

ОЦІНКА ЗАХИСТУ МЕРЕЖЕВОГО ДОСТУПУ НА БАЗІ ПЛАТФОРМИ CISCO IDENTITY SERVICES ENGINE

Вінницький національний технічний університет;

Анотація

Дослідження питань, пов'язаних з організацією концепції захисту інформаційної безпеки корпоративної мережі, що включає метод дослідження платформи Cisco Identity Services Engine.

Ключові слова: безпека, мережа, корпорація, маршрутизація, архітектура.

Abstract

Research of issues related to the organization of the concept of information security protection of the corporate network, which includes a research method of the Cisco Identity Services Engine platform.

Keywords: security, network, corporation, routing, architecture.

Вступ

Корпоративна мережа швидко змінюється, особливо коли справа стосується мобільності співробітників. Cisco Identity Services (ISE) - це система контролю доступу до мережі та управління політиками на основі ідентифікації [1].

Метою роботи є дослідження оцінки загрози на корпоративну мережу.

Результати дослідження

Захищеність інформаційної системи (K_{sec}) прямо пропорційна функції f (РЗ, МІС). Тому захищеність залежить від рівня значущості інформації та розмаху інформаційної системи.

Процес несанкціонованої дії зловмисника можна представити у вигляді стохастичною мережі, показаної на рисунку 1 [2].



Рис. 1. Стохастична мережа несанкціонованої дії зловмисника

За умови, що функції розподілу тимчасових процесів підпорядковані експоненціальному закону, розглянемо формули на рисунку 2.

$$D_i(t) = 1 - e^{-\alpha_i t}$$

$$B_j(t) = 1 - e^{-b_j t}$$

$$\Gamma_k(t) = 1 - e^{-\gamma_k t}$$

Отримаємо:

$$\delta_i(s) = \frac{\alpha_i}{\alpha_i + s}$$

$$\beta_j(s) = \frac{b_j}{b_j + s}$$

$$\gamma_k(s) = \frac{\gamma_k}{\gamma_k + s}$$

Рис. 2. Функції розподілу

Отримаємо графік середнього часу збереження інформацією своєї цінності на рисунку 3.

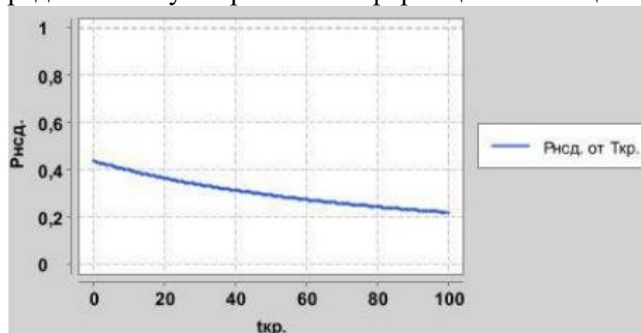


Рисунок 3. Залежність вірогідності несанкціонованого доступу від часу захищеності від доступу до змісту інформації

Висновки

З точки зору стану безпеки корпоративної інформації на базі архітектури Cisco ISE має інформаційна система за даною платформою має найвищий стан захищеності так як це ефективний інструмент побудови політик, приведений у відповідність стандартам (як загальним, так і галузевим) і підтверджений відповідності для зовнішніх і внутрішніх аудиторів.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Шевченко Д. В. Дослідження безпечного мережевого доступу на базі платформи Cisco Identity Services Engine : 172 / Шевченко Дмитро Вікторович – Київ, 2018. – 88 с.
2. Практика внедрения Cisco ISE [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: <https://habr.com/ru/company/jetinfosystems/blog/354888/>.

Кулібабчук Іван Павлович — студент групи КІТС-186, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail: ip1@gmail.com

Науковий керівник: **Семенченко Семен Семенович** — д-р техн. наук, професор, завідувач кафедри теплоенергетики та газопостачання, Вінницький національний технічний університет, м. Вінниця

Kulibabchuk Ivan P. — Department of Building Heating and Gas Supply, Vinnytsia National Technical University, Vinnytsia, email : Ivanov@sens.ua

Supervisor: **Semenchenko Simon S.** — Dr. Sc. (Eng.), Professor, Head of the Chair of Power Engineering, Vinnytsia National Technical University, Vinnytsia