Висновки. Усе це може здійснювати лише педагог з високою професійною компетентністю, розвиненими творчими, дослідницькими здібностями, високим рівнем інтелігентності, духовно-морального потенціалу.

ЛІТЕРАТУРА

1. Запорожець О.І. Основи охорони праці. Підручник / О.І. Запорожець, О.С. Протоєрейський, Г.М. Франчук // К. : Центр учбової літератури, 2009. - 264 с.
2. Жидецький В.Ц. Основи охорони праці. Підручник / В.Ц. Жидецький Львів: УАД, 2006 - 336 с.

Попович В.

Науковий керівник – доц. Франко Ю. П.

ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В КОРПОРАТИВНИХ МЕРЕЖАХ

Інформація цінувалася у всі часи. Для того, щоби володіти нею відбувалися вбивства, війни. В наші дні вона має не меншу цінність. Ця цінність може визначатися не тільки кількістю праці витраченої на її створення, але і кількістю прибутку, отриманого від її можливої реалізації. Проблема захисту інформації: надійне забезпечення її збереження і встановлення статусу використовування – є однією з найважливіших проблем сучасності.

Причини втрати і пошкодження інформації можуть бути різними. Найчастіше це зараження вірусами. Основним засобом захисту від вірусів можна вважати використання антивірусного програмного забезпечення, найкраще якщо це будуть дві незалежні програми, наприклад Dr.Web, AVP. Антивірусні засоби рекомендується встановити на ПЕОМ і на поштовому сервері, або змусити сканувати весь трафік, а також правильно налаштувати політику безпеки, що включає оновлення програм і антивірусних засобів, оскільки антивірусні засоби пасивні і не в змозі гарантувати 100 % захист від невідомих вірусів.

На сьогоднішній день найменш захищена передача інформації – це інформація, що надсилається за допомогою електронної пошти. Цим активно користуються інсайдери і несумлінні працівники, і левова частка конфіденційної або небажаної інформації витікає саме через Інтернет, за допомогою повідомлень електронної пошти. Наприклад, такі системи, як E-NIGMA, Secure, Altell використовують в своїх програмах методи розмежування прав доступу до e-mail повідомлень, за допомогою яких дотримується інформаційна безпека підприємства. Контроль за якістю роботи співробітників є важливим процесом в організації роботи цілого підприємства. Однією з складових цього контролю є моніторинг листування співробітників.

Актуальність дослідження. В наш час все більшого застосування набирає використання віддаленого доступу між територіально розмежованими інформаційними мережами. В підрозділах автоматизації це питання також актуальне. Комп'ютерні мережі мають необхідність в наявності сервера VPN, який буде дозволяти віддаленим абонентам використовувати ресурси приватної мережі через загальнодоступні мережі. Також VPN сервер може використовуватись для підвищення безпеки передачі інформації в локальній мережі, зменшивши вірогідність витоку чи крадіжки інформації, яка транспортується в мережі.

Безпека інформації на сьогодні – одна з найважливіших складових роботи системного адміністратора. І чим більше підрозділ автоматизації, тим більші можливості з'являються у зловмисників щодо перехоплення інформації, тим безпека каналів підрозділу критичніше [2, с. 233-304].

У статті розглядається захищений віддалений доступ до мережі, за допомогою якого здійснюється віртуальний локальний зв'язок між розподіленими мережами.

Мета статті: підвищення безпеки та надійності доставки інформації в мережі шляхом створення каналу з шифруванням.

Цілісність інформації це захист даних від умисного або неумисного пошкодження, знищення, доступу сторонніх осіб [2, 243-278].

Неправомірний доступ здійснюється, як правило, з використанням чужого імені, підроблених документів, зміною фізичних адрес технічних пристроїв, зміною програмного і апаратного забезпечення, розкраданням носіїв інформації, установкою апаратури перехоплення інформації з систем її передачі, а також порушенням систем захисту інформації. Неправомірний доступ до файлів законного користувача може бути здійснений через слабкі місця в захисті системи [2, с. 350-382]. Виявивши їх, злочинець може дослідити інформацію на комп'ютері, причому робити це можна так, що факт «злому» системи захисту буде встановлений дуже пізно.

Вірус може виявитися причиною виходу з ладу банківської системи, системи життєзабезпечення в лікувальних установах, систем навігації літаків, кораблів і т. д. Варіантів вірусів може бути безліч. На сьогоднішній день відомі сотні типів вірусів і десятки тисяч видів вірусів. Від найпростіших, які уповільнюють роботу комп'ютерів, до складних, що вносять серйозні пошкодження і повністю паралізують роботу.

Природно, що проти вірусів прийняті надзвичайні заходи, що призвели до створення захисних програм. Антивірусні програми можна розділити на три види: фільтруючі, що перешкоджають проникненню вірусу на

комп'ютер; проти інфекційні, що контролюють роботу додатків в системі; противірусні, що здійснюють пошук вірусів серед файлів комп'ютера і здійснюють «лікування файлів» [3, с. 432-440].

Однак при використанні комп'ютерної техніки існує одна особливість. Практично неможливо розробити алгоритм вирішення задачі, а вже тим більш програмно реалізувати його, без якихось дрібних помилок і неточностей. Помилки реалізації виявляються на етапі налагодження програми, та й то не завжди вони виключаються повністю. І якщо, наприклад, при будові якихось споруд (мостів, доріг, будинків) розрахунки ведуться з певним запасом надійності, то в області програмування така надійність дуже умовна. Сутність даного виду комп'ютерної злочинності полягає в наступному. Розробник програмного продукту замість, наприклад, побудови математичної моделі об'єкта, з метою отримання якихось вихідних параметрів, просто імітує отримання цих параметрів. Це може бути у випадку, коли об’єкт не відповідає вимогам, які накладаються на нього, а запуск виробництва цього об’єкта дуже важливий для третьої особи, і до того ж, розробити математичну модель складніше, ніж просто змоделювати вихідні дані.

Головні особливості корпоративних мереж (рис. 1) – глобальність зв'язків, масштабність і гетерогенність – представляють і підвищену небезпеку для виконання ними своїх функціональних завдань [4, с. 540-578]. Оскільки протоколи сімейства TCP / IP розроблені доволі давно, коли проблема безпеки ще не стяла так гостро, як сьогодні, то вони, в першу чергу, розроблялися як функціональні і легко переносимі, що допомогло розповсюджуватися стеку протоколів TCP/IP на велику кількість комп’ютерних платформ. Крім того, в теперішній час при використанні Інтернету в розпорядженні зловмисників з’являються численні засоби і методи проникнення в корпоративні мережі.

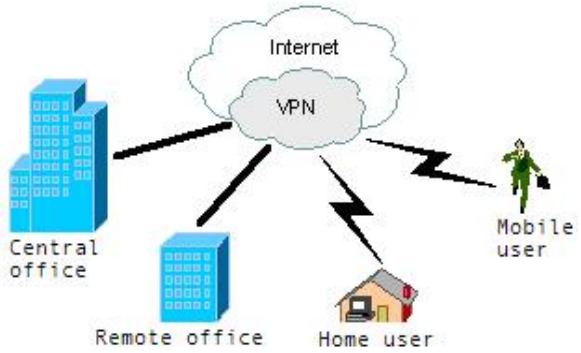

Рис. 1 Будова корпоративних мереж VPN

У зв’язку з гігантським ростом численності хостів, підключенних до інтернету, і ростом числа компаній, які використовують інтернет-технології для ведення свого бізнесу, значно збільшилось число інцидентів, пов'язаних з інформаційною безпекою (ІБ). Дані CERT (Computer Emergency Response Team) показують, що кількість виявлених вразливостей і кількість зареєстрованих інцидентів постійно збільшуються [6].

Віртуальна приватна мережа базується на декількох методах, які застосовуються при реалізації заходів безпеки в інформаційних мережах, одним з яких є тунелювання [4, с. 580-590].

Тунелювання забезпечує передачу даних між двома точками – закінченнями тунелю – таким чином, що для джерела і приймача даних виявляється прихованою вся мережева інфраструктура, що лежить між ними.

Транспортна середовище тунелю, як паром, підхоплює пакети використовуваного мережного протоколу біля входу в тунель і без змін доставляє їх до виходу. Побудови тунелю достатньо для того, щоб з'єднати два мережевих вузла так, що з точки зору працюючого на них програмного забезпечення вони виглядають підключеними до однієї (локальної) мережі. Однак не можна забувати, що насправді «паром» з даними проходить через безліч проміжних вузлів (маршрутизаторів) відкритої публічної мережі (рис. 2).

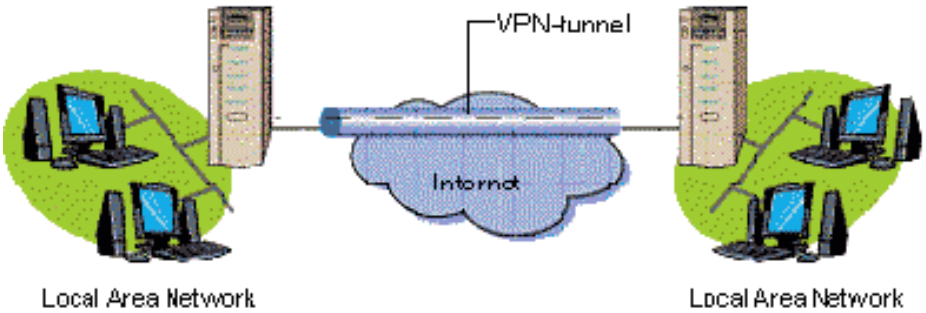

Рис. 2. Метод тунелювання

Такий метод має дві проблеми. Перша полягає в тому, що передається через тунель інформація може бути перехоплена зловмисниками. Якщо вона конфіденційна (номери банківських карток, фінансові звіти, відомості особистого характеру), то цілком реальна загроза її компрометації, що вже само по собі неприємно. Гірше того, зловмисники мають можливість модифікувати передаються через тунель дані так, що одержувач не зможе перевірити їх достовірність. Наслідки можуть бути жахливими. Враховуючи сказане, приходимо до висновку, що тунель в чистому вигляді придатний тільки для деяких типів мережевих комп'ютерних ігор і не може претендувати на більш серйозне застосування. Обидві проблеми вирішуються сучасними засобами криптографічного захисту інформації. Щоб перешкодити внесенню несанкціонованих змін в пакет з даними на шляху його проходження по тунелю, використовується метод електронного цифрового підпису (ЕЦП). Суть методу полягає в тому, що кожен переданий пакет забезпечується додатковим блоком інформації, який виробляється у відповідності з асиметричним криптографічним алгоритмом і унікальний для вмісту пакету і секретного ключа ЕЦП відправника. Цей блок інформації є ЕЦП пакету і дозволяє виконати аутентифікацію даних одержувачем, якому відомий відкритий ключ ЕЦП відправника. Захист переданих через тунель даних від несанкціонованого перегляду досягається шляхом використання потужних алгоритмів шифрування.

Висновки. У статті проаналізовано та порівнянно основні протоколи, які використовуються при створенні VPN підключення до мережі передачі даних, побудові розподіленої мережі та віддаленого доступу до мережі. Також практично реалізований тунельний канал за допомогою VPN сервера з використанням ЕЦП на базі операційної системи Windows Server 2003, та здійснено віддалений доступ до мережі сервера.

ЛІТЕРАТУРА

1. Болілий В. О. Комп'ютерні мережі: Навчальний посібник / В. О. Болілий, В. В. Котяк. – Кіровоград: ЦОП Авангард, 2008. – 146 с.
2. Крысин В. А. Безопасность предпринимательской деятельности / В. А. Крысин – М:Финансы и статистика, 2010. – 421 с.
3. Соколов А. В. Защита информации в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. – ДМК Пресс., 2012. – 656с.
4. Файльнер М. Виртуальные частные сети нового поколения LAN / М. Файльнер.– М.: Радио и связь, 2014.– 708 с.
5. ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації. Основні положення.
6. http://kiev-security.org.ua/ – Проблемы комплексной безопасности компьютерных систем

Подедвірна Н.

Науковий керівник – доц. Туранов Ю. О.

КОМПОЗИЦІЙНІ ЕЛЕМЕНТИ В ПРОЕКТУВАННІ ІНТЕР'ЄРІВ

Постановка проблеми. В Україні та усьому світі активно розвивається дизайн-проектування середовища. Цілісне рішення створюється за допомогою взаємозв'язку композиційних елементів та правил поєднань один з одним. Головним завданням є органічне поєднання частин інтер'єру в єдине ціле, відповідно до встановлених проектних вимог. Спроби розділити приміщення на окремі частини, проектуючи їх окремо один від одного є помилковими, оскільки перше, на що звертає увагу людина – це інтер'єр та атмосфера приміщення. Причиною таких помилок в більшості випадків є недостатньо правильне використання принципів, прийомів та засобів композиції дизайну.

Аналіз досліджень і публікацій. Теорія композиції вивчена добре, але для проектування інтер'єру недостатньо. Основні види композиції, її основні властивості і якості визначили Барташевич А. А. та Мельников А. Г. [1], також вони розглянули засоби композиційного формотворення і основи дизайну. Елементи композиції з точки зору геометрії розглянули Михайленко В. Є., Яковлєв М. І. [3].

Основи композиції в дизайні, закони, засоби гармонізації композиції, її види та специфіку кожного виду подав у посібнику Губаль Б. [2], а також описав композицію одно-, дво- та тривимірного простору. Композиційні особливості інтер'єрних просторів розглянули Олійник О. П., Чернявський В. Г., Гнатюк Л. Р. [4]. Особливості побудови формальної композиції, що становить найважливішу частину дизайнерської творчості описав Устін В. [5], розкривши засоби, принципи та прийоми цієї побудови.

Ілюстрований довідник пропонує Гілберт Р. [7], в якому висвітлила елементи дизайну, а також принципи і засоби композиції. Пайпс А. [8] описує на його думку основні елементи та правила композиції, наводить приклади у вигляді ілюстрацій.

Інноваційні проекти з описом та багаточисленними ілюстраціями внутрішнього інтер'єру та екстер'єру представляє Баласт К. [6] та описує ілюстрації без оцінки їх точки зору з теорії композиції.

Мета статті: розкриття основних елементів композиції, які використовуються при проектуванні дизайну інтер'єру.

Предметом дослідження даної статті є роль основних елементів композиції в дизайні інтер'єру.

Виклад основного матеріалу.

Композиція в інтер'єрі – це побудова інтер'єру приміщення або його функціональних зон, при якому його