

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДОНЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ВАСИЛЯ СТУСА
СТОРОЖЕВ ВЛАДИСЛАВ ВАЛЕРІЙОВИЧ

Допускається до захисту:

завідувач кафедри

інформаційних технологій,

к.т.н., доцент

_____ Нескородева Т.В.

« _____ » _____ 20__ р.

АПАРАТНО-ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ ІНТРАНЕТУ НА
ПІДПРИЄМСТВІ НА ПРИКЛАДІ ЦЕНТРУ ВАКЦИНАЦІЇ / HARDWARE
AND SOFTWARE PROTECTION OF THE INTRANET AT THE
ENTERPRISE ON EXAMPLE OF THE VACCINATION CENTER

Спеціальність 125 Кібербезпека

Кваліфікаційна (бакалаврська) робота

Керівник:

Крижановський В.Г., професор кафедри

інформаційних технологій

д-р.т.н, професор

Оцінка: ____/ ____/ _____

(бали за шкалою ЄКТС/за національною шкалою)

Голова ЕК: _____

(підпис)

Вінниця 2021

АНОТАЦІЯ

Сторожев В.В. Апаратно-програмні засоби захисту інтранету на підприємстві на прикладі центру вакцинації. Спеціальність 125 «Кібербезпека», Освітня програма «Кібербезпека». Донецький національний університет імені Василя Стуса, Вінниця, 2021.

У кваліфікаційній роботі обґрунтоване використання приватного віртуального серверу для розгортання внутрішньої мережі організації, описано модель діяльності обраного підприємства та запропоновано елементи, що складатимуть інтрамережу. Для захисту запропоновано використання смарт-карток для ідентифікації працівника на робочому місці та приведено приклад налаштування приватного віртуального серверу із набором програм ConfigServer Security and Firewall (CSF), fail2ban, Maldet.

Ключові слова: інтранет, системи захисту, захист бізнесу.

Табл. 2. Рис. 1. Бібліограф.: 19 найм.

Storozhev V. Hardware and software protection of the intranet at the enterprise on example of the vaccination center. Speciality 125 «Cybersecurity», Programme «Cybersecurity». Vasyl` Stus Donetsk National University, Vinnytsia, 2021.

The master`s work substantiates the use of a private virtual server for the deployment of the internal network of the organization, describes the model of the selected enterprise and proposes the elements that will form an intranet. For protection, the use of smart cards to identify the employee in the workplace is proposed and an example of setting up a private virtual server with a set of programs ConfigServer Security and Firewall (CSF), fail2ban, Maldet.

Keywords: intranet, security systems, business protection.

Tab. 2. Fig. 1. Bibliography: 19 items.

ЗМІСТ

ВСТУП	4
РОЗДІЛ 1. ПРОВЕДЕННЯ ПОПЕРЕДНЬОГО ОБСТЕЖЕННЯ	5
1.1 Основні поняття.....	5
1.2 Програмні і апаратні засоби забезпечення безпеки інформації.....	7
1.3 Опис моделі діяльності центру вакцинації “Здоров’я”	8
1.4 Виявлення інформації, що підлягає захисту.....	9
1.5 Типові інформаційні загрози для корпоративної мережі.....	9
1.6 Аналіз існуючих програмних рішень для безпеки корпоративних мереж	12
1.6.1 Міжмережевий екран	12
1.6.2 Системи виявлення вторгнень (IDS).....	16
1.6.3 Системи протидії вторгненням (IPS).....	17
1.6.4 Антивірусне програмне забезпечення.....	18
1.6.5 Системи управління обліковими записами (IDM)	20
1.6.6 Захист веб-додатків (WAF)	21
1.6.7 Резервне копіювання	22
1.7 Аналіз існуючих апаратних рішень для безпеки корпоративних мереж	24
РОЗДІЛ 2 . ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ.....	25
2.1 Сервіси, що складають мережу компанії.....	25
2.2 Схема внутрішньої мережі організації.....	31
2.3 Розміщення серверу	33
2.4 Порівняння операційних систем	37
РОЗДІЛ 3. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБЛЕННЯ ВНУТРІШНЬОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ ВІРТУАЛЬНОГО ПРИВАТНОГО СЕРВЕРУ.....	43
3.1 Налаштування приватного віртуального серверу	43
3.2 Практичні рекомендації з впровадження систем захисту	49
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	52
ДОДАТОК А – Аналіз популярних хостинг провайдерів в Україні	54

ВСТУП

Потреба у захисті інформації у сучасному суспільстві існує не тільки у підприємств великого і середнього бізнесу, але й у малого. Регулярна поява нових загроз вимагає постійного вдосконалення захищеності будь-якої організації, тому що у іншому випадку при реалізації загрози підприємству може бути нанесено непоправну шкоду. Можливості малого бізнесу часто не дозволяють організувати роботу спеціальних служб, що забезпечують інформаційну безпеку організації, та здійснюють виявлення, попередження та усунення загроз, що в ній виникають.

Малий бізнес являється одним з найменш захищених від загроз інформаційній безпеці з ряду причин:

1. Висока вартість засобів захисту інформації;
2. Потреба в залученні сторонніх кваліфікованих спеціалістів у області захисту інформації;
3. Недостатнє методичне забезпечення діяльності по розробці систем захисту інформації.

Актуальність даної роботи полягає у виборі достатніх програмних та апаратних засобів захисту інформації для впровадження нової організації на ринок реалізації медичних препаратів.

Об'єктом даної роботи є приватний центр вакцинації "Здоров'я", що займається вакцинацією населення.

Предметом бакалаврської роботи є система захисту інформації.

Метою бакалаврської роботи є аналіз існуючих апаратних та програмних засобів для реалізації та захисту бізнес-процесів підприємства, а також надання практичних рекомендацій для вибору оптимального рішення.

РОЗДІЛ 1. ПРОВЕДЕННЯ ПОПЕРЕДНЬОГО ОБСТЕЖЕННЯ

1.1 Основні поняття

Під інформацією, стосовно задачі її захисту розуміються відомості про осіб, предмети, факти, події явища і процеси незалежно від форми їх подання. Залежно від форми подання інформація може бути усною, телекомунікаційною, документованою.

Інформаційні процеси - процеси збору, накопичення, обробки, зберігання, розподілу та пошуку інформації.

Інформаційна система – сукупність документів і масивів документів та інформаційних технологій.

Операційна система ОС (Операційна система, ОС) – це сукупність програм, що діють як інтерфейс (панель взаємодії) між користувачем та апаратним забезпеченням комп'ютера. Щоб комп'ютер працював належним чином, потрібно встановити принаймні одну операційну систему. Без програмного середовища операційної системи всі комп'ютерні програми, такі як текстові та графічні редактори, електронні таблиці, бази даних, Інтернет-браузери тощо, не можуть працювати та виконувати свої завдання, а програмне середовище операційної системи надаватиме їм необхідні послуги.

Інформаційними ресурсами називають документи або масив документів існуючі окремо або в складі інформаційної системи.

Процес створення оптимальних умов для задоволення інформаційних потреб громадян, організацій, суспільства і держави називається інформатизацією. Інформатизація розділяється на відкриту і обмеженого доступу.

Інформація є одним з об'єктів цивільного права тому числі і прав власності, володіння, користування. Власник інформаційних ресурсів, технологій і систем - суб'єкт з правом володіння, користування і розподілу зазначених об'єктів. Власником ресурсів, технологій і систем є суб'єкт з повноваженнями володіння і користування зазначеними об'єктами. Під

користувачем розуміється суб'єкт, який звертається до інформаційної системи за отриманням потрібної інформації і користується нею.

До захищеної відноситься інформація, яка є предметом власності і підлягає захисту відповідно до вимог правових документів або вимогами, висунутими власником інформації.

Під витокіом інформації розуміють неконтрольоване поширення захищеної інформації шляхом її розголошення, несанкціонованого доступу і отримання розвідниками. Несанкціонований доступ - отримання захищеної інформації зацікавленим суб'єктом з порушенням правил доступу до неї.

Несанкціонований вплив на захищену інформацію це вплив з порушенням правил її зміни (наприклад, підміна електронних документів). Під ненавмисним впливом на захищену інформацію розуміється вплив на неї через помилку користувача, збій техніки, або програмних засобів, природних явищ та інших ненавмисних дій (наприклад, знищення документа на жорсткому диску).

Метою захисту інформації є запобігання нанесення шкоди користувачеві або власнику. Під ефективністю захисту інформації розуміється ступінь відповідності результатів захисту поставленої мети. Об'єктом захисту може бути інформація, її носій, інформаційний процес, щодо якого необхідно проводити захист відповідно до поставлених цілей.

Конфіденційність інформації - це знання про її зміст тільки тих суб'єктів, що мають відповідні повноваження.

Шифрування інформації - це перетворення інформації, в результаті, якого зміст інформації стає незрозумілим для суб'єкта, що не має відповідного доступу. Результат шифрування називається шифротекстом.

Під загрозою інформаційної безпеки в комп'ютерній системі(далі - КС) розуміють події або дії, які можуть викликати зміни функціонування КС, пов'язані з порушенням захищеності інформації оброблюваної в ній.

Уразливість інформації - це можливість виникнення на будь-якому етапі життєвого циклу КС такого її стану, при якому створюються умови для реальної загрози безпеці в ній.

Атака – це дії, що виконуються порушником для пошуку і використання тієї або іншої уразливості.

Загроза інформаційної безпеки – сукупність умов і факторів, що створюють небезпеку порушення інформаційної безпеки. Під загрозою розуміється потенційно можлива подія, дія або вплив, процес або явище, які можуть спричинити шкоду чиймось інтересам. Загрози можуть бути розділені на загрози, незалежні від діяльності людини і штучні загрози, пов'язані з діяльністю людини.

Результатом реалізації загроз може бути витік, спотворення або втрата інформації.

1.2 Програмні і апаратні засоби забезпечення безпеки інформації

До апаратних засобів захисту інформації відносяться апаратні та програмно-апаратні пристрої, що включаються до складу КС і виконують (як самостійно, так і за допомогою програмних засобів) деякі функції по забезпеченню безпеки інформації.

До основних апаратних засобів захисту інформації відносяться:

- пристрої введення інформації, що ідентифікує користувача;
- пристрої шифрування інформації;
- пристрої для запобігання несанкціонованого включення робочих станцій та серверів.

Під програмними засобами інформаційної безпеки розуміють спеціальні програмні засоби, що включаються до складу програмного забезпечення КС виключно для виконання захисних функцій.

До основних програмних засобів захисту інформації відносяться:

- програми ідентифікації, аутентифікації користувачів КС;
- програми розмежування доступу користувачів до ресурсів КС;

- програми для захисту від несанкціонованого доступу, копіювання, зміни і використання.

Під ідентифікацією користувача, стосовно забезпечення безпеки КС, однозначне розпізнання унікального імені суб'єкта КС. Аутентифікація означає підтвердження того, що пред'явлене ім'я відповідає саме даному суб'єкту.

До переваг програмних засобів захисту інформації відносяться:

- простота тиражування;
- гнучкість (можливість налаштування на різні умови застосування);
- простота застосування;
- практично необмежені можливості їх розвитку;

До недоліків програмних засобів відносяться:

- зниження ефективності КС за рахунок споживання її ресурсів, необхідних для функціонування програм захисту;
- більш низька продуктивність у порівнянні з аналогічними функціями захисту апаратними засобами.

1.3 Опис моделі діяльності центру вакцинації “Здоров’я”

Модель діяльності представляє собою опис базових бізнес-процесів, які представляють сукупність простих заходів, що слугують для створення кінцевої послуги. Дана модель необхідна для виявлення інформаційних потоків та інформації обмеженого доступу, що циркулює на підприємстві.[1]

Центр вакцинації являє собою структуру, що надає послуги з введення ін'єкцій для вироблення імунітету проти захворювань у людей. Основною діяльністю являється платна вакцинація людей у будівлі центру. Для реєстрації на отримання ліків використовується сайт компанії при заповненні форми чи заявки на зворотній виклик або за прямим телефонним дзвінком на гарячу лінію.

Додаткова діяльність бізнесу – проведення тестів на різні хвороби, виїзд лікаря на місце для проведення тестування або щеплення.

Обов'язковою умовою для надання послуг центром є реєстрація клієнта у базі, заповнення його особової картки, для якої використовуються персональні дані. За допомогою цієї картки здійснюється обов'язковий облік медичних послуг, які отримала людина.

1.4 Виявлення інформації, що підлягає захисту

В ході аналізу діяльності “Здоров'я” була виявлена інформація обмеженого доступу, яка представляє собою відомості, що відносяться до конфіденційної та службової інформації:

- персональні дані співробітників підприємства, клієнтів та партнерів, що збережені в БД і передаються по мережі;
- повідомлення електронної пошти та інформація БД, що містять службові відомості, інформацію про діяльність підприємства і т.п. ;
- конструкторська і технологічна документація, перспективні плани розвитку, модернізації виробництва, реалізації продукції та інші відомості, що становлять науково-технічну і технологічну інформацію, пов'язану з діяльністю підприємства;
- фінансова документація, бухгалтерська звітність, аналітичні матеріали досліджень про конкурентів і ефективності роботи на фінансових ринках;
- інші відомості, що становлять ділову інформацію про внутрішню діяльність підприємства.

1.5 Типові інформаційні загрози для корпоративної мережі

Загрози інформаційної (комп'ютерної) безпеки - це різні дії, які можуть привести до порушень стану захисту інформації. Іншими словами, це - потенційно можливі події, процеси або вплив, які можуть завдати шкоди інформаційним та комп'ютерним системам. Загрози ІБ можна розділити на два типи: природні і штучні. До природних відносяться природні явища, що не залежать від людини, наприклад урагани, повені, пожежі і т.д. Штучні загрози залежать безпосередньо від людини і можуть бути навмисними і

ненавмисними. Ненавмисні загрози виникають через необережність, неухважність і незнання. Прикладом таких загроз може бути встановлення програм, що не входять в число необхідних для роботи і в подальшому порушують роботу системи, що і призводить до втрати інформації. Навмисні загрози, на відміну від попередніх, створюються спеціально. До них можна віднести атаки зловмисників як ззовні, так і зсередини компанії. Результат реалізації цього виду загроз - втрати коштів та інтелектуальної власності організації.[2]

Залежно від різних способів класифікації всі можливі загрози інформаційної безпеки можна розділити на наступні основні підгрупи:

- небажаний контент;
- несанкціонований доступ;
- витік інформації;
- втрата даних;
- шахрайство;
- кібервійни;
- кібертероризм.

Небажаний контент – шкідливий код, потенційно небезпечні програми і спам, тобто те, що безпосередньо створено для знищення або крадіжки інформації.

Несанкціонований доступ – перегляд інформації співробітником, який не має дозволу користуватися нею, шляхом перевищення посадових повноважень. Несанкціонований доступ призводить до витоку інформації. В залежності від того, які дані і де вони зберігаються, витoki можуть організовуватися різними способами, а саме через атаки на сайти, злом програм, перехоплення даних по мережі, використання несанкціонованих програм.

Витоки інформації можна розділяти на умисні й випадкові. Випадкові витoki відбуваються через помилки обладнання, програмного забезпечення та

персоналу. Умисні, в свою чергу, організовуються навмисно з метою отримання доступу до даних, завдання шкоди.

Втрату даних можна вважати однією з основних загроз інформаційній безпеці. Порухення цілісності інформації може бути викликано несправністю обладнання або навмисними діями людей, співробітників або злоумисників.

Не менш небезпечною загрозою є шахрайство з використанням інформаційних технологій «фрод». До шахрайства можна віднести не тільки маніпуляції з кредитними картами «кардинг» і злом онлайн-банку, але і внутрішній фрод. Метою таких економічних злочинів є обхід законодавства, політики безпеки або нормативних актів, привласнення майна.[3]

Терористична загроза зростає щорічно по всьому світу, поступово переходячи при цьому в віртуальний простір. На сьогоднішній день нікого не дивує можливість атак на автоматизовані системи управління технологічними процесами (АСУ ТП) різних підприємств. Але подібні атаки не проводяться без попередньої розвідки, для чого застосовується кібершпіднаж, що допомагає зібрати необхідні дані. Існує також таке поняття, як «інформаційна війна»; вона відрізняється від звичайної війни тим, що в якості зброї виступає ретельно підготовлена інформація.[4]

Порушення режиму інформаційної безпеки може бути викликано як спланованими операціями злоумисників, так і недосвідченістю співробітників. Користувач повинен мати хоча б мінімальне поняття про ІБ, шкідливе програмне забезпечення, щоб своїми діями не завдати шкоди компанії і самому собі. Такі інциденти, як втрата або витік інформації, можуть також бути обумовлені цілеспрямованими діями співробітників компанії, які зацікавлені в отриманні прибутку в обмін на цінні дані організації, в якій працюють або працювали. Основними джерелами загроз є окремі злоумисники, так звані «хакери», кіберзлочинні групи і державні спецслужби (кіберпідрозділи), які застосовують весь арсенал доступних кіберзасобів, перерахованих і описаних вище. Щоб пробитися через захист і отримати доступ до потрібної інформації, вони використовують слабкі місця і помилки

в роботі програмного забезпечення і веб-додатків, вади в конфігураціях мережеских екранів і налаштуваннях прав доступу, вдаються до прослуховування каналів зв'язку і використання клавіатурних шпигунів.

1.6 Аналіз існуючих програмних рішень для безпеки корпоративних мереж

Для організації інформаційної безпеки існують спеціалізовані програми, розроблені на основі сучасних технологій:

- захист від небажаного контенту (антивірус, антиспам, веб-фільтри, анти-шпигуни);
- міжмережескі екрани та системи виявлення вторгнень (IDS);
- управління обліковими записами (IDM);
- захист від DDoS;
- захист веб-додатків (WAF);
- антифрод;
- захист від таргетованих атак;
- системи виявлення аномальної поведінки користувачів (UEBA);
- захист від витоків даних (DLP);
- шифрування;
- резервне копіювання;
- системи відмовостійкості.

1.6.1 Міжмережеский екран

Основним завданням міжмережеского екрану є запобігання несанкціонованому доступу до локальної мережі. Прикладом небажаного доступу є порушник, який намагається незаконно здійснити проникнення до систем, доступ до яких здійснюється через мережу. Можливо, він просто отримує задоволення від злому систем, а може він намагається пошкодити інформаційну систему чи використати її у власних цілях. Як приклад, він може використовувати інформаційну систему, щоб отримати компрометуючу інформацію про пацієнтів, яка може міститись у ній, з метою шантажу.

Міжмережеві екрани – це плагіни або програмно-апаратні засоби, що регулюють потік мережевого трафіку між хостами та цілими мережами, що мають різні вимоги до безпеки. Більшість міжмережевих екранів розташовано на межі мережевого периметра, і в першу чергу вони призначені для захисту внутрішніх хостів (комп'ютерів) від зовнішніх атак. Міжмережеві екрани пропускають або забороняють трафік, порівнюючи його характеристики з шаблонами, заданими в політиці брандмауера. Можливості фільтрування, виконуваного міжмережевими екранами, з плином часу постійно збільшувалась. Найчастіше можливості міжмережевих екранів порівнюють за кількістю рівнів в стеці протоколів TCP/IP, які вони можуть аналізувати.

Базовою можливістю брандмауера є фільтрування пакетів. Спочатку міжмережеві екрани були частиною маршрутизаторів, забезпечуючи управління доступом на основі адрес хостів і комунікаційних сесій. Ці пристрої, відомі як міжмережеві екрани без аналізу стану, не підтримували інформацію про стан потоку трафіку, який проходить через міжмережевий екран. Це означає, що вони не можуть визначити, що кілька запитів належать одній сесії. Фільтрування пакетів є основою більшості сучасних міжмережевих екранів, хоча залишилося небагато пакетних фільтрів, які виконують фільтрування без підтримки стану. На відміну від більш потужних фільтрів, пакетні фільтри аналізують тільки заголовки мережевого і транспортного рівнів, а не вміст пакетів. Управління трафіком визначається набором директив, які називаються ruleset. Можливості фільтрування пакетів вбудовані в більшість ОС і пристроїв, що виконують маршрутизацію. Найтипівішим прикладом є маршрутизатор, в якому визначені списки управління доступом.[5]

Основною перевагою пакетних фільтрів є їх швидкість. Так як пакетні фільтри зазвичай перевіряють дані тільки в заголовках мережевого і транспортного рівнів, вони можуть виконувати це дуже швидко.

З цих причин пакетні фільтри, вбудовані в прикордонні маршрутизатори, ідеальні для розміщення на кордоні з мережею з невисоким

ступенем довіри. Пакетні фільтри, вбудовані в прикордонні маршрутизатори, можуть блокувати основні атаки, фільтруючи небажані протоколи, виконуючи найпростіший контроль доступу на рівні сесій і потім передаючи трафік іншим міжмережевим екранів для перевірки даних на більш високих рівнях стека протоколів.

Переваги пакетних фільтрів:

- основною перевагою пакетних фільтрів є їх швидкість;
- пакетний фільтр є прозорим для хостів і серверів, тому що не розриває TCP-з'єднання.

Недоліки пакетних фільтрів:

- виходячи з того, що пакетні фільтри не аналізують більш високі рівні даних, вони не можуть попередити атаки, які використовують уразливості, специфічні для програми. Наприклад, пакетний фільтр не може блокувати конкретні команди додатку; якщо пакетний фільтр дозволяє даний трафік для додатка, то всі операції, визначені в цьому додатку, будуть дозволені;
- в логах пакетного фільтра знаходиться інформація лише про параметри мережевого і транспортного рівнів. Зазвичай у них знаходиться та ж інформація, яка використовувалася при прийнятті рішення про можливість доступу (адреса джерела, адреса призначення, вид трафіку і т.п.);
- більшість пакетних фільтрів не підтримують можливість аутентифікації користувача. Дана можливість забезпечується міжмережевими екранами, які аналізують більш високі рівні;
- пакетні фільтри зазвичай уразливі для атак, які використовують такі уразливості TCP / IP, як підробка (spoofing) мережевої адреси. Велика кількість пакетних фільтрів не можуть визначити, що в мережевому пакеті змінена адресна інформація транспортного рівня. Spoofing-атаки зазвичай виконуються для обходу управління доступом, що здійснюється фаєрволом.
- пакетні фільтри важко конфігурувати. Можна випадково змінити налаштування пакетного фільтра для пропускання типів трафіку, джерел і призначень, які повинні бути заборонені;

- так як номер порту клієнта може бути будь-яким, так званим «Великим номером» (від 1023 до 65535), то на міжмережевому екрані доводиться відкривати всі порти з номерами більше 1023.[6]

Аналіз стану відкриває можливість контролю стану з'єднання та блокування пакетів, які не з'являються в очікуваний час. Саме для цього виконується аналіз даних транспортного рівня.

Подібним чином, за допомогою простої фільтрації пакетів замість видалення матеріалу, екран проводить аналіз на відповідність правилам мережевого рівня. Але на відміну від фільтрації пакетів, контроль стану відстежує історію кожного із з'єднань, користуючись таблицею станів. Хоча деталі записів таблиці станів багато в чому залежать від конкретної реалізації брандмауера, як правило вони містять IP-адресу джерела, IP-адресу одержувача і інформацію про стан з'єднання.

По суті, міжмережеві екрани з аналізом стану додають в пакетний фільтр розуміння логіки протоколу транспортного рівня. Міжмережеві екрани з аналізом стану мають ті ж самі сильні і слабкі сторони, як і пакетні фільтри, але все ж міжмережеві екрани з аналізом стану зазвичай вважаються більш безпечними, ніж пакетні фільтри.

Останнім часом спостерігається тенденція до аналізу станів, що полягає в додаванні можливостей аналізу станів протоколу, яке деякими виробниками називається глибоким аналізом пакета (deep packet inspection). Аналіз стану протоколу додає в стандартний аналіз стану базову технологію виявлення вторгнення, яка проводить аналіз протоколу на прикладному рівні, порівнюючи поведінку його з визначеними виробником профілями і зазначаючи відхилення в поведінці. Це робить міжмережевий екран здатним дозволяти або забороняти доступ, ґрунтуючись на тому, як виконується програма. Наприклад, міжмережевий екран прикладного рівня спроможний визначити, що поштове повідомлення містить заборонений тип приєднаного файлу (наприклад виконуваний файл). Інша можливість полягає в тому, що він може блокувати з'єднання, в яких виконуються деякі підозрілі дії (наприклад,

присутні команди put в FTP). Дана можливість також дозволяє вирішувати або забороняти передавати веб-сторінки в залежності від конкретних типів вмісту, такого як Java або ActiveX, або перевіряти, що SSL сертифікати підписані конкретним ЦС.

Міжмережеві екрани прикладного рівня отримали можливість визначати небажану послідовність команд, таку як деякі повторювані команди або команда, якій не передуює інша команда, від якої залежить дана команда. такі підозрілі команди часто означають атаки переповнення буфера, DoS-атаки або інші атаки, пов'язані з прикладними протоколами, таким як HTTP.

Можна з точністю сказати, що використання лише тільки міжмережєвих екранів не забезпечує повного захисту від усіх проблем, породжених Інтернетом. Як результат, міжмережеві екрани є тільки однією з цеглин у фундаменті інформаційної безпеки.

В будь-якому випадку, використання міжмережевого екрану є обов'язковою складовою для внутрішньої мережі організації для чіткого визначення периметру. Головною функцією фаєрволу є захист від зовнішніх загроз для окремо взятого вузла мережі. Але це не означає, що для кожного серверу потрібно встановлювати власний – навпроти, набагато зручніше буде встановлення одного фаєрволу в периметрі, але налаштованого передавати відповідний трафік до різних вузлів відповідно їх функціональним ролям.

1.6.2 Системи виявлення вторгнень (IDS)

Система виявлення вторгнень (Intrusion Detection System) – це комплекс програмного та апаратного забезпечення, метою якого виступає виявлення фактів несанкціонованого доступу до комп'ютера чи мережі комп'ютерів, а також попередження можливості управління ними. Будь-яка зловмисна діяльність або порушення зазвичай повідомляється або збирається централізовано, використовуючи інформацію про безпеку та систему управління подіями.

Системи виявлення вторгнень реалізують функцію для виявлення шкідливої діяльності, яка може негативно вплинути на безпеку внутрішньої мережі. Прикладами такої діяльності є атаки, спрямовані на вразливі сервіси, або на підвищення привілеїв (Escalation of Privilege), несанкціонований доступ до захищених ресурсів, чи негативний вплив від роботи шкідливого програмного забезпечення (віруси, трояни і т.д.).

IDS призначені для автоматизації процесу моніторингу та аналізу подій, що відбуваються у внутрішній мережі, або на конкретному вузлі з метою виявлення шкідливих дій (атак чи вторгнень).

Для вирішення поставленого завдання IDS повинна виконувати такі основні функції:

- моніторинг подій з метою виявлення інцидентів інформаційної безпеки (ІБ);
- запис інформації про дані інциденти як локально, так і з відправкою в будь-яку централізовану систему збору логів або SIEM-систему;
- повідомлення адміністраторів ІБ про інциденти (email, SNMP-трапи, SMS, консоль управління системи IDS);
- створення звітів, що уточнюють або, навпаки, узагальнюючих інформацію по одному або декільком подіям.[7]

1.6.3 Системи протидії вторгненням (IPS)

Таким чином, IDS може попередити про шкідливу активність, але найпоширенішим завданням є саме попередження шкідливої діяльності на ранній стадії. У цьому можуть допомогти системи Intrusion Prevention System. Методи її роботи, на відміну від IDS, яка виконує пасивні функції, відносяться до своєчасних (превентивних) та ініціативних. Варто зазначити, що IPS є підкатегорією IDS, тому заснована на її методах виявлення атак. IPS може працювати як на рівні хоста (HIPS), так і на рівні мережі (NIPS). Можливість запобігання атак реалізована за рахунок того, що мережева IPS, як правило, вбудовується “в розрив” мережі і пропускає весь трафік через себе, а також має зовнішній інтерфейс, на який приходить трафік і внутрішній інтерфейс,

який пропускає трафік далі, якщо він визнається безпечним. Існує також можливість роботи з копією трафіку в режимі моніторингу, але тоді втрачається основний функціонал даної системи.

У глобальному масштабі IPS можна розділити на такі, що аналізують трафік і порівнюють його з відомими сигнатурами і ті, які на основі аналізу протоколів здійснюють пошук нелегітимного трафіку, ґрунтуючись на базі даних про знайдені раніше вразливості. За рахунок другого класу забезпечується захист від невідомого типу атак. Що стосується методів боротьби з атаками, то їх накопичилась велика кількість, але з основних можна виділити наступні: блокування з'єднання з використанням TCP-пакета з RST-прапором або за допомогою брандмауера, зміна налаштувань комунікаційних пристроїв, а також блокування записів користувачів або конкретного хоста в інфраструктурі.

Врешті-решт, найбільш ефективною концепцією захисту інфраструктури є спільне використання систем IDS і IPS в одному продукті - міжмережевому екрані, який використовує поглиблений аналіз мережевих пакетів, виявляє атаки і блокує їх. Варто зазначити, що мова йде тільки про один рубіж захисту, який, як правило, розташований за фаєрволом.[8]

1.6.4 Антивірусне програмне забезпечення

Антивірус (антивірусна програма, засіб антивірусного захисту, засіб виявлення шкідливих програм) – спеціалізована програма для виявлення комп'ютерних вірусів, а також небажаних (тих, що вважаються шкідливими) програм і відновлення заражених (модифікованих) такими програмами файлів, а також для профілактики – запобігання зараженню (модифікації) файлів або операційної системи шкідливим кодом.

Для захисту від вірусів використовують три групи методів:

- методи, засновані на аналізі вмісту файлів (як файлів даних, так і файлів з кодами команд). Ця група включає сканування сигнатур вірусів, а також перевірку на цілісність і сканування підозрілих команд;

- методи, засновані на відстеженні поведінки програм під час їх виконання. Ці методи мають реєструвати всі події, які загрожують безпеці системи. Такі події відбуваються під час фактичного виконання коду, що перевіряється або під час його програмного моделювання;

- методи управління порядком роботи з файлами і програмами. Ці методи стосуються адміністративних заходів забезпечення безпеки.

Даний вид програм є необхідним для встановлення на АРМ працівників та поштовий сервер. Для робочих станцій вони потрібні тому що робітник у процесі роботи може не помітити різницю між звичайним робочим файлом і тим, у який вбудовано шкідника. В результаті запуску такої програми зловмисник, що її створив може отримати доступ до ресурсів компанії. Для серверу електронної пошти антивірус є необхідним тому що вона є одним з найчастіше використовуваних векторів атак шляхом соціальної інженерії, при цьому прикріплюючи до повідомлення файли з “дуже важливою” інформацією.

Ще одним важливим елементом для працездатності поштового серверу та для покращення досвіду користування нею потрібно передбачити антиспам систему. Антиспам - це програма, яка використовується для виявлення і фільтрації небажаних електронних повідомлень, які можуть надходити через поштові сервери компанії та публічні сервіси електронної пошти. Зазвичай під спамом розуміється масова розсилка реклами, проте зловмисники можуть також відправляти і особисті повідомлення користувачам, які не бажають отримувати таку інформацію.

У будь-якій системі, яка передбачає спілкування користувачів, завжди існує проблема спаму, або масової розсилки небажаних електронних листів, яка вирішується за допомогою антиспам системи. Антиспам система встановлюється для фіксування та фільтрації спаму на різних рівнях. Контроль і ідентифікація спаму актуальні на корпоративних серверах, які підтримують роботу корпоративної пошти, тут система антиспаму фільтрує повідомлення ще на сервері, перш ніж спам потрапить до поштової скриньки.

Існує багато програм, які можуть допомогти впоратися з цим завданням, проте не всі вони однаково корисні. Основним завданням таких програм є припинення пересилання небажаних листів, проте методирозцінювання та припинення таких дій можуть принести не тільки користь, але і шкоду для організації. Так, згідно з правилами та політикою поштового серверів, домен може бути внесений до «чорного списку» і через нього буде обмежено передачу листів, причому власник може навіть не бути про це попереджений.

Основні види установки і використання антиспам систем:

- установка спеціалізованого обладнання, шлюзу, яке займається фільтрацією пошти перед тим, як вона потрапить на сервер;
- використання зовнішніх антиспам систем для аналізу листів та вмісту;
- настройка антиспам системи з можливістю навчання на сам поштовий сервер;
- установка програми фільтрації спаму на комп'ютері робітника.

1.6.5 Системи управління обліковими записами (IDM)

Системи управління обліковими записами і доступом (Identity and Access Management) – це клас рішень для автоматичного управління обліковими записами і ролями користувачів інформаційних систем. Системи управління обліковими записами також дозволяють проводити аудит доступу користувачів, обробляти електронні заявки на отримання доступу та готувати звіти. Даний клас рішень дозволяє вирішувати наступні завдання:

- зменшення кількості заявок, що надходять до внутрішньої служби технічної підтримки користувачів;
- зменшення часу, необхідного для отримання доступу користувачем;
- права, що призначаються користувачам, вже заздалегідь введені у рольову модель, і не призначаються стихійно;
- зниження ризиків інформаційної безпеки і помилок, заснованих на людському факторі;
- виконання контролю прав доступу користувачів.

Особливість використання системи управління обліковим записом полягає в тому, що потрібно розробити зразок для наслідування доступу користувачів у компанії, перш ніж вводити її в комерційні операції. Крім цього, потрібна інтеграція IdM-системи з кадрової системою. Таким чином, система управління обліковими записами знатиме, яких співробітників та посади має компанія відповідно до матриці доступу та які права доступу повинні бути їм призначені. У разі звільнення або підвищення співробітника всі зміни, виконані в кадровій системі, потраплять в систему IdM, а обліковий запис буде автоматично заблоковано або змінено права доступу.

1.6.6 Захист веб-додатків (WAF)

Web Application Firewall (скорочено - WAF) – засіб фільтрації трафіку прикладного рівня, спеціально орієнтований для веб-додатків. Застосування Web Application Firewall традиційно вважається найбільш ефективним підходом до захисту веб-ресурсів. WAF може бути реалізований як хмарний сервіс, агент на веб-сервері або спеціалізований фізичний або віртуальний пристрій. Вважається, що прикладний рівень – це останній рівень моделі і вище нього розташовуються тільки дані кінцевих додатків, які не можна формалізувати і згрупувати. Однак з розробкою стандартів подання інформації прикладними сервісами вже можна говорити про те, що частково дані, якими оперують певні групи додатків, добре формалізуються, і їх правила подання є, по суті, набором деяких пропрієтарних протоколів або, спрощено кажучи, закономірностей.

Таким чином, можна говорити про появу нового рівня міжмережевої взаємодії, який прихований для класичних міжмережевих екранів прикладного рівня. Новий клас пристроїв – Web Application Firewall – характеризується здатністю розуміти властивості групи протоколів і залежностей, характерних для побудованих над прикладними протоколами http / https веб-додатків.

Класичне розміщення WAF в мережі – в режимі зворотного проксі-сервера перед захищуваним веб-сервером. Залежно від виробника можуть підтримуватися і інші режими роботи, такі як прозорий проксі-сервер, міст або навіть пасивний режим, коли продукт використовується для аналізу реплікації трафіку. Після встановлення WAF і запуску виробничого трафіку починається машинне навчання, основний компонент захисту, який протягом всього періоду формує еталонну модель зв'язку із захищеним об'єктом, формуючи тим самим "білий список" ефективних ідентифікаторів доступу. На даний момент в веб-додатках використовуються три типи ідентифікатора доступу: HTTP-параметри (представлені типами: Raw, XML, JSON), ідентифікатори ресурсів (URL, URN), ідентифікатори сеансів (файли cookie). Завдання WAF – визначення допустимих значень ідентифікаторів для веб-додатку. З певних значень згодом буде складатися еталонна (позитивна) модель. Конкретні значення ідентифікаторів, включених у модель, базуються на використанні математичних та статистичних алгоритмів, які оцінюють, чи ці значення є прийнятними шляхом вибірки виробничих потоків.

1.6.7 Резервне копіювання

Завданням резервного копіювання є збереження даних для найшвидшого відновлення (disaster recovery), якщо ІТ-система компанії виходить з ладу, атакується вірусом тощо. Час зберігання цього типу резервної копії є відносно коротким (зазвичай це день-два, а потім резервна копія оновлюється), до даних можна отримати доступ дуже швидко. Копіюються призначені для користувача і бізнес-дані, а також налаштування операційної системи, прикладного ПЗ і вся інформація, необхідна для відновлення працездатності системи.

Також можливо створювати довгострокові інформаційні файли про діяльність компанії, і, якщо потрібно, їх можна використовувати для отримання даних попередніх періодів. Такі архіви будуть зберігатися тривалий час (місяці та роки), і швидкість доступу до них не дуже важлива –

якщо отримання їх займає кілька днів, це, як правило, не страшно. Зберігаються в основному лише бізнес-дані та дані користувачів, не зберігаючи жодної системної інформації за відсутності потреби.

Види резервного копіювання в організації.

Існують різні технології резервного копіювання, які відрізняються витратами коштів і часу:

- повне резервне копіювання – вибрані дані будуть повністю скопійовані. Найбільш надійний метод, але потребує найбільшої кількості ресурсів, місця для зберігання даних і часу копіювання, тому в чистому вигляді застосовується рідко, як правило, використовується у комбінації з іншими видами (наприклад, перший раз з системи знімається повна копія, а потім резервуються тільки внесені зміни). Дозволяє відновити втрачені дані з нуля швидше за всі інші види копіювання;

- інкрементне копіювання – записуються тільки ті дані, які були змінені з часу попереднього резервного копіювання. Порівняно з повною копією, цей тип копії вимагає набагато менше пам'яті та набагато швидше знімається. Звичайно, для такого методу необхідно періодично робити і повну резервну копію, при будь-якій аварії систему відновлюють з такої копії, а потім накочуються на неї всі наступні інкрементні копії в хронологічному порядку. Важливий момент: інкрементне копіювання відновлює видалені файли і багато проміжних версій, які змінювалися, тому на цей випадок при відновленні слід передбачити додатковий простір на диску;

- диференціальне резервне копіювання – схоже на інкрементне, тобто копіюються тільки зміни, зроблені з моменту останнього повного копіювання. Різниця полягає в тому, що в кожній наступній копії зберігаються зміни з попередньої і додаються нові. Виходить, що для відновлення після аварії потрібна тільки повна копія і остання з диференціальних, що значно скорочує час відновлення. Мінусами, в порівнянні з інкрементним копіюванням, є великий обсяг копій (іноді близький до повного копіювання) і збільшений час копіювання.

1.7 Аналіз існуючих апаратних рішень для безпеки корпоративних мереж

На комп'ютерах працівників здійснюється обробка персональних даних клієнтів, тому знадобиться двофакторна аутентифікація для доступу до ПК. В цьому випадку додатково до програмних використовують апаратні засоби управління доступом. Такими засобами можуть бути:

- електронні замки;
- сенсори відбитків пальців;
- usb-токени;
- смарт-картки з універсальним зчитувачем.

Використання смарт-карток є найбільш зручним тому що одна така карта може містити в собі електронний пропуск співробітника, електронний цифровий підпис та вищеописані елементи. Такий вибір є найбільш зручним для центру вакцинації, так як дозволить також обмежити доступ до лікарських препаратів, що зберігаються на підприємстві за допомогою дверей з електронним замком.

Для того, щоб використовувати смарт-карти на персональному чи робочому комп'ютері, потрібно підключити засіб, що зчитує з неї інформацію

Висновки по 1 розділу

Здійснено опис основних понять, аналіз бізнесу “центр вакцинації” з боку процесів, що приносять прибуток. Проведено обстеження по результатах аналізу та виявлено головні інформаційні потоки всередині інтранету. Оглянуто загрози, що найбільш часто використовуються при виборі вектору атак на організацію. Описано популярні на ринку програмні та апаратні засоби захисту інформації для забезпечення безпеки бізнес-процесів.

РОЗДІЛ 2 . ТЕОРЕТИЧНЕ ОБҐРУНТУВАННЯ ВИБОРУ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

2.1 Сервіси, що складають мережу компанії

Висока популярність мережі Інтернет та стрімкий розвиток інформаційних технологій змусило, всі компанії, незалежно від виду діяльності, створювати локальні мережі для поліпшення передачі та обробки даних як на підприємстві, з потенційними партнерами, контрагентами або клієнтами ззовні.

Відповідно до сучасних тенденцій на підприємстві “Здоров’я” передбачається використання наступного комплексу програмних засобів для обліку клієнтів, працівників, взаємодії з клієнтами та інших бізнес-процесів:

- корпоративний сайт, що буде доступний як для робітників, так і для клієнтів;
- база даних, що включає інформацію про клієнтів та робітників;
- електронна пошта.

У наш час компанії стикаються з важливими питаннями: «Чи слід створювати інтернет-ресурс сприяння розвитку бізнесу? Навіщо потрібен бізнес-сайт і чи корисний він для компанії?». Якщо відповідь була неоднозначною кілька років тому, то зараз, коли люди проводять значно більше часу в інтернеті, можна з упевненістю стверджувати, що власний сайт неодмінно принесе користь його власникові. Крім того, значення інтернет-технології стають все більш важливими в житті людей, тому, що створення сайту є необхідною умовою для розвитку бізнесу.

Метою веб-сайту компанії є надання клієнтам або діловим партнерам свіжої довідкової інформації про компанію, її послуги та наявність медикаментів.

Для підвищення ефективності інформація повинна бути структурованою та відповідати критеріям правдивості та релевантності. Може трапитися так, що клієнт хоче дізнатися інформацію про фірму, але не наважується

зателефонувати в компанію і дізнатися відповідь на своє питання. Таким чином фірма може втратити нових клієнтів.

При наявності детальної інформації на сайті про компанію користувач зможе відразу ж дізнатися все необхідне для нього, та вирішити, чи варто скористатися послугами компанії.

Функціонал сайту центру “Здоров’я” надає можливість для реєстрації на прийом за допомогою форми, або можливістю залишити заявку на зворотній дзвінок від консультанта.

Найактуальнішою інформацією для майбутніх пацієнтів є список фармацевтів та лікарів, що ведуть свою практику у стінах центру. Також на сайті представлено перелік препаратів, їх наявність та вартість.

В даному випадку сайт компанії несе ключову роль у мережі організації, так як він допомагає взаємодіяти співробітникам між собою та з клієнтами.

Наступною ланкою у роботі медичного центру як бізнесу є база даних клієнтів. Вона містить масу маркетингової інформації про пацієнтів, лікарів, послуги клініки. Аналіз клієнтської бази даних дозволяє об'єктивно поглянути на роботу бізнесу. Отримане бачення забезпечує прийняття ефективних рішень щодо управління маркетингом медичних послуг.

Аналіз кількості пацієнтів в базі даних клініки показує результат діяльності по залученню нових пацієнтів і утриманню поточних.

Розподіл клієнтів на старих і нових дозволяє зрозуміти структуру бази і виявити наявність приросту чи втрати числа людей, що користуються послугами центру. Детальне вивчення співвідношення нових і старих клієнтів дозволяє виділити пріоритет обслуговування цих груп для забезпечення максимального росту клієнтської бази.

На додаток до частки старих і нових клієнтів, можна відстежувати і частку постійних клієнтів. Її зниження сигналізує про існування проблеми з утриманням залучених споживачів.

Обсяг «живої» бази клієнтів, структура пацієнтів і фінансові показники клієнтської бази необхідні при розгляді питання про реальну вартість

медичного центру. Це важливо не тільки при купівлі клініки, а й при оцінці вартості пакета одного з власників бізнесу.

Поширення набула ідея, що створення внутрішнього корпоративного порталу приносить користь лише великим компаніям. Безумовно, для них вигода від впровадження цього рішення є найбільш вагомою, але багато функцій необхідні і невеликим фірмам. Отже, які завдання може вирішити впровадження інтранету?

Користувачі корпоративного порталу зможуть отримати всі необхідні робочі документи, в будь-який момент часу, з будь-якої точки земної кулі і практично з будь-якого сучасного пристрою, що дуже важливо для компанії з віддаленими співробітниками. Крім того, інтранет може все, що раніше вирішувалося за допомогою поштових розсилок: тут можна розмістити оголошення від керівництва компанії, новини і зміни в політиці фірми, правилах та інструкціях.

Необхідно сформувати та впровадити власну «базу знань» або FAQ, які допоможуть новачкам швидше освоїти унікальні техніки, що застосовуються у відділі, вивчити прийняту в фірмі термінологію, перейнятися корпоративним духом. І все це без допомоги наставника, тобто без додаткових витрат на навчання.

Навіть найпростіші функції інтранету, такі як наявність карток співробітників, допоможуть будь-якому працівнику краще зрозуміти структуру компанії, своїх колег і їх функції. Можливо, для невеликої фірми це не настільки важливо, як у великих корпораціях, але для отримання персоналом такого інструменту безумовно позитивно вплине на внутрішній настрій. Також при віддаленій роботі персоналу це – необхідний сервіс. Сповіднення про дні народження співробітників, інтерактивні голосування, оголошення та онлайн-обговорення важливих тем допоможуть перетворити робочий колектив в команду.

Донедавна для передачі завдання або повідомлення до співробітника необхідно було особисто контактувати або надсилати e-mail. З внутрішнім

Інтернетом такого методу можна уникнути, або використовувати його у крайніх випадках: планувальники завдань вирішують цю проблему. На інтранет-порталі можна знайти контактну інформацію співробітника і в багатьох випадках навіть зателефонувати йому безпосередньо через вбудовану службу. Не потрібно витрачати час на пошук працівника, відповідального за те чи інше питання, шукати його на поверхах будівлі, з'ясовувати, хто замінив цього співробітника на час відпустки тощо ; все можна швидко побачити на порталі.

Для керівників фірм будь-якого розміру важливою є можливість контролювати робочий процес. Корпоративний портал дозволяє зробити це в будь-який момент часу: перевірити, яке завдання в даний момент виконує відділ або конкретний співробітник, скільки часу було витрачено на ту чи іншу діяльність.

Через злам робочого листування на особистій пошті може бути поцуплена важлива стратегічна або інша інформація. Інтрамережа можливо, і не здатна на сто відсотків захистити дані компанії від проникнення хакерів, але вона набагато безпечніше, ніж безкоштовні поштові сервіси або месенджери, якими неминуче користується більшість співробітників при відсутності корпоративних рішень.

Оформлення стандартних документів, таких як заява на відпустку або відрядження, довідки до посольства та для оформлення іпотеки і т.д. – це часті операції, виконання яких вручну витрачає багато часу, що є економічно невигідно.

Якщо в компанії є інтранет з функціоналом workflow для заявок, на замовлення і отримання довідки співробітник витрачає не більше двох хвилин. В особистому кабінеті він відкриває розділ «Довідки», знаходить потрібний документ, заповнює і відправляє його на візування до відділу кадрів. Залишиться забрати документ у секретаря, що можна зробити по дорозі додому. На все йде не більше п'яти хвилин.

Інtranет-портал для центру вакцинації зручно зробити на базі сайту. Утворюється два різних типи акаунтів – для робітників та для клієнтів. При реєстрації заявки клієнтом, вона потрапляє до працівника, що знаходиться онлайн. Він здійснює її обробку та підтвердження шляхом зворотнього зв'язку з людиною.[9]

У розвернутому інtranет-порталі для організації “Здоров’я” передбачаються наступні функції для спрощення роботи персоналу:

- введення обов’язкової реєстрації усіх працівників фірми для того, щоб кожного можна було знайти всього за кілька хвилин та передати інформацію або завдання;
- електронна форма, що заповнюється для кожного клієнта та заноситься до бази даних із внесенням інформації про особу, стан здоров’я, проблеми, з якою вона звернулась та іншої супутньої інформації;
- персоналізований календар, який містить графік роботи для кожного співробітника, в якому в тому числі знаходиться інформація для безпосередньо медиків, скільки пацієнтів записано на прийом та на котру годину.

Незважаючи на те, що сервіси електронної пошти все частіше залишаються без уваги, а деякі компанії взагалі нею не користуються через ризики зламу та перехоплення, у центрі “Здоров’я” для зв’язку з клієнтами передбачається встановлення власного серверу електронної пошти.[10]

Для впровадження електронної пошти існує декілька популярних рішень зі своїми плюсами та мінусами. Можливо використовувати Email, зареєстрований на загальнодоступному поштовому сервісі. Такою електронною поштою зазвичай користуються у повсякденному житті: для особистого листування, підписок на розсилки, реєстрації у різних сервісах і т.д. Пошта має вигляд: mail@yandex.ua, mail@gmail.com, mail@hotmail.com.

Плюси безкоштовної пошти:

- простий і функціональний інтерфейс;
- безкоштовне користування сервісом;

- відсутність необхідності налаштування ресурсних записів;

Мінуси:

- обмежена поштова квота (дисковий простір на сервері, що виділено під клієнтську пошту);
- більшість красивих імен зайняті;
- складно підкреслити бренд або зазначити належність поштової скриньки;
- не є безпечною (наприклад, при звільненні співробітник може змінити пароль до поштової скриньки, з якою він працював, а компанія втратити доступ до важливих даних).[11]

Іншим способом для впровадження пошти є реєстрація домену, співзвучного до назви компанії, і використовувати його для створення поштових скриньок у будь-якому сервісі, що надає послуги пошти на домені. Так, ім'я поштової скриньки буде завершуватись назвою компанії, а починатись будь-як: з назви відділу, прізвища та імені співробітника і т.д. Така скринька буде мати вигляд mail@yourdomain.com.

Плюси пошти на домені:

- більшість сервісів надає послуги пошти безкоштовно, оплата здійснюється тільки за обслуговування домену;
- робота з кореспонденцією як у web-інтерфейсі, так і в будь-якому зручному поштовому клієнті;
- широкий функціонал, доступний одразу після створення поштової скриньки: антиспам, збільшення поштової квоти, налаштування фільтрів, переадресації, накопичення пошти і т.д.

Мінуси пошти на домені:

- відсутність можливості тонкого налаштування “під себе”;
- при виникненні збою у роботі сервера, неможливо особисто вплинути на їх усунення.

Останнім варіантом є розгортання власного поштового серверу. В цьому випадку можна налаштовувати не тільки домен, але й сам сервер. Такий спосіб надає наступні переваги:

- гнучке налаштування серверу під свої потреби: резервне копіювання, розмежування доступу, правила пересилання та видалення листів, білі та чорні списки і т.д;
- моніторинг роботи поштового серверу і доступ до логів (наприклад, якщо лист не буде надісланий, є можливість знайти причину та вирішити проблему);
- контроль роботи та надійності серверу.

Недоліки утримання власного серверу електронної пошти:

- матеріальні витрати та купівлю або оренду необхідного обладнання;
- технічні знання (для налаштування серверу знадобиться спеціаліст з навичками адміністрування Linux або Windows Server).

Незважаючи на те, що сервіси електронної пошти все частіше залишаються без уваги, а деякі компанії взагалі нею не користуються через ризики зламу та перехоплення, у центрі “Здоров’я” передбачається встановлення власного серверу електронної пошти.

2.2 Схема внутрішньої мережі організації

У результаті аналізу бізнес-процесів складено функціональну схему інтранету для центру “Здоров’я”, яка буде забезпечувати його життєздатність.[12]

На рис.2.1 зображено загальну схему, що не включає деякі елементи безпеки, які буде описано пізніше. Основні правила, використані при розробці схеми – це розділення елементів за функціональними ролями та відсутність прямого незахищеного доступу до зовнішнього інтернету важливих ресурсів, таких як сервери пошти та баз даних.

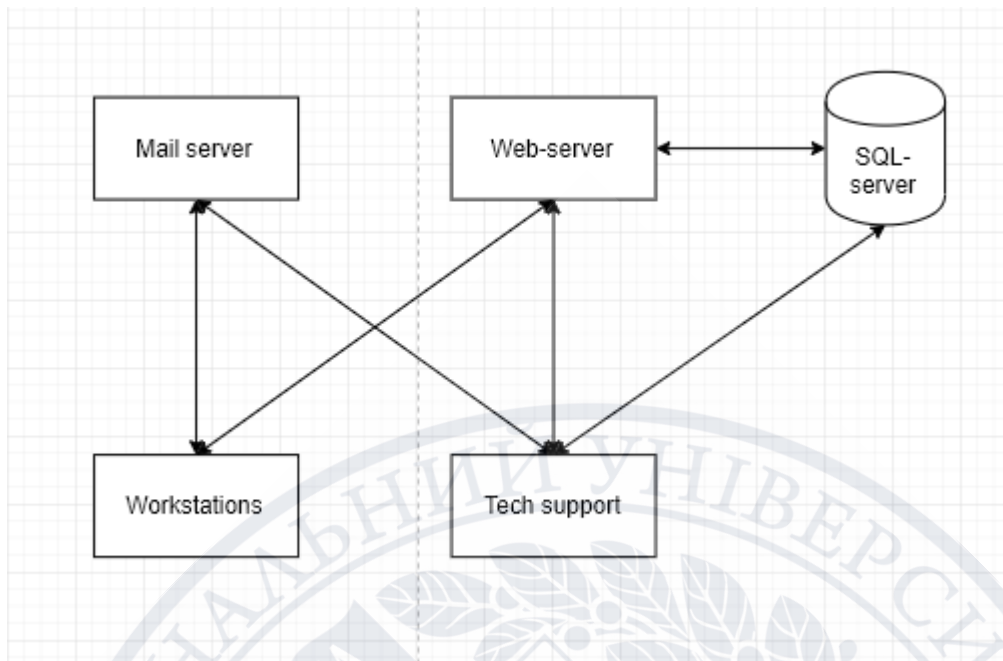


Рис.2.1 – Функціональна схема внутрішньої мережі центру вакцинації “Здоров’я”.

Всі інформаційні потоки знаходяться в межах внутрішньої мережі, яка обмежена вихідним маршрутизатором. Доступ працівників до зовнішньої мережі, або внутрішніх ресурсів також реалізовано за допомогою спеціалізованого обладнання.

Для організації мережі використовується наступне обладнання:

- веб-сервер для роботи сайту, розділеного на backend та frontend;
- поштовий сервер;
- сервер для баз даних (клієнтів та працівників);

Усередині ІС виділяються наступні інформаційні потоки:

- передача файлів між файловими серверами і призначеними для користувача робочими станціями;
- передача повідомлень електронної пошти;
- передача юридичної і довідкової інформації між серверами БД і призначеними для користувача робочими станціями;
- ділове листування;
- передача звітної інформації;

- передача бухгалтерської інформації між призначеними для користувача робочими станціями і сервером БД;

В якості зовнішніх інформаційних потоків використовуються:

- передача звітних документів (виробничі дані) від філій підприємства, по каналах корпоративної мережі, а також з використанням магнітних носіїв;
- передача платіжних документів в Банки;
- передача фінансових і статистичних звітних документів;
- внутрішньовідомчий і міжвідомчий обмін електронною поштою;
- передача інформації по комутованих каналах віддаленим користувачам;
- різні види інформаційних обмінів між ІС і мережею Інтернет.

2.3 Розміщення серверу

Реалізація такої мережі не потребує розгортання декількох серверів, так як всі перераховані засоби інформатизації можливо запустити та підтримувати на одній обчислювальній машині. Звичайно, є можливість утворити розподілену мережу, в якій кожен елемент буде знаходитись на окремому сервері, але це покличе за собою збільшення витрат на реалізацію у декілька разів.

Для підприємства, що лише відкривається постає важливе питання – де встановлювати бізнес системи – на власному сервері, чи на хмарному. Якщо раніше для ведення обліку та забезпечення роботи було достатньо кількох таблиць у MS Excel та стаціонарних комп'ютерів, то тепер для ведення бізнесу потрібно використовувати більш серйозні рішення. Саме тут постає питання, чи варто розгортати виділений сервер у офісі чи перенести все до хмари.[13]

Встановлення виділеного серверу у офісі має наступні недоліки:

- потрібна організація безперебійної подачі електроживлення;
- необхідність у регулярному резервному копіюванні;

- створення потрібних умов у приміщенні, де встановлено сервер (температура та вологість повітря), а це – придбання додаткового кліматичного обладнання;

- дорогі серверні комплектуючі, які потрібно змінювати раз на 1-2 роки;
- щомісячні витрати на електроенергію та вентиляцію;
- найм системного адміністратора до штату компанії, або замовлення послуг у сторонньої компанії.

Натомість, перевагами такого рішення буде те, що сервер завжди під рукою, та можливість фізично бачити, де саме зберігаються дані. Для того, щоб утримувати всього один сервер, цих аргументів буде недостатньо, щоб нівелювати перераховані недоліки. Тому, від такого рішення варто відмовитись.

Деякі провайдери надають послугу колокації серверу для клієнтів, які бажають мати фізичний сервер “у полі зору”. Тобто клієнт купляє виділений сервер, але він зберігається на території провайдера, або компанії, з якою укладено договір. На перший погляд здається, що це ідеальне рішення, але обслуговувати його, купляти та замінювати комплектуючі повинен сам клієнт. Провайдер може надавати послуги обслуговування, але погодинно та окрему платню. Все, що може надати провайдер у такому випадку – це виділене місце для локації серверу та гарантію відсутності перебоїв з живленням чи інтернетом. Недоліком описаного способу є відсутність миттєвого доступу до серверу технічної підтримки у випадку виникнення несправностей. Відповідальність за сервер несе організація-власник, а не провайдер; сервер не знаходиться у її межах, а тому час для усунення збою буде надто великим.

При переносі серверу у хмару недоліки попередніх методів зникають. Вибір такого рішення має наступні переваги:

- оплата здійснюється лише за ресурси, які використовуються. Немає необхідності для оренди цілого серверу, якщо системні вимоги значно нижчі за його потужність;
- не потрібно купляти обладнання та комплектуючі;

- резервне копіювання відбувається регулярно (індивідуально для провайдера);
- ризик фізичного доступу до файлів виключено, так як вони знаходяться за межами офісу, а сервери провайдера охороняються;
- відсутність платні за електроживлення – лише щомісячна абонплата.

Окрім того, стандартною послугою для хостинг провайдера є надання приватного виділеного сервера з уже встановленими системами безпеки, тобто клієнт лише встановлює свої сервіси. Але при виборі послуг від конкретного провайдера існує можливість відмовитись від запропонованих рішень та отримати пустий сервер з встановленою операційною системою із набором стандартних програм.

Для роботоздатності серверу при виборі такого рішення в разі виникнення проблем достатньо підібрати команду технічної підтримки, яка зможе взаємодіяти з техпідтримкою дата-центру.

Для коректного порівняння необхідно визначити вартість кожного з методів розташування серверу. Усі витрати на власний сервер занесено у таблицю 2.1. Для визначеності визначимо модель серверу Cisco C460M4, що має такі характеристики: 2 × E7-4850 v2 (2.3 GHz, 12 cores), 8 × 16 GB DDR3, 2 × 960 GB 2.5” Enterprise Value 6 G SATA SSD, Cisco 12 G SAS Modular Raid Controller w/ 512 GB, Cisco VIC 1225 Dual Port 10 Gb SFP+, 2 × 1200 W, Support 3y NBD., або сервер аналогічної конфігурації.

Назва витрати	Щомісячно, грн	Витрати за 1 рік, грн
Купівля серверу	Одноразово	300000
ПЗ, адміністрування та обслуговування	20000	240000
Система безперебійного живлення	Одноразово	25000

Системи контролю температури та вологості повітря	Одноразово	20000
Витрати на електроенергію	1000	12000
Всього	16000	597000

Таблиця 2.1 – Витрати на утримання власного серверу.

При колокації серверу у провайдера, відпадають статті витрат, що направлені на підтримання необхідних умов. Таким чином, ціна такого рішення складається з придбання серверу, адміністрування та плати провайдеру за надання послуг згідно договору.

Але найбільш вигідним рішенням є придбання у хостинг-провайдера приватного віртуального серверу. Для втілення проекту внутрішньої мережі компанії здійснюється вибір однієї з таких компаній, яка надає віртуальний приватний сервер (VPS). Критеріями, згідно яких обирається провайдер є наявність серверів з встановленою серверною операційною системою CentOS. Так як для роботи сайту потрібна мінімальна затримка, вибір звужується до провайдерів, чії сервери знаходяться в межах України. Результат аналізу ринку зведений до таблиці у додатку А. Окрім того, важливим є наявність стеку програмних засобів захисту, описаних у першому розділі та зручної панелі управління. Класичні показники uptime (час роботи серверу безперебійної роботи) та ping (час затримки повідомлення) також занесені до таблиці. У результаті аналізу ринку виявлено, що витрати на підтримання такого серверу є значно нижчими та зводяться до вартості оренди згідно договору з компанією. Також необхідним є найм команди технічної підтримки, що у сумі на рік складає

$$\sim 1000 \text{ грн} * 12 \text{ міс} + 12000 \text{ грн} * 12 \text{ міс} = \sim 360000 \text{ грн.} \quad (1)$$

Отже, найкращим вибором платформи для реалізації внутрішньої мережі організації є придбання віртуального приватного серверу (VPS).

2.4 Порівняння операційних систем

Вибір операційної системи, на якій буде будуватись структура сервісів є вкрай важливим кроком, оскільки від нього буде залежати вибір систем захисту цих сервісів. Для різних операційних систем утворені власні додатки, які функціонуватимуть справно лише на визначеній архітектурі.

Серверна операційна система використовує більше пам'яті для обчислень, а також може виступати в якості веб-сервера, сервера додатків, сервера електронної пошти та багатьох інших серверів, необхідних корпоративним ІТ-системам. Серверна операційна система може підключити до локальної мережі та Інтернету багатьох користувачів, а не єдиного. Тому серверні операційні системи також дорожчі.

На сьогоднішній момент ринок серверних операційних систем має неосяжний асортимент, серед яких слід виділити Windows Server та системи на базі OS Linux. На користь операційних систем від компанії Microsoft говорять їх практичність, швидкодія та наявність широких можливостей. За рахунок своєї надійності Windows Server ідеально підходить для терміналів та файлових серверів.

Остання версія Windows Server 2019 має можливість працювати як на серверах підприємства, так і на орендованих хмарних серверах.

Нові функції у Windows Server 2019:

- підтримка гібридної хмари. ІТ-систему підприємства можна розширити у хмарне середовище Azure і отримати там додаткові функції та сервіси, а також збільшити ємність для збереження та розрахункову потужність;

- підтримка Linux. Windows Server 2019 містить вдосконалену версію підсистеми для підтримки Windows Subsystem for Linux (WSL). Тому розробники на базі Windows Server 2019 отримали можливість розробляти програми для ОС Linux безпосередньо в середовищі Windows, в якому можуть працювати віртуальні машини Linux. Крім того, розробники можуть писати програми на популярній мові команд Bash, а також Ruby і Python;

- підтримка системи управління контейнерами Kubernetes. Контейнерні технології здобувають все більшу популярність, оскільки вони дозволяють замість віртуальних машин, яким потрібна окрема ОС, запускати контейнери, в яких сервіси та додатки працюють на ОС, яка вбудована безпосередньо в контейнер;

- безпека – можливість захисту від атак шкідливих сторонніх програм і попередження несанкціонованого проникнення у віртуальні машини.

Але дана операційна система має і ряд недоліків, які пояснюють той факт, що з Windows Server працює трохи більше 10% користувачів. По-перше, Windows потребує значно більших ресурсів, ніж будь-який інший аналог. По-друге, не всі версії цієї ОС підтримують 32-розрядну архітектуру. По-третє, ця операційна система є суворо ліцензованим програмним забезпеченням. Не варто забувати і про те, що більшість вірусів, що запускаються у мережі, розроблені саме під Windows.[14]

Наступною системою, яку варто розглянути є Red Hat Enterprise Linux (RHEL) – популярний дистрибутив розподіленої серверної ОС, розробленої на базі ОС Linux компанією Red Hat, перша версія якого була випущена на ринок у 2003 році.

Хоча RHEL відноситься до класу “відкритого ПЗ” і його вихідний код безкоштовний і доступний усім бажаючим, однак виконуваний (двійковий) код купується за плату. Раз на два роки Red Hat випускає версії RHEL в двійковому коді з підтримкою протягом десяти років, причому Red Hat відстежує критичні виправлення Linux і оновлює вже випущені версії серверної ОС. Крім того, Red Hat є найбільшим вкладником проекту ОС Linux за обсягом програмного коду.

Ключовими особливостями операційної системи Linux від Red Hat є:

- висока продуктивність, надійність і безпека;
- спільна середовище для додатків, розгорнутих в фізичних, віртуальних і хмарних системах;
- масштабованість від робочих станцій до серверів і сейнфреймів;

- сертифікація провідних виробників обладнання та програмного забезпечення.

У 2019 році компанія Red Hat оголосила про загальну доступність дистрибутива Red Hat Enterprise Linux (RHEL) 8, заснованого на Fedora 28. Red Hat Enterprise Linux 8 - це інтелектуальна операційна система, яка є основою для корпоративної гібридної хмари.

Red Hat – довірений партнер для корпоративних клієнтів, постачальників хмарних технологій, програмного та апаратного забезпечення, а також для розробників продуктів із відкритим вихідним кодом.[15]

Третім та останнім варіантом, на якому слід зупинитись є операційна система CentOS. Це Linux дистрибутив, вихідний код якого відкритий, ОС заснована на RHEL (Red Hat Enterprise Linux). Він призначений для корпоративного використання, а його розробка підтримується спільнотою. Тісний зв'язок з RHEL забезпечила цій системі масу корисних можливостей від Red Hat.

CentOS (Community Enterprise Operating System) - перш за все стабільна і безпечна система. Це стало можливим завдяки тому, що CentOS користується офіційною підтримкою Red Hat. CentOS можна легко встановити налаштувати відповідно до потреб підприємства.

Так як CentOS функціонально сумісна з Red Hat Enterprise Linux і побудована з програмних блоків RHEL, то згідно життєвому циклу Red Hat Enterprise Linux, CentOS версій 5, 6 і 7 буде підтримуватися до 10 років.[16]

2.5 Порівняння апаратних засобів захисту

Для вибору конкретних рішень із встановлення апаратного захисту потрібно встановити необхідність їх встановлення та завдання, які вони будуть виконувати. По-перше, слід визначити які засоби відносяться саме до галузі захисту інтранету в організації. Апаратне забезпечення означає фізичні пристрої, які дозволяють убезпечити ресурси компанії від викрадення або спотворення. Найбільш поширеним і різноманітним видом комп'ютерних

порушень є несанкціонований доступ (НСД). НСД використовує будь-яку помилку в системі захисту і можливий при нераціональному виборі засобів захисту, їх некоректному встановленні та налаштуванні.[17]

До апаратних засобів захисту відносяться різні електронні, електронно-механічні, електронно-оптичні пристрої. На теперішній час розроблено значну кількість апаратних засобів різного призначення, проте найбільшого поширення отримали наступні:

- спеціальні реєстри для зберігання реквізитів захисту: паролів, ідентифікують кодів, грифів або рівнів секретності;
- пристрої ідентифікації індивідуальних характеристик людини (голосу, відбитків) з метою його ідентифікації;
- пристрої для шифрування інформації (криптографічні методи).

На підприємстві “Здоров’я” розміщено ком’ютери робітників, які є об’єктами, для яких необхідно обмежити доступ стороннім особам. Для цього найбільш доцільними є наступні пристрої:

- біометричні засоби захисту;
- апаратні ключі захисту.

Біометрика – наукова дисципліна, що вивчає способи вимірювання різних параметрів людини з метою встановлення схожості або відмінностей між людьми і виявлення конкретної людини з безлічі інших людей, або, іншими словами, - наука, що вивчає методики розпізнавання конкретної людини за його індивідуальними параметрами.

Біометрична система, незалежно від того, на якій з технологій вона побудована, працює за наступним принципом: спочатку записується зразок біометричної характеристики людини, для більшої точності часто робиться кілька зразків. Зібрані дані обробляються, переводяться в цифровий код.

При ідентифікації та верифікації в систему вводяться характеристики людини. Далі вони оцифровуються, а потім порівнюються з збереженими зразками. За певним алгоритмом система виявляє, збігаються вони чи ні, і

виносить рішення про те, чи вдалося ідентифікувати людину за пред'явленими даними чи ні.

Даний тип систем захисту є зручним у використанні, адже людина може загубити ключ чи карту, але для біометричної системи ідентифікації ключем являється сама людина – відбиток пальця, сітківки чи роговиці.

Натомість така система є складною та дорогою у реалізації, процедура реєстрації нового користувача може займати до кількох днів. Якщо брати за увагу той факт, що вартість системи захисту повинна бути меншою за ризики, яких вона дозволяє уникнути, то впровадження такої системи не є доцільною.

Смарт-карти все частіше приймаються як вибір для надійного контролю фізичного доступу до даних. Смарт-ідентифікаційні картки на основі стандартів можна використовувати для легкої автентифікації особи, визначення відповідного рівня доступу та фізичного допуску власника картки до закладу або приміщень з обмеженим доступом. Водночас їх можливо використовувати для доступу до ПК. Для цього необхідно приєднати до кожного автоматизованого робочого місця пристрій для зчитування таких карток.

Технологія смарт-карт надає організаціям економічно ефективний логічно розподілений доступ. Смарт-картки забезпечують позитивний бізнес-аргумент щодо впровадження будь-якої технології автентифікації. Підвищена продуктивність користувачів, зниження витрат на адміністрування паролів, зменшення ризику та впорядкованість бізнес-процесів – все це сприяє значній позитивній віддачі інвестицій.[18]

Висновки до 2 розділу.

Виконано опис функціональних частин внутрішньої мережі організації “Здоров’я”. Проведено аналіз методів реалізації такої мережі та обрано найбільш зручний метод – розміщення сервісів на приватному віртуальному сервері (VPS). Виконано порівняння операційних систем для такого серверу та обрано операційну систему Linux CentOS. Описано популярні методи захисту АРМ співробітників від несанкціанованого доступу та обрано систему смарт-карток.



РОЗДІЛ 3. ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО РОЗРОБЛЕННЯ ВНУТРІШНЬОЇ МЕРЕЖІ ОРГАНІЗАЦІЇ НА БАЗІ ВІРТУАЛЬНОГО ПРИВАТНОГО СЕРВЕРУ

3.1 Налаштування приватного віртуального серверу

При розгортанні нового VPS-сервера існує вибір чи довірити організацію системи захисту провайдеру, чи впроваджувати її власноруч. Далі представлено приклад налаштування серверу без участі технічної підтримки хостинг-провайдера. У такому випадку надається сервер із обраною операційною системою, а всі наступні дії по його налаштуванню бере на себе підприємство “Здоров’я”. Для початку слід виконати кілька операцій, які дозволять підвищити його безпеку і функціональність.

Перед початком роботи слід авторизуватись на сервері як користувач root. Щоб це зробити, потрібна публічна IP-адреса сервера і пароль облікового запису адміністратора (root). Якщо вони відомі, в консолі вводиться наступна команда, в якій слід замінити запропоновану IP-адресу на адресу свого сервера: `ssh root@194.61.0.6.*`

* IP-адреса приведена як приклад, на її місце потрібно підставити актуальну.

Якщо з'явиться попередження про перевірку справжності – слід прийняти його. Потім система запитає пароль або приватний ключ. Якщо вхід здійснюється вперше за допомогою пароля, система запропонує задати новий. Після введення пароля авторизація пройде успішно, дозволяючи налаштувати сервер на CentOS.[19]

Користувач root в дистрибутивах Linux має необмежені права. Однак, не варто працювати під ним постійно. При наявності великих можливостей досить зробити одну невірну дію, яка призведе до незворотних наслідків. Тому варто створити додатковий профіль користувача, для якого можна встановити деякі обмеження.

Для початку створимо додатковий профіль користувача з іменем “demo”:

```
adduser demo
```

Назначимо для нього пароль:

```
passwd 123
```

Далі вводимо новий пароль та повторюємо його після наступного запиту. Новий створений акаунт “demo” отримав стандартні права. В той самий час, при налаштуванні серверу потрібно буде провести глибоке налаштування VPS-серверу, для чого знадобляться root-права.

Для того, щоб не змінювати постійно стандартний акаунт на профіль адміністратора, можна зробити з demo “суперкористувача”. Для того, щоб запускати команди з правами адміністратора, перед ними достатньо дописати команду `sudo`.

Далі – додаємо профіль demo до групи “wheel”. У CentOS користувачі даної групи можуть використовувати команду `sudo`. Для цього використовуємо наступну команду:

```
# gpasswd -a demo wheel
```

Щоб покращити захист сервера, можна додати аутентифікацію користувачів за допомогою відкритого ключа. Це на порядок збільшує безпеку сервера, оскільки дозволяє виконувати авторизацію шляхом введення ключа SSH. Для створення нової пари ключів SSH досить введення команди:

```
ssh-keygen
```

Термінал виведе наступну відповідь:

Generating public/private rsa key pair.

Enter file in which to save the key (/Users/newluser/.ssh/id_rsa):

Підтверджуємо натисканням кнопки Enter прийняття цього імені файлу і шляху до нього. Система запропонує задати пароль для захисту ключа. Втім, цей крок необов'язковий і можна обійтися без пароля. Ця процедура згенерує закритий ключ `id_rsa` і відкритий ключ `id_rsa.pub` у внутрішньому каталозі `.ssh`.

Коли пара SSH-ключів буде успішно згенерована, знадобиться скопіювати на новий сервер відкритий ключ. Зробити це можна за допомогою скрипта `ssh-copy-id`, який потрібно попередньо встановити на CentOS 7. Він

допоможе встановити відкритий ключ кожному авторизованому користувачеві.

Для цього вписуємо до консолі команду:

```
ssh-copy-id
```

Після її виконання вводиться ім'я користувача і IP-адреса сервера, на який додається ключ:

```
ssh-copy-id demo@194.61.0.6
```

Коли пароль буде введений, відкритий ключ додається в файл віддаленого користувача по шляху `.ssh / authorized_keys`. Відповідний закритий ключ буде використовуватися для входу на сервер.

Після застосування змін необхідно виконати перезавантаження SSH, щоб система почала працювати з новою конфігурацією. Для цього використовуємо наступну команду, щоб перезапустити демон SSH:

```
systemctl reload sshd
```

Перед тим, як покинути сервер, рекомендується перевірити, чи правильно він налаштований. Далі слід закрити та відкрити термінал, щоб в ньому створити нове з'єднання з нашим сервером. Однак, в даному випадку замість входу в профіль «root», використовується вже створений «demo».

До налаштованому віддаленого сервера можна підключитися командою:

```
ssh demo@194.61.0.6.
```

Для встановлення на сервері організації обрано наступні програмні рішення:

- міжмережевий екран ConfigServer Security and Firewall(CSF);
- система попередження вторгнень fail2ban;
- антивірусне програмне забезпечення Maldet.

Встановлення міжмережевого екрану. Порівняно з іншими подібними рішеннями, ConfigServer Security and Firewall (CSF) - це безкоштовне програмне забезпечення брандмауера з відкритим кодом з широким спектром функцій. CSF також інтегрований у панелі керування хостингом VDS, такі як

cPanel та DirectAdmin. Отже, після встановлення CSF можливо налаштувати безпосередньо з цих панелей управління.

Першим чином для встановлення CSF потрібно підключитись по SSH з правами суперкористувача (root). Для роботи CSF необхідний Perl, а також бібліотека Time / HiRes. Якщо ці пакети не встановлені, установник CSF виведе помилку. Для установки цих пакетів потрібно ввести наступні команди:

```
yum install perl-libwww-perl
```

```
yum install perl-Time-HiRes
```

Для того, щоб встановити цей фаєрвол, необхідно завантажити установчий архів CSF, розпакувати його і запустити виконуваний файл. Для цього потрібні команди:

```
rm -fv csf.tgz //Видаляємо файл csf.tgz, якщо такий є
```

```
wget https://download.configserver.com/csf.tgz //Завантажуємо архів
```

```
tar -xzf csf.tgz //Розпаковуємо архів
```

```
cd csf //Переходимо в розпаковану директорію
```

```
sh install.sh //Виконуємо установчий скрипт
```

Установка відбувається в автоматичному режимі. Після її завершення необхідно перевірити, чи є на VPS необхідні модулі IPTables:

```
perl /etc/csf/csftest.pl
```

Результат виконання команди повинен бути приблизно таким:

```
Testing ip_tables/iptables_filter...OK
```

```
Testing ipt_LOG...OK
```

```
Testing ipt_multiport/xt_multiport...OK
```

```
Testing ipt_REJECT...OK
```

```
Testing ipt_state/xt_state...OK
```

```
Testing ipt_limit/xt_limit...OK
```

```
Testing ipt_recent...OK
```

```
Testing ipt_owner/xt_owner...OK
```

```
Testing iptable_nat/iptables_REDIRECT...OK
```

```
RESULT: csf should function on this server
```

Як правило, зазначені у висновку модулі встановлені на VPS за замовчуванням. Якщо який-небудь з потрібних модулів відсутній, результати тесту про це повідомлять, після чого необхідно буде провести установку зазначених модулів, щоб функціональність CSF була обмежена.

Після установки ConfigServer Security and Firewall працює в тестовому режимі, який рекомендується відключати тільки після того як буде відредагований конфігураційний файл `/etc/csf/csf.conf` для потреб підприємства.

У файлі конфігурації необхідно як мінімум переконатися в тому, що всі необхідні для роботи TCP і UDP порти відкриті. Приклад таких параметрів в файлі конфігурації може бути наступним:

```
# Allow incoming TCP ports
TCP_IN = "20,21,22,25,53,80,110,143,443,465,587,993,995"
# Allow outgoing TCP ports
TCP_OUT = "20,21,22,25,53,80,110,113,443"
# Allow incoming UDP ports
UDP_IN = "20,21,53"
# Allow outgoing UDP ports
# To allow outgoing traceroute add 33434:33523 to this list
UDP_OUT = "20,21,53,113,123"
```

Відключення тестового режиму виконується шляхом зміни значення параметра `TESTING` в файлі конфігурації, а саме необхідно значення 1 змінити на 0. Після цього можна зберегти зміни.

Система попередження вторгнень. Для встановлення обрано систему Fail2ban. Це – фреймворк для запобігання проникненню, призначений для блокування невідомих IP-адрес, які намагаються проникнути у внутрішню систему. Цей пакет програм важливий для захисту від будь-яких атак грубої сили на сервіси.

Щоб встановити пакет, використовується така команда:

```
apt-get install fail2ban
```


Після встановлення програмного пакету потрібно змінити файл конфігурації, щоб налаштувати його відповідно до потреб. Перш ніж вносити зміни, рекомендується створити резервну копію файлу конфігурації, ввівши таку команду:

```
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.conf.backup
```

Потім відкриваємо файл:

```
nano /etc/fail2ban/jail.conf
```

Після виконання змін, слід перезавантажити сервіс, використовуючи наступну команду:

```
/etc/init.d/fail2ban restart
```

Встановлення утиліти для сканування maldetect для сканування Linux сервера. MalDetect може використовувати дані від систем виявлення атак щоб виявляти шкідливий код (malware). Також може використовувати антивірусну базу інших сканерів, таких як ClamAV.

MalDetect не доступний у репозиторіях ПЗ, тому завантажити та встановити його потрібно вручну:

```
cd /usr/local/src; wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
```

```
tar -xzf maldetect-current.tar.gz; cd maldetect-*
```

```
sh ./install.sh; cd ../
```

```
rm -rf maldetect-*
```

Після встановлення оновлюємо:

```
maldet -update-ver
```

```
maldet -update
```

Сканування відбувається наступним чином:

```
maldet -a /home?/?/public_html
```

Кожному скануванню присвоюється унікальний ID.

MalDetect не видаляє файли під час сканування. По закінченню кожного сканування буде запропоновано команду, за допомогою якої можна переглянути лог сканування.

```
maldet -report %report.ID%
```

Для видалення знайдених файлів потрібно виконати наступну команду:

```
maldet -q %report.ID%
```

Після перерахованих засобів можна власне переходити до встановлення демонів для роботи сайту та електронної пошти. Сервер бази даних MySQL встановлено за замовчуванням. Для роботи веб-сайту потрібно встановити веб-сервер. Обираючи серед таких популярних серверів як NGINX, Apache Tomcat, Node.js, Apache HTTP Server, вибір падає на останній, так як він є найбільш часто використовуваним.

3.2 Практичні рекомендації з впровадження систем захисту

Безпека бізнесу є надзвичайно важливою, але для компанії може бути складним питанням. Незалежно від того, чи метою є запобігання злому, захист своїх цінних даних, попередження крадіжок, варто пильно стежити за своїм персоналом, є багато речей, які варто продумати, щоб ваша безпека відповідала потребам компанії.

Кожен бізнес має свої особливості, а це означає, що заходи безпеки, які підходять одній компанії, не обов'язково будуть задовільняти потреби іншої. Важливо спочатку проаналізувати потреби в безпеці, тобто, що найкраще підійде для конкретного підприємства та що воно може собі дозволити. Це включає низку таких питань, як:

Чи потрібно застосовувати заходи безпеки в приміщенні, на відкритому повітрі, або в обох випадках?

Чи потрібно буде покривати велику площу чи малу?

Чи необхідно, щоб система працювала цілодобово, чи лише тоді, коли бізнес працює?

Чи доречним є впровадження обраних засобів захисту?

Вектори атак на корпоративні інфраструктури зазвичай базуються на використанні відомих вразливостей та недоліків у подібних системах, для

усунення яких, як правило, достатньо застосувати базові принципи забезпечення інформаційної безпеки:

- обмежити число інтерфейсів мережеслужб, доступних для підключення на мережевому периметрі;
- регулярне оновлення програмного забезпечення і встановлення оновлень безпеки операційної системи;
- використання SIEM-системи для своєчасного виявлення атак;
- для захисту веб-сайтів від атак ботів використовувати капчі;
- проводити регулярні лекції з метою підвищення обізнаності працівників в питаннях інформаційної безпеки (важливо оцінювати ефективність таких лекцій);
- регулярно проводити тестування на проникнення щоб своєчасно виявляти нові вектори атак і перевірки вжитих заходів захисту на практиці;
- використовувати спеціалізовані антивірусні програми для захисту від шкідливого ПЗ, розповсюджуваного за допомогою соціальної інженерії;
- захищати або відключати в локальній обчислювальній мережі протоколи канального або мережевого рівня, які не використовуються та розділяти мережу на сегменти;
- мінімізувати привілеї користувачів і служб, використовувати сувору політику щодо паролів;
- захищати облікові записи, що мають підвищений доступ;
- не зберігати конфіденційну інформацію у загальнодоступному вигляді або у публічному доступі.

ВИСНОВКИ

Під час виконання бакалаврської роботи проведено аналіз бізнес-процесів організації “Здоров’я”, що спеціалізується на вакцинації населення, підбір сервісів, що виконують завдання створення внутрішньої мережі організації для потоків інформації. Виконано огляд популярних методів реалізації таких сервісів. Обрано спосіб розміщення сервісів на віртуальному приватному сервері. Приведено приклад налаштування приватного віртуального серверу, що включає встановлення програмного забезпечення. Надано рекомендації щодо впровадження систем захисту внутрішньої мережі організації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Опис бізнес-процесів організації.
URL:<http://orgstructura.ru/activity-or-business-process-model>
2. Актуальні кіберзагрози: III квартал 2017р. URL:
<https://www.ptsecurity.com/ru-ru/research/analytics/>.
- 3.<https://www.anti-malware.ru/threats/information-security-threats>
4. Chronology of Data Breaches, березень 2018 року. URL:
<https://www.privacyrights.org/data-breaches>.
5. Основы сетевой безопасности. Часть 1. Межсетевые экраны О.Р. Лапони́на.
6. Web Application Firewall. URL: <https://www.anti-malware.ru/security/web-application-firewall>.
7. What is a Intrusion Detection System? URL:
<https://www.barracuda.com/glossary/intrusion-detection-system>.
8. Шелухин О.И. Сакалема, Д.Ж. Филинова: АС Обнаружение вторжений в компьютерные сети сетевые аномалии. Учебное пособие для вузов : учебное пособие для вузов Москва 2014.
9. Белоногова Н. М. – Интранет-портал. Яким організаціям потрібна дана технологія та навіщо. URL:<https://www.kp.ru/guide/intranet.html> (Last accessed: 01.06.2021)
- 10.Dark Reading, 27 август 2018 года. URL:
<https://www.darkreading.com/endpoint/64-billion-fake-emails-sent-each-day/d/d-id/1332677>.
- 11.Naked Security, 24 травня 2018 року.
URL:<https://nakedsecurity.sophos.com/2018/05/24/2-million-stolen-identities-used-to-make-fake-net-neutrality-comments/>.
- 12.Куда перенести важные бизнес-процессы
URL:<https://www.key4.com.ua/blog/server-vs-oblako-kuda-perenesti-vazhnye-biznes-sistemy/>

13. Структура локальної мережі підприємства URL: <https://www.sviaz-expo.ru/ru/articles/struktura-lokalnoj-seti-redpriyatiya/>.

14. Build your future. URL: <https://www.microsoft.com/ru-ru/windows-server>.

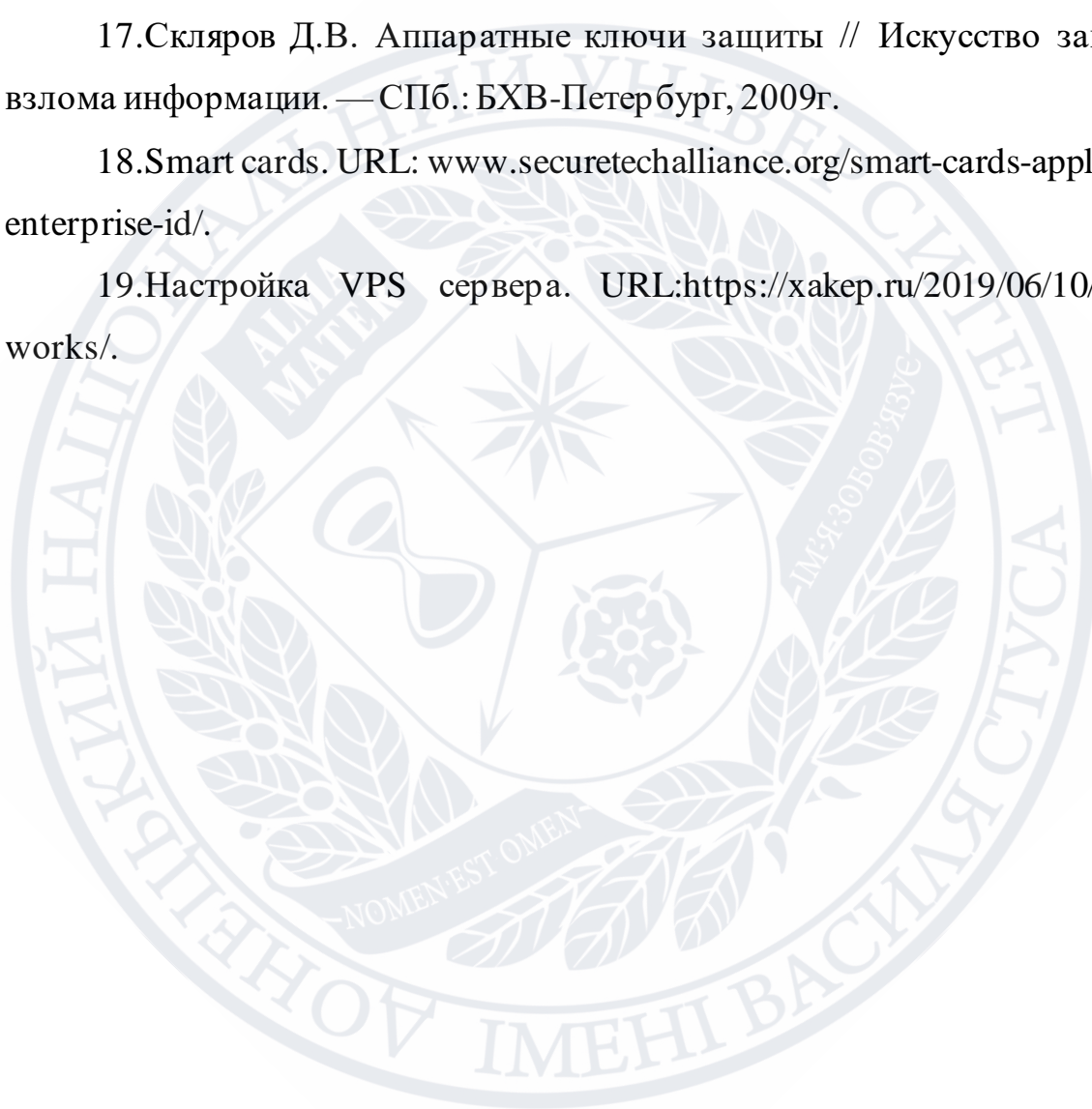
15. Clouds that complete can still connect. URL: <https://www.redhat.com/en>.

16. The CentOS Project. URL: <https://www.centos.org/>.

17. Скляр Д.В. Аппаратные ключи защиты // Искусство защиты и взлома информации. — СПб.: БХВ-Петербург, 2009г.

18. Smart cards. URL: www.securetechalliance.org/smart-cards-applications-enterprise-id/.

19. Настройка VPS сервера. URL: <https://xakep.ru/2019/06/10/how-av-works/>.



ДОДАТОК А – Аналіз популярних хостинг провайдерів в Україні

Назва	Панель управління	Наявність VPS з CentOS	Uptime	Ping	Ціна за місяць, грн
Hostiq	cPanel, DirectAdmin, ISPmanager, Plesk, SolusVM	Так	99.99%	14ms	725грн за 60ГБ
Hostpro	CentOS Web Panel, cPanel	Так	99.99%	17ms	820грн за 70ГБ
S-Host	DirectAdmin, cPanel, BrainyCP	Так	99.99%	49ms	215грн за 60ГБ
HostLife	cPanel, DirectAdmin	Так	99.93%	42ms	850грн за 64ГБ
Хостинг Україна	власна	Так	99.98%	24ms	714 грн за 70ГБ