УДК 004.056.57

СИСТЕМА КОНТРОЛЮ ІНФОРМАЦІЙНИХ ПОТОКІВ У КОМП'ЮТЕРНІЙ МЕРЕЖІ СТУДЕНТСЬКОГО ГУРТОЖИТКУ

Луговський Г.В.
студент
gremypud999@gmail.com
Воротніков В.В.
Професор кафедри
комп'ютерних технологій і моделювання систем,
доктор технічних наук, доцент
Поліський національний університет

Описується система контролю інформаційними потоками у комп'ютерній мережі студентського гуртожитку, що передбачає реєстрацію та перевірку даних користувачів, а також здійснює контроль відвідування сервісів, сайтів тощо, для запобігання виведенню з ладу складових комп'ютерної мережі.

Загальновідомо що у студентському гуртожитку, як динамічному інформаційному середовищі необхідним є потужна підтримка інформаційних потоків освітньої діяльності та блокування так званих "шумів" та "завад" під якими можна розуміти контент, що не несе корисної, з точки зору забезпечення освітньої діяльності, функції захисту дуже потрібні .

В останні десятиліття інформація є одним із основних ресурсів розвитку суспільства, а інформаційні системи та технології – є засобом підвищення ефективності роботи продуктивності праці. Тому вони повинні відповідати вимогам: **Безпеки.** У сучасному суспільстві інформація стала одним із найважливіших стратегічних ресурсів, що забезпечує подальший розвиток підприємства. Саме тому інформація, як і решта ресурсів, потребує особливого захисту. Проблема інформаційної безпеки набула особливого значення в сучасних умовах широкого застосування автоматизованих інформаційних систем. У зв'язку із зростаючою роллю інформаційних ресурсів у житті сучасного суспільства, також через реальність великої кількості загроз проблеми інформаційної безпеки вимагають постійної і серйозної уваги. Системний характер впливу на інформаційну безпеку великої сукупності різних обставин, які за характером мають різну фізичну природу та переслідують різні цілі і викликають різні наслідки, приводять до появи необхідності комплексних підходів при вирішенні даної проблеми. **Зручності.** Зручність користування досить важлива вимога, бо саме вона відображає те наскільки система здатна забезпечити якісну роботу інфраструктури. Але також важливо щоби вона не створювала завад безпечному користуванню, в протилежному випадку будь який користувач який не має достатнього досвіду роботи за комп'ютером може сам того не помітивши наробити негарних речей і тим самим спричинити шкоду системі. **Стабільності.** Стабільність системи – це можливість повернутись до нормального функціонування всіх її елементів, у випадку коли система досить довго знаходилась у режимі бездіяльності (після обриву електромережі) щоби забезпечити подібну відновлюваність та надійне збереження даних система повинна мати доступ до серверів які зберігають інформацію користувачів а також до баз даних які допоможуть їй відновитись. **Швидкості.** Швидкодія технічних систем визначається обсягом даних, оброблюваних або переданих за одиницю часу. Висока швидкодія необхідна для динамічних систем, з якими управляються в реальному масштабі часу. **Якості.** Якість зв'язку, передачі даних та захисту залежить від того як дана інформаційна система обслуговується а також від зовнішніх та внутрішніх факторів які на неї можуть впливати.

Висвітлення теми надійності мереж навчальних закладів, та вирішення питання щодо можливих кібератак спрямованих проти викладачів та студентів з метою викрадення персональних даних є головною метою даної статті.

Система контролю інформаційних потоків у комп'ютерній мережі студентського гуртожитку може бути створена за декількома різновидами технологій та їх комбінацій а саме:

1.Один фізичний сервер та два віртуальних, фізичний антивірус.
2.Три хмарні сервери, програмний антивірус.
3.Один фізичний сервер та два віртуальних, програмний антивірус.
4.Три фізичних сервери, фізичний антивірус.
5. Один фізичний, один віртуальний та один хмарний сервери, програмний антивірус.

Згідно з результатами досліджень найвигіднішим різновидом системної комбінації є використання одного фізичного сервера з двома віртуальними та програмним антивірусом. Бо, по перше, це набагато дешевше аніж використовувати фізичний фаєрвол разом із додатковою апаратурою та у разі відмови легше підняти віртуальні машини аніж фізичні. Але для створення подібної системи необхідно враховувати що ваш спеціаліст не зробить помилкову інсталяцію підставного «антивіруса» який насправді буде являти собою шкідливу програму класу «троянський кінь».

Сама система представляється як сукупність елементів, які використовуються для перегляду та аналізу інформаційних потоків. Для цього використовуються як програмні антивіруси та фаєрволи так і програми для відслідковування IP-адрес, з метою зменшення ризиків отримати шкоду від сайтів які заражені вірусами, являють собою фішингові схеми або здатні заразити мережу "троянським конем" або "програмою вимагачем" і т.п. Планові оновлення, перевірки та техобслуговування мережі можуть допомогти із виявленням небезпечних каналів зв'язку та їх наступним блокуванням, чисткою або повною ліквідацією.

Основними елементами системи є антивіруси, бази даних - яка веде облік історії запитів, паралельно увімкнені програми сканери які мають постійно оновлювану базу сигнатур та має можливість виявляти шкідливі IP та URL адреси. Усі дані елементи використовуються адміністратором для виявлення та блокування, лікування або ліквідацію шкідливих інформ-потоків.

Цікавою особливістю сучасного суспільства є та обставина, що до активної участі в процесах інформаційного обміну у дуже стислі строки долучилася велика кількість широких мас користувачів, які у переважно більшій кількості не мають необхідного рівня підготовки до прийняття участі в корисній для суспільства інформаційній діяльності. Для великої частини учасників обмінів інформацією самовираження поки що є значущим як процес в Інтернеті. Тому сьогодні інформаційний простір перевантажений іноді випадковою та низькоякісною інформацією, що у свою чергу ускладнює можливості використання значимих для суспільства ресурсів. «Однак останнім часом з розвитком інформаційних технологій, удосконаленням загальносуспільної системи соціальних інформаційних комунікацій в Україні ми спостерігаємо характерний також і для інших країн світу процес самоорганізації вітчизняного інформаційного простору, формування системи соціальних інформаційних мереж» [1].

Можливість реалізації підходу відокремлення даних призвела до створення баз даних і їх систем керування, що мають забезпечувати ефективність виконуваних процесів уведення й доступу до даних. «**База даних** – це сукупність взаємозалежних даних, що зберігаються спільно в зовнішній пам'яті обчислювального комплексу й використовуються, як правило, більш ніж однією програмою або користувачем» [2]. Але даними необхідно якось керувати, тому нам допоможе **система управління базами даних** (надалі СУБД). **СУБД** – це програмна система, яка здатна забезпечувати використання й ведення БД користувачами. «Основне призначення

СУБД – надання користувачам БД засобів маніпулювання даними в абстрактних термінах, не пов'язаних зі способом їхнього зберігання в обчислювальній системі» [2].

Для безпечної роботи системи моніторингу потрібно забезпечити надійний захист, який повинні надавати спеціалізовані засоби.

«Фізичні засоби захисту – це засоби, необхідні для зовнішнього захисту засобів обчислювальної техніки, території та об'єктів» [3]. Реалізуються на базі ЕОМ, що призначені для створення різних фізичних перешкод на можливих шляхах проникнення та несанкціонованого доступу до життєво необхідних компонентів інформаційних систем, які захищаються.

«Апаратні засоби захисту – це різні електронні, електронно-механічні та інші пристрої, які вмонтовуються в серійні блоки електронних систем обробки і передачі даних для внутрішнього захисту засобів обчислювальної техніки: терміналів, пристроїв введення та виведення даних, процесорів, ліній зв'язку тощо» [3].

Програмні засоби захисту, які спеціально вмонтовані у склад програмного забезпечення системи, потрібні для виконання логічних та інтелектуальних захисних функцій.

«Апаратно-програмні засоби захисту – це засоби, які основані на синтезі програмних та апаратних засобів» [3].

«Законодавчі засоби – комплекс нормативно-правових актів, що регулюють діяльність людей, які мають доступ до відомостей, що охороняються, і визначають міру відповідальності за втрату або крадіжку секретної інформації» [3].

Таким чином запропонована інформаційна система надає змогу створити безпечні умови роботи мережі за яких користувач може працювати без завад, які можуть виникнути у випадку присутності мережевих "шумів" та "перешкод" та не надасть доступу програмам стороннього типу, які можуть утворити безлад у мережі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Мехед Д. ІНФОРМАЦІЙНА БЕЗПЕКА В СОЦІАЛЬНИХ МЕРЕЖАХ. МЕТОДИ ПОШИРЕННЯ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ // Чернігівський національний технологічний університет УДК 004.773
2. Грицунов ІО. В. ІНФОРМАЦІЙНІ СИСТЕМИ ТА ТЕХНОЛОГІЇ НАВЧАЛЬНИЙ ПОСІБНИК. – Харків – ХНАМГ – 2010 р.
3. ІНФОРМАЦІЙНА БЕЗПЕКА ТА МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ Северина С.В., к.е.н., асистент Запорізький національний університет Україна, 69600, м. Запоріжжя, вул. Жуковського, 66. Вісник Запорізького національного університету № 1 (29), 2016