УДК 004.056.53
DOI: 10.31673/2409-7292.2025.031342

Пархоменко І.І.

ПРИНЦИПИ ПОБУДОВИ ЗАХИЩЕНИХ КАНАЛІВ ПЕРЕДАЧІ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В УМОВАХ ДИНАМІЧНОГО СЕРЕДОВИЩА

Сучасні системи передачі конфіденційної інформації в умовах зростаючої кількості кібератак та збоїв у функціонуванні інфраструктури вимагають нових принципів побудови захищених каналів. Потреба в динамічному, стійкому та адаптивному управлінні передачами даних особливо актуальна в контексті розвитку критичної інформаційної інфраструктури, розподілених мереж та мобільних комунікацій. Ця стаття пропонує концепцію побудови захищених каналів, адаптовану з акцентом на адаптивність, оптимальність, стійкість і розподіленість систем управління. Для формалізації принципів побудови захищених каналів використано системний аналіз та аналітико-синтетичний метод. Здійснено трансформацію підходів з подальшим моделюванням процесів адаптивного управління каналами, що функціонують в умовах змінного середовища. Функціональні компоненти включають моніторинг стану мережі, адаптивне керування ресурсами, автоматичне реагування на загрози, та ієрархічну структуру прийняття рішень.

Ключові слова: захист інформації, кібербезпека, загрози, прийняття рішень, конфіденційність, цілісність.

Вступ

У сучасному цифровому середовищі інформація стала стратегічним ресурсом, а забезпечення її конфіденційності, цілісності та доступності – одним із ключових завдань інформаційної безпеки державного, корпоративного й особистого рівнів. Зростання обсягів переданої інформації, поширення бездротових технологій, мобільність користувачів, динамічність мережевої інфраструктури та поява складних гібридних загроз обумовили необхідність перегляду традиційних підходів до побудови каналів зв’язку. В таких умовах особливого значення набуває створення захищених каналів передачі, здатних забезпечити надійність і безпеку комунікації навіть у змінному, агресивному або частково невизначеному середовищі.

Сучасні рішення, такі як TLS, IPsec, VPN-технології, забезпечують базовий рівень криптографічного захисту та шифрування трафіку. Однак ці засоби, як правило, орієнтовані на фіксовані умови функціонування мережі, що не дозволяє їм ефективно реагувати на зовнішні впливи, зокрема на зміну завадової обстановки, втрати зв’язку, DDoS-атаки, перебої живлення або фізичне переміщення вузлів мережі. Більше того, зростає кількість атак, спрямованих не лише на перехоплення даних, а й на спотворення процесів маршрутизації, компрометацію керуючих сигналів і дестабілізацію процесів передачі. У відповідь на ці виклики виникає потреба у створенні каналів зв’язку, що не лише шифрують дані, але й мають здатність адаптуватися до умов середовища, самостійно перебудовувати топологію з’єднань, управляти пріоритетами трафіку, виявляти та нейтралізовувати загрози.

Аналіз літературних джерел та формулювання проблеми

Питання побудови захищених каналів передачі конфіденційної інформації є одним із ключових напрямів сучасної теорії та практики інформаційної безпеки. Базовим підходом, який широко застосовується у цивільному середовищі, є використання криптографічних протоколів, зокрема Transport Layer Security (TLS), Internet Protocol Security (IPsec), Secure Shell (SSH), а також віртуальних приватних мереж (VPN). У дослідженнях, представлених у працях [Goodin, 2017; Krawczyk et al., 2016], ці протоколи демонструють високий рівень захищеності при забезпеченні цілісності та конфіденційності переданої інформації в умовах фіксованого середовища. Однак більшість з них не передбачає гнучкої адаптації до змін завадової обстановки, не гарантує QoS (Quality of Service) для трафіку з різним пріоритетом, і не враховує вимог до стійкості мережі в умовах динамічного середовища або активного зовнішнього впливу.

Розширення поняття безпеки каналів зв’язку у напрямку стійкості та адаптивності стало предметом численних досліджень у сфері мобільних ad hoc мереж (MANET), бездротових сенсорних мереж (WSN), розподілених обчислень та IoT-середовищ. Наприклад, у роботах

Akyildiz et al. (2002), Hu et al. (2003), Wang et al. (2019) наголошується на важливості побудови маршрутів, стійких до атак типу “чорна діра”, “переповнення черги” та “селективне перехоплення”, проте більшість з розглянутих рішень мають вузькоспеціалізований характер, і не формують цілісної архітектури захищених каналів із урахуванням принципів системного управління.

У контексті динамічного управління трафіком і ресурсами мережі значна увага приділяється застосуванню технологій Software Defined Networking (SDN) та Network Function Virtualization (NFV), що дозволяють централізовано програмно переналаштовувати правила маршрутизації та розподілу трафіку. Праці authors such as Kreutz et al. (2015), Mijumbi et al. (2016) і Yazici et al. (2020) підкреслюють, що SDN/NFV підходи забезпечують гнучкість у керуванні трафіком, проте питання безпеки таких систем залишаються актуальними, зокрема з огляду на вразливість контролера, недостатню стійкість до деструктивних змін у середовищі та залежність від централізованих сценаріїв обробки загроз.

Поряд з інфраструктурними підходами активно розвивається напрям застосування штучного інтелекту та машинного навчання в задачах захисту каналів зв’язку. Зокрема, застосування нейронних мереж, байєсівських моделей, підкріплювального навчання дозволяє виявляти аномалії в трафіку, здійснювати прогнозування атак і здійснювати адаптивне переналаштування каналів. У працях Alshamrani et al. (2020), Vinayakumar et al. (2019) наведено приклади високоефективних моделей IDS/IPS, проте їх інтеграція в реальні комунікаційні канали обмежується обчислювальними витратами та нестачею пояснюваності рішень.

Окрему групу складають дослідження, присвячені побудові протоколів безпечної маршрутизації у складних динамічних умовах. Наприклад, протоколи SEAD, ARAN, SAODV у рамках MANET-підходів спрямовані на верифікацію маршруту, а не лише на шифрування переданих даних. Однак ці підходи залишаються переважно дослідницькими і не охоплюють системного управління ресурсами, що критично важливо для повноцінного функціонування захищених каналів у реальному часі.

Таким чином, проаналізовані дослідження охоплюють окремі аспекти проблеми: криптографічну безпеку, виявлення атак, адаптивне управління трафіком або ресурсами мережі. Водночас відсутня єдина системна концепція, яка б об'єднувала ці підходи в межах цілісної моделі управління каналами зв’язку з урахуванням динаміки середовища, багаторівневих загроз, вимог до стійкості, QoS, автономності та оперативності. У цьому контексті – адаптивність, адекватність, оптимальність, стійкість, розподіленість та ієрархічність – дозволяє запропонувати нові принципи побудови захищених каналів передачі конфіденційної інформації.

Таким чином, аналіз сучасних джерел свідчить про зростаючий інтерес до формалізації та систематизації принципів побудови захищених каналів передачі конфіденційної інформації на основі адаптивного управління в умовах динамічного інформаційного середовища.

Мета роботи та цілі дослідження

Метою статті є формалізація та систематизація принципів побудови захищених каналів передачі конфіденційної інформації на основі адаптивного управління в умовах динамічного інформаційного середовища.

Виклад основного матеріалу

У межах цього дослідження застосовано аналітико-синтетичний та системний підходи до розроблення принципів побудови захищених каналів передачі інформації, які функціонують у складних і змінних умовах мережевого середовища.

Ключовою дослідницькою гіпотезою є припущення, що концептуальні засади побудови систем зв’язку в умовах апріорної невизначеності можуть бути успішно адаптовані до цивільного середовища – зокрема для захисту даних у хмарних платформах, розподілених IoT-системах, критичній інфраструктурі, мобільному зв’язку та публічних комунікаціях.

© Пархоменко І.І. (2025) Принципи побудови захищених каналів передачі конфіденційної інформації в умовах динамічного середовища. Сучасний захист інформації, 3(63), 108–115. https://doi.org/10.31673/2409-7292.2025.031342

Побудова ефективних, стійких і гнучких каналів передачі конфіденційної інформації в умовах динамічного середовища потребує дотримання низки базових принципів. Ці принципи не є ізольованими, а формують цілісну методологію, що забезпечує не лише фізичну й криптографічну безпеку, а й управлінську ефективність системи зв'язку в умовах змінності, невизначеності та потенційної загрозливості середовища. Вони були сформульовані на основі узагальнення концепцій, закладених у системах оперативного управління військовим радіозв'язком, і адаптовані до цивільних IT-середовищ.

Розглянемо основні принципи її побудови [6, 9].

Принцип адаптивності

Адаптивність передбачає здатність системи реагувати на зміни умов зовнішнього середовища, параметрів каналу, стану вузлів або структури трафіку шляхом динамічного оновлення конфігурацій, маршрутів та політик безпеки. Реалізація цього принципу базується на використанні:

- телеметричних даних про стан каналів зв'язку;
- механізмів виявлення зниження якості обслуговування (QoS degradation);
- адаптивного шифрування й переключення між алгоритмами з різною криптостійкістю та обчислювальним навантаженням;
- зміни маршрутизації у відповідь на виявлену загрозу або затримку.

Завдяки адаптивності канал може зберігати працездатність навіть за умови часткової втрати мережевої інфраструктури або активного зовнішнього впливу.

Завдання адаптивного управління полягає в забезпеченні передачі заданої кількості повідомлень з необхідною якістю (достовірністю, оперативністю, надійністю і ін.). Виконання його залежить як від топології, інтенсивності зовнішніх впливів, інтенсивності потоків повідомлень, вимог до якості їх обслуговування, так і в значній мірі від ефективності управління.

Надалі під оперативним управлінням каналом передачі конфіденційної інформації розумітимемо процес динамічної організації та корекції такої цілеспрямованої дії на елементи об'єкту управління, в результаті якого забезпечується максимальне значення показника ефективності функціонування каналом передачі. Оперативне управління припускає рішення наступних завдань: формування і видачу дій, що управляють, відповідно до плану зміни стану каналу передачі; контроль стану каналу; формування і видачу додаткових управляючих впливів, призначених для ліквідації наслідків дії на канал передачі різних збурень, що призводять до зниження якості.

Мета управління в залежності від показника ефективності функціонування формулюється у вигляді:

$$\begin{aligned} W^*(T) &= \arg \min_{W^*(T)\in\Omega} P_{pom}(\Psi_i(T), W(T)); \\ W^*(T) &= \arg \min_{W^*(T)\in\Omega} \beta_E(\Psi_i(T), W(T)); \\ W^*(T) &= \arg \min_{W^*(T)\in\Omega} k_a(\Psi_i(T), W(T)), \end{aligned} \tag{1}$$

де Ω – обмеження, що накладаються на вибір управління, $i = \overline{1,m}$. Вони пов'язані з вимогами до якості обслуговування потоків даних і можливостями каналу передачі.

Принцип адекватності

Адекватність вказує на відповідність рішень, що приймаються системою, реальному стану середовища, у якому вона функціонує. Це передбачає:

- наявність актуальної, достовірної інформації про стан каналу;
- коректне перетворення цієї інформації в керуючі команди;

© Пархоменко І.І. (2025) Принципи побудови захищених каналів передачі конфіденційної інформації в умовах динамічного середовища. Сучасний захист інформації, 3(63), 108–115. https://doi.org/10.31673/2409-7292.2025.031342

- узгодженість цілей управління із наявними ресурсами та обмеженнями.

Недостовірна, застаріла або надмірно агрегована інформація призводить до неадекватних рішень, які знижують рівень захисту або погіршують параметри QoS.

Недостатня надійність і нестійкість роботи каналів передачі обумовлюється їх нестаціонарністю, а також сигналами природних і навмисних завад від сторонніх джерел. Тому потрібно забезпечувати контроль стану каналу передачі та якості його функціонування, а також передачу службової (контрольної) інформації про стан каналу.

Адекватність управління полягає в здатності цього процесу перетворювати інформацію стану в командну, на основі якої підсистема оперативного управління переходить у стан, що відповідає сформованої ситуації. Очевидно що при коректності всіх перетворень інформації стану в командну, але недостовірної інформації і (або) неправільних цілях, управління не буде адекватним. Таким чином, адекватність управління в істотному ступені залежить від достовірності і повноти інформації, коректності операцій перетворення інформації і їх послідовності, а також правильності цілей управління і траєкторій їх досягнення.

Принцип оптимальності

Принцип оптимальності формалізує компроміс між двома ключовими характеристиками керування каналом передачі: обсягом оброблюваної інформації (I) та часом реагування (T). У межах цього принципу система повинна:

- забезпечувати достатній рівень інформованості для прийняття обґрунтованих рішень;
- утримувати час збору й обробки інформації у межах, прийнятних для динамічної зміни стану каналу;
- мінімізувати витрати на службовий трафік і телеметрію.

У разі перевищення межі інформованості спостерігається зростання затримок у прийнятті рішень, що критично у разі інцидентів безпеки або відмов. Водночас, недостатній обсяг інформації збільшує ризик помилкових рішень. Тому метою є мінімізація сумарних втрат:

$$J = W_{\text{inf}} + W_{ded}(I,T) \to \min. \tag{2}$$

Адаптивне управління каналом передачі забезпечує відповідну корекцію режимів і алгоритмів функціонування її елементів. Кінцевою метою функціонування підсистеми оперативного управління каналом передачі може бути екстремум деякого функціонала (див. вирази (2)). Для реалізації принципу оптимальності управління потрібний збір значної кількості інформації про стан каналу передачі і рішення двох взаємопов'язаних завдань [6, 8].

1) Керуючі впливи в більшості способів управління виробляються на основі інформації про стан каналу передачі і зовнішнього середовища. Чим більше інформації має підсистема оперативного управління, тим більш обґрунтованим може бути рішення. Однак на одержання інформації витрачаються певні ресурси. Тому однією з умов ефективного управління є визначення оптимального об'єму службової (командної і вимірювальної) інформації, що відображає з необхідною повнотою поточний стан каналу передачі (оптимальна інформованість підсистеми оперативного управління).

Тоді перша умова оптимального управління:

$$W_0^2 = \min\left\{W_{\text{inf}}^2(T) + W_{dec}^2(T)\right\}, \tag{3}$$

де W_{inf} – витрати на отримання інформації про стан каналу, W_{dec} – втрати від необґрунтованості прийнятих рішень, I – обсяг обробленої підсистемою оперативного управління інформації, а T – час збору і обробки інформації та формування керуючих впливів.

2) Поряд з інформованістю підсистеми оперативного управління важливе значення має оперативність керування, тобто оперативність збору і обробки інформації стану та виробітки керуючих впливів. Тому другою умовою оптимальності є своєчасність збору, доставки, обробки службової інформації:

© Пархоменко І.І. (2025) Принципи побудови захищених каналів передачі конфіденційної інформації в умовах динамічного середовища. Сучасний захист інформації, 3(63), 108–115. https://doi.org/10.31673/2409-7292.2025.031342

$$W_0^{O'} = \min\left\{W'_{\inf}(O') + W'_{dec}(O')\right\}, \quad (4)$$

де $W'_{\inf}(O')$ – відображає вид залежності втрат в ефективності управління від часу реалізації дій, що управляють; $W'_{dec}(O')$ – залежності витрат на збір і обробку інформації стану.

Але при управлінні повинні враховуватися обидва ці умови, тобто

$$W^{opt} = \min_{I,T}(W_0^I + W_0^T). \quad (5)$$

Як видно, між повнотою інформації про стан каналу і своєчасністю вироблення дій, що управляють, існує протиріччя. Рішення цієї дилеми зазвичай забезпечується компромісом між оперативністю і обґрунтованістю дій, що управляють, що є одним з найбільш складних завдань.

Принцип стійкості

Стійкість визначається як здатність системи зберігати задані функціональні характеристики (затримки, надійність, цілісність, безперервність) при наявності зовнішніх і внутрішніх впливів. До таких впливів належать:

- активні атаки (DoS, MITM, spoofing);
- природні завади (перешкоди у бездротовому середовищі);
- часткові відмови або втрати вузлів;
- спотворення службової інформації.

З метою підвищення стійкості використовуються: надлишковість каналів, багаторівневе резервування, селективна маршрутизація, контроль цілісності, ізоляція пошкоджених сегментів, а також багатофакторна автентифікація на рівні службового трафіку.

Стійкість управління визначається здатністю підсистеми оперативного управління виконувати свої функції в складної, різко мінливій обстановці, в умовах наявності природних завад. Стійкість визначається живучістю, завадостійкістю і надійністю, під якими розуміється здатність вести управління в умовах впливу всіх видів завад і зберігаючи у встановлених межах значення всіх показників управління відповідно.

Принцип розподіленості

У складних мережах централізоване управління не здатне забезпечити оперативність реагування та масштабованість. Розподіленість полягає у тому, що вузли мають змогу:

- самостійно приймати рішення у межах локального контексту;
- обмінюватися службовою інформацією із сусідніми вузлами;
- здійснювати локальну маршрутизацію та адаптацію політик безпеки.

Цей принцип знижує навантаження на центральні компоненти та підвищує живучість системи в умовах фрагментації або деградації інфраструктури.

У функціональній структурі каналу передачі можна виділити два функціональні рівні, що знаходяться між собою в ієрархічному підпорядкуванні [160].

На першому (нижньому) рівні розв’язуються завдання контролю і управління окремими каналами передачі:

- визначення оптимальних режимів їх роботи;
- автоматичне входження в зв’язок, його ведення і відновлення;
- оперативний контроль процесів передачі інформації.

Вказані завдання розв’язуються децентралізовано для кожного напрямку або каналу передачі.

На другому (верхньому) рівні розв’язуються завдання контролю й управління мережею:

- оперативний контроль і прогнозування умов ведення передачі даних;
- оперативний аналіз інформаційної обстановки на мережі;
- формування обхідних шляхів передачі;

© Пархоменко І.І. (2025) Принципи побудови захищених каналів передачі конфіденційної інформації в умовах динамічного середовища. Сучасний захист інформації, 3(63), 108–115. https://doi.org/10.31673/2409-7292.2025.031342

- перерозподіл потоків, які поступають на елементи мережі.

Рішення задач другого рівня вимагає певної централізації (у розумному поєднанні з децентралізованими методами) контролю й управління.

Багатоцільова функціональна структура системи управління обумовлює достатньо велику кількість можливих варіантів побудови каналів передачі на мережевому рівні.

Принцип ієрархічності

Ієрархічна структура управління дозволяє розділити процеси на стратегічні (глобальні) та тактичні (локальні). На верхньому рівні система виконує:

- довгострокове планування ресурсів;
- прогнозування поведінки трафіку;
- корекцію політик маршрутизації.

На нижньому рівні – здійснюється негайне реагування, контроль стану каналів, формування реакцій на загрози. Таке розділення дозволяє уникнути перенавантаження керуючих систем і забезпечити масштабованість.

Необхідність забезпечення вимог до якості функціонування каналу передачі і створення множини функціональних можливостей оперативного управління по формуванню доцільної поведінки і плануванню послідовності операцій управління з активною адаптацією до впливів зовнішнього середовища і варіаціях поточного стану обумовлюють розробку засобів і методів оперативного управління, заснованих на комплексному застосуванні мір і засобів підвищення ефективності функціонування каналів передачі в умовах динамічного середовища.

Приклад застосування інтелектуальні енергосистеми (Smart Grid)

Інтелектуальні енергосистеми, або Smart Grid, є інфраструктурним прикладом складного технічного середовища, в якому обмін конфіденційною інформацією відбувається між великою кількістю розподілених, гетерогенних та автономних вузлів. Мережа таких вузлів включає смарт-лічильники, автоматизовані розподільчі підстанції, пристрої керування мікрогенерацією та балансувальні системи. Інформаційна взаємодія між ними має бути не лише ефективною з точки зору затримок, пропускної здатності та надійності, а й захищеною в умовах динамічної зміни мережевої топології, трафіку, рівня загроз і доступності каналів.

Типові загрози у цьому контексті включають: перехоплення команд диспетчеризації, несанкціоновану зміну даних лічильників, деструктивний вплив на канали передачі, DoS-атаки на центральні елементи керування, компрометацію службової інформації тощо. Складність полягає в тому, що система має не лише виявити аномалії або збої, а й перебудувати власну конфігурацію у спосіб, який зберігає цілісність та безпеку переданих даних.

На відміну від традиційної енергетичної інфраструктури, де управління здійснюється централізовано і переважно вручну, Smart Grid орієнтована на розподілену обробку, самоорганізацію й адаптацію. Це передбачає автоматичну реконфігурацію каналів, перехід між різними фізичними носіями (наприклад, від LTE до PLC або LoRaWAN), локальне прийняття рішень вузлами, а також забезпечення стійкості комунікацій навіть за відсутності зв’язку з головним центром керування. Окрім того, в умовах швидкої зміни навантаження на мережу та активного використання відновлюваних джерел енергії виникає потреба у каналізації службового трафіку з урахуванням його пріоритетності та критичності для системного балансу.

Застосування концепції побудови захищених каналів, заснованої на принципах управління в умовах невизначеності, дозволяє сформувати таку архітектуру комунікацій, що здатна до структурної та функціональної адаптації, підтримує сценарії ізоляції скомпрометованих сегментів, здатна до маршрутизації обхідними шляхами, враховує клас інформації при шифруванні й дозволяє досягати узгодженості дій у багаторівневій системі управління без централізованого втручання.

З технічної точки зору, впровадження такого підходу дозволяє:

- зменшити ймовірність втрати цілісності критичних телеметричних та керуючих даних;

© Пархоменко І.І. (2025) Принципи побудови захищених каналів передачі конфіденційної інформації в умовах динамічного середовища. Сучасний захист інформації, 3(63), 108–115. https://doi.org/10.31673/2409-7292.2025.031342

- знизити залежність від сталих маршрутів та конфігурацій;
- підвищити відмовостійкість системи у разі атак або природних збурень;
- забезпечити взаємодію вузлів, здатних самостійно виявляти та обходити загрози;
- оптимізувати обсяг службового трафіку для підтримки режимів реального часу.

Таким чином, інтелектуальні енергосистеми є прикладом середовища, де розроблена архітектура захищених каналів може бути не лише ефективно реалізована, але й виступає ключовим елементом забезпечення стійкого, надійного та безпечного функціонування усієї енергетичної екосистеми.

Результати та дискусія

Запропонована у цій статті концепція побудови захищених каналів передачі конфіденційної інформації формалізує підходи до проєктування інформаційно-комунікаційних систем нового покоління, що здатні ефективно функціонувати в умовах невизначеності, мобільності, обмежених ресурсів і активного протидіючого середовища. На відміну від традиційних підходів, орієнтованих переважно на фіксовані параметри середовища та статичні політики безпеки, модель, представлена в цій роботі, має функціональну здатність до динамічної реконфігурації на основі внутрішнього стану системи та зовнішніх впливів.

Однією з ключових відмінностей запропонованого підходу є розгляд системи захищеного зв'язку як *керованої динамічної структури*, яка не просто виконує функцію транспортування даних, а активно впливає на хід інформаційної взаємодії через управлінські рішення. Таким чином, підхід розширює розуміння комунікаційного каналу – від абстрактної транспортної сутності до активного елемента ситуаційної адаптації й захисту.

Порівняння з класичними механізмами безпечної передачі – такими як TLS, IPsec, VPN або ізольовані канали MPLS – свідчить, що хоча ці технології забезпечують базову конфіденційність і автентичність, вони не інтегрують у свою архітектуру принципи управління, адаптації або ієрархії рішень. Зокрема, вони не враховують пріоритетність трафіку, не оперують поняттями селективного резервування маршрутів, не мають механізмів локального прийняття рішень та зазвичай залежать від єдиного центру політик. Це суттєво обмежує їхню застосовність у сценаріях з високою динамікою мережевого середовища або у випадках часткової деградації інфраструктури.

Слід зазначити, що потенціал запропонованого підходу значною мірою залежить від можливості його масштабування та автоматизації. Подальші дослідження повинні зосередитись на:

- формалізації поведінкових шаблонів системи на основі сценарного моделювання;
- алгоритмах самоналаштування на основі машинного навчання або евристичного аналізу;
- верифікації стабільності системи за умов одночасної зміни кількох факторів ризику.

У цілому, обговорення результатів показує, що застосування запропонованих принципів є перспективним напрямом не лише з точки зору безпеки, а й з погляду системного підходу до побудови стійкої цифрової інфраструктури.

Висновки

У цій статті представлено системний підхід до побудови захищених каналів передачі конфіденційної інформації в умовах динамічного, нестабільного або загрозливого середовища. Здійснено формалізацію шести фундаментальних принципів – адаптивності, адекватності, оптимальності, стійкості, розподіленості та ієрархічності – як основи для проектування архітектур, здатних динамічно реагувати на зміни умов функціонування, підтримувати безперервність обміну та забезпечувати цілісність, конфіденційність і доступність інформації. Обґрунтовано, що ці принципи не лише покращують рівень безпеки, але й підвищують ефективність управління трафіком, ресурсами та загрозами у складних мережевих сценаріях.

Продемонстровано застосовність запропонованого підходу на прикладі інтелектуальних енергетичних систем (Smart Grid), де потреба в захищеній, адаптивній та автономній

© Пархоменко І.І. (2025) Принципи побудови захищених каналів передачі конфіденційної інформації в умовах динамічного середовища. Сучасний захист інформації, 3(63), 108–115. https://doi.org/10.31673/2409-7292.2025.031342

комунікації є критичною для підтримки стабільності та керованості розподіленої інфраструктури. Наведений приклад підтверджує, що дотримання зазначених принципів забезпечує не лише захист інформації, але й знижує залежність від централізованих структур, підвищує стійкість до збоїв і сприяє швидкому відновленню функціональності системи після інцидентів.

Подальші дослідження доцільно спрямовувати на математичну формалізацію процесів прийняття рішень у таких системах, розробку самонавчальних алгоритмів адаптації до загроз, а також експериментальну верифікацію запропонованих моделей у тестових середовищах з обмеженою довірою.

Перелік посилань

1. Goodin D. The sorry state of TLS security: Most servers are vulnerable [Електронний ресурс] // Ars Technica, 2017. Режим доступу: https://arstechnica.com/information-technology/2017/10/the-sorry-state-of-tls-security-most-servers-are-vulnerable/

2. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF) [Електронний ресурс] // RFC 5869. 2010. Режим доступу: https://datatracker.ietf.org/doc/html/rfc5869.

3. Akyildiz I. F., Su W., Sankarasubramaniam Y., Cayirci E. Wireless sensor networks: a survey // Computer Networks. 2002. Vol. 38, no. 4. P. 393-422. DOI: https://doi.org/10.1016/S1389-1286(01)00302-4.

4. Hu Y.-C., Perrig A., Johnson D. B. Ariadne: A secure on-demand routing protocol for ad hoc networks // Wireless Networks. 2005. Vol. 11. P. 21-38. DOI: https://doi.org/10.1007/s11276-004-0636-4.

5. Wang Y., Zhang Q., Li M., Sun Y. Survey on Security in Emerging Wireless Sensor Networks // Frontiers of Computer Science. 2019. Vol. 13, no. 3. P. 419-438. DOI: https://doi.org/10.1007/s11704-017-6242-z.

6. Kreutz D., Ramos F. M. V., Verissimo P. E., Rothenberg C. E., Azodolmolky S., Uhlig S. Software-defined networking: A comprehensive survey // Proceedings of the IEEE. 2015. Vol. 103, no. 1. P. 14-76. DOI: https://doi.org/10.1109/JPROC.2014.2371999.

7. Mijumbi R., Serrat J., Gorricho J. L., Bouten N., De Turck F., Boutaba R. Network Function Virtualization: State-of-the-art and research challenges // IEEE Communications Surveys & Tutorials. 2016. Vol. 18, no. 1. P. 236-262. DOI: https://doi.org/10.1109/COMST.2015.2477041

8. Yazici A., Aydin M. A., Akinci M. A survey on security and privacy issues in SDN-based networks // Computer Networks. 2020. Vol. 166. 106980. DOI: https://doi.org/10.1016/j.comnet.2019.106980.

9. Alshamrani A., Myneni S., Chowdhary A., Huang D. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities // IEEE Communications Surveys & Tutorials. 2020. Vol. 21, no. 2. P. 1851-1877. DOI: https://doi.org/10.1109/COMST.2019.2957221.

10. Vinayakumar R., Soman K. P., Poornachandran P. Applying deep learning approaches for network traffic classification and intrusion detection // Procedia Computer Science. 2019. Vol. 132. P. 20-27. DOI: https://doi.org/10.1016/j.procs.2018.05.135.

11. Лаптев О.А., Собчук В.В., Саланди И.П., Сачук Ю.В. Математична модель структури інформаційної сеті на основі нестаціонарної ієрархічної та стаціонарної гиперсети. Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. К.: ВІКНУ, Вип. 64, 2019. С. 124-132.

12. Lubov Berkman, Oleg Barabash, Olga Tkachenko , Andri Musienko, Oleksand Laptiev, Ivanna Salanda. The Intelligent Control System for infocommunication networks. International Journal of Emerging Trends in Engineering Research (IJETER) Volume 8. No. 5, May 2020. Scopus Indexed - ISSN 2347 – 3983. P.1920-1925.

13. Звіт ETSI Security Aspects of Channel Coding in 6G Systems (TR 103 756 V1.1.1). 2024.

14. Serhii Yevseiev, Khazail Rzayev, Oleksandr Laptiev, Ruslan Hasanov, Oleksandr Milov, Bahar Asgarova, Jale Camalova, Serhii Pohasii. Development of a hardware cryptosystem based on a random number generator with two types of entropy sources. Eastern-European journal of enterprise technologies. Vol.5 №9 (119). 2022 P. 6-16. ISSN (print) 1729-3774. ISSN (on-line) 1729-4061. DOI: https://doi.org/10.15587/1729-4061.2022.265774.

Надійшла 17.07.2025