використовуються криптографічні методи захисту інформації в протокольному блоці (PDU).

Механізм «Заповнення трафіку» використовує спеціальні біти, октети чи інші блоки даних, які додаються в кінці протокольних блоків (PDU).

Механізм «Шифрування» використовується для закриття даних чи іншої інформації криптографічними методами. Функціонування підсистеми управління мережевою безпекою повинно забезпечуватися рядом служб безпеки, які підтримують прикладні процеси управління (рис. 2) [3; 4].

Рис. 2. Служби підсистеми управління мережевою безпекою

Служба «Аутентифікація рівноправних об'єктів» використовується для гарантування зв'язку з рівноправним об'єктом, як єдиним, що допустимий.

Служба «Аутентифікація достовірності даних» використовується для того, щоб гарантувати, що джерело даних саме те, що замовив користувач.

Служба «Управління доступом» гарантує, що несанкціонований користувач не отримає доступ до ресурсу мережі.

Служба «Конфіденційність з'єднання» гарантує, що дані N-го користувача мережі в К-му з'єднанні з М-користувачем чи з J-ресурсом мережі засекречені.

Служба «Конфіденційність без встановлення з'єднання» гарантує конфіденційність даних кожного кінцевого користувача.

Служба «Конфіденційність вибраної області» використовується, щоб забезпечити конфіденційність деяких елементів даних всередині можливих баз даних.

Служба «Конфіденційність потоку трафіку» гарантує, що буде забезпечене запобігання аналізу трафіку користувача потенційним порушенням.

Служба «Цілісність з'єднання з відновленням» гарантує, що всі дані кінцевого користувача відносно К-го з'єднання будуть захищені від змін чи вставок. Ця служба також вдається до спроб відновлення даних у випадку необхідності.

Служба «Цілісність з'єднання без відновлення» виконує ті самі функції, але без відновлення даних в цій службі.

Служба «Цілісність вибраних полів з'єднання» гарантує збереження вибраних полів всередині блоків даних послуг (SDU) шляхом захисту від змін, видання, вставки чи відтворення.

Служба «Цілісність без встановлення з'єднання» забезпечує збереження одиночного SDU відносно змін і відтворення.

Служба «Цілісність вибраних полів без встановлення з'єднання» гарантує, що вибрані поля всередині протокольного блоку даних PDU без встановлення логічного з'єднання не змінені.

Служба «Підтвердження з доказом походження» надає послугу, що забезпечує безсумнівну ідентифікацію відправника і гарантує, щоб він не зміг спростувати факт передачі даних.

Служба «Підтвердження з доказом доставки» надає відправнику даних послугу, яка гарантує, що дані були доставлені й отримувач не зможе заперечувати отримання даних.

Служба «Специфіка мережі» забезпечує адаптацію інших служб підсистеми управління мережевою безпекою до особливостей функціонування конкретної телекомунікаційної мережі мультисервісної мережі зв'язку.

Підсистема управління мережевою безпекою з одного боку є підсистемою оперативно-технічного управління, а з іншого – підсистемою системи комплексної безпеки телекомунікаційної мережі й повинна постійно взаємодіяти як з елементами системи управління, так і з засобами забезпечення безпеки (рис. 3) [5].

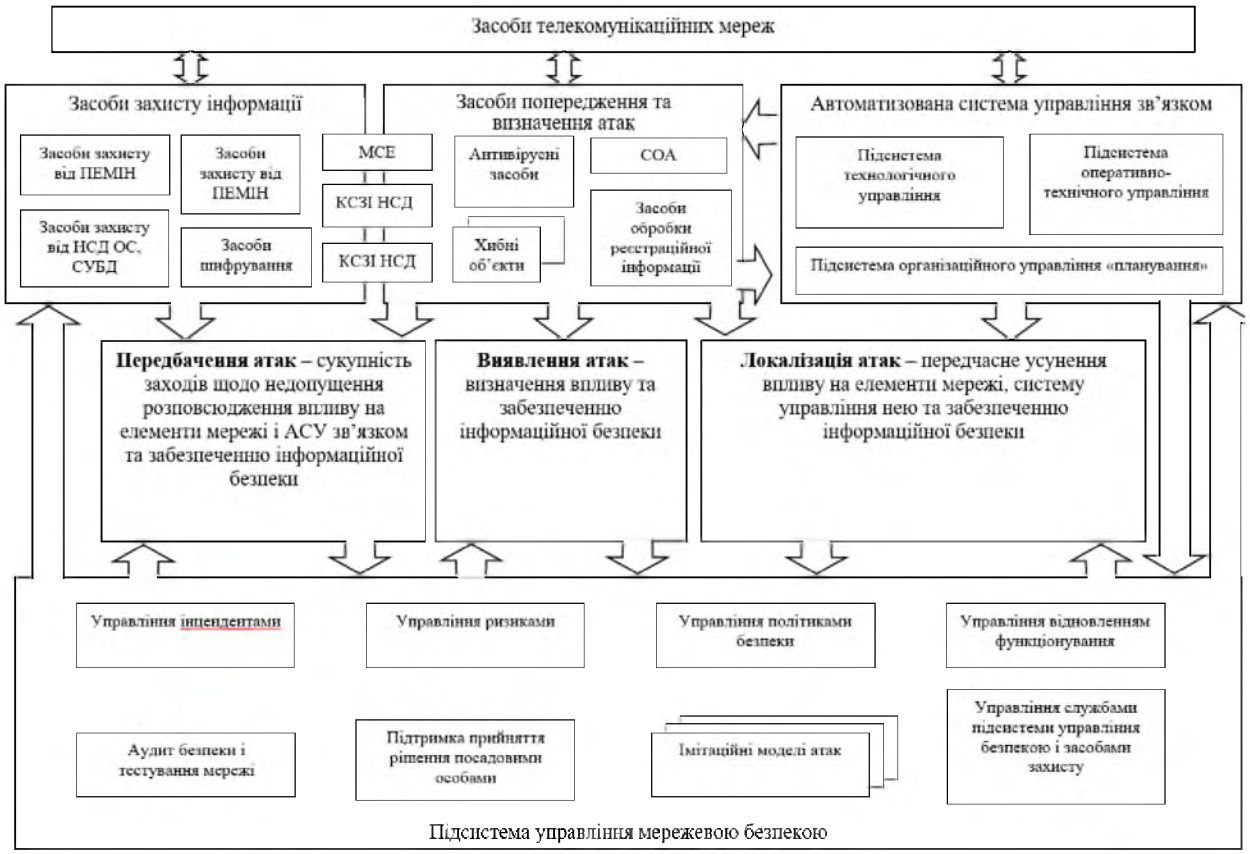

Рис. 3. Функціональна архітектура підсистеми управління мережевою безпекою

Функціонально архітектура підсистеми управління мережевою безпекою, як правило, містить різні програмно-апаратні засоби, що виконують функції управління службами підсистеми та засобами захисту, ризиками, конфліктами, політиками безпеки, відновленням функціонування мережі після впливу та атак на неї; здійснює аудит безпеки та тестування мережі, підтримку обґрунтованих рішень посадовими особами по безпеці, а також імітаційне моделювання наслідків атак і втручання потенційних порушників.

Джерелом інформації моніторингу стану мережі в контексті безпеки є дані, отримані від комплексів засобів захисту інформації від несанкціонованих дій (КЗЗІ НД), випадкових впливів та аварійних ситуацій (КЗЗІ ВВАС), від підсистеми технологічного управління, від засобів попередження та виявлення атак на елементи телекомунікаційної мережі та її систему управління (систему виявлення атак або СВА, антивірусні засоби і т. п.)

Логічна архітектура підсистеми управління мережевою безпекою складається із керуючих та керованих елементів і будується за схемами «агент – менеджер» та «клієнт – сервер» (рис. 4) [6].

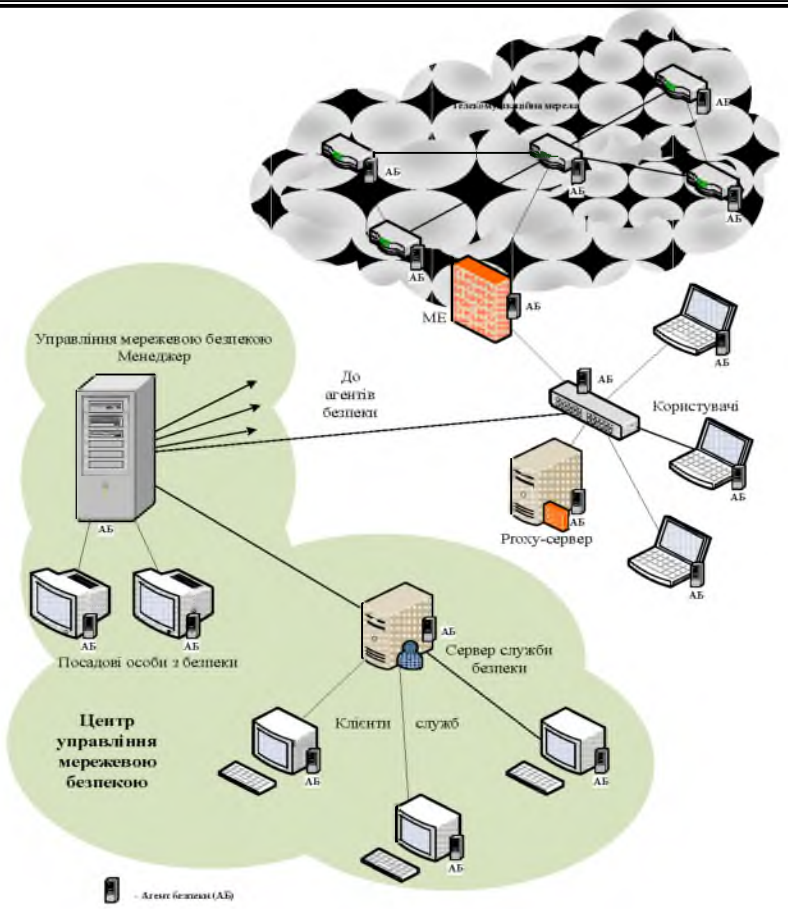

Рис. 4. Логічна архітектура підсистеми управління мережевою безпекою

Локальний агент безпеки (АБ) являє собою програму, що розміщена на кінцевому пристрої (клієнт, сервер, шлюз) та виконує наступні функції захисту:

- аутентифікація об'єктів політики безпеки, включаючи інтеграцію різних сервісів аутентифікації;
- визначення користувача в мережі та подій, пов'язаних з даним користувачем;
- забезпечення централізованого управління засобами безпеки та контролю доступу;
- управління ресурсами в інтересах додатків, підтримка управління доступом до ресурсів прикладного рівня;
- захист та аутентифікація трафіку;
- послідовне протоколювання, моніторинг, тривожна сигналізація;
- локальний антивірусний захист.

Одним із головних модулів локального агента є модуль, який інтерпретує локальну політику безпеки і розподіляє виклики між рештою модулів та компонентами.

АБ, встановлені на різних елементах мережі, направлені на захист даних та інших інформаційних ресурсів. Так, АБ, встановлений на будь-якому персональному комп'ютері, орієнтований на захист користувача, що є клієнтом в додатках «клієнт – сервер».

АБ, встановлений на сервері додатків, орієнтований на забезпечення захисту серверних компонентів розподілених додатків.

АБ, встановлений на шлюзовому комп'ютері, забезпечує розв'язку сегментів мережі всередині різних об'єктів чи між об'єктами.

Головною функцією центру управління є опис, зберігання та управління мережевою політикою безпеки в масштабі всієї мережі, трансляція мережевої політики в локальні політики безпеки пристроїв захисту, завантаження пристроїв захисту та контроль стану всіх агентів безпеки. Для організації розподіленої схеми управління безпекою в мережі може бути встановлено декілька серверів управління мережевою безпекою.

Висновок. Розглянутий варіант архітектури підсистеми управління мережевою безпекою може бути використаний при функціонуванні мультисервісних мереж з високими показниками щодо ефективності в умовах інформаційної протидії та досить жорстких вимог до них з боку різних користувачів (посадових осіб органів управління).

Ефективність функціонування підсистеми управління мережевою безпекою може бути оцінена деяким функціоналом якості, розрахунок якого буде проведено в подальших дослідженнях.

Напрями подальших досліджень: відпрацювання методики ефективності функціонування підсистеми управління мережевою безпекою.

ЛІТЕРАТУРА

1. ДСТУ ISO/IEC 7498-2-99. Інформаційні технології. Взаємозв'язок відкритих систем. Базова еталонна модель. 4.2. Архітектура захисту інформації.

2. ДСТУ ISO/IEC 10164-7. Інформаційні технології. Взаємозв'язок відкритих систем. Адміністративне керування системами. Частина 7. Функція сповіщення за допомогою сигнального пристрою про захист. [Чинний від 01.01.2015]. Київ: Держстандарт України, 2015.

3. ДСТУ ISO/IEC 10164-8:2015. Інформаційні технології. Взаємозв'язок відкритих систем. Адміністративне керування системами . Частина 8. Функція аудиторського спостереження за безпекою. [Чинний від 01.01.2015]. Київ: Держстандарт України, 2015.

4. ДСТУ ISO/IEC 10164-9:2015. Інформаційні технології. Взаємозв'язок відкритих систем. Адміністративне керування системами. Частина 9. Об'єкти й атрибути для контролю за доступом. [Чинний від 01.01.2015]. Київ: Держстандарт України, 2015.

5. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей. ИД «Форум»: ИНФА – М, 2008.

6. Буренин А. Н., Винниченко А. В. Проблемы управления информационной безопасностью в процессе функционирования систем управления телекоммуникационными сетями специального назначения // Телекоммуникационные технологии. 2018. № 4. С. 12–20.