УДОСКОНАЛЕННЯ ОЦІНЮВАННЯ РИЗИКУ ПРИСТРОЇВ У СИСТЕМАХ NETWORK ACCESS CONTROL КОРПОРАТИВНИХ БЕЗДРОТОВИХ МЕРЕЖ

Леонова А.О., В'юхін Д.О.
Харківський національний університет радіоелектроніки, Харків, Україна

Зростання кількості кінцевих пристроїв, що підключаються до корпоративних бездротових мереж, ускладнює контроль їхнього доступу до мережевих ресурсів. Рівень ризику таких пристроїв може змінюватися залежно від технічного стану, контексту підключення та поведінки в мережі, тому використання незмінних параметрів контролю не завжди забезпечує своєчасне реагування [1]. У зв'язку з цим важливого значення набуває застосування ризик-орієнтованих механізмів, які дають змогу адаптувати умови мережевого доступу та інтенсивність повторного контролю до поточного стану кінцевого пристрою.

Метою доповіді є удосконалення контролю доступу кінцевих пристроїв у корпоративних бездротових мережах шляхом застосування різних політик і рівнів доступу залежно від оціненого ризику. Крім того, пропонується адаптивно змінювати інтервал повторної перевірки пристрою: скорочувати його за підвищеного або зростаючого ризику та збільшувати за низького і стабільного рівня ризику.

Системи NAC призначені для контролю доступу користувачів і кінцевих пристроїв до ресурсів корпоративної мережі. Їх використання дозволяє ідентифікувати пристрої, перевіряти їхній стан і відповідно до встановлених політик визначати допустимий рівень мережевого доступу. Окрім цього, системи NAC можуть здійснювати оцінювання ризику пристрою, періодично повторно перевіряти його та коригувати рівень доступу залежно від отриманого результату [2].

Для формування оцінки ризику можуть використовуватися різні характеристики кінцевого пристрою. Зокрема, показник ризику може формуватися з урахуванням установлених застосунків, використання шифрування, відкритих портів та стану оновлень [2]. Отже, набір окремих характеристик пристрою може бути узагальнений у показник, що надалі використовується під час прийняття рішення щодо його мережевого доступу.

Важливою складовою NAC є повторне оцінювання стану кінцевого пристрою після надання доступу. У Cisco ISE Posture механізм Periodic Reassessment виконує повторну перевірку через визначений адміністратором інтервал від 1 до 24 годин. Механізм Continuous Reassessment забезпечує подієве виявлення окремих змін, а для параметрів, що потребують періодичного опитування, застосовується інтервал 10 хвилин. До таких параметрів належать, зокрема, стан антивірусного програмного забезпечення, шифрування диска, брандмауера та керування оновленнями [3].

Таким чином, у наявних механізмах можуть застосовуватися як періодичні, так і покрокові перевірки. Однак за періодичного переоцінювання інтервал задається конфігурацією і безпосередньо не визначається поточним інтегральним ризиком конкретного пристрою. Це створює передумови для дослідження підходу, за якого періодичність подальшого контролю залежить від поточного ризику пристрою та характеру зміни цього ризику.

Методологічною основою формування оцінки ризику може бути NIST SP 800-30 Rev. 1. У документі до факторів ризику віднесено загрози, вразливості, імовірність, потенційний вплив та умови, що сприяють реалізації загроз. NIST допускає використання якісних, кількісних та напівкількісних підходів до оцінювання. У межах такого оцінювання можуть застосовуватися числові шкали, а конкретні алгоритми об’єднання окремих факторів визначаються відповідно до обраної моделі ризику [4].

Можливість використання динамічної оцінки ризику під час керування доступом продемонстровано в моделі Adaptive Risk-Based Access Control (AdRBAC). Для формування оцінки використовуються контекст користувача, критичність ресурсу, критичність виконуваної дії та історія ризику. Отримане значення порівнюється з політиками ризику для прийняття рішення щодо доступу, а після його надання передбачається моніторинг поведінки користувача протягом активної сесії [5].

Одним із підходів до числового оцінювання ризику в системах risk-based access control є застосування ANFIS-моделі. Її вхідними факторами є контекст користувача, критичність ресурсу, критичність дії та історія ризику. На виході формується числове значення ризику, яке використовується для прийняття рішення про доступ [6]. Це підтверджує можливість використання інтегрального числового показника як основи для адаптивного керування доступом.

Проведений аналіз показує, що інтегральна оцінка ризику вже використовується для прийняття рішень щодо доступу, а стан кінцевих пристроїв може переоцінюватися періодично або контролюватися майже безперервно. Водночас у розглянутих джерелах не виявлено підходу, за якого поточний інтегральний ризик кінцевого пристрою та швидкість його зміни безпосередньо використовуються для розрахунку індивідуального інтервалу наступного повторного оцінювання. Тому пропонується доповнити процес risk-based контролю механізмом адаптивного визначення такого інтервалу.

Інтегральний показник ризику кінцевого пристрою пропонується визначати як функцію декількох груп параметрів:

$$R_t = f(D_t, C_t, B_t, H_t, S),$$

де R_t – інтегральна оцінка ризику в момент часу t; D_t – характеристики технічного стану пристрою; C_t – контекст його підключення; B_t – поведінкові характеристики; H_t – історія попередніх оцінок; S – критичність ресурсу, до якого здійснюється доступ.

Значення окремих факторів доцільно нормувати, а інтегральну оцінку представляти в межах від 0 до 1, де значення, близьке до 0, відповідає низькому ризику, а наближення до 1 свідчить про його зростання. Конкретний спосіб визначення ваг окремих факторів та функції f потребує подальшого обґрунтування відповідно до характеристик корпоративної мережі.

Для адаптивного визначення моменту наступної перевірки пропонується враховувати не лише поточне значення ризику, а й швидкість його зміни. Вона може бути визначена як

$$V_t = \frac{(R_t - R_{t-1})}{\Delta t},$$

де R_{t-1} – значення ризику під час попереднього оцінювання; Δt – проміжок часу між оцінюваннями. Додатне значення V_t характеризує тенденцію до зростання ризику, а від'ємне – до його зменшення.

Інтервал до наступного повторного оцінювання стану пристрою пропонується визначати залежністю

$$T_{next} = \max\left[T_{min}; \frac{T_{\max}}{(1 + \alpha R_t + \beta \cdot \max(0; V_t))}\right],$$

де T_{next} – інтервал до наступного оцінювання; T_{min} – мінімально допустимий інтервал; T_{max} – максимально допустимий інтервал; α – коефіцієнт чутливості до поточного рівня ризику; β – коефіцієнт чутливості до швидкості його зростання.

Запропонована залежність забезпечує обернений зв'язок між ризиком та інтервалом контролю. За низького і стабільного значення R_t інтервал T_{next} наближається до T_{max} зі зростанням поточного ризику інтервал скорочується. Якщо абсолютне значення ризику ще не є високим, але показник V_t свідчить про його швидке зростання, наступне оцінювання також виконується раніше. Використання функції $\max(0; V_t)$ дозволяє враховувати саме негативну з погляду безпеки тенденцію – зростання ризику. Для критичних подій доцільно передбачити позапланове повторне оцінювання незалежно від розрахованого значення T_{next}. Таким чином, інтегральну оцінку ризику пропонується використовувати у двох взаємопов'язаних процесах. Перший визначає поточний рівень мережевого доступу:

$$A = g(R_t),$$

де A – політика або рівень доступу до ресурсів корпоративної мережі.

Другий процес визначає інтенсивність подальшого контролю:

$$T_{next} = h(R_t, V_t).$$

Такий підхід розділяє два рішення: який рівень доступу може бути надано кінцевому пристрою в поточний момент та через який проміжок часу доцільно

повторно перевірити обґрунтованість цього рішення. За фіксованого періодичного переоцінювання всі пристрої, на які поширюється однакова політика контролю, повторно перевіряються через заданий інтервал незалежно від поточного рівня та динаміки ризику. Наприклад, за інтервалу 4 години пристрій зі стабільно низьким ризиком і пристрій, ризик якого поступово зростає, будуть перевірені через однаковий проміжок часу. У запропонованому підході для першого пристрою інтервал може наближатися до максимального, тоді як для другого він скорочується відповідно до поточного значення ризику та швидкості його зміни.

Відмінність від фіксованого режиму проявляється також у розподілі інтенсивності контролю. Замість однакової періодичності перевірок для всіх пристроїв частіше переоцінюються кінцеві точки, для яких спостерігається підвищення або зростання ризику. Для пристроїв зі стабільно низьким ризиком кількість повторних перевірок може бути зменшена. Водночас скорочення інтервалу контролю для пристроїв зі зростаючим ризиком дає змогу раніше виявити погіршення їхнього стану та за потреби застосувати більш обмежувальну політику доступу після досягнення встановленого порогового значення.

Отже, запропонований підхід до удосконалення оцінювання ризику кінцевих пристроїв у системах NAC передбачає використання інтегрального показника ризику не лише для вибору відповідної політики та рівня мережевого доступу, а й для адаптивного визначення інтервалу повторного оцінювання стану пристрою. Врахування поточного значення ризику та швидкості його зміни дає змогу диференціювати інтенсивність подальшого контролю залежно від фактичного стану кінцевої точки.

Подальше дослідження доцільно спрямувати на обґрунтування структури інтегрального показника, визначення параметрів моделі та експериментальне порівняння адаптивного й фіксованого режимів повторного оцінювання.

Список літератури

1. Сидоренко З. М. Безпека інформації при використанні мобільних пристроїв в корпоративних мережах // Сучасні напрями розвитку інформаційно-комунікаційних технологій та засобів управління. 2024. Т. 2. С. 53.

2. Matthews J. F. Challenges to Implementing Network Access Control. SANS Institute, 2017. 22 p.

3. Cisco Secure Client (Including AnyConnect) Administrator Guide, Release 5.1. Cisco Systems, Inc. Updated June 30, 2026. 345 p.

4. Guide for Conducting Risk Assessments / National Institute of Standards and Technology. NIST Special Publication 800-30, Revision 1. Gaithersburg : NIST, 2012. 95 p.

5. Atlam H. F., Alenezi A., Hussein R. K., Wills G. B. Validation of an Adaptive Risk-based Access Control Model for the Internet of Things. International Journal of Computer Network and Information Security. 2018. Vol. 10, No. 1. P. 26–35. DOI: 10.5815/ijcnis.2018.01.04.

6. Atlam H. F., Wills G. B. ANFIS for risk estimation in risk-based access control model for smart homes. Multimedia Tools and Applications. 2023. Vol. 82. P. 18269–18298. DOI: 10.1007/s11042-022-14010-8.