Святослав Годнюк
студент 2 СТН курсу спеціальності «Менеджмент»
Науковий керівник: **Пастух Ю.А.**
к.е.н., доцент кафедри інформаційних технологій
Подільський державний аграрно – технічний університет
м. Кам'янець-Подільський

МЕТОДИ І ТЕХНОЛОГІЇ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ

Питання захисту комп'ютерних мереж від можливих атак, направлених на порушення функціонування мереж та окремих вузлів, несанкціонованого доступу до інформації та несанкціонованого використання сервісів мережі є одним з актуальніших, особливо для корпоративних мереж, до яких відносяться і мережі вищих навчальних закладів. Для захисту мереж розробляються і реалізуються комплексні системи захисту інформації, які складаються з набору організаційно-технічних заходів – від правил роботи користувачів у корпоративній мережі та розмежування прав доступу до інформаційних ресурсів та сервісів до встановлення та налаштування високо функціональних апаратно-програмних комплексів – між мережних екранів для захисту корпоративної мережі від зовнішніх атак [1, с.35].

Найчастіше у якості основної технічної складової КСЗІ використовують апаратні між мережні екрани (ММЕ), які поділяються на ряд категорій за своїм функціоналом та пропонуються різними виробниками телекомунікаційного обладнання. Тим не менш, можна виділити ряд недоліків використання ММЕ: ММЕ не вирішують усіх задач захисту (перш за все захисту від внутрішніх атак, які виконуються з середини корпоративної мережі, розподілених (DDos) атак на зовнішні канали тощо), вартість таких апаратно-програмних комплексів досить висока. Сучасне телекомунікаційне обладнання для комп'ютерних мереж усіх провідних світових виробників підтримує цілий ряд функціоналу,

який може бути успішно використаний для вирішення питань захисту комп'ютерних мереж без додаткових фінансових вкладень [2, с.1].

Існує досить велика кількість підходів до класифікації загроз та можливих атак на комп'ютерні мережі. Враховуючи, що апаратні та програмні засоби комп'ютерних мереж працюють на відповідних рівнях моделі взаємодії відкритих систем (модель OSI), для аналізу методів і технологій захисту використаємо класифікації, які також орієнтовані на модель OSI. Найбільша кількість атак найчастіше реалізується на п'яти рівнях (фізичний, канальний, мережний, транспортний, прикладний). Загрози на сеансовому та представницькому рівнях пов'язані, в першу чергу, з процедурами ідентифікації, автентифікації та шифрування, алгоритми і протоколи яких реалізовані в операційних системах і вплив на роботу яких з боку адміністраторів мереж мінімальний. У цій статті ми більш детально розглянемо фізичний та канальний рівень [3, с.3].

Методи захисту на фізичному рівні: найбільш розповсюдженими атаками фізичного рівня на такі об'єкти, як канали передачі даних, є: фізичне пошкодження, несанкціоновані зміни у функціональному середовищі, вимкнення фізичних каналів передачі даних, постановка шумів по всій полосі пропускання каналу. Для реалізації каналів передачі у сучасних мережах використовуються обмежені середовища (відповідно до діючих стандартів на структуровані кабельні системи використовуються оптичні кабелі та мідні кабелі «звита пара» у незахищеному та захищеному виконанні) та необмежені середовища передачі (відкритий ефір).

Вибір середовища передачі для побудови каналів передачі даних здійснюється виходячи з таких основних вимог: призначення каналу (магістральні, лінії зв'язку мереж доступу) та його довжина, безпека передачі інформації, швидкість передачі даних, електромагнітна сумісність, вартість створення і експлуатації. З точки зору захисту від наведених вище атак найбільш захищеним рішенням є використання оптичного кабелю. Оптичний канал за своєю фізичною природою унеможливлює прослуховування, зняття

інформації та постановку шумів. Пропускна здатність оптичних каналів з використанням сучасних технологій щільного та розрідженого мультиплексування за довжинами хвиль може досягати декількох сотень Гб/с, а мінімальна протяжність без використання проміжного підсилення від 10 до 40 км (залежить від потужності лазерного випромінювача). Як альтернативу для коротких відстаней (до 100 м), яка дозволяє захиститися від атак, пов'язаних з електромагнітних впливом на канал, можна використати екрановану виту пару [4, с. 1].

Для запобігання можливим атакам, направленим на несанкціоновані зміни у функціональному середовищі, необхідно, перш за все, забезпечити обмеження фізичного доступу до кабельних каналів, комутаційних вузлів та дата-центрів, розробити та реалізувати політику віддаленого доступу до мережного обладнання, розгорнути допоміжні системи відео спостереження та контролю доступу. Важливим фактором при забезпеченні надійності роботи інформаційно-комунікаційних систем можна вважати резервування найбільш критичних каналів, мережних пристроїв та серверів [5, с.1].

Методи та технологій захисту канального рівня: найбільш розповсюдженими атаками канального рівня є генерація широкомовних кадрів з метою перевантаження каналів передачі даних і комутаційного обладнання (до таких же наслідків приводять і так звані «широкомовні шторми» у великих комутованих мережах), підміна MAC-адрес вузлів, атаки на протоколи. Технології захисту канального рівня передбачають, перш за все, роботу з MAC-адресами вузлів, хоча ряд захисних функцій комутаторів аналізує і використовує й IP–адреси вузлів, що розширює область їх дії і на мережний рівень. Можна виділити такі підходи до захисту на канальному рівні: застосування MAC-фільтрації та прив'язок MAC-адрес до портів комутаторів, застосування додаткових захисних функцій комутаторів, таких, як DHCP, IP, сегментація мережі на окремі зони (домени широкомовлення) з використанням технології віртуальних локальних мереж (Virtual Local Area Network – VLAN), автентифікація та авторизація на канальному рівні [6, с.2].

Задача створення ефективних комплексних систем захисту комп’ютерних мереж може бути вирішена з використанням сукупності методів та технологій, які реалізовані в сучасному телекомунікаційному обладнанні для комп’ютерних мереж, як основи технічної складової таких систем. Виходячи з найбільш поширених загроз фізичного та канального рівнів моделі OSI проаналізовано особливості методів і технологій захисту та визначено, для вирішення яких задач захисту вони можуть бути застосовані. Розглянуті у роботі підходи до захисту на канальному рівні дозволяють ефективно протидіяти внутрішнім порушенням інформаційної безпеки. Проведений в роботі аналіз методів та технологій захисту дозволяє прийняти обґрунтовані рішення щодо вибору методів захисту для мереж різного призначення та з різними вимогами щодо захисту інформації [7, с. 1].

Список використаних джерел

1. Комп’ютерні мережі / А. Г.Микитишин, М. М. Митник, П. Д. Стухляк, В.В.Пасічник. – Львів: Магнолія, 2013. – 256 с. – (ISBN 978-617-574-087-3).

2. Методика і технології захисту комп’ютерних мереж (фізичні та канальні рівні) [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://elc.kpi.ua/article/view/113191.

3. Технології захисту інформації в інформаційних системах та комп'ютерних мережах [Електронний ресурс]. – 2016. – Режим доступу ресурсу:https://stud.com.ua/50143/informatika/tehnologiyi_zahistu_informatsiyi_informatsiynih_sistemah_kompyuternih_merezhah.

4. Безпека комп'ютерних мереж [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: csf.cv.ua/shara/cn/security.pdf.

5. Проблеми захисту інформації в комп`ютерних мережах [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: http://ua-referat.com/Проблеми_захисту_інформації_в_комп%60ютерних_мережа.

6. Комп’ютерні мережі і захист інформації [Електронний ресурс]. – 2015.–

Режим доступу до ресурсу: https://stud.com.ua/komputerni_merezhi_ta_zahust_komputernux_merezh.

7. Методи і технології захисту комп'ютерних мереж [Електронний ресурс]. 2017. – Режим доступу до ресурсу: https://elc.kpi.ua/article/download/