АНОТАЦІЯ

Ключові слова: МЕРЕЖА, ВРАЗЛИВОСТІ, ЗАГРОЗА, ВИЯВЛЕННЯ ВТОРГЕНЬ, НАВЧАННЯ, VLAN, SSL, ACTIVE DIRECTORY

Об'єкт дослідження: комп’ютерна мережа офісу ZoomSupport

Мета роботи (проекту): Провести аналіз мережі офісу ZoomSupport та вразливостей, та запропонувати заходи, які необхідно провести для покращення здатності протистояти потенційним загрозам Методи дослідження: аналіз, системний підхід, методи: статистичні, контрольованого навчання, неконтрольованого навчання, на основі щільності розподілу набору даних, кластеризації та класифікації.

У спеціальній частині детально описано та проаналізовано процес внутрішньої фішингової атаки та її результати. Також опписано результат захисту від зовнішньої фішингової атаки на мережу офісу В економічному розділі визначено економічну ефективність від розробки і реалізації запропонованого алгоритму.

Практичне значення роботи полягає в можливості інтеграції розробленого алгоритму в існуючу систему виявлення аномалій для покращення ефективнотсі проведення навчання персоналу.

Результати проведених в дипломній роботі досліджень можуть бути використані для подальшої роботи над удосконаленням систем розробки захищенних мереж.

Наукова новизна дослідження полягає в вдосконалення методу виявлення вразливостей з метою зменшення кількості можливих загроз для мережі та підвищення ефективності її роботи.

ANNOTATION

Keywords: NETWORK, VULNERABILITY, THREAT, EMERGENCY DETECTION SYSTEMS, TRAINING, VLAN, SSL, ACTIVE DIRECTORY

Object of Study: The ZoomSupport Office Computer Network

Purpose of the project: To analyze the ZoomSupport office network and vulnerabilities, and to suggest measures that need to be taken to improve the ability to withstand potential threats. data, clustering, and classification.

The special part describes and analyzes in detail the process of internal phishing attack and its results. The result of protection against external phishing attack on the office network is also described. The economic section defines the economic efficiency from the development and implementation of the proposed algorithm.

The practical value of the work lies in the possibility of integrating the developed algorithm into the existing anomaly detection system to improve the efficiency of staff training.

The results of the research carried out in the thesis can be used to further work on improving the systems of development of secure networks.

The scientific novelty of the research is to improve the method of vulnerability detection in order to reduce the number of possible threats to the network and increase its efficiency.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AD – Active Directory

КСЗІ – Комплекс засобів захисту інформації

ПЗ – Програмне забезпечення

ЕОМ – електронна обчислювальна машина

ІКС – інформаційно-комунікаційна система

CA – Certification authority

VLAN – Virtual Local Area Network

DHCP – Dynamic Host Configuration Protocol

DNS – Domain Name System

ВСТУП

Діяльність будь-якої корпорації тісно пов’язана з використанням інформаційних мереж зв’язку, які будуються із застосуванням електронних технологій передавання, збереження, опрацювання, використання корпоративної інформації. Надійне функціонування цих систем безпосередньо впливає на економічну діяльність та фінансовий стан корпорації. В управлінні корпоративною діяльністю разом із фінансовими ризиками необхідно враховувати і ті, які пов’язані із використанням інформаційних систем. Тому для управління ризиками повинна проводитися консолідація інформації системи обліку і вивчення усіх подій, що спричиняють збитки, визначення ймовірностей їх настання, ризики поширення, способи їх упередження. Це завдання є надзвичайно важливим у сучасній корпоративній діяльності, його виконання має першочергове значення.

Система менеджменту інформаційної безпеки корпоративної мережі пов’язана із впливом різних чинників діяльності користувачів мережі і є основою економічної стабільності та збереження високого рівня безпеки корпорації. Для захисту корпоративної інформації, особливо конфіденційної, адміністраторам необхідно приймати своєчасні та зважені управлінські рішення, опрацьовуючи консолідовану інформацію загроз та слабких місць мережі.

Консолідована інформація діяльності системи безпеки корпоративної мережі дає змогу отримати вичерпну інформацію про стан мережі та здійснювати ефективний моніторинг подій, виявляти атаки, несправності та слабкі місця, ізолювати загрози безпеці корпоративної інформації. На основі консолідованої інформації проводиться діагностика, контроль та адаптація менеджменту інформаційної безпеки, проведення прямого контролю безпеки. Адаптація менеджменту інформаційної безпеки необхідна для задоволення бажаних результатів, незважаючи на зміну цілей управління корпорації, технологічних умов або розширення діяльності корпорації.

На основі консолідованої інформації створюється оцінка уразливості мережі та запобігання можливим вторгненням, корегується у відповідному напрямі стратегія менеджменту інформаційної безпеки корпорації, визначення методів та засобів захисту даних, прийняття відповідних рішень для виявлення прихованих загроз інформації.

РОЗДІЛ 1 ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

1.1 Загальна характеристика системи безпеки. Рівні захисту мережевих систем

Захист даних є однією з головних проблем комп'ютерної мережі, оскільки перевагою мережі є доступ до спільних даних та пристроїв, а це зумовлює можливість несанкціонованого доступу до даних.

Безпека даних це захист ресурсів мережі від руйнування та захист даних від випадкового чи навмисного розголошення, а також від неправомірних змін.

Гарантувати безпеку даних покликаний адміністратор мережі. У великих мережах з цією метою передбачені спеціальні посади (security officers). Для гарантування безпеки даних розробляють багаторівневу систему захисту:

-вбудовані засоби захисту – програмно-системні (паролі, права доступу);

-фізичні засоби захисту – замки, двері, охорона, сигналізація тощо;

-адміністративний контроль – організаційні заходи, накази адміністрації;

-законодавство та соціальне оточення – закони про захист авторських та майнових прав, нетерпимість до комп'ютерного піратства.

Рівні захисту інформаційних систем

Міністерство оборони США у книзі "Критерії оцінки безпеки комп'ютерів", (Оранжева книга), визначило сім рівнів безпеки комп'ютерних та мережевих систем. Ця розробка стала загальноприйнятою в світі для класифікації ступеня захищеності системи. Визначено такі рівні захисту:

- D – рівень мінімального захисту (Minimal Protection). Зарезервовано для систем, які за іншими рівнями не гарантують потрібного рівня безпеки;

- C1 – рівень вибіркового захисту (Discretionary Protection). Дає змогу користувачам застосовувати обмеження доступу для захисту приватної інформації;

- C2 – рівень керованого доступу (Controlled Access Protection). Містить вимоги рівня C1, а також захист процесу реєстрації у системі, облік подій захисту, ізоляцію ресурсів різних процесів;

- B1 – рівень захисту за категоріями (Labeled Protection). До вимог рівня C2 додається можливість захисту окремих файлів, записів у файлах, інших об'єктів системи спеціальними позначками безпеки, що зберігаються разом з цими об'єктами. Вважають, що подолати такий захист може добре підготовлений хакер, а звичайний користувач - ні;

- B2 – рівень структурованого захисту (Structured Protection). До вимог рівня B1 додається повний захист усіх ресурсів системи прямо чи посередньо доступних користувачу. Вважають, що хакери не зможуть проникнути у систему з таким захистом;

- B3 – рівень доменів безпеки (Security Domains). До вимог рівня B2 додається явна специфікація користувачів, яким заборонено доступ до певних ресурсів, повніша реєстрація потенційно небезпечних подій. Вважають, що навіть досвідчені програмісти не в стані подолати систему з таким рівнем безпеки;

- A1 – рівень верифікованої розробки (Verified Design). Повний захист інформації. Специфіковані та верифіковані механізми захисту. Вважають, що у систему з таким рівнем захисту без дозволу не може проникнути ніхто (навіть спеціалісти спецслужб).

1.2 Персональна ідентифікація

У деяких системах (наприклад, банківських чи податкових) потрібна ідентифікація не користувача, а фізичної особи. Розрізнюють кілька способів такої ідентифікації.

За персональними фізичними ознаками (біометрія). Знімають відбиток пальця, або геометрію руки, сітківку ока, зіницю, риси обличчя, а потім аналізують. Інший спосіб: система пропонує повторити певну кількість випадково вибраних слів та аналізує особливості голосу.

За предметом**,** який особа-користувач носить з собою. Таким предметом може бути спеціальний значок, магнітна картка з кодом. Цей спосіб є дешевим, проте ненадійним, предмет можна підробити, вкрасти тощо.

За тим, що особа повинна знати або пам'ятати**.** Треба пам'ятати пароль або правильно відповісти на низку запитань. Цей метод найдешевший і найпоширеніший, однак ненадійний (пароль можна підібрати, відповіді вгадати).

1.3 Надання права на доступ, автентифікація і реєстрація підключень

Безпека використання мережі забезпечується шляхом надання права на доступ, автентифікації і реєстрації підключень.

Процес ідентифікації користувача називається автентифікацією**.** Стандартний метод автентифікації - використання імені користувача і пароля як попередня призначена пара ідентифікаторів, які користувач повинен ввести у відповідь на запит системи для діставання доступу до мережевих засобів. При цій, найбільш простій, формі автентифікації ідентифікатор користувача і пароль передаються по мережі відкритим текстом (тобто не в зашифрованому вигляді). Сам процес автентифікації – порівняння переданої пари ідентифікаторів із записами таблиці, що знаходиться на сервері, – виконується відповідно до протоколу автентифікації по паролю (Password Authentication Protocol, PAP). Записи, що зберігаються, зашифровані, на відміну від передаваної пари ідентифікаторів, і це є слабкою стороною даного методу автентифікації.

Більш вдосконалена система запит-відповідь функціонує відповідно до протоколу автентифікації за запитом при встановленні зв'язку (Challenge Handshake

Authentication Protocol, CHAP). Згідно цьому протоколу, агент автентифікації (ПЗ, що знаходиться на сервері) передає користувачеві ключ, за допомогою якого той шифрує своє ім'я і пароль і пересилає цю інформацію назад на сервер. Авторизація – процес надання користувачеві права доступу до засобів системи, під час якого ім'я користувача і призначений йому пароль записуються в спеціальну таблицю системи.

Широко поширена система, що забезпечує високий рівень захисту при автентифікації, система запит-відповідь, в якій використовуються смарт-карти.
Регіструючи спроби доступу до мережі, можна легко визначити, чи не намагався неавторизований користувач проникнути у систему, а також дізнатися, чи не забув свій пароль хто-небудь з співробітників.

Блокування доступу. В багатьох організаціях як ідентифікатори користувачів вказувалися їх ініціали і прізвища. Зловмисникові, щоб спробувати проникнути в систему, досить було дізнатися такі. Розробники ПЗ створили програму блокування доступу до системи. Дуже часто ПЗ, що виконує блокування доступу, дозволяє задати ще один поріг: цим порогом визначається час, протягом якого система буде заблокована.

Важливим поняттям проблематики захисту даних у мережах є розпізнавання.
Розпізнавання – це гарантування, що інформація (пакет) надійшла від законного джерела законному одержувачу.

Справді, однією з найпоширеніших практик зловмисників у мережах є перехоплення пакетів та підміна їх своїми або скерування їх іншому адресату. Тому всі сучасні мережеві протоколи, зазвичай, оснащені засобами розпізнавання. Одним з механізмів розпізнавання пакетів є розміщення у відправника та одержувача однакових генераторів псевдовипадкових чисел. Кожен пакет позначають псевдовипадковим числом, яке порівнюється з таким же числом одержувача.

Аналогічне завдання виконує електронний підпис - послідовність байтів, які формують спеціальними алгоритмами та автентичність яких можна перевірити.

Для розпізнавання використовують окремі сервери, які видають електронні сертифікати. Сервери сертифікації застосовують у всіх достатньо потужних операційних системах.

Одним з найвідоміших вирішень є система централізованого розпізнавання Kerberos (вона реалізована програмним шляхом та сумісна з усіма типами систем. Працює система у клієнт-серверній парадигмі. Вона складається з програм-клієнтів, розміщених на робочих станціях користувачів, та серверних програм. Є три типи серверних програм: сервер розпізнавання, сервер надання дозволів та сервер адміністрування. У процесі розпізнавання клієнта беруть участь перші два з цих серверів. Кожен сервер має свою сферу дії, визначену змістом його бази даних користувачів).

Для вимірювання точності розпізнавання використовують два показники: відсоток хибного розпізнавання (False Acceptance Rate (FAR)) та відсоток хибного нерозпізнавання (False Rejection Rate (FRR)).

1.4 Захист мережі з використанням брандмауерів та серверів-посередників

Первинне значення терміна брандмауер (firewall) - це стіна у будівлі, зроблена з вогнетривких та незаймистих матеріалів, яка може перешкодити поширенню пожежі. У комп'ютерній мережі брандмауер - це комп'ютер з програмною системою, який встановлюють на межі мережі і який перепускає тільки авторизовані певним чином пакети. Найчастіше брандмауери захищають внутрішню корпоративну мережу від зазіхань із зовнішньої мережі. Однак їх можна використовувати для фільтрування вихідної інформації, обмеження доступу користувачів внутрішньої мережі назовні.

Сервери-посередники (proxy-server). Інколи функції брандмауера в складних системах розподілені між власне брандмауерами та серверами-посередниками. Брандмауер захищає мережу від зовнішнього впливу. Він фільтрує кадри канального рівня, розпізнає сеанс, який відкриває зовнішній користувач. Сервер-посередник

контролює та обмежує вихід внутрішнього користувача назовні, а також часто є його представником. Функції сервера-посередника: приховування адреси внутрішніх станцій, подаючи всю мережу назовні як один комп'ютер з адресою сервера; кешування популярних web-сторінок, файлів, так що користувачі не змушені звертатися до зовнішньої мережі. Популярну інформацію сервер оновлює автоматично з визначеною періодичністю.

Класифікація брандмауерів. Брандмауери застосовують різні алгоритми фільтрування, вони мають різні ступені захисту та вартість. Для класифікації брандмауерів їхню роботу описують з використанням еталонної моделі OSI.

Розрізняють:

-брандмауери з фільтруванням пакетів (packet filtering firewall; працюють на канальному, мережевому рівнях);

-шлюзи сеансового рівня (circuit level gateway; працюють на сеансовому рівні, розпізнають сеанс);

-шлюзи рівня застосувань (application level gateway; фільтрують інформацію за застосуваннями);

-брандмауери експертного рівня (stateful inspection farewall; виконують функції брандмауерів усіх нижчих рівнів).

Зазвичай, чим вищий рівень роботи брандмауера, тим більший рівень захисту він забезпечує.

Брандмауери з фільтруванням пакетів працюють разом з апаратним або програмним маршрутизатором. Вони аналізують зміст IP-заголовків пакетів і на підставі інформації у них та своєї таблиці правил й ухвалюють рішення про проходження пакета чи його відкидання. Найчастіше інформацією, на підставі якої ухвалюють рішення про проходження пакета, є його повна адресна інформація, інформації про протокол та застосування, номери портів одержувача та відправника. Якщо пакет не задовольняє жодного з правил, то діє правило "за замовчуванням". Воно найчастіше відкидає пакет. Конкретна конфігурація правил залежить від політики організації. Брандмауери генерують невелику затримку передавання

повідомлень. Часто функції фільтрування пакетів інтегрують у маршрутизаторах. Водночас рівень захисту у таких брандмауерів незначний - зловмисник може підмінити адресну частину IP -пакета.

Шлюзи сеансового рівня розпізнають учасників сеансу. Процедури перевірки виконують тільки на початку сеансу. Після того, як автентичність клієнта та сервера підтверджена, такий шлюз просто копіює пакети, не виконуючи фільтрування. Шлюзи сеансового рівня підтримують таблицю діючих сеансів і, коли сеанс завершується, знищують відповідний запис. Копіювання пакетів виконують спеціальні програми, які називають канальними посередниками (pipe proxies). Шлюзи сеансового рівня можуть виконувати і функцію сервера-посередника, який відображає внутрішні адреси локальної мережі в одну (фактично адресу брандмауера). Для пакетів, що надходять у зворотному напрямі, виконується зворотна операція. Отже, адресний простір мережі захищено - зовнішній користувач не бачить внутрішніх адрес. Однак такі шлюзи не забезпечують достатнього захисту і тому, зазвичай, не є окремим продуктом, їх постачають разом зі шлюзами рівня застосувань.

Шлюзи рівня застосувань**.** Застосуванням відповідають спеціальні програми-посередники. Вони можуть виконувати фільтрування на рівні застосувань. Кожне застосування може мати свого посередника. На відміну від посередників у шлюзах сеансового рівня, посередники рівня застосувань аналізують пакети на рівні застосувань. Наприклад, посередник застосування FTP може заборонити використання команди “put” для заборони передавання інформації на свій сервер.

Брандмауери експертного рівня поєднують риси всіх попередніх систем. Вони виконують фільтрування пакетів на канальному рівні, розпізнають сеанс як шлюзи сеансового рівня і мають змогу аналізувати й фільтрувати пакети за ознаками рівня застосувань. На відміну від брандмауерів рівня застосувань, які фактично передають інформацію між двома розірваними ланками передавання клієнт-шлюз та шлюз-зовнішній комп'ютер і спричинюють значну затримку в передаванні інформації, брандмауери експертного рівня налагоджують пряме сполучення між розпізнаним

клієнтом та сервером. Для фільтрування потоку використовують спеціальні шаблони, евристичні правила, порівняння зі зразками, інші методи з арсеналу експертних систем. Брандмауери експертного рівня забезпечують найвищий рівень захисту та високі параметри продуктивності.

Захист мережі за допомогою брандмауерів. Брандмауер зазвичай встановлюється між маршрутизатором і мережею, яку захищають, і є комп'ютером з двома мережевимиі адаптерами. Один адаптер підключений до концентратора так званої демілітаризованої мережі (DMZ), інший – до концентратора мережі, яку захищають. Брандмауер зазвичай підключають, аби через нього проходив увесь трафік "Інтернет – мережа, яку захищають". Важливо відмітити, що, оскільки доступ до DMZ-концентратору мають тільки маршрутизатор і брандмауер, весь обмін даними з Інтернетом проходить через брандмауер.

Програмним забезпеченням брандмауера здійснюється: перевірка вмісту пакету, виконання прокси-служб, шифрування, автентифікація і генерування попереджень. Для перевірки підозрілого трафіку (наприклад, неодноразових спроб підключення до мережі) проводиться аналіз вмісту пакетів з однаковою IP-адресою пункту призначення. Далі дії залежать від конфігурації брандмауера: або відкидаються всі подальші підозрілі пакети, або про цю ситуацію повідомляється адміністратор брандмауера.

Прокси-служба є посередником між хостом, що запрошує службу, і самою службою і застосовується з такими протоколами, як FTP, Telnet. Брандмауер обробляє запити на з'єднання, а це означає, що він функціонує в якості прокси-служби. Багато прокси-служб FTP дозволяють задіяти або відключати певні FTP-команди.

1.5 Захищені з’єднання та віртуальні приватні мережі

Одним із недоліків базового стека протоколів мережі Internet є відсутність криптографічного захисту та автентифікації передавань. Водночас такий захист потрібний у роботі корпоративних мереж, особливо для об'єднання мереж філій з

головною мережею, а також для зовнішнього доступу у мережу з окремих комп'ютерів. Завдання захисту можна вирішити шляхом побудови окремої приватної мережі корпорації. Використання Internet є дешевою альтернативою побудові приватних захищених мереж.

Для забезпечення захисту передавань через Internet розроблено велику кількість різноманітних протоколів, які розміщені на декількох рівнях, починаючи з прикладного і закінчуючи канальним. Можливості та обмеження окремих протоколів залежать від протокольного рівня, до якого вони належать. Наприклад, захищені протоколи прикладного рівня пов'язані з конкретним прикладним протоколом, і з іншими протоколами не працюють. Отже, сполучення інших протоколів є незахищеними.

Протоколи сеансового та рівня відображення надають сервіс всім прикладним протоколам, однак застосування, що працюють з ними, все одно доводиться переписувати, проставляючи звертання до захищеного протоколу, що незручно. Протоколи мережного рівня не потребують переписування застосувань і тому, напевно, найзручніші. Захищені протоколи канального рівня, відповідно, пов'язані з мережевимиі технологіями канального рівня, їх використовують для вирішення обмеженого кола завдань, таких як захист віддаленого доступу до корпоративної мережі.

Розглянемо головні протокольні вирішення, які використовують для створення захищених сполучень.

1. Протокол SSL (Secure Socket Layer- рівень захищених сокетів).

Щоб забезпечити можливість використовувати в операціях купівлі-продажу в мережі, корпорацією Netscape був розроблений протокол передачі закритих даних між web-серверами і web-браузерами - протокол SSL. SSL є протоколом рівня відображення, він надає протоколам прикладного рівня сервіс зі створення захищених застосувань. Цей протокол використовує протокольний стек TCP/IP. Відкритою реалізацією SSL є протокол TLS (Transport Layer Security- безпека транспортного рівня). По протоколу SSL відкритий ключ передається браузером через SSL-з'єднання. Потім він

використовується для отримання з сервера секретного ключа, за допомогою якого шифруються дані**.** Протокол SSL підтримується всіма найбільш популярними браузерами. Якщо для звернення до web-сторінки потрібне SSL-підключення, її URL починається з префікса https://, а не http://.

Протокол SSL вирішує три завдання:

-розпізнавання сервера на запит клієнта. Це особливо актуально, якщо клієнт передає конфіденційну інформацію, наприклад, номер кредитної картки;

-розпізнавання клієнта на запит сервера;

-захищене, зашифроване сполучення.

Складається SSL з двох протоколів: record protocol (визначає формати даних, які використовують для передавання) та handshake protocol (використовує record-протокол у фазі прив'язання сеансу). Під час обміну повідомленнями між клієнтом та сервером відбувається таке: розпізнавання сервера; сервер та клієнт обирають криптографічні алгоритми, які вони обидва підтримують; розпізнавання клієнта для сервера (необов'язково); визначення зашифрованого SSL-сполучення. Вибір алгоритму шифрування залежить від багатьох чинників. Наприклад, можна використовувати такі методи, як 3DES, AES, MD5, RSA, SHA.

Другим протоколом, що визначає порядок захищеної передачі даних через Web, є захищений HTTP – S-HTTP.

2. Протокол S-HTTP (Secure HTTP), RFC 2660, є розширенням до HTTP.

На відміну від SSL, яким передбачається створення безпечного з'єднання між клієнтом і сервером, S-HTTP призначений для передачі індивідуальних повідомлень Цей протокол створює захищені канали на прикладному рівні, даючи змогу шифрувати повідомлення. Він пов'язаний з HTTP та кожне http-повідомлення шифрує окремо.

Повідомлення S-HTTP складається з трьох частин: HTTP-повідомлення та криптографічних вимог відправника й одержувача. Відправник використовує відомі йому вимоги відправника та одержувача для шифрування повідомлення, а одержувач–для його дешифрування.

S-HTTP не потребує отримання відкритого ключа клієнтом і використовує тільки метод роботи з симетричними ключами. Це дуже важливо, тому що уможливлює надсилання запиту клієнтом без попереднього отримання відкритого ключа (спонтанну комунікацію). Використання захищеного протоколу відображене у заголовках запиту та статусу відповіді. Водночас S-HTTP є достатньо гнучким та може застосовувати багато різноманітних механізмів шифрування й розпізнавання. Протокол S-HTTP передбачає попередню домовленість між відправником та одержувачем про параметри захищеного сполучення. Ще однією перевагою S-HTTP є змога використання електронного підпису. Можливе передавання і без шифрування, однак з підписуванням.

3. Протоколи IPSec - це набір відкритих стандартів для організації захищеного передавання в мережах TCP/IP на мережевому рівні протоколу. Комплекс протоколів гарантує цілісність (незмінність даних), автентичність (дані надійшли від автентифікованого адресата); конфіденційність (не було несанкціонованого доступу до даних). IPSec, як і багато інших популярних технологій захисту даних, створює двопунктове захищене сполучення (тунель) між відправником та одержувачем даних.

4. Протокол PPTP (Point-to-Point Tunneling Protocol), розробки ф. Microsoft, кадри канального рівня під час передавання через Internet інкапсулюють у кадри IP. На боці одержувача відбувається зворотний процес. Виникає враження, що між учасниками обміну налагоджується пряме канальне сполучення, яке зазвичай можливе тільки в межах локальної мережі. Таке сполучення назвали тунелем. Технологія тунелювання є основою створення віртуальних приватних мереж (Virtual Private Networks (VPN)) - це двопунктові сполучення, які налагоджують у межах комутованої мережі. Вони подібне до призначеного каналу або тунелю, який прокладають через багато проміжних пристроїв. Передавання даних цим тунелем автентифікують та шифрують. VPN створюють для вирішення двох завдань: віддаленого сполучення з корпоративною мережею; сполучення двох локальних мереж. PPTP використовує на транспортному рівні протокол TCP, так що фактично PPTP-тунель є TCP-сполученням.

Побічним ефектом від налагодження тунелю канального рівня є те, що через такий тунель можна передавати пакети мереж, які не підтримують протоколи TCP/IP (наприклад, пакети IPX, Appletalk та ін.). Справді, вихідний пакет канального рівня PPTP може містити довільний пакет мережного рівня. Коли цей пакет дійшов до адресата через мережу TCP/IP, його розпаковують, і мережевий пакет надходить для опрацювання у внутрішній корпоративній мережі. Отже, через Internet можна мати доступ у мережу, яка працює з іншим протокольним стеком.

5. Протокол L2TP. Недоліком PPTP є підтримка його головно в продуктах однієї ф. Microsoft. Корпорація Cisco розробила аналогічний стандарт L2TP (Layer 2 Tunneling Protocol) на базі L2F (Layer 2 Forwarding. За функційними можливостями L2TP наближений до PPTP: він також створює двопунктовий тунель канального рівня від комп'ютера користувача до сервера корпоративної мережі через Internet. Як і PPTP, L2TP забезпечує розпізнавання у разі налагодження каналу, однак не потребує обов'язкового шифрування. На відміну від PPTP, пакети L2TP інкапсулюють у пакети UDP. Для транспортування пакетів можна використовувати інші мережі (ATM, Frame Relay).

1.6 Шифрування даних

При передачі інформації застосовуються два методи шифрування даних: з використанням секретного ключа і з використанням відкритого ключа. В першому випадку відправник і одержувач виконують шифрування і розшифровку повідомлення за допомогою одного і того ж ключа, в другому - із застосуванням двох ключів: відкритого, який відомий кожному і служить для шифрування даних, і секретного, відомого тільки одержувачеві повідомлення. При розшифруванні повідомлення виконуються складні математичні обчислення, в яких беруть участь обидва ключі.

В обох системах для шифрування і розшифровки даних застосовується операція додавання по модулю 2. Шифрування повідомлення виконується таким

чином: спочатку з використанням ключа генерується псевдовипадковий потік даних, який потім складається по модулю 2 з відкритим текстом. Той же ключ використовується одержувачем повідомлення для його розшифровки.

При обміні даними виконується наступна послідовність дій: на передавачі для отримання потоку зашифрованих даних генерується псевдовипадковий рядок (PN-дані), який потім складається по модулю 2 з відкритим текстом. На приймачі за допомогою того ж ключа генеруються ті ж PN-дані, які складаються по модулю 2 з отриманими зашифрованими даними для отримання відкритого тексту.

Шифрування	**Код**
Відкритий текст (дані, що підлягають шифруванню)	10110110
PN-дані, що згенерували за допомогою ключа	01101101
Зашифровані дані	11011011
Розшифровка	**Код**
Зашифровані дані	11011011
PN-дані, що згенерували за допомогою ключа	01101101
Відкритий текст (розшифровані дані)	10110110

Рис. 1.1 Приклад шифрування даних

Оскільки обидві сторони, що беруть участь в обміні даними, використовують однаковий ключ, існує вірогідність того, що із збільшенням числа користувачів, що беруть участь в обміні, ключ перестане бути таємним. Крім того, великі проблеми виникають при адмініструванні і розподілі секретних ключів, оскільки для кожної пари (відправник і одержувач) потрібний свій секретний ключ. Внаслідок цих причин система шифрування з використанням секретного ключа не набула широкого поширення в середовищі World Wide Web. У системі з використанням відкритого ключа будь-який користувач, звертаючись на захищений web-вузол, отримує відкритий ключ, за допомогою якого шифрує свої дані і відправляє їх на вузол, де

вони будуть розшифровані із застосуванням секретного ключа, який відомий тільки на цьому вузлі.

Системи з використанням секретного ключа називають також системами симетричної криптографії, оскільки для шифрування і розшифровки даних використовується один і той же ключ. Такі системи вважаються відносно нескладними в роботі і не вимагають виконання великого об'єму обчислень. Недоліки – проблеми, пов'язані з адмініструванням і розподілом ключів. Кожен ключ потрібно якимсь способом передати одній або обом сторонам, що беруть участь в обміні даними. Системи шифрування з використанням відкритого ключа позбавлені проблем, пов'язаних з розповсюдженням ключа (відкритий ключ доступний для всіх), проте, як це нерідко буває, вирішення однієї проблеми породжує іншу. У цих системах при розшифровці повідомлень виконуються дуже складні математичні обчислення, де задіяні обидва ключі, як відкритий, так і секретний, що вимагає наявність на комп'ютері одержувача достатньо потужного процесора. В деяких випадках використовуються обидві системи – відкритий ключ застосовується для передачі другій стороні секретного ключа, за допомогою якого потім шифруються передавані дані.

1.7 Цифрові сертифікати

Щоб упевнитися в тому, що користувач протилежної сторони дійсно є тим, за кого він себе видає, була розроблена система цифрових сертифікатів і організована служба, що поширює ці сертифікати; її назва - інфраструктура відкритих ключів (Public Key Infrastructure, PKI).

Цифровий сертифікат, що додається до передаваного повідомлення, призначений для посвідчення «достовірності» користувача або організації, що відправляють повідомлення, а також для надання одержувачеві інформації, яка буде використана ним при відправці відповіді. Цифровий сертифікат є тільки «посвідченням особи» відправника, але не дозволом на виконання яких-небудь дій.

Користувач (або організація), бажаючий передати зашифроване повідомлення, звертається до сервера сертифікатів (Certification Authority, CA). Сервер CA видає йому зашифрований цифровий сертифікат, в якому міститься відкритий ключ і додаткова інформація. Одержувач повідомлення також повинен звернутися до сервера сертифікатів і отримати відкритий ключ для розшифровки цифрового сертифікату, доданого до повідомлення. Це дає можливість одержувачеві упевнитися, що отриманий цифровий сертифікат є справжнім. Крім того, йому видається відкритий ключ відправника повідомлення.

CA можна розглядати як посередника, який дозволяє переконатися, що на протилежній стороні знаходиться саме той користувач, який потрібен. Поширеним стандартом видачі цифрових сертифікатів є ITU-T X.509.

1.8 Захист з використанням маршрутизаторів

Головною функцією, що виконується маршрутизаторами, була і залишається передача пакетів з однієї мережі в іншу. Але оскільки одна з цих мереж може бути приватною, а інша, скажімо, Інтернетом, маршрутизатори виступають в ролі першої лінії оборони, захищаючи дані закритої мережі.

Будь-який користувач, що має доступ до Інтернету, здатний проникнути в корпоративну мережу. Таким користувачем може бути потенційний покупець товарів, пропонованих через Інтернет, або просто цікава людина. Але, на жаль, це може бути і користувач, що намагається проникнути в корпоративну мережу з певною метою, їх саме прийнято називати хакерами. Для захисту корпоративних мереж застосовуються різні методи і використовуються різні типи мережного обладнання. Одним з таких методів захисту є обробка списку доступу, що виконується на маршрутизаторі.

Список доступу ACL (Access Control List) містить декілька операторів, призначених для управління потоком пакетів, які приходять на порт маршрутизатора.

Більшість виробників маршрутизаторів підтримують два типи списків доступу: стандартний і розширений.

Стандартні списки доступу**.** У стандартному, або базисному, списку доступу є один або більше операторів, що складаються з IP-адреси джерела і ключового слова permit або deny**.**Під час вступу пакету на порт маршрутизатора, де задіяна функція захисту за списком доступу, перевіряється IP-адреса джерела. Якщо вона співпадає з адресою, що міститься в операторові списку доступу, і в цьому операторові вказано ключове слово permit, маршрутизатор пропускає пакет в мережу, що захищається. Але якщо в операторові вказано ключове слово deny, пакет відкидається.

У маршрутизаторах Cisco стандартний список доступу має наступний формат: access-list номер_списку {permit/deny} IP-адреса маска_адреси. Номером списку може бути будь-яке значення з діапазону від 1 до 99, що ідентифікує групу операторів, що належать одному списку доступу. Маска адреси, що складається з 32 біт, вказаних в десятковому вигляді, служить як спеціальний оператор, що ідентифікує конкретну IP-адресу або групу адрес. На відміну від маски підмережі значення бітів маски адреси трактуються протилежним чином. Тобто біти, що мають значення 0, повинні співпадати з бітами, що знаходяться на цих же позиціях в адресі, що перевіряється, а біти, що мають значення 1, можуть не співпадати.

Приклад використання стандартних списків доступу. Припустимо, що мережа організації підключена до Інтернету в двох географічно віддалених пунктах (тобто мережа організації складається з двох віддалених мереж А і Б). Якщо мережа А має адресу 205.131.195.0, то, для того, щоб мережа Б могла отримувати пакети тільки з мережі А, на її маршрутизаторі повинен бути наступний список доступу: access- list I permit 205.131.195.0 0.0.0.255.

У цьому операторові маска адреси виглядає так: 0.0.0.255. Як вже згадувалося вище, значення 0 указують, що біти адреси відповідних позицій повинні співпадати, а значенням 1 можуть відповідати як одиниці, так і нулі. Отже, оскільки в масці адреси перші 24 біта мають значення 0, маршрутизатор пропустить в мережу Б тільки ті пакети, адреса мережі яких в точності співпадатиме з IP-адресою, вказаною

в списку доступу (205.131.195.0), тобто тільки пакети мережі А. Останній байт маски має в десятковому вигляді значення 255, що відповідає запису 11111111 в бітовому виді. Себто, маршрутизатор пропустить в мережу Б пакети, відправлені будь-яким комп'ютером мережі А.

Слід зазначити одну важливу деталь, що відноситься до цього прикладу, – оператор дозволяє прийняти пакети, що поступають з мережі 205.131.195.0, проте тут немає жодного оператора, який би забороняв маршрутизатору пропускати певні пакети. Більшість маршрутизаторів, у тому числі і Cisco, конфігуровані так, що в їх списках доступу забороняється пропускати всі пакети, окрім тих, які явно визначені в операторах з ключовим словом permit. Тобто можна вважати, що в списках доступу після операторів permit слідує нескінченна послідовність «прихованих» операторів deny.

Розглянемо ще приклад. Припустимо, що потрібно пропускати в мережу тільки пакети, що відправляються хостом, IP-адреса якого 205.131.195.12. Для цього указують в списку доступу наступного оператора**:** access-list I permit 205.131.195.12 0.0.0.0. Замість цієї послідовності нулів і крапок можна скористатися ключовим словом host. Іншими словами, попередній оператор може бути записаний так: access-list I permit host 205.131.195.12.

Розширені списки доступу надають додаткові можливості при фільтрації пакетів. Вони забезпечують фільтрацію на основі як IP-адреси відправника, так і IP-адреси одержувача, фільтрацію на основі номера порту протоколу (IP, ICMP, TCP, UDP) тощо. Загальний формат розширених списків Cisco виглядає так: access-list номер__списка {permit/deny} (протокол) адреса відправника маска_адреси [порт відправника] адреса_отримувача маска_адреси [порт отримувача] [додаткові^параметри].

Номер розширеного списку доступу може бути представлений значенням з діапазону від 100 до 199. Як і в стандартному списку доступу, номер розширеного списку ідентифікує тип списку, а також оператори, з яких він складається. У будь-який момент часу для перевірки пакетів, що поступають на один порт

маршрутизатора, може використовуватися тільки один список доступу, проте можна створити декілька списків доступу і застосовувати їх в міру необхідності. Крім того, для потоків пакетів, що входять і виходять через один інтерфейс, можна застосовувати різні списки доступу.

Приклад використання розширеного списку IP-доступу. Припустимо, що мережа організації має IP-адресу 205.121.175.0; в мережі розташовані web-сервер з IP-адресою 205.121.175.10 і telnet-сервер з IP-адресою 205.121.175.14. Адміністратор прагне дозволити всім користувачам мережі з IP-адресами 205.131.195.0 звертатися до web-серверу, а доступ до telnet-серверу треба надати тільки адміністраторові, комп'ютер якого має IP-адресу 205.131.195.007. Для виконання такого непростого сценарію необхідно створити наступний розширений список доступу:

-access-list 101 permit 205.131.195.0 0.0.0.255 host 205.121.175.10

-access-list 101 permit host 205.131.195.7 host 205.121.175.14

Перший оператор списку доступу дозволяє будь-якому хосту мережі 205.131.195.0 звертатися до хосту (web-серверу) мережі, IP-адреса якого – 205.121.175.10. Згідно другому операторові, для того, щоб пакет був пропущений в мережу, IP-адреса його джерела повинна бути рівною 205.131.195.7, а IP-адреса пункту призначення – 204.121.175.14. Пакети з будь-якими іншими адресами джерел і пунктів призначення будуть відкинуті.

Методика обробки операторів списку доступу. При перевірці пакету оператори списку доступу обробляються послідовно зверху вниз до першої відповідності вмісту заголовка пакету параметрам оператора списку доступу. Після виявлення збігу пакет або пропускається в мережу, або відкидається. Тому дуже важливо при створенні списку доступу враховувати не тільки зміст операторів, але і порядок їх перерахування

Списки доступу на маршрутизаторах, на жаль, не завжди ефективні. Існує можливість імітувати з'єднання і тим самим подолати бар'єр, встановлений за допомогою списку доступу. З таким методом злому можна боротися, заборонивши, наприклад, пропуск всіх пакетів, але це рівносильне відключенню від Інтернету.

Крім того, при фільтрації пакетів за допомогою списків доступу не перевіряється їх вміст. Це означає, що хто-небудь може спробувати проникнути в закриту призначену для користувача групу на сервері шляхом послідовного перебору різних паролів. Дана технологія злому називається атакою із словником. Для подолання подібних проблем були розроблені пристрої мережного захисту ще одного типу – брандмауери.

Однією з функцій брандмауера, є вибіркове шифрування**,** що дозволяє шифрувати тільки ті дані, які на шляху до пункту призначення проходять через певні мережі, залишаючи інші дані незашифрованими. Використовуючи вибіркове шифрування і автентифікацію, можна створити логічний тунель, що з'єднує віддалені мережі організації через Інтернет. Створювані таким чином VPN стали альтернативою дорогим виділеним лініям.

VLAN є групою хостів загальним набором вимог, що взаємодіють так, ніби вони прикріплені до одного домену, незалежно від їх фізичного розташування. VLAN має ті самі атрибути, як і фізична локальна мережа, але дозволяє кінцевим станціям бути згрупованими разом, навіть якщо вони не перебувають на одному мережевому комутаторі. Реконфігурація мережі може бути зроблена за допомогою програмного забезпечення замість фізичного переміщення пристроїв.

Щоб фізично копіювати функції VLAN, необхідно встановити окремий, паралельний збір мережевих кабелів і перемикачів, які зберігаються окремо від первинної мережі. Однак на відміну від фізичної відділеної мережі, VLAN ділить пропускну здатність; дві окремих одно- гігабітних віртуальних мережі які використовують одно-гігабітний зв'язок мають знижену пропускну здатність. Це віртуалізує поведінку VLAN (настроювання портів комутатора, позначки кадрів при вході в мережу VLAN, пошук MAC таблиці, щоб перейти до магістральних зв'язків і видалення тегів при виході з VLAN).

VLAN, які створені, щоб забезпечити послуги сегментації, зазвичай надаються маршрутизаторами в конфігурації локальної мережі. VLAN, розглядають такі питання, як масштабованість, безпека та управління мережею. Маршрутизатори в топологіях VLAN забезпечують фільтрацію, безпеку, узагальнення адрес та

управління трафіком. За визначенням, комутатори не можуть з'єднувати IP-трафік між мережами VLAN, так як це буде порушенням цілісності широкомовного домену VLAN.

Це також корисно, якщо хтось хоче створити кілька мереж 3-го рівня на тому ж комутаторі 2 рівня. Наприклад, якщо сервер DHCP (який буде перевіряти його наявність) підключений до комутатора він буде обслуговувати будь-який хост, який налаштований на отримання свого IP від сервера DCHP. За допомогою віртуальних локальних мереж можна легко розділити мережу так, щоб вузли не використовували цей сервер DHCP і отримували локальні адреси, або отримували адресу з іншого серверу DHCP.

1.9 Висновки до розділу 1

Використання сучасних засобів для захисту мережі та її побудови є важливою складовою будь-якого мережевого середовища. Також мережа повинна бути стійкою до потенційних загроз. Управління мережею має відбуватися легко з використання групових політик для персоналу та користувачів.

РОЗДІЛ 2 ДОСЛІДЖЕННЯ ВРАЗЛИВОСТЕЙ МЕРЕЖІ ТА ПРОДУКТУ КОМПАНІЇ

2.1 Структура мережі та її характеристика

Мережа офісу локального офісу ZoomSupport скаладається з:

-серверної частини

-світчів

-роутерів

-службових ЕОМ

-персональних ЕОМ

-камери

-NAS сервери

-Firebox

-гіпервізори

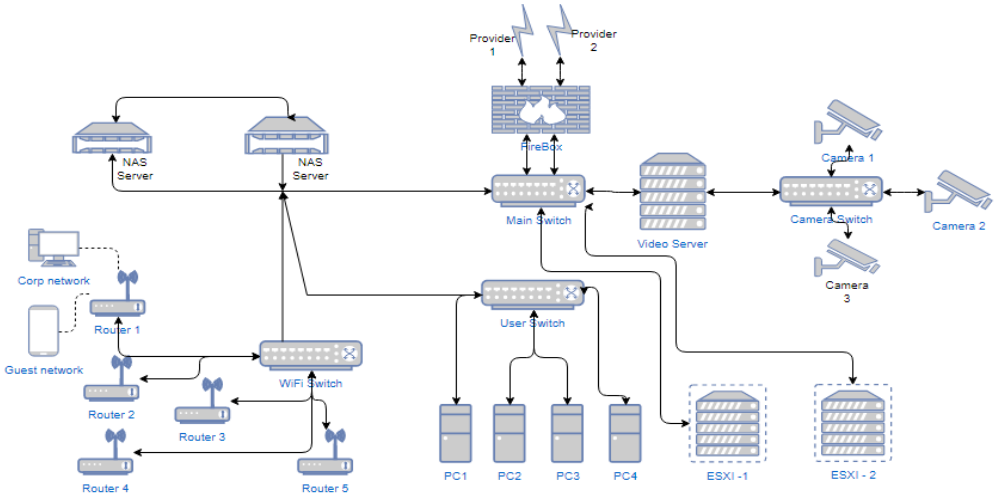

Рис. 2.1 Схема мережі офісу

2.2 Active Directory

Active Directory, далі AD, являє собою сховище даних про об’єкти мережі, яке є ієрархічно організоване. Комп’ютер, далі ПК чи ЕОМ, на котрому працює AD, є контролером домену. AD – це один з найпростіших способів вести адміністрування складної мережі. Технологія AD базується на стандартних Інтернет-протоколах і дозволяє чітко визначати структуру мережі.

Для Active Directory використовується система доменних імен. Domen Name System, далі DNS. DNS являє собою стандартну службу Інтернету, яка здатна організовувати групи з кількох ПК в домени. Після організації такого типу комп’ютери, домени організації та домени верхнього рівня будуть мати свої ідентифікації.

Для доступу до ресурсів в домені використовується повноцінна назва вузла, в нашому випадку це user@zoomsupport.com.ua. User – тут це назва індивідуального користувача/комп’ютера, @zoomsupport – домен мережі, ну а com – домен верхнього рівня. Загалом домени верхнього рівня складають базу ієрархії DNS і зазвичай називаються кореневими доменами, далі root domains.

Active Directory поєднує і фізичну, і логічну структури для складових мережі. За допомогою логічних структур AD можна організувати об’єкти каталогу і керувати обліковими записами, а також загальними ресурсами в мережі. Логічна структура складається з:

-організаційного юніта (organizational unit) – це підгрупа ЕОМ, які відображають структуру компанії;

-домен (domain) – група ЕОМ, які задіяні в використанні загального каталогу БД;

-дерево доменів (domain tree) – кілька чи один доменів, що використовують спільний неперервний простір імен;

-ліс доменів (domain forest) – кілька чи одне дерево, що юзають інформацію каталогу;

Фізичні ж елементи створюють реальну структуру мережі. На їх базі створюються зв’язки в мережі та фізичні ліміти мережевих ресурсів. До фізичної структури відносяться:

-підмережа (subnet) – група в мережі з заданою областю IP-адрес и мережевою маскою.

-сайт (site) – одна чи кілька subnet.

Використовуючи AD, на базі мережі ZoomSupport, запит від юзера, під час ідентифікації, прямує від ПК до юзерського світча, звідти до керуючого світча, де запит попадає на гіпервізор, де його уже розглядає AD і свою чергу надає права.

Також, щогодини AD пушить запит на всі світчі, які ті в свою чергу до всіх активних юзерів в своїх підмережах. Якщо всі налаштування задовольняють мережу і сесія активна , в якій знаходиться користувач, то система лишає все як було. Якщо після перевірки сесія не активна чи налаштування не відповідають зазначеним, воно звільняє даний IP-адрес і надає його іншому користувачеві, який зараз зробить перший запит. Групові політики пуляться постійно.

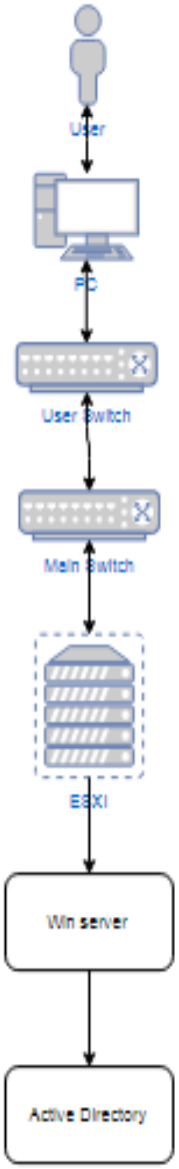

Рис. 2.2 Приклад взаємодію AD з User

2.3 Протокол 802.1x

Протокол 802.1x використовується в мережі офісу ZoomSupport, він працює на канальному рівні і надає права доступу до мережі на основі залежності від порту, тут як точка під’єднання до мережі.

Завдяки цьому протоколу, доступ до мережі отримують тільки ті юзери, які пройшли автентифікацію, якщо ж вони не змогли прийти автентифікацію, то доступ відповідно буде заборонений з порта.

Зазвичай використовується модель PTP (point to point), тобто в такому випадку він не може бути застосований, коли кілька хотів є з'єднаними з комутатором.

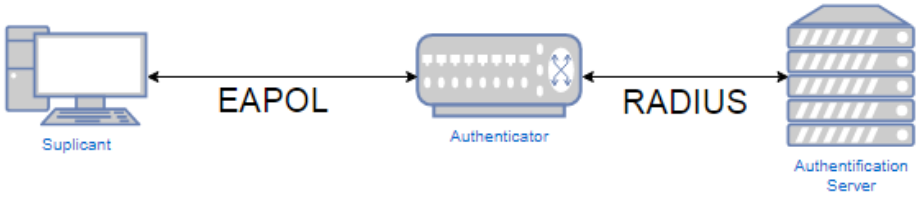

Рис. 2.3 Схема автентифікації

Supplicant/User/PC – пристрій, який запитує доступ до мережі у Authenticator (Автентифікатора) і відповідає на його запити. Для коректної роботи протоколу на клієнті має бути інстальоване ПЗ, яке забезпечить роботу 802.1x

Authenticator – пристрій, який виступає у ролі посередника, як проксі сервер, між суплікантом та сервером.

На кожному порті, який підтримує 802.1x, створюється два інших віртуальних порти. Перший з них це контролюючий порт, який відкривається тільки після того як автентифікація по 802.1x пройшла успішно. Другий – неконтрольований – передає тільки EAPOL трафік.

Authentication Server – сервер, який здійснює перевірку юзера і надає йому права до доступу до мережі.

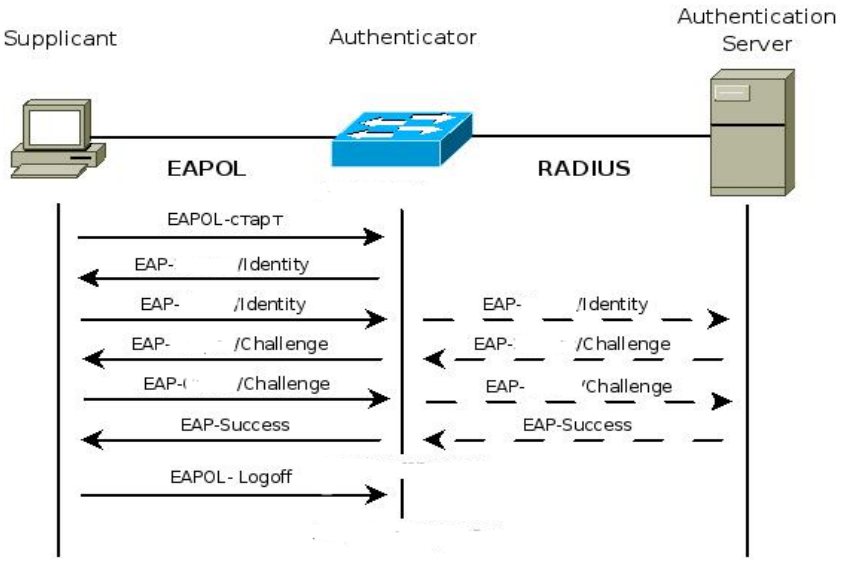

Рис. 2.4. приклад роботи протоколу 802.1x

1. Юзер відправляє запит EAPOL-старт до так званого посередника
2. Посередник пулить клієнту EAP-запит і клієнт EAP відповідає
3. Автентифікатор інкапсулює відповідь в формат RADIUS і пушить запит на сервер
4. Сервер надсилає EAP-MD5 Challenge на сторону клієнта , а клієнт присилає відповідь
5. Сервер підтверджує правдивість користувача і надає можливість автентифікатору дозволити доступ до мережі юзеру
6. Посередник авторизує порт і юзер отримує доступ до мережі

2.4 Hypervisor

Для створення робочих місць на хардварній частині мережі використовуються гіпервізори. Це програма, яка дозволяє керувати фізичними ресурсами ЕОМ і

розподіляти вищезгадані ресурси між кількома різними операційними системами, дозволяючи запускати і підтримувати їх одночасно.

Гіпервізори використовують технологію віртуалізації, яка дозволяє в свою чергу створення кількох комп’ютерів чи серверів на базі однієї фізичної машини. Зазвичай ця машина називається хост і в неї є свої певні конфігурації процесора , RAM, HDD і т.д. Саме ці фізичні ресурси розподіляються між кількома «уявними» комп’ютерами чи серверами.

Програма створює з одного фізичного пристрою кілька копій, клонів його апаратного забезпечення, і кожен з них, зі сторони юзера, виглядає як окремий пристрій.

Гіпервізор ізолює кожну ОС одна від одної так, що кожна використовує виділені під неї ресурси монопольно. Також можна дозволити ОС кількох ЕОМ взаємодіяти один між одним. Це може виглядати як доступ до певних файлів чи обмін ними мережею.

Існує два типи гіпервізорів - перший та другий.

Розглянемо перший тип, так як він використовується в мережі офісу ZoomSupport.

Такий тип гіпервізора виконується на «голій» хардварній частині, прямо «на залізі». Йому притаманні основні признаки ОС, а саме абстрактний набір ресурсів для прикладних програм, а також управління набором ресурсів, розподіляє процесорні пам'ять, час, пристрої вводу та виводу.

В ПЗ гіпервізора є важлива, навіть дуже, якість – об’єм його коду на два порядки менший, ніж у переважній більшості ОС. Завдяки цьому кількість помилок в роботі системи зменшується. Якщо ОС на одній з багаточисленних віртуальних машин станеться збій, то він ніяк не зачепить роботу іншим віртуалок, розміщених на цьому ж залізі.

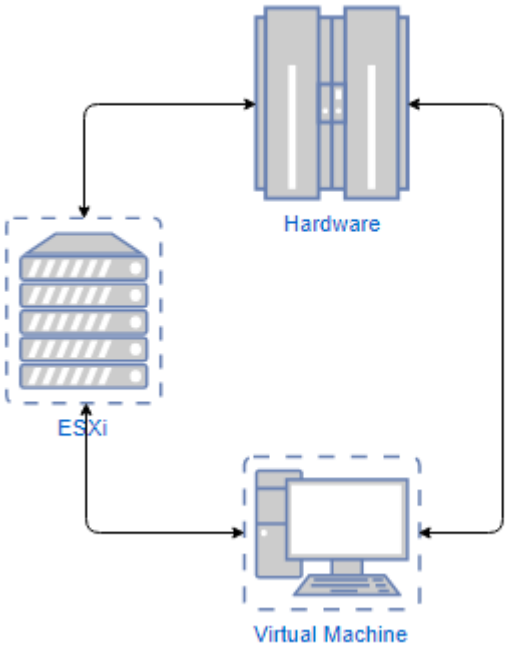

Рис. 2.5 Приклад роботи гіпервізора першого типу

В мережі офісу ZoomSupport використовується автономний гіпервізор VMware ESXi. Він надає змогу централізовано керувати всіма віртуальними машинами на усіх хостах домену з допомогою vCenter та vSphere платформ.

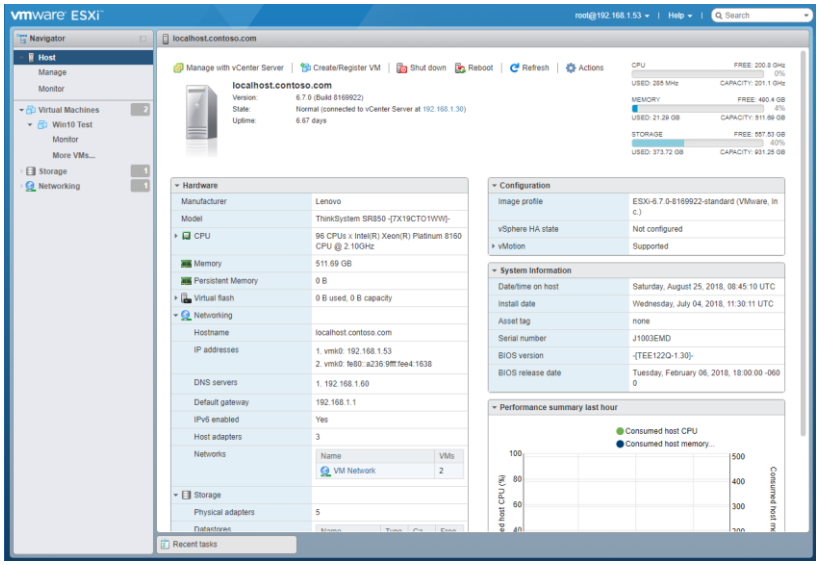

Рис. 2.6 Приклад інтерфейсу vCenter

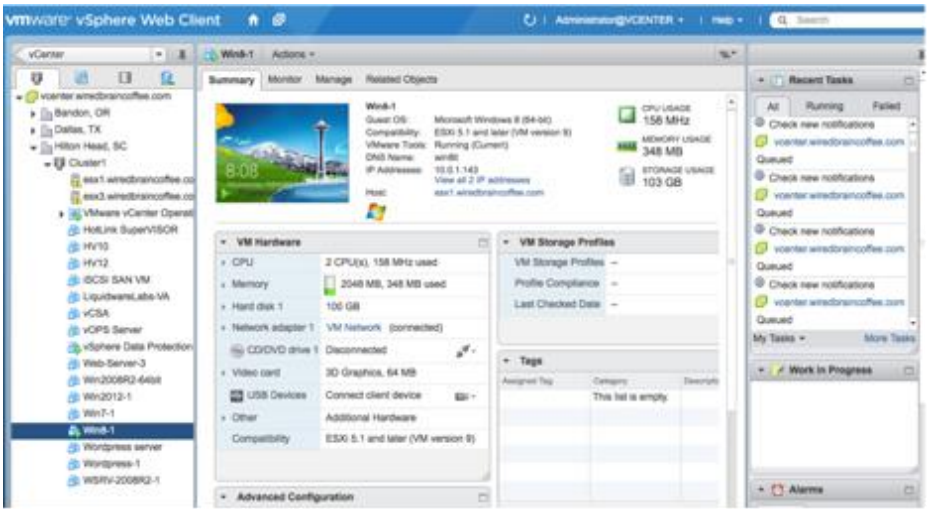

Рис. 2.7 приклад інтерфейсу vSphere

Натомість гіпервізори другого типу працюють на попередньо встановлених ОС. Він керує гостьовими ОС, а емуляція і керування фізичними ресурсами віддається хостова ОС.

Яскравим прикладом є Oracle VM VirtualBox.

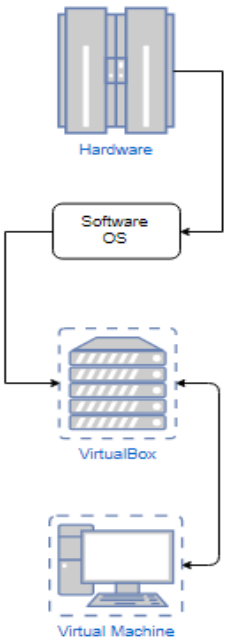

Рис. 2.8. Схема роботи гіпервізора другого типу

2.5 Доступ до мережі Інтернет

Доступ глобальної мережі інтернет з мережі офісу ZoomSupport забезпечує два провайдери. Перший – головний, та другий – резервний. Весь зовнішній трафік з обох каналів проходить через так званий Firebox.

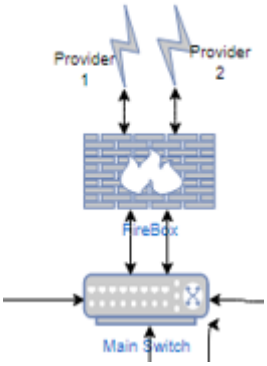

Рис. 2.9 Firebox

Firebox – це «розумна» і розширена версія Firewall, яка забезпечує швидкісним підключенням, без затримок, та має можливість підключення через DSL, оптоволокно чи ISDN роутер.

Гостьова мережа VLAN використовує другий канал зв’язку, в свою чергу перший канал використовується для робочого процесу. В разі відмови Provider 1, спрацьовує тригер, який змінює основному мережу на Provider 2. В разі відновлення зв’язку на першому каналі, тригер знову перемикає основний потік на нього. Якщо частота дропів перевищує 1дроп/хв, то основна мережа буде триматись на другому каналі.

В разі втрати живлення офісу, починають працювати UPS’и. Також спрацьовує тригер, який надсилає повідомлення адміністраторам мережі, про відмову в електропостачанні, щоб вони в свою чергу могли поступово виключити сервери в

поступовому порядку в безпечному режимі. В іншому випадку, UPS'и будуть дропати сервери поступово.

Продуктивність мережі характеризується часом реакції, пропускною здатністю та затримкою передавання.

Час реакції та затримка передавання дуже близькі за змістом між собою, проте різниця полягає в тому, що другий характеризує лише мережеві етапи оброблення даних, без затримок оброблення самих ЕОМ.

Пропускна ж здатність показує об'єм даних, які передаються мережею за одиницю часу. Вимірюється в бітах за секунду або в пакетах за секунду.

```
Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  10.61.70.254
  2    <1 ms    <1 ms    <1 ms  te-gw.zs.lcl [10.61.222.250]
  3     6 ms    13 ms     8 ms  78.154.171.161.ett.ua [78.154.171.161]
  4     7 ms     6 ms     5 ms  80.93.113.78.ett.ua [80.93.113.78]
  5     6 ms    10 ms     6 ms  108.170.248.131
  6     9 ms     6 ms     7 ms  108.170.234.224
  7    21 ms    21 ms    21 ms  216.239.46.121
  8    21 ms    20 ms    20 ms  108.170.250.209
  9    20 ms    20 ms    20 ms  216.239.40.213
 10    20 ms    19 ms    20 ms  dns.google [8.8.8.8]

Trace complete.
```

Рис. 2.10 Приклад команди ping стандартного DNS

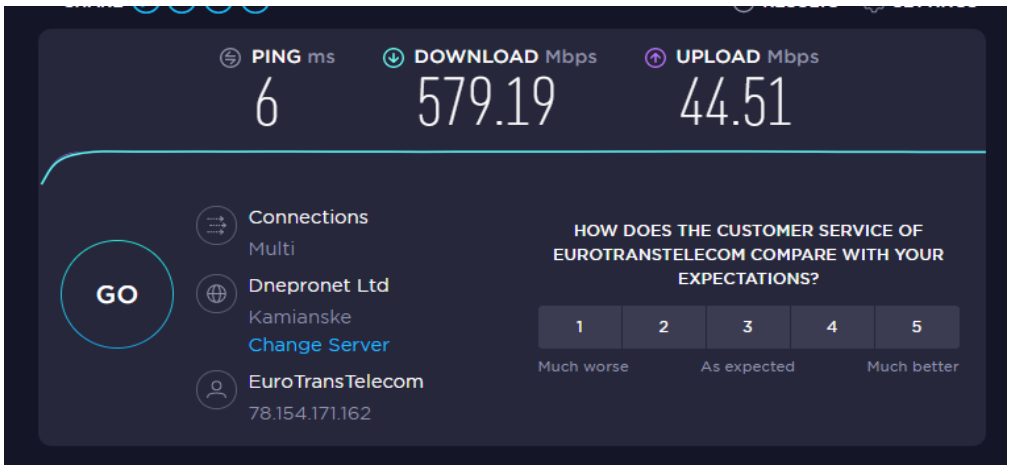

Рис. 2.11 Приклад пропускної здатності мережі

Наступні складові характеристики системи це безпека та надійність. Для оцінки надійності буде використовуватись коефіцієнт готовності згідно ДСТУ ISO/IEC TR 13335-1:2001

$$K = MTBF/(MTBF+MTTR)$$

Де:

MTBF (Mean time between failure) – середній час роботи між відмовами

MTTR (Mean time to repair) – середній час відновлення роботоздатності

Відмовостійкість на рівні мережі зумовлена такими технологіями:

-резервні блоки живлення мережевого обладнання, а також серверної частини мережі;

-резервна копія (бекап) головного серверу мережі;

-розміщення інформації на дискових системах зберігання даних з використанням відмовостійких груп дисків типу RAID

Вірогідність несправності одного з компонентів мережі за рік часу складає:

$$P = 1/MTBF$$

Де (P) вірогідність несправності

Вичисливши коефіцієнти несправності для кожного ресурсу мережі, методом їх сумування, можна отримати наступну формулу:

$$Ps = \sum Pi$$

І так як компоненти зазвичай відмовляють рівномірно в часовому періоді, то знаючи можливість відмови компонентів мережі, можна отримати час його роботи до відмови:

$$MTBFs = 1/Ps$$

Отже коефіцієнт готовності елементів системи дорівнюватиме:

$$Ks = MTBFs/(MTBFs + MTTR)$$

2.6 Забезпечення безпеки системи

Наступний аспект системи це її безпека. А саме здатність протистояти несанкціонованому доступу. Та відмовостійкість, а саме здатність системи функціонувати при відмови кількох її компонентів. При виникненні ситуації з відмовою, система тільки знижує якість своєї роботи, а не припиняє повністю функціонувати.

В наступній таблиці буде наведено можливі загроз для інформації, яка циркулює в мережі.

Таблиця 2.2 Потенційні загрози інформації в мережі

№ п/п	Потенційні загрози інформації	Властивості, які порушуються		
		К	Ц	Д
1.1	Стихійні явища й аварії (повені, землетруси, пожежі)		+	+
2.1	Збої та відмови системи електроживлення		+	+
2.2	Збої та відмови обчислювальної техніки		+	+
2.3	Збої та відмови програмного забезпечення		+	+

3.1	Недбале зберігання та облік: документів, носіїв інформації, даних		+	+
3.2	Порушення нормальних режимів роботи	+	+	
3.3	Розголошення, втрата атрибутів розмежування	+		
3.4	Ігнорування організаційних обмежень	+		
3.5	Пересилання даних за адресою абонента, яка є хибною	+		+
3.6	Ненавмисне ураження програмного забезпечення комп'ютерними вірусами	+	+	+
3.7	Ненавмисне пошкодження носіїв інформації і каналів зв`язку		+	+
3.8	Необережні дії, що призводять до розголошення конфіденційної інформації	+		

Таблиця 2.3 Потенційні загрози та їх реалізації

№ п/п	Потенційні загрози інформації	Властивості, які порушуються			Способи реалізації загрози		
		К	Ц	Д	*	**	***
1	Фізичне руйнування системи		+	+		+	+
2	Вимкнення чи виведення з ладу підсистем забезпечення функціонування.		+	+		+	+
3	Перехоплення даних, переданих по каналу зв'язку	+			+		
4	Розкрадання і вивчення виробничих відходів	+					+

5	Несанкціоноване перехоплення інформації	+			+		+
6	Несанкціоноване підключення до технічних засобів	+	+	+			+
7	Розкрадання носіїв інформації	+	+	+			+
8	Незаконне заволодіння паролями	+	+				+
9	Несанкціоноване використання терміналів користувачів	+	+				+
10	Впровадження програмно-апаратних закладок і вірусів	+	+	+			+

Пояснення до використаних позначень у наведених таблицях 2.2 і 2.3:

* — технічними каналами, до яких належать канали побічного електромагнітного випромінювання і наведень, а також акустичні, оптичні, радіотехнічні, хімічні та інші канали;

** — канали спеціального впливу шляхом формування полів і сигналів із метою руйнування системи захисту або порушення цілісності інформації;

*** — шляхом несанкціонованого доступу через підключення до засобів та ліній зв`язку, маскування під зареєстрованого користувача, подолання заходів захисту з метою використання інформації або нав`язування хибної інформації, застосування програмного-апаратних закладок і впровадження комп`ютерних вірусів.

Модель порушника — це всебічна структурована модель порушника.

Порушниками можуть бути такі категорії осіб:

-Суб’єкти, що мають доступ до території

-Зовнішні порушники

Метою порушника може бути:

-Отримання та розповсюдження інформації про замовлення, клієнтів, використані технології, вихідний код програм

-Завдання збитків шляхом зміни або видалення програмного коду

-Отримання конфіденційної інформації, що циркулює в мережі та всередині компанії

Технічна оснащеність порушника:

-Програмні засоби

-Апаратні засоби

Кваліфікація порушника:

-Порушник має високу кваліфікацію

Механізми захисту на рівнях ІКС

Захист від несанкціонованого використання ресурсів системи:

-Контроль за виділенням ресурсів, квоти

-Контроль за складом програмних засобів ІКС

-Захист програм від копіювання, дослідження, модифікації та несанкціонованого запуску

Рівень захисту від некоректного використання ресурсів системи:

-Підтримка цілісності даних

-Попередження користувачів перед виконанням небезпечних дій

Захист від НСД до ресурсів системи:

-Ідентифікація мережних пристроїв за IP та MAC-адресами

-Ідентифікація й автентифікація користувачів

-Керування доступом користувачів до об`єктів

-Керування доступом до інтерфейсів, програмних модулів, даних

Рівень внесення інформаційної та функціональної надмірності:

-Резервування інформації

-Відновлення і самовідновлення

Доступ до мережі посторонніх лиць контролюється наявністю охорони на першому поверсі та пропускного турнікету. Кожному агенту фірми видано пропуск, який прив’язаний до його робочого місця дислокації (в офіс компанії в іншому місті не можливо потрапити навіть за наявності пропуску). На робочому місці кожен агент має свої унікальні логін та пароль для входу в систему. Встановлювати посторонній софт, відмінній від наявного на робочих машинах не має можливості, без доступу до прав локального адміністратора.

Доступ до робочих ресурсів таких як база даних клієнтів чи групові робочі чати, з-за меж локальної мережі офісу неможлива.

Будь-яка спроба отримати відповідь від серверу повертає відповідь:

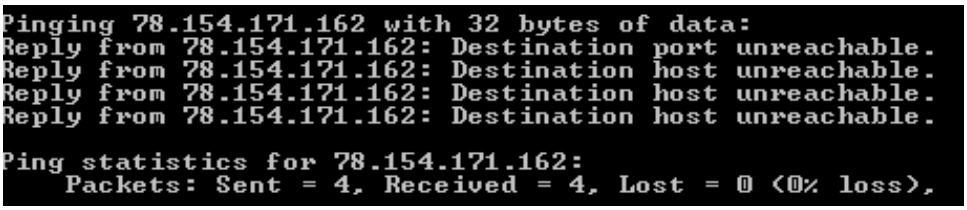

Рис. 2.12 Приклад відповіді від адреси мережі

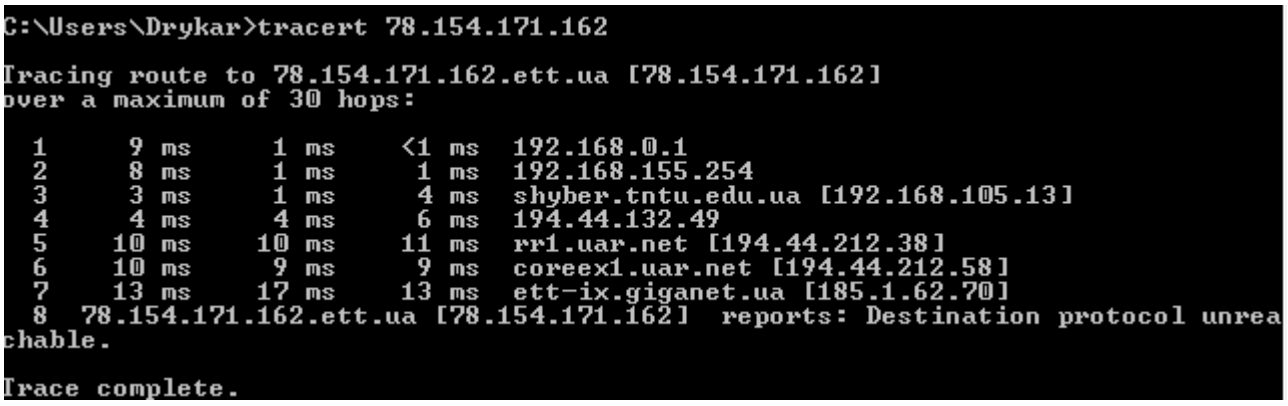

Рис. 2.13 Приклад трасування адресу мережі

Як можна помітити на рисунку вище, дослідження мережі методом респондів не є можливим з-за меж локального домену, утиліти OS Kalilinux не дали результатів при спробах отримати дані від мережі ззовні. Тому надалі розглядатиметься тільки внутрішній порушник (людський фактор), який може завдати шкоди мережі системи офісу ZoomSupport.

2.7 Висновки до розділу 2

Характеристики мережі офісу ZoomSupport, з точки зору практичності та захищеності, знаходяться на високому рівні. Це являється запорукою добре побудованої локальної мережі, та способу її адміністрування. Єдиний недолік в безпеці це недостатній рівень обізнаності робочого персоналу. Використання гіпервізорів дозволяє трекати всі зміни в мережі як на локально, так і віддалено. Резервні системи зберігання даних присутні і працюють справно. Зауважень до вразливості системи щодо зовнішніх атак не має.

РОЗДІЛ 3 ОТРИМАННЯ НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО МЕРЕЖІ МЕТОДОМ ФІШИНГУ

3.1 Фішинг і його спосіб реалізації

Великою вадою будь-якої ІКС є людський фактор. Це те на що вплинути майже не можливо і завжди буде становити загрозу політиці безпеки. Саме тому було обрано спосіб проведення атаки методом фішингу. Для її проведення я узгодив свої дії з відділом IT-security нашої фірми і ми розпочали спроби атаки методом фішингу.

Фішинг –це вид атаки чи, іншими словами шахрайства, коли ціллю є самі співробітники компанії чи будь-якого іншого підприємства. Від них, обманними шляхами, стараються отримати будь-які дані, з допомогою яких можна буде скомпрометувати особу чи отримати доступ до закритих БД. Найчастіше це свого роду «биті» посилання, що дуже подібні на оригінальні, проте редірект, який вони проводять, кидає користувача на інший ресурс, де його різними нотифікаціями стараються ввести свої дані.

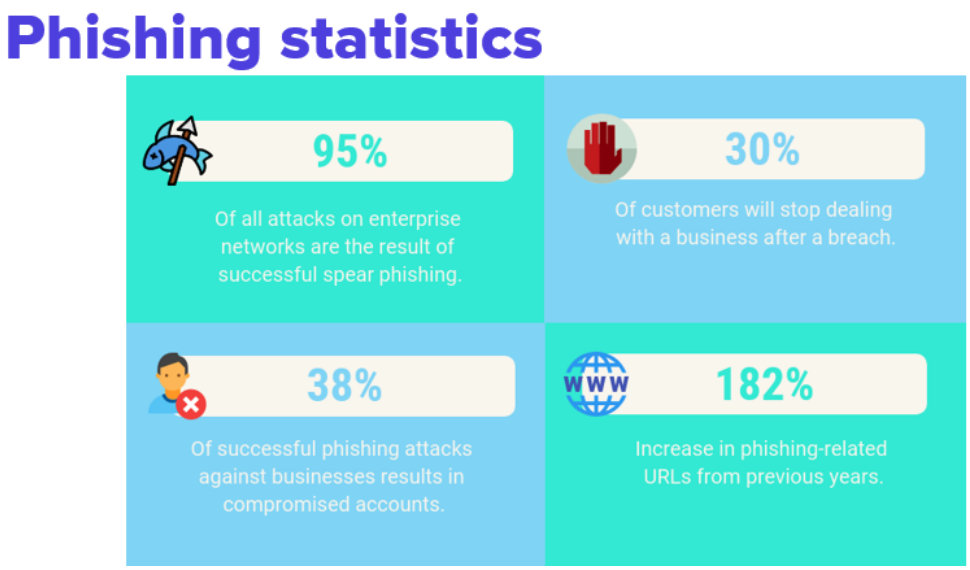

Рис. 3.1 Статистика фішингових атак за 2019 рік

Рис. 3.2 Поради щодо захисту від фішингу

3.2 Спроба реалізації фішингу

Для початку ми створили домен, подібний за свої складом до домену компанії ZoomSupport by Kromtech та ZEO Alliance. Ми надіслали повідомлення, яке містило посилання на зовнішній ресурс. В листі ми розмістили прохання зареєструватися за допомогою своїх робочих даних в формі, привичній для ока робітників, для чергового івенту.

Чого це вартувало нам і що ми отримали?

Ми витратили 20$ для реєстрації свого домену, 2 дні для отримання SSL сертифікату та залучення одного інсайдера, який розповів нам, як зазвичай виглядають подібні листи про івенти.

Отримали ми 36 паролів та логінів від співробітників, які зареєструвалися в перший же день. Що здивувало, так це те, що паролі, незважаючи на мінімальні

вимоги (8 символів, спеціальні знаки, верхній та ніжні регістри), були на диво прості.

Згодом ми повідомили всіх співробітників про цей лист та сказали змінити паролі тим, хто все-таки клюнув на це. Лише 20% юзерів змінили свої попередні паролі, що не є хорошим результатом.

3.3 Спроба захисту

Для другої спроби ми склали договір з сторонньою pentest-компанією для перевірки працівників та оцінити шкидкість реакції структури в цілому та спробу фішинга.

Їх атака відбувалася в три хвилі. За першу спробу розсилання, вони отримали активність 6 користувачів, від яких отримали 2 паролі. За другу розсилку було зафіксовано 16 юзерів та отримано 4 паролі. Після 2-ої серії листів, ми засікли підозрілу активність і невідомий до того домен, зразу ж повідомили всі агентів у всіх офісах про спробу фішингу. І на третю спробу, після інформування працівників, було помічено активність з 28 юзерів, проте не було отримано жодного паролю.

Далі нам знадобилося 20 годин, щоб повністю зупинити їхню активність з уже використаними даними, які вони отримали з перших двох хвиль. Було заблоковано домен, з якого йшов спам. Згодом визначено, якими сервісами вони встигли скористуватись, а сліди пентестерів було знайдено вже в 8 сервісах компанії, та закриття віддалених сесій. Паролі скомпрометованих користувачів було змінено в суворому порядку.

Здається, що інцидент зупинено та проблему вирішено. Через кілька днів після завершення процедури, одна з агентів побачила не прочитане повідомлення (одне з тим, які були вислані) та спробувала перейти по посиланню, не змогла, оскільки

воно вже було заблоковане в нашій мережі. Однак, вона зконтактувала з відправником (який представлявся як Сергій (адмін)), та отримала від нього вказівки спробувати перейти за посиланням, використовуючи мобільний 3G, оскільки в мережі виникли проблеми, через які на разі не можна отримати доступ до посилання з-під домену мережі. Так зловмисники знову змогли отримати дані для доступу в мережу.

3.4 Висновки до розділу 3

За даними спроб з фішингу, можна отримати очевидні результати, що найвразливішим місце будь-якої системи є людський фактор. Система, яка роками вважалась захищеною, може бути скомпрометована буквально за кілька годин, без зайвих зусиль зловмисника. Data breach для компанії це не тільки втрата певних ресурсів, але в свою чергу довіри клієнтів компанії, що в свою чергу несе фінансовий збиток. Для корпорації варто проводити аудити для своїх співробітників частіше, а також впевнитись, що кожен їх пройшов, щоб не траплялося ситуацій, які ми спостерігали під час спроб фішингу.

РОЗДІЛ 4 СПЕІАЛЬНА ЧАСТИНА

4.1 Знаходженя вразливостей додатків, які використовуються в мережі офісу

Для об’єтку дослідження було обрано додаток, який використовується для зворотнього зв’язку користувачів продукту з підтримкою Zoom Diagnostics.

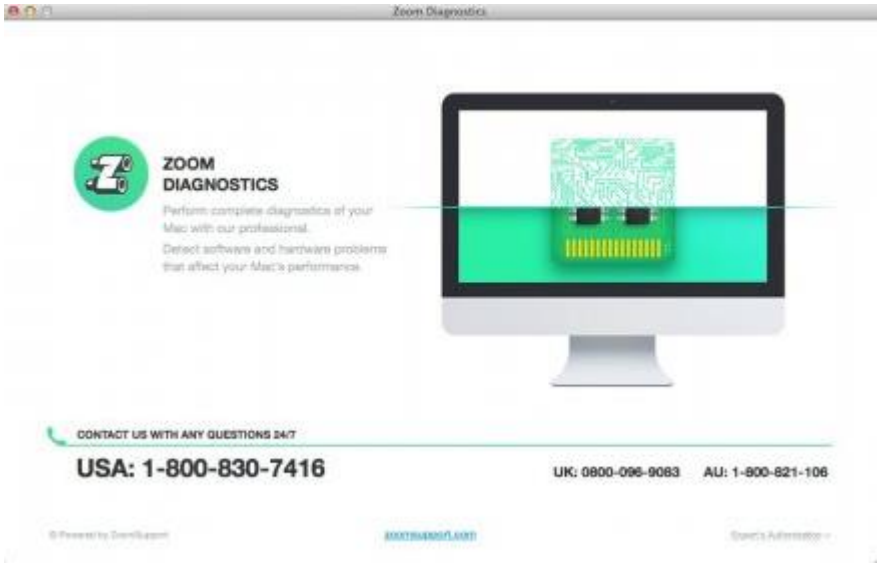

Рис. 4.1 Приклад додатку

Для здійснення контаку використовується вікно чату, яке розташоване в правій частині додатку. Чат стає активний при відправленні користувачем повідомлення до підтримки. Для створення сесії користувач повинен бути залогінений в додаток для створення сесії і його ідентифікації.

При активній сесії користувач зі своєї сторони може бачити всю історію переписки, де можуть бути написані його паролі, персональні чи кредитні дані.

Зловмисник, знаючи цю вразливість, може, методом брутфорсу, перебирати, отриманні злочинним шляхом, електронні поштові адреси, які можуть виявитися

нашими користувачами, і він отримає доступ до чату в якому збере всю необхідну йому інформацію.

Ця вразливіть є критичною для забезпечення цілісності інформації. Перебудова додатку, може ускладнити роботу споживачів з ним, тому додаткові служби автентифікації були відкинуті, як можливі варіанти вирішення проблеми.

Натомість було змінено методи відображення інформації в чаті. Раніше було видно всі повідомлення на дислані за період часу, зараз же користувач може бачити зі своєї сторони тільки повідомлення за останню добу.

Цей спосіб в рази зменшує ймовірність зловмисника отримати доступ до матеріалів чату саме того конкретного користувача в конкретний день. В свою чергу, з нашої сторони, сторони компанії, буде видно всі логи попередніх розмов.

4.2 Висновки до розділу 4

Було виявлено вразливість додатку, який слугує для комунікації між споживачами та компанією. Розроблено заходи, які зменшують можливість експлуатації цієї вразливості.

РОЗДІЛ 5 ОБГРУНТУВАННЯ ТЕХНІКО-ЕКОНОМІЧНОЇ ЧАСТИНИ РОБОТИ

5.1 Економічна складова

Для техніко–економічного обгрунтування прпонується розгляти використаня зовнішніх ресурсів, які були залучені для проведення дослідження вразливості мережі щодо фішингових атак.

Будуть враховані такі змінні витрати як:

-орієнтований загальний дохід;

-можливі збитки;

- обслуговуючий персонал (мережі);

- проведення навчання;

-залучення зовнішніх ресурсів;

ІТ-ринок – це сфера яка постійно розвивається в геометричній прогресії, на ринку постійно з’являються нові конкуренти і якщо не підтримувати свій продукт належним чином чи не розвивати його, то можна непотімно для всіх покинути територію.

Обсяг споживачів в ІТ-галузі теж зростає з кожним роком. Ринок адаптується під їхні потреби і старається забезпечити їх необхідним продуктом для вирішення тих чи інших проблем.

Спираючись на статистичні дані, 77% користувачів продукту відмовляться його використовувати в разі витоку персональних даних. В свою чергу це спричинить економічну кризу для компанії і втрату позиції на ринку.

Так як компанія ZoomSupport базується на утримані тривалих ділових стосунків з клієнтами, тенденція до отримання негативної репутації є фатальним фактором з діволої точки зору. Тому запобігти факторам, які можуть призвести до цього є пріоритетом.

Основні джерела припудтку це:

-платні підписки на продукти компанії;

-підтримання сервісів сторонніх продуктів;

-підписки на RA (Remote Assistance);

Запланований мінімальний прибуток компанії на цей рік ставновить 10 мілліонів доларів. В разі витоку даних, які можуть відбутися в разі успішної фішингової атки, можна втратити як і наявний покупців, які можуть отримати ріфанд, так і налякати можливих потенційних кових клієнтів та партнерів в сфері ринку.

Внутрішня перевірка на вразливість, вартувала не більше 20 долларів та двох днів часу, не велика ціна забля забезпечення цілей компанії.

Зовнішній фішинг тест вартував близько 2 тисяч доларів. Це з урахуванням всіх ресурсів, які були задіяні для ліквідації наслідків отримання доступу до мережі ресірсів компанії.

В разі більш глибокої загрози, можливе зупинення роботи сервісів компанії, що призведе, пропущенних дзвінків уже присутніх та потенційних клієнтів. Це може вартувати компанії близько 50 тисяч долларів на день.

Тому доцільність проведення тренінгів серед персоналу, що працює в компанії, щодо безпепи в мережі є беззаперечною. Рекомендованна кількість проведення тренінгів: раз на два місці. Витрати, які компанія повинна буде покрити це:

-витрати на переїзд між офісами;

-витрати на спеціаліста з безпеки, що буде проводити тренінги;

-витрати на проживання для спеціаліста;

Додаткового програмного чи апаратного забезпечення мережа офісу не потребує. Витрати будуть базуватися тільки на навчання персоналу.

5.2 Висновки до розділу 5

Безпека інформації, яка циркулює в мережі, а саме персональна інформація користувачів є ключовою ціллю зловнисників. В разі витоку цієї інформації буде підірвано як і довіру до компанії, так і її позицію на ринку. Саме тому вважаю доцільним проводити тренінги з безпеки для персоналу. Витрати на проведення тренінгів у всіх офісах покриваються протягом року менше, ніж 0.001% прибутку компанії, а результат це зереження >50% прибутку компанії протягом року.

РОЗДІЛ 6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Охорона праці

Робоче місце офісу ZoomSupport має відповідати вимогам щодо охорони праці при організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин (ВДТ).

Дане приміщення має 10 робочих місць. Розглянемо відповідність характеристик робочого місця нормативним. Для цього зведемо основні вимоги до організації робочого місця з і відповідні фактичні значення для робочого місця, за яким виконується робота, у табл. 6.1.

Робоче приміщення та місце відповідає вимогам щодо охорони праці при організації роботи з ВДТ електронно-обчислювальних машин.

Таблиця 6.1 — Характеристики робочого місця

Параметр	Позначення	Величина
Довжина, м	A	30
Ширина, м	B	20
Висота, м	H	3
Кількість робочих місць	N	10
Площа, $м^2$	S	600
Об’єм, $м^3$	V	1800

Відповідно до ДСН 3.3.6.042-99 роботи, що виконуються користувачами ЕОМ, відносяться до легких фізичних робіт – категорії Іа. У виробничих приміщеннях на робочих місцях з ВДТ мають забезпечуватись оптимальні значення параметрів мікроклімату.

Згідно ДБН В.2.5-28:2018 приміщення, що розглядається, повинне мати природне і штучне освітлення.

Денне (природне) освітлення приміщення відбувається за системою однобічного бічного освітлення. Природне світло проникає у приміщення через три світлові прорізи (віконні отвори), які мають регулювальні пристрої для відкривання. Також наявні штори (жалюзі) з можливістю захисту працюючих від прямого попадання сонячних променів і регулювання рівня освітленості в приміщенні. Вікна приміщення орієнтовані на північний схід. Оскільки будинок розташований у відносній віддаленості від прилеглих будівель, то які небудь перешкоди природному освітленню розглянутого приміщення відсутні.

Всередині приміщення стіни обклеєні світлими шпалерами, стеля побілена (переважає білий колір), у якості підлогового покриття використаний лінолеум світло-жовтого кольору.

Наявність постійного шуму в робочій зоні призводить до розладу центральної нервової системи і до таких захворювань як неврози, однак фактичний обмірюваний рівень шуму в робочій зоні склав 43 дБА, що задовольняє нормативному рівню шуму (не повинен перевищувати 50 дБА), тому додаткових заходів по поліпшенню цього фактору не потрібно.

Проаналізуємо стан електробезпеки в робочому приміщенні:

-всі прилади в кабінеті використовують напругу 220 В;

-електропроводка захована і ізольована від працівників спеціальним коробом;

-всі робочі місця з ПЕОМ використовують спільні розетки по 220 В;

-споживачі електроенергії — 3 ПЕОМ у вигляді ноутбуків;

-відносна вологість повітря – 60%, температура повітря +18 °С — +23 °С, струмопровідний пил і хімічно активні речовини в повітрі відсутні;

-підлога: ізолююча – лінолеум.

Проаналізувавши наведене вище, можемо сказати, що кабінет відноситься до приміщень без підвищеної електронебезпеки.

ПЕОМ, що використовуються в даному кабінеті підключаються до трифазної мережі і мають захисне занулення (за допомогою окремого захисного нульового провідника). Корпуси ВДТ та принтера виготовлені з пластику і не являються струмопровідними. Щодо корпусів самих ПЕОМ, вони виготовлені зі струмопровідного матеріалу, крім передньої панелі, що виготовлена з пластику.

При виконанні робіт по ремонту і обслуговуванню ПЕОМ обслуговуючий персонал зобов'язаний керуватися “Правилами техніки безпеки при експлуатації електроустановок споживачами". До роботи не допускаються особи, які не пройшли навчання з техніки безпеки.

Джерелом електромагнітного випромінювання в сучасному офісі є візуальні дисплейні термінали. Нормування електромагнітного випромінювання ВДТ а здійснюється згідно НПАОП 0.00-7.15-18 “Вимог щодо безпеки та захисту здоров’я працівників під час роботи з екранними пристроями”.

6.2 Особливості роботи та розлади здоров'я користувачів комп'ютерів, що формується під впливом роботи за комп’ютером

Характерною ознакою сучасного науково-технічного прогресу, практично, в усіх сферах діяльності людини, є широке застосування комп'ютерних технологій, заснованих на використанні електронно-обчислювальних машин. Сьогодення, а тим більше майбутнє, вже важко уявити без комп'ютерів та іншої електронної техніки.

Адже саме завдяки їм стала можливою швидка переробка величезних обсягів інформації, проведення необхідних розрахунків, виконання різних видів робіт, організація оперативного отримання та передачі інформації, збереження її значних обсягів електронним способом.

Стрімке впровадження комп'ютерів не тільки у сфері управління виробництвом, але також на транспорті, в банківській системі, бізнесі, системі освіти та інших сферах призвело до того, що мільйони людей виявились втягнутими у взаємодію людини з комп'ютером. Природно виникає запитання – на скільки безпечною є ця взаємодія для людини? Адже відомо про те, що будь- яка взаємодія людини та засобів праці – є двостороння. Людина впливає на удосконалення засобів праці, а останні – на працюючу людину.

Сучасні технології та техніка, до яких, безперечно належать комп'ютерні технології та ЕОМ, несуть у собі певні потенційні небезпеки та шкідливий вплив. В зв'язку з цим набуває актуальності вивчення фізіологічних, психологічних, соціальних та виробничих наслідків у системі "людина-комп'ютер-середовшце" та розробка і впровадження заходів щодо нормалізації праці та збереження здоров'я працівників під час роботи за комп'ютером.

Дослідження, проведені фахівцями Всесвітньої організації охорони здоров'я (ВООЗ) показали, що у професійних операторів та канцелярських службовців, які в своїй діяльності використовують відеодисплейний термінал (ВДТ), частіше зустрічаються порушення органів зору, опорно-рухового апарату, центральної нервової, серцево-судинної, імунної та статевої системи, захворювання шкіри. Необхідно зазначити, уже в перші роки впровадження ВДТ в Європі та США була зафіксована значна кількість скарг операторського персоналу на загальне недомагання, передчасне стомлення, головний біль, порушення органів зору, які здійснювали несприятливий психофізіологічний вплив на самопочуття та працездатність операторів.

В Інституті медицини праці Академії медичних наук України проводились дослідження інтенсивності захворюваності осіб, що використовують у своїй роботі комп'ютер. Була вивчена захворюваність працівників з різною тривалістю використання комп'ютерів та характером діяльності самих користувачів. Розглядалися 3 групи користувачів: у першу ввійшли інженери- програмісти

(тривалість роботи за комп'ютером більше 6 годин на день), у другу – інженери-економісти (тривалість роботи від 4 до 6 год.), у третю – математики-постановники завдань, які використовували комп'ютери не більше ніж 2 години на день.

Стан здоров'я	Користувачі ВДТ			Контрольна група
	1 група	2 група	3 група	
Функціональні порушення НС (ас- тенопічний синдром та ін.)	15,6	8,2	6,3	2,7
Хвороби системи кровообігу	57,7	60,3	29,2	23,0
Хвороби органів дихання	20,0	21,7	11,2	4,1
Хвороби органів травлення	40,0	38,6	29,8	18,9
Здорові	6,7	20,1	29,8	46,6

Рис. 6.1 Рівень захворюваності (%) різних тестових груп

З наведених даних видно, що фізіологічні порушення спостерігаються у користувачів, які довше та інтенсивніше використовували ВДТ.

Враховуючи несприятливий вплив цілого комплексу різноманітних виробничих факторів у користувачів можуть розвинутись певні розлади здоров'я, що пов'язані з роботою за комп'ютером.

Діяльність користувачів комп'ютерів характеризується тривалою багатогодинною (8 годин і >) працею її одноманітному напруженому сидячому положенні, малою руховою активністю при значних локальних динамічних навантаженнях, що припадають лише на кисті рук. Такий характер роботи може призвести до появи низки хворобливих симптомів, що об'єднані загальною назвою – синдром довготривалих статичних навантажень (СДСН). Повідомляється про

захворювання шкіри у користувачів комп'ютерів, які проявляються у вигляді папульозної висипки, свербіжу та лущення шкіри, еритеми, перорального та себорейного дерматитів, рожевих вугрів.

Дослідження впливу роботи за комп'ютером на жінок, особливо в період вагітності, показують, що серед жінок, які під час вагітності працювали більше 20 годин на тиждень за комп'ютером, число спонтанних абортів, мертвонароджених дітей та передчасних пологів майже в 2 рази перевищує аналогічні показники у жінок, які не працювали за комп'ютером під час вагітності. Вказується на несприятливий вплив роботи за комп'ютером також на серцево-судинну систему оператора, що пов'язано з гіподинамією, яка характерна для роботи операторів ВДТ.

Тривале обмеження навантаження на м'язовий апарат оператора може стати причиною функціональних порушень, а в деяких випадках призвести до виникнення атеросклерозу, аритмії, гіпертонічної хвороби, інфаркту міокарда. Відмічено зниження опірності організму та розвиток схильності до вірусних і багатьох інфекційних захворювань у операторів ВДТ. Збільшується відсоток хвороб органів травлення у осіб, які інтенсивніше використовували ВДТ. Частіше за інші форми відзначені хронічні гастрити та холецистити.

Довготривале перебування в одноманітній сидячій позі призводить до застійних процесів, зокрема в області малого таза, що може викликати гінекологічні порушення.

РОЗДІЛ 7 ЕКОЛОГІЯ

7.1 Методи визначення якості та обсягу забруднень

Методи визначення якості та обсягів забруднень. Для з'ясування, ступеня забруднення довкілля та впливу того чи іншого забруднювача (полютанта, токсиканта) на біоту й здоров'я людини, оцінки шкідливості забруднювачів і міри їхньої небезпечності, проведення екологічних експертиз довкілля в межах районів, регіонів чи окремих об'єктів.

Сьогодні в усьому світі використовують такі поняття, як гранично допустимі концентрації (ГДК) шкідливих речовин, гранично допустимі викиди (ГДВ) і скиди (ГДС), гранично допустимі екологічні навантаження (ГДЕН), ступінь екологічної витривалості ландшафту (СЕВЛ), максимально допустимий рівень забруднення (МДРЗ), кризова екологічна ситуація (КЕС), санітарно-захисні зони (СЗЗ) та ін. Гранично допустимі концентрації визначаються головними санітарними інспекціями в законодавчому порядку або рекомендуються відповідними установами, комісіями на підставі результатів складних комплексних наукових досліджень, лабораторних експериментів, а також відомостей, добутих під час і після різних аварій і катастроф на виробництвах, воєн, стихійних лих, із використанням матеріалів тривалих медичних спостережень на шкідливих підприємствах[7].

Використовують два нормативи ГДК шкідливих речовин:

1) максимальна разова доза, яка не викликає рефлекторних реакцій у людини;

2) середньодобова ГДК — максимальна доза, що не шкідлива для людини в разі тривалої (впродовж місяців, років) дії.

За даними ВООЗ, у чистому й здоровому довкіллі продуктивність праці підвищується на 10—15 %. Людині, яка перебуває в зеленій зоні, для відновлення

сил після важкого робочого дня потрібно на 60 % менше часу, ніж в індустріальному місті. В Україні стан довкілля контролюється кількома відомствами. Основний контроль здійснюється Міністерством екології і природних ресурсів, Міністерством охорони здоров'я, санітарно-епідеміологічними службами, гідрометслужбою та їхніми відділами в областях і районах, а додатковий контроль — службами комунального господарства, рибнагляду, геології та охорони надр, товариствами охорони природи, «зеленими» організаціями.

В основу нормування всіх забруднювачів покладено визначення ГДК у різних середовищах. У нормативних документах різних країн ГДК забруднювачів у воді, повітрі й фунтах, на жаль, часто відрізняються, хоча й неістотно (за рідкісним винятком, наприклад, норми вмісту діоксинів). ГДК полютанта — це такий його вміст у природному середовищі, за якого не знижується працездатність і не погіршується самопочуття людей, не завдається шкода їхньому здоров'ю в разі постійних контактів, а також відсутні небажані негативні наслідки для нащадків. Визначаючи ГДК, ураховують не лише ступінь впливу полютанта на здоров'я людей, а й також його дію на свійських і диких тварин, рослини, гриби, мікроорганізми й природні угруповання в цілому.

Новітні дослідження свідчать, що нижніх безпечних меж впливу канцерогенів та іонізуючої радіації немає. Будь-які дози, що перевищують звичайний природний фон, шкідливі. За наявності в повітрі або воді кількох забруднювачів їхня сукупна концентрація має не перевищувати одиницю (1). Для визначення максимальної разової ГДК використовують різні високочутливі тести, за допомогою яких виявляють мінімальні впливи забруднювачів на здоров'я людини в разі короткочасних контактів (вимірювання біопотенціалів головного мозку, реакції ока тощо). Для з'ясування наслідків тривалих впливів полютантів проводять експерименти на тваринах, використовують дані спостережень під час епідемій, аварій, додаючи до певного граничного значення коефіцієнт запасу, який знижує ГДК ще в кілька разів.

Для різних середовищ значення ГДК одних і тих самих токсикантів різні, як і максимальні разові та середньодобові ГДК одних і тих самих забруднювачів. На сьогодні визначено близько 3 тис. ГДК для забруднювачів води (близько 1500), повітря (близько 1000) і ґрунтів (близько 300), що найчастіше трапляються в оточенні людини, хоча необхідно знати принаймні 20 тис. ГДК різних забруднювачів, які виробляє людина й які негативно впливають на її здоров'я та існування. Якщо жабу кинути в посудину з гарячою водою, вона намагатиметься виплигнути звідти різким стрибком. Та коли посадити жабу в посудину з холодною водою й повільно її нагрівати, жаба загине, не помітивши поступового зростання температури.

Для того щоб, за законом про охорону довкілля, контролювати якість димогазових викидів різних підприємств і об'єктів, здійснюються обов'язкова інвентаризація всіх джерел забруднення атмосфери, їх екологічна паспортизація й періодична екологічна експертиза. Перевіряється відповідність затвердженим екологічним стандартам розмірів санітарно-захисних зон (їх п'ять класів — завширшки від 5—50 до 1000 м і більше, залежно від ступеня небезпечності токсикантів, які викидаються підприємством), їхнього стану, стану очисних установок, ефективності їхньої роботи тощо. Оцінюючи екологічні ситуації при складанні екологічних карт, використовують такі поняття, як екологічне навантаження, рівень техногенного навантаження[7].

7.2 Статистична оцінка техногенних впливів

Розвиток людського суспільства завжди відбувався і відбувається в тісній взаємодії з природою. Взаємодіючи з природою, людина завжди прагнула поліпшити свій добробут, зробити життя більш комфортним і матеріально забезпеченим. Це обумовило збільшення виробництва необхідної продукції промисловості та

сільського господарства і спричинило необмежене використання різноманітних природних ресурсів. Виробництво продукції, як відомо, пов'язане з утворенням відходів, які, потрапляючи в навколишнє природне середовище, забруднюють його.

Крім того, в процесі життєдіяльності людина цілеспрямовано перетворює природу, створюючи на місці природних систем техногенні об'єкти і території — міста і промислові комплекси, шляхи і лінії електропередач, водосховища і кар'єри.

Процес незворотного перетворення людиною частин біосфери на техногенні об'єкти і території дістав назву техногенезу, а частина біосфери, штучно перетворена в результаті життєдіяльності людини і заповнена її продуктами, називається технічною оболонкою біосфери (техносферою).

Основне завдання комплексної оцінки техногенного впливу:

-вивчення техногенних чинників забруднення довкілля,

-класифікація джерел забруднень,

-визначення джерел походження забруднень,

-всі проблемами людства, які породжують забруднення біосфери.

Техногенні чинники забруднення довкілля об'єднують у такі групи:

-атмосферні - хімічне, фізичне, механічне і теплове забруднення;

-водні - океани і моря, забруднення поверхневих і підземних вод;

-грунтові - хімічне, ерозійне забруднення, ущільнення, засолення, заболочення тощо;

-геологічні - негативні екзогенні процеси - зсуви, підтоплення, обвали, абразії берегів тощо;

-біотичні - деградації екосистем, збіднення біорізноманіття, мутації,

зникнення лісів і пасовищ, біогенна акумуляція шкідливих речовин тощо;

-комплексні - порушення природної структури ландшафтів, поява пустель, деградація земель.

Забруднення класифікують за галузевим принципом:

-промислові - хімічна промисловість, металургійна, видобувна тощо;

-транспортні - автотранспорт, авіаційний, морський тощо;

-енергетичні - теплові і атомні електростанції;

-сільськогосподарські - засоби захисту рослин, мінеральні та органічні добрива тощо;

-пов'язані з військовою діяльністю.

Вплив техносфери на стан атмосфери:

-найбільший вплив на стан атмосфери чинять теплоенергетика, металургійна промисловість, підприємства хімічної та будівельної індустрії, автотранспорт, що викидають у повітря пил, важкі метали, вуглеводні, оксиди карбону, бензапірен та інші речовини;

-найбільший вплив на хімічний склад атмосферного повітря чинить спалювання кам'яного вугілля;

-найпотужнішим негативним техногенним чинником є енергетика - підприємства чорної металургії утворюються пил та оксид сірки, хімічна і нафтохімічна промисловість продукують майже у два рази менше викидів при значно більшій різноманітності забруднюючих речовин; крім газоподібних речовин у повітря потрапляють рідкі і тверді частинки у вигляді аерозолів;

-серед усіх видів транспорту автомобільний посідає перше місце за кількістю і різноманітністю забруднюючих речовин, а також за кількістю незворотних змін ландшафтів та інших негативних впливів на довкілля. У містах з розвинутою

промисловістю внесок автотранспорту в забруднення довкілля досягає 80% усіх забруднень.

Проблеми, пов'язані з гідросферою, зумовлені нестачею прісної води для потреб людства, її' забрудненням, порушенням природних кругообігів та зменшенням продуктивності водних екосистем. Найбільшими забрудниками водних ресурсів є промисловість, комунальне і сільське господарства країни, яких в структурі забруднення водних ресурсів України складають стосовно 60, 20 і 17%. Важливою проблемою України є також забруднення підземних вод. У підземні води забруднюючі речовини потрапляють зі звалищ побутових і промислових відходів, при будівництві метро, бурінні свердловин внаслідок виливів нафти і нафтопродуктів під час добування чи переробки, у разі протікання нафтопроводів тощо. Всі ці забруднювачі (пестициди, нітрати, важкі метали, вуглеводні) можуть потрапляти з питними водами і в організм людини, спричиняючи отруєння чи захворювання.

Будь-який вплив людини на природні екосистеми призводить до їх змін, які викликають позитивні чи негативні наслідки для економіки і для всього суспільства. При вирішенні сучасних екологічних проблем великого значення набуває комплексна оцінка регіональних екологічних проблем, яка базується на глибокому вивченні та врахуванні всіх природних і соціально-економічних умов і факторів регіонів. Суть такої оцінки полягає в дослідженні просторової структури історично складених природно-територіальних комплексів та проведенні на цій основі розділу території країни (районуванню) на природні зони (області), округи та райони.

Основне завдання комплексної оцінки в конкретних регіонах полягає у:

-виявленні комплексу несприятливих факторів, що складають необхідний вихідний матеріал для прогнозування можливих негативних наслідків господарської діяльності,

-визначенні характеру і масштабів наслідків;

-виявленні причини на основі встановлення причинно-наслідкових зв'язків,

-розробці заходів, спрямованих на ліквідацію,

-попередженні і компенсації цих наслідків.

Основною метою комплексної оцінки території є встановлення суспільної значимості наслідків за існуючих масштабів господарського впливу на рівновагу екосистем[7].

Види негативного впливу на організм людини умовно можна об'єднати у дві групи: процеси прямого впливу і процеси непрямого впливу.

Процеси прямого впливу обумовлені безпосереднім контактом людини з техногенними об'єктами (механізмами, машинами) або робочими агентами цих об'єктів (високою температурою, токсичними речовинами, електричним струмом, електромагнітними полями чи іншими формами енергетичного впливу, активними біологічними організмами, ін.), що можуть завдавати шкоди здоров'ю людини або навіть призводити до її загибелі.

Процеси непрямого впливу на організм людини пов'язані з погіршенням умов життя і діяльності людини (склад повітря, температура, вологість, ін.), які зумовлюють процеси метаболізму в організмі людини. Щоб зрозуміти природу цих факторів впливу, досить задуматися про особливості функціонування такої складної матеріально-енергетично-інформаційної системи, якою є людський організм. Зміна будь-якого з тисяч параметрів (хімічних, фізичних, механічних, біологічних), що до того ж дуже тісно взаємодіють між собою, може виявитися достатньою, щоб серйозно погіршити фізіологічні функції організму людини.

Погіршення якості їжі і питної води є однією з найбільш небезпечних форм непрямого впливу. Це пояснюється чутливістю організму до процесів інтоксикації продуктів, у першу чергу тих, що відповідають за стан метаболізму в організмі людини. Слід підкреслити взаємозв'язок ступеня впливу таких екодеструктивних

факторів, як забруднення харчових продуктів і питної води, які, зрештою, визначають імунітет організму і його біологічну стійкість.

Серед основних факторів можна назвати: збалансованість і достатність харчування, можливості повноцінного відпочинку, здоровий спосіб життя та ін. Інтегральними оцінками впливу на організм людини є показники захворюваності і смертності населення.

Зниження інформаційної цінності природних систем, на відміну від попереднього виду впливу, діє не на організм людини, а на її особистісні характеристики. Повноцінне формування особистості людини може відбуватися тільки на тлі інформаційного контакту з природними системами. Інформаційне руйнування природних систем також негативно впливає на психологічний стан людини, а це збіднює резерви її природної життєвої активності, що, у свою чергу, негативно позначається на формуванні соціальних позицій[7].

ВИСНОВКИ

Під час виконання роботи було досліджено основні типи атак на комп’ютерні мережі, їх вразливості та методи захисту від них. Були розглянуті технології, які використовуються для побудови захищенною мережі, як від зовнішніх, так і внутрішніх загроз.

Мережа офісу ZoomSupport була досліджена та схематично відображена в роботі. Принцип надання прав доступу до ресурсів в мережі були розглянуті та описані. Сама мережа офісу була досліджена на вразливості, та можливі загрози. Відбулась спроба проведення атаки методом фішингу для отримання результатів, щодо вразливості мережі,а саме людського фактору в ній. За результатами дослідження було надано рекомендації щодо проведення тренінгів для робочого персоналу фірми, що зменшить можливість експлуатації цієї вразливості.

В спеціальному завданні було досліджено продукт компанії, який використовується для зворотнього зв’язку споживача з технічною підтримкою. Була виявлена вразливість, яка дозволяла зловмиснику, методом брутфорсу, отримати конфіденційну інформацію клієнта фірми. Були вжиті заходи для мінімізації можливої успішної експлуатації цієї вразливості.

Загальний стан захищенності мережі офісу ZoomSupport вважаю задовільним. Можливе подальше дослідження цієї проблеми з часом, після застосувань рекомендованої профілактики персоналу. Як результат, буде мінімізована можлива втрата конфіденційної інформації користувачів продукту компанії та утримання позиції на ринку.

БІБЛІОГРАФІЯ

1. Гайворонський М.В., Новіков О. М. Безпека інформаційно-комунікаційних систем. — К.: Видавнича група BHV, 2009. — 608с

2. Олифер В.Г, Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. – СПб.: Питер, 2003;

3. Якубайтис Э.А. Архитектура вычислительных сетей. – М.: Статистика, 1980. – 279 с.

4. Решетняк В.Н., Гузик В.Ф., Сидоренко В.Г. «Проектирование распределенных информационно-вычислительных систем.» Учеб. пособие. Таганрог: ТРТУ

5. Д. Филлипс, А. Гарсия-Диас «Методы анализа сетей», М., Мир, 1984. - 496 с.

6. Таненбаум Э. Компьютерные сети. 4-е изд. [Текст]/ Э. Таненбаум. – СПб.: Питер, 2008. – 992 с.

7. Тарасова В.В. «Екологічна статистика», 2008, - 392с.

8. Hypervisors [Інтернет ресурс] - Режим доступу: https://www.sim-networks.com/blog/hypervisors-vmware-kvm-xen-openvz

9. Протокол 802.1X [Інтернет ресурс] – Режим доступу: http://xgu.ru/wiki/802.1X

10. Active Directory [Інтернет ресурс] – Режим доступу: http://itmu.vsuet.ru/Posobija/AD/htm/1_t.htm

11. VLAN [Інтернет ресурс] – Режим доступу: http://xgu.ru/wiki/VLAN

12. Мережеві атаки. Види. Засоби боротьби [Інернет ресурс] – Режим доступу: https://moluch.ru/conf/tech/archive/5/1115/

13. Вплив комп’ютерів на працездатність людини [Інтернет ресурс] – Режим доступу: https://pidruchniki.com/92830/bzhd/vpliv_kompyuteriv_pratsezdatnist_zdorovya_koristuvachiv

14. ДСТУ ISO/IEC TR 13335-1:2001 Інформаційні технології. Настанова для керування ІТ безпекою.

15. Гарасим Ю.Р. Структура технологій функціонування систем захисту інформації корпоративних мереж зв’язку / Ю.Р. Гарасим, В.Б. Дудикевич // матер. IV Міжнар. наук.-практ. конф. “Спеціальна техніка у правоохоронній діяльності”. – К., 2009. – С. 226–228.

16. Біленчук П. Концепція забезпечення безпеки інформації на об’єкті в умовах необхідної ситуації // Бизнес и безопасность. – 2008. – № 5. – С.96–98.

17. Стан і проблеми забезпечення інформаційної безпеки [Електронний ресурс]. – Режим доступу: http://old.niss.gov.ua/book/otch/roz13.htm.

ДОДАТКИ