Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавра
(назва освітнього ступеня)

на тему: Побудова системи мережевої безпеки на базі КНП «Дубівська лікарня»

Виконав(ла): студент(ка) IV курсу, групи СБс-42
спеціальності 125 Кібербезпека
(шифр і назва спеціальності)

(підпис) Кубарич З. П. (прізвище та ініціали)

Керівник (підпис) Марценюк В. П. (прізвище та ініціали)

Нормоконтроль (підпис) Лобур Т. Б. (прізвище та ініціали)

Завідувач кафедри (підпис) Загородна Н. В. (прізвище та ініціали)

Рецензент (підпис) (прізвище та ініціали)

Тернопіль 2022

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н. В.
(підпис) (прізвище та ініціали)
« » 20___ р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня бакалавр
(назва освітнього ступеня)

за спеціальністю 125 кібербезпека
(шифр і назва спеціальності)

студенту Кубаричу Захару Петровичу
(прізвище, ім'я, по батькові)

1. Тема роботи Побудова мережевої системи безпеки на базі КНП «Дубівська лікарня»

Керівник роботи Марценюк Василь Петрович, доктор технічних наук, професор кафедри КБ
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*23*» *березня* 20*22* року № *4/7-178*

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи технічна документація, інтернет-джерела

4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. Розділ 1.Теоретичні засади поняття мережевої безпеки. 1.1. Безпека мережі. 1.2. Джерела загроз. 1.3. Типи атак. 1.4.Основні елементи створення системи мережевої безпеки. Розділ 2. Характеристика об'єкта діяльності. 2.1.Огляд підприємства. 2.2. Обстеження наявного обладнання та рішень політики безпеки. 2.3. Постановка завдання. Розділ 3. Побудова мережевої системи безпеки. 3.1. Розробка політик безпеки. 3.2. Програмно-апаратні засоби для побудови захищеності системи. Розділ 4. Безпека життєдіяльності, основи охорони праці. 4.1. Ергономічні аспекти безпеки життєдіяльності. 4.2. Психологічні чинники безпеки. 4.3. Висновок до розділу безпека життєдіяльності, основи охорони праці. Висновки. Перелік джерел.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Титулка. 2. Актуальність. 3. Мета, задачі дослідження. 4. Перелік можливих загроз. 5. Топологія мережі

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи охорони праці	Пулька Ч. В., професор кафедри МТ		

7. Дата видачі завдання 23.03.2022

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Ознайомлення з завданням кваліфікаційної роботи	23.03-30.03	**виконано**
2	Підбір інформаційних джерел про загрози мережевій безпеці	31.03-06.04	**виконано**
3	Опрацювання інформаційних джерел про загрози мережевій безпеці	06.04-13.04	**виконано**
4	Підбір інформаційних джерел про засоби захисту мережевої інфраструктури	14.04-21.04	**виконано**
5	Опрацювання інформаційних джерел про засоби захисту мережевої інфраструктури	22.04-29.04	**виконано**
6	Аналіз діяльності підприємства	30.04-04.05	**виконано**
7	Аналіз наявних політик безпеки на підприємстві	05.05-06.05	**виконано**
8	Розробка політик безпеки	07.05-14.05	**виконано**
9	Вибір програмно-апаратних безпеки	15.05-21.05	**виконано**
10	Оформлення розділу «Теоретичні засади поняття мережевої безпеки»	22.05-24.05	**виконано**
11	Оформлення розділу «Характеристика об’єкта діяльності»	25.05-27.05	**виконано**
12	Оформлення розділу «Побудова мережевої безпеки»	28.05-31.05	**виконано**
13	Виконання завдань до підрозділу «Безпека життєдіяльності, основи охорони праці»	01.06-03.06	**виконано**
14	Оформлення кваліфікаційної роботи	04.06-08.06	**виконано**
15	Нормоконтроль	09.06-14.06	**виконано**
16	Перевірка на плагіат	15.06-20.06	**виконано**
17	Захист кваліфікаційної роботи	24.06	

Студент _____ Кубарич З. П.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Марценюк Василь Петрович
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Побудова мережевої системи безпеки на базі КНП «Дубівська лікарня» // Кваліфікаційна робота освітнього рівня «Бакалавр» // Кубарич Захар Петрович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2022 //с. 55, Рисунок 8, табл. 5, кресл. 0, додат. 0, бібліогр. 16.

Ключові слова: МЕРЕЖЕВА БЕЗПЕКА, ПОЛІТИКИ БЕЗПЕКИ, ПРОГРАМНО-АПАРАТНІ ЗАСОБИ

Кваліфікаційна робота присвячена побудові мережевої системи безпеки, використовуючи сучасні апаратно-програмні засоби та організаційні заходи. У роботі проаналізовані основні джерела загроз, типи атак та розроблено рекомендації, щодо забезпечення системи безпеки на підприємстві. При дослідженні мережевої системи було проведено аналіз технічних та організаційних заходів системи безпеки на підприємстві.

У роботі проаналізовано діяльність підприємства, обрано цілі для забезпечення захисту. Виявлено проблеми у наявних політиках забезпечення системи безпеки та надано рекомендації, щодо їх посилення. Доведена доцільність використання обраних програмно-апаратних засобів та запропонованих політик безпеки.

ANNOTATION

Construction of network security system on the basis of KNP "Dubivska Hospital" // Qualification work of educational level "Bachelor" // Kubarych Zakhar Petrovich // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and Software Engineering // Ternopil, 2022 // Explanatory note size — 55 pages, 8 illustrations, 5 tables, 16 bibliography items.

Keywords: NETWORK SECURITY, SECURITY POLICIES, SOFTWARE AND HARDWARE

Qualification work is devoted to building a network security system using modern hardware and software and organizational measures. The main sources of threats, types of attacks are analyzed and recommendations for ensuring the security system at the enterprise are developed. During the study of the network system, an analysis of technical and organizational measures of the security system at the enterprise was conducted.

The paper analyzes the activities of the enterprise, selected goals to ensure protection. Problems in existing security policies have been identified and recommendations for strengthening them have been provided. The expediency of using the selected software and hardware and the proposed security policies is proved.

ЗМІСТ

ВСТУП

Актуальність теми. В Україні проходить активна стадія впровадження реформи охорони здоров'я. А саме: з 2020 року впровадження електронної системи охорони здоров'я. Дана система дасть змогу кожній людині звернутися за допомогою до будь-якої лікарні без потреби нести з собою велику кількість паперів, виписок, рецептів, які можуть загубитися або бути знищеними. Метою такої системи є внесення всіх відомостей про пацієнта до «Електронної системи охорони здоров'я», котра буде зберігати всі чутливі дані у одному місці, де їх можна буде отримати у будь-який момент. Внесення цих даних покладено безпосередньо на місця надавання медичної допомоги за допомогою медичних інформаційних систем, з якими будуть працювати медичні заклади. Саме тому, починаючи з грудня 2020 року, все більше таких закладів проводило швидку комп'ютеризацію з метою не відставати від поставленої задачі – сформувати єдиний реєстр пацієнтів, де можна отримати інформацію за будь-який конкретний випадок у житті людини.

Швидкий темп розгортання може призвести до багатьох проблем з безпекою, якими нехтують на користь швидкості виконання поставленого завдання. Це призводить до потреб вносити зміни у штатному розпису і вже сьогодні можна побачити нові робочі місця у медичних закладах, такі як «Системний адміністратор». І саме на нього покладено завдання провести комп'ютеризацію закладу. Якщо говорити про великі міста, то там проблем з спеціалістами не буде, завжди знайдеться досвідчена людина, яка зможе зробити все потрібне для правильного впровадження нових ланок у роботі закладу. Але й такі медичні заклади, що є важливими територіальними пунктами для багатьох людей, які знаходяться у селах, повинні брати участь у цій реформі. Тому часто там проводиться комп'ютеризація своїми силами. Десь запросять спеціалістів, десь будуть намагатися розгортати локальні мережі своїми руками. Основним завданням у такому випадку є забезпечення комп'ютеризованих робочих місць для всіх працюючих лікарів та стабільне підключення до мережі Інтернет.

Отже, обрана тема є актуальною з точки зору сучасних завдань покладених на медичні заклади. Розгортання мережі у закладі мусить нести з собою і відповідні політики безпеки, адже працювати у такій мережі будуть з чутливими даним, такими як особисті дані пацієнтів.

Об’єктом дослідження є комунальне некомерційне підприємство «Дубівська лікарня».

Предметом дослідження є локальна мережа комунального некомерційного підприємства «Дубівська лікарня».

Мета роботи. Побудувати систему мережевої безпеки на базі КНП «Дубівська лікарня».

Завдання роботи. 1. Описати теоретичні засади поняття мережевої безпеки. 2. Провести огляд підприємства та його обладнання. 3. Оглянути наявні політики безпеки та програмно-апаратні засоби і розробити, за потреби, рекомендації щодо їх поліпшення.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ЗАСАДИ ПОНЯТТЯ МЕРЕЖЕВОЇ БЕЗПЕКИ

1.1 Безпека мережі

Безпека мережі — є заходи, які направлені на захист мережі від несанкціонованого доступу, навмисного втручання у її роботу, випадкового або цільового руйнування її компонентів.

Як правило до безпеки мережі входять наступні пункти: захист обладнання, захист програмного забезпечення, захист даних та захист персоналу. Складається вона з нормативних документів, положень та політик щодо роботи з нею, які були прийняті підприємством при розробці такої мережі. За мету такі пункти ставлять запобігання неправильного використання мережі, запобіганню несанкціонованого доступу до неї та виключення чинників, які можуть призвести до її відмови або зміни, чи то випадкової, чи то націленої. Мережева безпека містить правила доступу до даних мережі кожного користувача у рамках виділених їм повноважень.

Охоплює мережева безпека всі види комп’ютерних мереж, такі як: державні, приватні, тощо.

Кожна безпека з чогось починається, у випадку мережевої безпеки вона має початок з автентифікації користувача, що досягається введенням відповідного імені користувача та паролю. Розрізняють багато видів автентифікації: однофакторну, двофакторну та трифакторну автентифікації. Однофакторна автентифікація має на увазі одне джерело автентифікації користувача, наприклад, ім’я користувача. Двофакторна — у додаток до імені користувача він повинен використати який-небудь маркер безпеки чи ключ-карту. Трьохфакторна автентифікація має на увазі, що окрім перших двох обов’язкових пунктів має бути і третій, наприклад, сканування сітківки ока, або відбитків пальців. Після проходження визначеного на підприємстві алгоритму та підтвердження особи, брандмауер забезпечує користувачу доступ до мережі.

Але система безпеки мережі не ґрунтується лише на одному методі автентифікації користувача, це є комплекс засобів захисту, що забезпечує роботу мережі та її захист навіть якщо якась частина з них буде пошкоджена, або відключиться. Зокрема встановлення рівнів безпеки надає можливість доступу до даних різного типу доступу, що дає змогу отримати доступ до них з будь-якого місця, де є доступ до мережі і захищає їх від несанкціонованого доступу.

Окрім несанкціонованого доступу для мережі становлять загрозу і віруси. Саме тому одним з пунктів мережевої безпеки є антивірусне програмне забезпечення або системи запобіганню вторгненням, що перевіряють потенційно шкідливих вміст у даних, що передаються по мережі. Такі рішення допомагають виявляти та пригнічувати активність вірусів. Системи виявлення вторгнень на основі аномалій можуть відстежувати мережу і реєструвати аномальний трафік для подальшого аудита. Новіші системи, які засновані на машинному навчанні з повним аналізом мережі, можуть виявляти активні атаки з боку вірусів.

Також до системи безпеки мережі можна віднести і шифрування з’єднання в її середині.

Ще одним засобом системи безпеки мережі є так званий «honeypot». «Honeypot», як каже його назва, є приманкою для зловмисників. Це є така точка у мережі, які є незахищеною та вразливою, але є ізольованою та контрольованою. Використання «honeypot» у мережі дає змогу адміністраторам побачити які саме техніки експлуатації вразливостей хотів використати зловмисник та стежити за новими методами використання цих загроз. Такі точки доступу можуть перетягати увагу під час атаки на себе та грати на виснагу з атакуючим, адже вони є спеціально створеними так, щоб мати у собі основні вразливості, які легко побачити при скануванні мережі.

З вище написаного можна виділити, що система безпеки мережі складається з:

— захищеності від внутрішніх та зовнішніх мережних атак;

— забезпечує конфіденційність даних та їх обміну;

— контролює доступ до даних;

— забезпечує надійність мережі.

Використання системи безпеки мережі може бути відмінним у різних ситуаціях. Так для домашньої мережі не потрібно використовувати багатофакторну автентифікацію користувача. Але її повне ігнорування може призвести до великих проблем у подальшому.

1.2 Джерела загроз

Системи мережевої безпеки використовуються різних сферах діяльності, тому і цілі у систем безпеки можуть бути різні, щоб вони задовольняли всі аспекти потреб сфери діяльності.

Основі галузі у яких використовуються мережеві системи безпеки наступні:

— безпека корпоративних мереж;

— захист локальних мереж;

— безпека мережі основного та віддаленого офісу;

— захист важливих вузлів трафіку;

— налаштування відділеного доступу через VPN для доступу до корпоративної мережі;

— безпека у мережах провайдера;

— забезпечення захисту сховищ інформації.

Джерела загроз поділяють на три основні групи:

— антропогенні джерела;

— техногенні джерела;

— стихійні джерела.

Антропогенні джерела загроз є обумовлені діями суб’єкта. Це можуть бути дії, які спричиняють порушення безпеки мережі та класифікуються як навмисні або випадкові. До навмисних джерел загроз виділяють різні атаки на мережу, або через фізичний доступ до неї, або через відділений. До таких загроз відносять: атаки у відмові обслуговування, фішинг, тощо. У свою чергу випадкові джерела

загроз є викликані, зазвичай, неуважністю працівників. Це може бути невірне використання пристроїв, неуважність у використанні програмного забезпечення. Джерела загроз такого типу можуть призвести до порушення безпеки як зовні, так і середини. Зазвичай, їх можна спрогнозувати та запобігти за допомогою відповідних політик безпеки.

Техногенні джерела загроз це такі, що є спричиненими технічними засобами. Такі джерела загроз вже є менш прогнозовані, бо залежать від певних властивостей обладнання та програм, які використовуються у мережі. Вони так само можуть бути викликані як зсередини мережі, так і ззовні.

Стихійні джерела загроз є деякою групою обставин, що неможливо спрогнозувати. До них відносять переважно природні катаклізми, які, як правило, є зовнішніми. Заходи проти таких загроз мають застосовуватися на підприємстві постійно.

Основними загрозами для мережі все ж є людський та технічний чинник. Якщо до людських чинників відносять дії, що пов’язані з людиною, то до технічних – загрози, які можуть бути спричинені програмно-апаратними засобами.

Людський чинник пов’язаний з діями конкретних людей, які мають, або намагаються отримати доступ до мережі. Він може надходити як ззовні так і зсередини підприємства. До зовнішніх загроз належать: хакери, конкуренти, шахраї. До внутрішніх відносяться люди, що безпосередньо працюють на підприємстві та призводять до порушень політик безпеки навмисно або випадково.

Основні джерела загроз для мережі поширюються наступними способами:

— через мережу Інтернет, тобто зловмисники розміщують шкідливе програмне забезпечення на інтернет ресурсах, формують фішингові сайти, безпосередньо атакують мережу через нього;
— через корпоративну мережу, тобто через доступ безпосередньо до мережі, наприклад, таким чином можна розповсюджувати шкідливі програмні засоби;

— через електронну пошту, яку можна використати для безпосереднього розсилання фішинг-листів, передачі шкідливого програмного забезпечення, підробки листів та для соціальної інженерії;
— через носії інформації, на яких зберігається шкідливе програмне забезпечення та використовується для доступу до локальної мережі підприємства або для доступу до інформації, що зберігається на них чи у мережі.

1.3 Типи атак

Як правило розрізняють два типи атак ініційованих зловмисниками: пасивні та активні. Під пасивними атаками розуміють такі атаки, коли зловмисник перехоплює дані, що проходять через мережу. Активні же, коли зловмисник за допомогою команд хоче порушити нормальну роботу мережі, або провести розвідку, щоб знайти вразливі місця у мережі.

До пасивного типу атак відносять:

— прослуховування мережі;
— сканування портів;
— сканування в режимі очікування
— шифрування
— аналіз трафіку

Прослуховування мережі — це прихований моніторинг Інтернет зв’язку. Досягається він через розміщення відповідних пристроїв для моніторингу на самому пристрої, біля нього або на проводах. Перехоплювачі пакетів — це програми, що використовують для перехоплення даних, які передаються у мережі та є широко використовуваними. Також є різні програмні рішення для цього, зокрема трояни, що дають таку змогу.

Сканування портів відбувається за допомогою програм, що надсилають клієнтські запити до діапазону адрес портів сервера з метою пошуку активного порту, через який, потенційно, можна зробити атаку.

Сканування у режимі очікування — це метод сканування TCP портів, який базується на відправці підроблених пакетів на комп'ютер та пошуку доступних сервісів для його прийняття. Досягається імітацією роботи іншого сервера або комп'ютера, який повільно працює, справжній же не працює. Таку дію можна виконати за допомогою звичайних мережевих утиліт, таких як: nmap або hping. Дана вразливість виконує одразу дві цілі — сканування портів та створення таблиці довірених ip-адрес між комп'ютерами у мережі. Основна мета цієї атаки це перевірити статус конкретного порту та залишитися невидимим для цільового хоста.

Аналіз трафіку це процес перехоплення повідомлень у мережі та перевірки їх з метою пошуку шаблону комунікацій, навіть якщо повідомлення є зашифрованим.

До активних атак відносять:

— віруси;

— модифікації даних;

— атаки у відмові обслуговування;

— активне сканування портів;

— підробку DNS;

— атаки типу «Людина-по-середині» ;

— підробку пакетів ARP;

— переключення VLAN;

— атака широкомовними пакетами ICMP ECHO;

— переповнення буфера;

— переповнення купи;

— SQL ін'єкції;

— фішинг;

— міжсайтовий скріптинг;

— міжсайтова підробка запиту.

Віруси це тип програмного забезпечення, який при виконанні свого коду модифікує інші програми на комп’ютері та вставляє у них свій код. Всі вірусні програми мають програму-носія, так звану «host program», і при її запуску спочатку запуститься саме вірусна програма, якщо не замість потрібної. Але є деякі віруси, які не потребують інших програм для свого запуску, зокрема черв’яки.

Модифікація даних це вид атаки, коли зловмисник хоче якимось чином змінити дані на комп’ютері. До них відносять програми-вимагачі, такі як «WannaCry». Завданням цих програм є ураження операційних систем та подальше шифрування всіх файлів.

Атаки у відмові обслуговування, більш відомі як «DoS-атаки» або «DDoS-атаки». Під час такої атаки зловмисник намагається порушити роботу мережевого ресурсу або зробити його недоступним на деякий час. DoS-атака досягається заповненням цільового мережевого ресурсу великою кількістю запиту, що призводить до перевантаження системи та до її відмови. DDoS-атака використовує такий самий метод з тією різницею, що запити надходять не з одного джерела а з багатьох, зазвичай для цього використовують так звані «ботнети».

Активне сканування портів це теж саме сканування портів тільки з тією різницею, що зловмисник використовує інші програми для цього, у яких вже націлено обирає діапазон портів або вводить їх вручну.

Підробка DNS є формую злому мережі, при якому пошкоджені DNS дані відправляються у DNS хеш, що у результаті призводить до того, що мережевий ресурс повертає іншу відповідь, наприклад, ip-адресу. Це призводить до того, що трафік буде перенаправлений на комп’ютер зловмисника.

Атаки типу «Людина-по-середині», більш відомі як «man-in-the-middle», це атаки, при яких зловмисник таємно влізає у комунікацію між двома мережевими обладнаннями та передає потрібні йому команди, або змінені відправлені цими

сторона. Прикладом такої атаки є підключення зловмисника до незахищеної точки Wi-Fi та налаштування вхідного та вихідного трафіку з цієї точки через свій девайс.

Підробка ARP пакетів це метод, за допомогою якого зловмисник відправляє ARP (address resolution protocol – протокол визначення адрес) повідомлення у локальну мережу. Ціль такої атаки полягає у тому, щоб зв’язати MAC-адресу зловмисник з IP-адресою другого хоста у результаті чого зловмисник може перехопити весь трафік який був направлений на ту ip-адресу. Така атака дозволяє зловмиснику перехоплювати трафік, модифікувати його або взагалі зупиняти.

Переключення VLAN — це вразливість у комп’ютерній безпеці, яка дає змогу провести атаку на мережеві ресурси у віртуальній локальній мережі. Завдання такої атаки полягає у тому, щоб атакувати хост у VLAN та отримати доступ до інших VLAN.

Атака широкомовними пакетами ICMP ECHO — це розподілена атака тип DDoS, при якому велика кількість пакетів протоколу ICMP з підроблених вихідних ip-адрес цілі передаються до мережі з використанням широкомовної ip-адреси.

Переповнення буферу — це атака, що спрямована на перезапис оперативної пам’яті, що використовується програмою. А саме тої частини оперативної пам’яті, де знаходиться виконуваний код програми та заміняє її на свій, що є шкідливим.

Переповнення купи — це тип переповнення буфера у області даних купи. Використання такої атаки відбувається шляхом пошкодження цих даних відповідним чином, для того, щоб програма перезаписала внутрішню структуру, наприклад, показники зв’язаних списків.

SQL ін’єкції є методом ін’єкції шкідливого SQL коду, при якому цей код вставляється для виконання у поле вводу SQL. Такі ін’єкції можуть бути використані лише тоді, коли для них є така можливість. Як приклад їх можна

використати коли вихідний код не має суворо типізованого показника для роботи з символами стрічкового літерала.

Фішинг є одним з найбільш відомих типів атак. Його мета полягає у тому, щоб змусити людину ввести свою конфіденціальну інформацію. Зазвичай для цього використовують посилання, що ведуть на нібито легітимний сайт, але насправді він є сфабрикований зловмисником та ніяким чином не належить офіційному джерелу. Часто за допомогою такого методу атаки люди самостійно передають зловмиснику свої паспортні дані, дані від кредитних карток, паролі, тощо.

Міжсайтовий скріптинг — це атака, яка дозволяє зловмиснику робити ін'єкцію свого шкідливого коду на стороні клієнта веб-сторінки, яку переглядають інші користувачі.

Підробка міжсайтових запитів є атакою, яка дозволяє використовувати веб-сайту несанкціоновані команди. На відмінку від міжсайтового скріптингу цей метод атаки використовує не довіру користувачі конкретній веб-сторінці, а довіру браузера до веб-сторінки.

1.4 Основні елементи створення системи мережевої безпеки

Є безліч стандартів та документів у яких описані етапи та процеси створення систем мережевої безпеки. До таких стандартів відносять ISO/IEC 17779, у якому описані практичні правила менеджменту інформаційної безпеки та включає у себе наступні розділи:

— політика безпеки;

— організація інформаційної безпеки ISO 177779;

— управління ресурсами ISO 177779;

— безпека людських ресурсів ISO 177779;

— фізична безпека та безпека середовища;

— управління передачею даних і операцій;

— контроль доступу;

— розробка та обслуговування систем;

— управління розслідуванням інцидентів інформаційної безпеки;

— управління неперервністю бізнесу;

— відповідність до вимог.

Також є й інші документи, які описують методики побудови безпеки мереж, як RFC 2196, ISO/IEC27000 та ряд інших. Побудова мережі та її безпеки також базується на нормативних документах. Деякі компанії навіть розробляють свої власні стандарти, до таких компаній відноситься, наприклад, Cisco.

Одними з основних елементів захищеної мережі є міжмережеві екрани та антивірусні програми.

Міжмережевими екранами прийнято називати системи мережевої безпеки, які відслідковують увесь трафік та контролюють його на основі описаних правил безпеки. Зазвичай такі екрани використовують для встановлення бар'єру між надійною, тобто локальною мережею та ненадійною, наприклад, мережею Інтернет.

Мережеві екрани є мережевою системою або хост-системою. Мережева система — це програмне рішення, яке працює на обладнанні загального призначення, або апаратний пристрій, який працює на обладнанні спеціального призначення, або віртуальний пристрій, який працює на віртуальному хосту та яке управляється гіпервізором. Пристроєм мережевого екрану також можуть бути і служби DHCP або VPN. Мережеві екрани на базі хост-системи розгортаються безпосередньо на самому хості для контроля мережевого трафіку. Це може бути daemon або служба в основі операційної системи чи програма-агент для захисту.

Виділяють три типи міжмережевих екранів: мережного рівня, прикладного та рівня з'єднання.

Міжмережевий екран мережного рівня є представленим екрануючим маршрутизатором. Цей маршрутизатор займається контролем службових пакетів мережевого та транспортного рівня моделі OSI. Основною проблемою такого рішення є те, що маршрутизатор не контролю ще 5 інших рівнів цієї моделі. Не

меншою проблемою є і те, що більшість маршрутизаторів здійснюють лише фільтрацію трафіку, але у них відсутні механізми аудиту або системи подачі сигналів тривоги. Тобто, це означає, що такі пристрої можуть бути атакованими та успішно відбивати націлені на них атаки, але якось про це дізнатися буде проблематично.

Міжмережеві екрани прикладного рівня займаються тим, що встановлюють поділ між локальною мережею та мережею Інтернет. Так би мовити встають посередниками між цими двома мережами. Саме через це їх можна вважати одним з найкращих способів захисту мережі. Такі міжмережеві екрани називають проксі-серверами. Їхнім недоліком є те, що їхня звичайна робота по аналізу трафіку та його контролю, щодо встановлених правил призводять до зменшення продуктивності самої мережі. Це все можна, у деякій, мірі вирішити використанням більш досконалого обладнання.

Міжмережеві екрани які працюють на рівні з'єднання є, у деякій, мірі схожими на екрани прикладного рівня. Їхня схожість полягає у тому, що вони також є посередниками у роботі локальної та глобальної мережі. А от відмінність полягає у тому, що такі міжмережеві екрани обслуговують більшу кількість протоколів. Тоді як міжмережеві екрани прикладного рівня вимагають відповідного програмного забезпечення для кожного протоколу мережевої служби.

Першим зареєстрованим типом міжмережевих екранів був фільтр пакетів, який перевіряє пакети, що передаються між комп'ютерами. Такі системи підтримували списки контролю доступу, що визначали, які пакети будуть переглянуті та що з ними робити у подальшому за встановлених правил, якщо ж у списку не було вказано яку дію слід обрати для відповідного пакету, то вони, за замовчуванням, відхиляли їх. Три основні дії щодо вхідних пакетів є: тихе відхилення, це коли пакет був відхилений без подальших дій, відхилення за допомогою протоколу ICMP або відповіді на перевірці пакетів по протоколу TCP та пересилання його до наступного одержувача. Пакети також можуть фільтрувати за допомогою ір-адрес джерел, протоколів, портів. Такі міжмережеві

екрани використовували протокол TCP або UDP, які були направлені у відповідні порти пристрої, що дозволяло таким екранам розрізняти який тип трафіку вони отримують, веб-перегляд, віддалений друк, передача електронного листа чи файла.

Наступні межмережеві екрани, або так звані міжмережеві екрани другого покоління, виконували роботу фільтрації пакетів, але вже почали вести запис всіх з'єднань між конкретними портами, які використовували два пристрої на 3 рівні моделі OSI, що дозволяло перевіряти весь трафік між конкретними двома вузлами.

У подальшому міжмережеві екрани стали використовувати для фільтрації пакетів на прикладному рівні, метод яких полягав у тому, що такий екран може розуміти відповідні програми та протоколи, як, наприклад, протокол FTP, DNS, HTTP. Така особливість дозволяє йому ідентифікувати небажані програми або служби, які використовують нестандартний порт чи навіть виявляти зловживання дозволеним протоколом. Також такі екрани можуть забезпечити єдине управляння безпекою мережі, у тому числі шифрування DNS та VPN.

Сучасні міжмережеві екрани забезпечують більший спектр для захисту. Вони дозволяють забезпечити більш широкий діапазон перевірки на прикладному рівні, що у свою чергу суттєво збільшує можливість перевірки вхідних пакетів та дозволити розгортання веб-фільтрів, систем запобігання вторгненням, керування ідентифікацію користувачі, або навіть налаштовувати міжмережеві екрани для веб-додатків.

Міжмережеві екрани, які основані на конкретних кінцевих точках функціонують, визначаючи, чи повинен процес приймати будь-яке з'єднання. Тобто вони фільтрують з'єднання, перевіряючи ідентифікатор процесу пакетів даних на відповідність до набору правил локального процесу, який бере участь у передачі даних. Такі міжмережеві екрани у програмах, які підключаються до викликів сокетів, також називають фільтрами сокетів.

Антивірусне програмне забезпечення являє собою комп'ютерну програму, що використовується для попередження, виявлення та видалення шкідливого

програмного забезпечення. На сьогоднішній день таке забезпечення захищає користувачів від усіх відомих комп'ютерних загроз. Наприклад: вони дозволяють захистити комп'ютер від програм-вимагачів, троянів, хробаків, клавіатурних шпіонів, бекдорів, руткітів, тощо. Деякі антивірусні програми також дозволяють захищати користувача від спаму, фішингу, шкідливих веб-сторінок, DDoS-атак, тощо.

Для ідентифікації шкідливих програм антивіруси часто використовують наступні методи: перевірка програми у пісочниці, метод інтелектуального аналізу даних, виявлення на основі сигнатур.

Перевірка програми у пісочниці має під собою метод аналізу поведінки програми у захищеному віртуальному середовищу. У такому середовищі, яке є ізольоване від основної системи, шкідлива програма запускається та ядро антивірусної програми аналізує які дії буде виконувати шкідливих код. У залежності від зареєстрованих дій, вона може виявити чи дійсно перевірена програма є шкідливою чи ні. Цей метод дуже рідко використовується для кінцевого продукту, адже він є досить ресурсозатратним та може призводити до сильного уповільнення роботи система користувачі.

Метод інтелектуального аналізу є одним з найновіших методів аналізу шкідливих програм. Його метою є використання певних алгоритмів аналізу даних та машинного навчання у спробі класифікації поведінки шкідливого коду, тобто визначення його характеристик, які витягуються з самого файлу шкідливої програми.

Виявлення на основі сигнатур являється вже традиційним методом ідентифікації шкідливих програм. Він складається з того, що фірми, які випускають антивірусні програми, аналізують всі зразки шкідливих програм, які вони можуть отримати та, як тільки вони визначають ці програми шкідливими, додають у базу даних антивірусного програмного забезпечення сигнатур по яким цей вірус можна виявити.

Хоч такий підхід є ефективним для вже відомих вірусів, він не захищає від нових рішень зловмисників, які можуть використовувати нові методи

використання вразливостей комп’ютера, або займатися обфускацією коду, що дозволяє обходити такий метод. Зловмисники почали впроваджувати такі частинки коду, що шифрують самі себе або якимось іншим чином себе змінюють, для того, щоб не співпадати з створеними для них сигнатурами у базах даних антивірусного програмного забезпечення.

Через використання таких методів обходу антивірусного програмного забезпечення комп’ютерні віруси можна зрівняти з вірусами, які відомі з медицини. Багато вірусів починаються як інфекція, які згодом можуть мутувати у дещо інше, через використання зловмисниками різних методів маскування, що призводить до великої кількості різних варіантів одного й того самого вірусу. Тому для більш швидкої ідентифікації вірусу використовують метод загальної сигнатури, що містить у собі основні маркери цілого сімейства вірусів, замість одного конкретного. Спеціалісти з аналізу вірусів знаходять унікальні області впливу на систему, що дозволяє виділяти одну спільну сигнатуру вірусів. Під час аналізу шкідливого програмного забезпечення антивірусна програма переглядає такі спільні сигнатури і навіть, якщо вірус був змінений, але впливає на конкретний процес системи, це дозволяє виявити його. Виявлення таким методом називається «евристичним виявленням».

Антивірусне програмне забезпечення також може бути використане для сканування системи на наявність руткітів. Руткіт — це тип шкідливого програмного забезпечення, який націлений на те, щоб отримати контроль типу «адміністратор» над комп’ютерною системою. Вони можуть використовуватися для зміни роботи системи, уповільнення її роботи, тощо.

Всі ці методи можна використовувати для захисту системи у реальному часі, чим і займається антивірус. У його роботу включається відстежування підозрілої активності на комп’ютері, наприклад: шпіонського програмного забезпечення, рекламного програмного забезпечення, тощо. Захист у режимі реального часу дозволяє сканувати програми прямо під час їх роботи.

РОЗДІЛ 2. ХАРАКТЕРИСТИКА ОБ’ЄКТУ ДІЯЛЬСНОСТІ

2.1 Огляд підприємства

Комунальне некомерційне підприємство «Дубівська лікарня» Дубівської селищної ради Тячівського району Закарпатської області є державною установою для надання медичної допомоги населенню по наступним пакетам програми медичних гарантій:

- Профілактика, діагностика, спостереження, лікування та реабілітація пацієнтів у амбулаторних умовах.
- Стаціонарна допомога дорослим та дітям без проведення хірургічних операцій.
- Стоматологічна допомога дорослим та дітям.
- Ведення вагітності в амбулаторних умовах.

Метою діяльності є надання населенню, згідно з вимогами відповідних нормативно-правових актів, медичної допомоги, медичних послуг, спрямованих на збереження, поліпшення та відновлення здоров’я населення в обсязі бюджетних асигнувань; здійснення іншої діяльності, необхідної для належного забезпечення профілактики, діагностики, лікування хвороб, в тому числі на платній, або альтернативній основі.

Знаходиться на території селища Дубове Тячівського району Закарпатської області. За адресою 90531, Закарпатська обл., Тячівський район, селище міського типу Дубове, вулиця Миру, будинок 131.

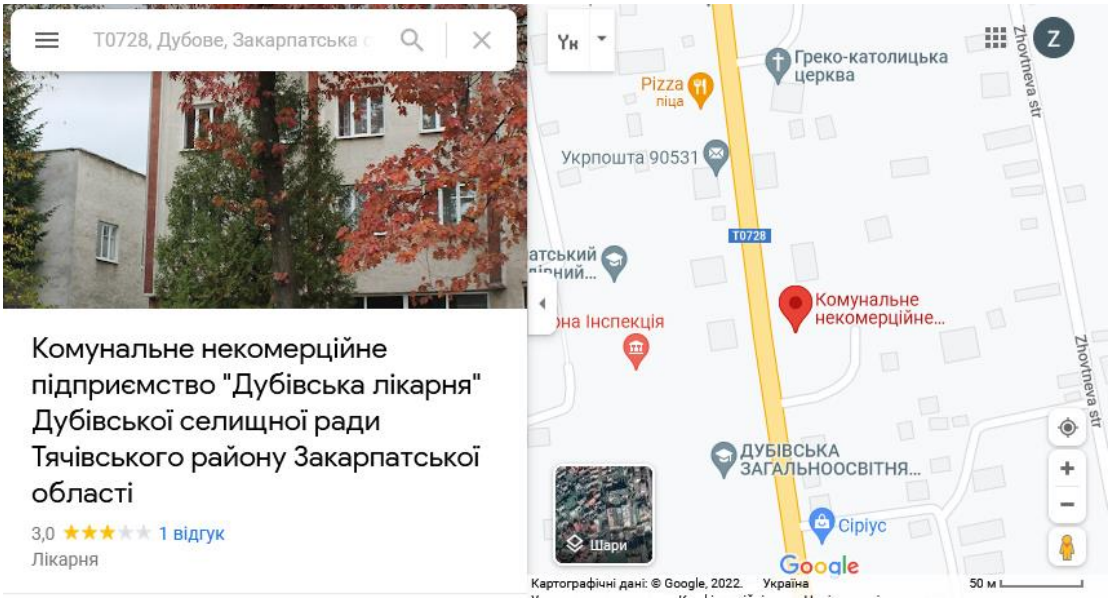

Рисунок 2.1 — Адреса КНП «Дубівська лікарня» у Google Maps

Будівля складається з двох корпусів. Перший — це будівля, висотою чотири поверхи, яка відведена для роботи з амбулаторними пацієнтами. У ньому знаходяться основні кабінети працюючих лікарів: дерматовенеролога, ортопед-травматолога, акушер-гінеколога, хірурга, стоматолога, невролога, терапевта.

Також тут знаходяться і кабінети відведені під клінічну лабораторію та рентген лабораторію.

У цьому ж корпусі знаходяться і декілька інших підрозділів:

Бухгалтерія — займається веденням фінансової сторони підприємства. Відповідає за фінансові операції, рахунки та проведенням тендерів підприємства.

Відділ кадрів — займається набором кваліфікованого персоналу, адаптацією персоналу на підприємстві, питаннями охорони праці та безпеки. Тут зберігаються всі особисті справи працівників.

Рисунок 2.2 —Вигляд поліклінічного корпусу з архівних фото лікарні

Другий корпус відведений для стаціонарного відділення на 30 ліжок з 4 ліжками інтенсивної терапії. У ньому знаходяться пацієнти на стаціонарному лікуванні. Всього є 14 палат, ординаторська та прийомний покій.

Рисунок 2.3 — Вигляд стаціонарного корпусу з архівних фото лікарні

Можна побачити, що існує досить велика кількість робочих місць, які мають бути оснащені комп’ютеризованим робочим місцем. І не тільки з доступом до необхідних програм тільки медичного призначення, а й для роботи з фінансами, персоналом та проведенням медичних аналізів.

У своїй роботі персонал, який по штатному розпису відноситься до категорії медичного, використовує медичну інформаційну систему «Medics IT», яка працює через мережу Інтернет та має веб-інтерфейс. Відповідно до цієї інформації кожне робоче місце медичного персоналу має мати вихід до глобальної мережі Інтернет. Тож доцільно буде створити певні політики безпеки та для роботи у браузерах та на самому комп’ютеризованому робочу місці.

Персонал, що відносить до бухгалтерії використовує у своїй роботі багато програм та використовує багатофункціональні пристрої. Важливим для їх роботи буде створення локальної мережі ізольованої від локальної мережі підприємства, у якій буде налаштовано доступ до багатофункціональних пристроїв, принтерів та спільних папок. Відповідно потрібно розробити політики безпеки щодо цієї мережі.

У відділі кадрів на даний момент більшість інформації зберігається у паперовому виді, але ця інформація дублюється у програмі «Медичні кадри України». Втрата таких даних може призвести до компрометації персоналу працюючого на підприємстві. Тому для забезпечення безпеки такого відділу потрібно встановити суворий контроль доступу до приміщення, де зберігаються документі. Також доцільно буде звузити перелік осіб, які можуть внести зміни у комп'ютерній програмі «Медичні кадри України».

Інформація, що оброблюється у кожному з цих відділів конфіденційна, тому втрата даних у будь-якому відділі може призвести до значних проблем, як для підприємства, так і для громадян, адже у медичному закладі міститься, як інформація про персонал, так і персональні дані населення.

Інформація підприємства, яку можна віднести до комерційної таємниці є лише заробітна плата персоналу.

До інформації з обмеженим доступом можна віднести:

— трудові договори;

— особисті справи працівників;

— зміст бухгалтерського обліку;

— бухгалтерська звітність;

— перелік наркотичних засобів, психотропних речовин та прекурсорів;

— персональні дані пацієнтів.

До відкритої інформації можна віднести:

—статут та установчий документ;

—перелік закупівель та тендерів;

—затверджений прайс-лист.

На основі вище написано можна спрогнозувати можливі загрози на підприємстві:

— здійснення несанкціонованого доступу до документів, у тому числі і тих, що знаходяться на носіях інформації, та подальше ознайомлення з ними;

— здійснення так званого плечового серфінгу, тобто спостерігання за роботою персоналу на комп'ютеризованих місцях або з документами;

— маскування під адміністратора мережі для перехоплення управління операційною системою.

Таблиця 2.1 — Перелік можливих загроз мережі підприємства

Загроза безпеці	Міри протидії загрозі	
	Технічні	Організаційні
Крадіжка носіїв інформації		Інструкції для персоналу
Крадіжка паролів		Інструкції для персоналу
Шкідливі програмні засоби	Антивірусне програмне забезпечення	Інструкції для персоналу
Фішинг	Антивірусне програмне забезпечення	Інструкції для персоналу
Встановлення програмного забезпечення не пов'язаного з виконанням обов'язків	Налаштування політики користувачів	Інструкції для персоналу

Продовження таблиці 2.1

Загроза безпеці	Міри протидії загрозі	
	Технічні	Організаційні
Вихід з ладу обладнання або програмного забезпечення	Використання резервних копій	Охорона, інструкції для персоналу
Збій у роботі електропостачання	Використання безперебійних джерел живлення	
Розголошення персональної інформації	Налаштування політики доступу	Інструкції для персоналу

Також потрібно розуміти, що підприємство відноситься до охорони здоров’я населення та вхід до будівлі є відкритим для будь-кого. Це може призвести до можливої загрози несанкціонованого доступу до мережі через фізичний доступ. Для того, щоб унеможливити загрозити з таких джерел потрібно розташовувати комп’ютерне робочі місце так, щоб до нього можна було дістатися лише через працівника. Тобто встановлювати такі робочі місця подалі від дверей, забезпечити постійне перебування на одному робочому місці хоча б одного працівника закладу, який зможе контролювати доступ до нього та використання інструкцій для персоналу по роботі з комп’ютеризованим робочим місцем.

2.2 Огляд наявного обладнання та рішень щодо політик безпеки

Підприємство має у використанні 20 комп’ютеризованих робочих місць виділених для роботи персоналу. Всі робочі місця знаходяться у відповідних

кабінетах та постійно використовуються. До такого місця відносимо сам комп’ютер, периферію, багатофункціональні пристрої, принтери.

Їхня конфігурація наступна:

Таблиця 2.1 — Конфігурація комп’ютеризованого робочого місця

Корпус	Vinga CS110B
Материнська плата	ASUS J1800I-C
Процесор	Intel Celeron J1800
Оперативна пам’ять	Goodram DDR3-1600 4096MB PC3-12800 1 штука
Твердотілий накопичувач	Patriot Burst Elite 240GB PBE240GS25SSDR
Блок живлення	CHIEFTEC 350W (SFX-350BS-L)
Відеокарта	Інтегрована
Монітор	Asus VT168H (90LM02G1-B02170)
Переферія	Logitech MK120 USB
USB-адаптери	TP-LINK TL-WN727N
Операційна система	Windows 10 Pro

Рисунок 2.4 — Корпус Vinga CS110B

Дана конфігурація комп’ютеризованого робочого місця дає змогу робочому персоналу виконувати їхню роботу по внесенню пацієнтів до електронної системи охорони здоров’я, ведення бухгалтерського обліку та роботи відділу кадрів.

З мережевого обладнання є 5 маршрутизаторів TP-LINK TL-WR841N, 1 комутатор TP-LINK TL-SF1008D, 1 маршрутизатор MikroTik RB951Ui-2HnD

Маршрутизатори TP-LINK TL-WR841N використовуються на підприємстві для організації локальної мережі та налаштовані у режим мосту, що дозволяє використовувати їх як точки доступу до глобальної мережі Інтернет. Їхнє розташування обумовлене максимальною дистанцією роботи таких маршрутизаторів та знаходяться вони у обох корпусах: поліклінічному корпусі на другому, третьому та четвертому поверсі, у стаціонарному корпусі у ординаторській. У якості паролю доступу тут використовується пароль за замовчуванням, що є дуже легким у зломі, шляхом простого перебору паролів.

Таблиця 2.2 — Характеристики маршрутизатора TP-LINK841N

Частота роботи Wi-Fi	2.4 ГГц
Інтерфейси	4 порти 10/100M LAN (типу RJ45) 1 порт 10/100M WAN (типу RJ45)
Швидкість LAN портів	100 Мбіт/с
WAN-порт	Ethernet
Стандарт зв'язку Wi-Fi	802.11b/g/a 802.11n
Швидкість Wi-Fi, Мбіт/с	300 Мбіт/с
Додаткові режими роботи	Wisp Точка доступу Підсилювач Wi-Fi сигналу
Підтримка протоколів	PPPoE
Функції VPN	PPTP, L2TP, IPSec
Підтримка операційних систем	Windows 98 / NT / 2000 / XP / Vista / 7 / 10 MacOS NetWare UNIX or Linux
Габарити і вага	192 x 130 x 33 мм

Рисунок 2.5 — Маршрутизатор TP-LINK841N

Для комутації мережі використовується комутатор TP-LINK TL-SF1008D, який є простим комутатором до якого підключаються два маршрутизатора, що знаходяться у відділі бухгалтерії та ординаторській.

Таблиця 2.3 — Характеристики комутатора TP-LINK TL-SF1008D

Кількість і тип портів Ethernet	8 x 10/100 Мбіт/сек Auto-Negotiation RJ45 портів
Додаткові можливості	Топологія - Зірка Протокол CSMA/CD Підтримувані протоколи та стандарти IEEE 802.3 10Base-T, IEEE 802.3u 100Base-TX
Габарити	140 x 85 x 30 мм
Тип	Некерований
Тип портів	8 x Fast Ethernet (10/100 Мбіт/с)

Рисунок 2.6 — Комутатор TP-LINK TL-SF1008D

У якості основного маршрутизатора, який використовується для виходу до глобальної мережі Інтернет, використовується маршрутизатор MikroTik RB951Ui-2HnD. До нього підключений провід WAN, який дає доступ до мережі Інтернет та через LAN порт підключений до комутатора, через який реалізована комутація інших маршрутизаторів. На цьому маршрутизаторі вже змінений пароль, який оснований на 8 цифрах, що також є вразливим для атаки перебором. До адміністративної панелі цього маршрутизатора також можна отримати доступ за допомогою логіну та паролю за замовчуванням. Дана вразливість може використовуватися для доступу до мережі з правами адміністратора, що може нести за собою загрозу витоку інформації з локальної мережі та змінення конфігурацій всіх маршрутизаторів доступних у локальній мережі. На даному маршрутизаторі є можливість налаштування політик доступу по білому списку MAC-адрес, або білому списку IP-адрес. Але тут вони не використовується. На даному маршрутизаторі Mikrotik використовуються налаштування за замовчуванням міжмережевого екрану, що виконує скидування всіх вхідних та транзитних підключень, які йдуть не з локальної мережі, дозволені ipsec, використання icmp, дозволені всі вже встановлені з’єднання. Також налаштований NAT через WAN інтерфейс.

Таблиця 2.4 — Характеристики маршрутизатора MikroTik RB951Ui-2HnD

Частота роботи Wi-Fi	2.4 ГГц
Інтерфейси	1 x WAN порт 10/100BASE-TX 4 x LAN порти 10/100BASE-TX 1 x USB 2.0 порт
Швидкість LAN портів	100 Мбіт/с
WAN-порт	Ethernet USB 3G/4G
Стандарт зв'язку Wi-Fi	802.11b/g/a 802.11n
Швидкість Wi-Fi, Мбіт/с	300 Мбіт/с
USB-порт	1 x USB 2.0
Особливості	Підтримка PoE
Конструкція антен	Вбудовані
Додаткові режими роботи	Точка доступу
Підтримка протоколів	DHCP, L2TP, PPPoE, PPTP
Функції брандмауера	Міжмережевий екран Firewall
Інші функції	Налаштовується через веббраузер, Winbox або через консоль Пристрій може роздавати PoE-живлення
Додаткові характеристики	Процесор: Atheros Atheros QCA9531 650 МГц. Пам'ять: 128 МБ
Габарити і вага	138 x 113 x 29 мм, 250 г

Рисунок 2.7 — Маршрутизатор MikroTik RB951Ui-2HnD

Сама мережа представляється підключенням маршрутизатора MikroTik RB951Ui-2HnD до глобальної мережі Інтернет з підключеними трьома комп’ютеризованими робочими місцями, що знаходяться у комп’ютерному кабінеті, кабінеті секретаря та у кабінеті директора підприємства. У подальшому від маршрутизатора проводом підключений комутатор TP-LINK TL-SF1008D, який вже підключений, так само проводами, до двох маршрутизаторів: перший знаходиться на четвертому поверсі поліклінічного корпусу у відділі бухгалтерії, другий — у корпусі стаціонару на другому поверсі у ординаторській. Якщо другий маршрутизатор використовується лише для доступу до глобальної мережі Інтернет, має підключених п’ять комп’ютеризованих робочих місць та немає інших підключень, то перший використовується також для підключення чотирьох робочих місць у локальну мережу типу «шина». Наступний маршрутизатор у цій мережі налаштований у режим роботи «WISP», що дозволяє використовувати ір-адресу одного і того самого маршрутизатора для доступу до глобальної мережі Інтернет та підключити його до попереднього з використанням безпровідної технології. Знаходиться цей маршрутизатор на третьому поверсі поліклінічного відділу та використовується безпосередньо лікарями неврологічного кабінету, кабінету гінекології та кабінетами стоматології. Останній маршрутизатор використовується так само як і попередній. Розташований він на другому поверсі поліклінічного корпусу та використовується кабінетами клінічної лабораторії, рентгенівської лабораторії та кабінетом хірурга. Мережа представлена у топології.

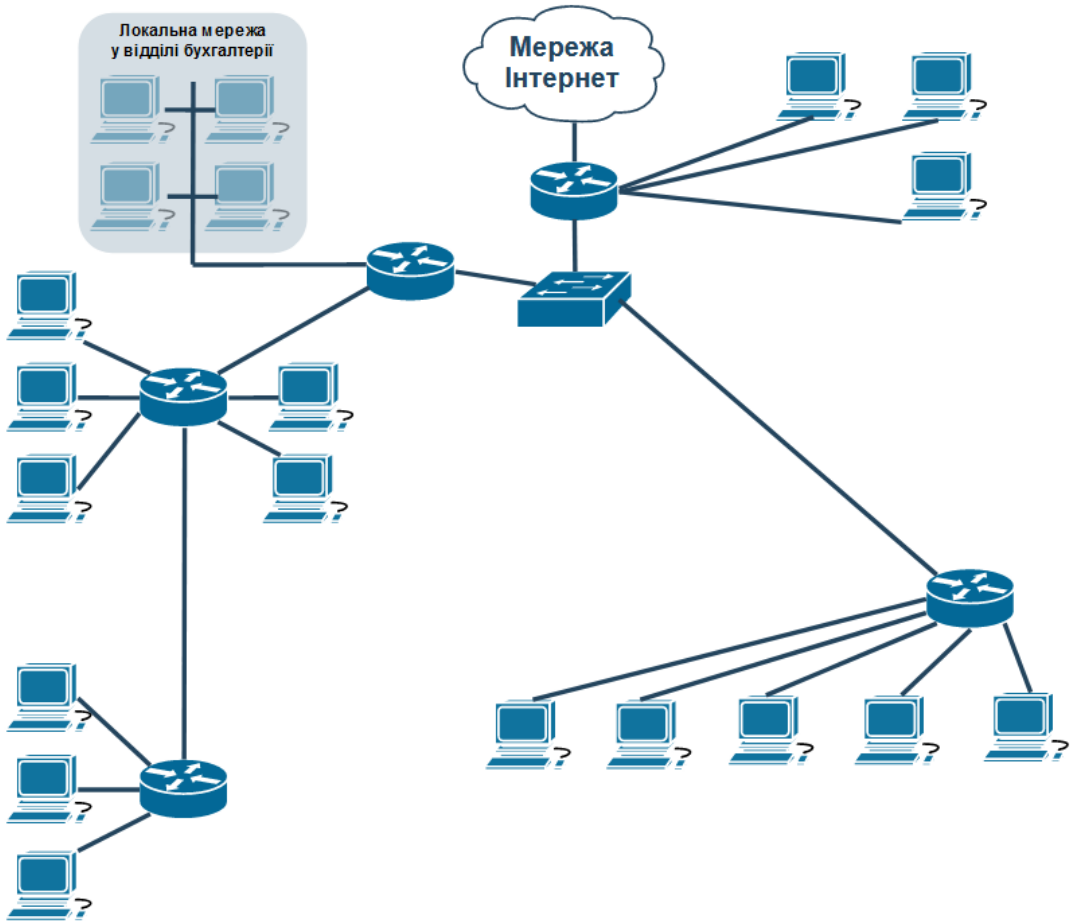

Рисунок 2.8 — Топологія мережі

2.3 Постановка завдання

Наведений вище аналіз підприємства та перелік можливих загроз політиці безпеки підприємства дає змогу визначити, які є вразливі місця у мережі підприємства. Вони можуть призвести до втрати важливих даних, таких як: особисті дані працівників, документи підприємства, паролі та логіни для роботи з електронною системою охорони здоров’я, кваліфікованих електронних підписів.

Необхідно побудувати таку мережеву систему безпеки КНП «Дубівська лікарня», яка буде включати програмно-апаратні засоби захисту, а також політики безпеки, що буду впроваджені у підприємство.

При аналізі наявної мережі та обладнання було виявлено наступні проблеми безпеки:

— використання простих паролів;

— збереження паролів без використання спеціальних програм;

— не відбувається своєчасна зміна паролів;

— відсутність політик користувачів у мережі;

— відсутність політик користувачів на комп’ютерних робочих місцях;

— низький рівень свідомості персоналу в інформаційні безпеці;

— носії інформації та токени, на яких зберігається кваліфікований електронний підпис, не зберігаються у захищених контейнерах;

— відсутність безперебійних систем електропостачання;

— відсутня система моніторінгу мережі;

— відсутнє антивірусне програмне забезпечення та мережеві екрани.

До першого етапу створення мережевої безпеки підприємства буде розробка відповідних політик безпеки вмістом яких буде:

— посадові обов’язки пов’язані з роботою на комп’ютеризованому робочому місці;

— навчання персоналу;

— контроль доступу до веб-ресурсів;

— забезпечення фізичної безпеки носіїв інформації.

Другий етап буде націлений на налагодження обладнання та налагодження програмних засобів захисту.

Для цього етапу потрібно буде визначити яке обладнання потребує додаткового налаштування та які саме апаратні засоби захисту інформації потрібні. Налаштування маршрутизаторів враховуючи методи захисту периметрів безпеки. Встановлення програмних мережевих екранів, налаштування антивірусних програм, налаштування програм для безпечного зберігання паролів, створення відповідних політик безпеки при роботі у мережі Інтернет, налаштування користувацьких акаунтів для роботи на комп’ютеризованому робочому місці.

Третім етапом буде ергономічне впровадження всіх цих політик безпеки.

РОЗДІЛ 3. ПОБУДОВА МЕРЕЖЕВОЇ СИСТЕМИ БЕЗПЕКИ

3.1 Розробка політик безпеки

Політикою безпеки прийнято вважати набір вимог, правил, обмежень, рекомендацій, які регламентовані нормативними документами на підприємстві та спрямовані на досягнення достатнього захисту мережевої системи для нормальної роботи підприємства.

Такі політики необхідно впроваджувати на підприємстві, адже є відповідні вимоги наявності таких документів від державних регуляторів, тобто від організацій, що визначають правила роботи підприємств у галузі медичної допомоги населенню. Відсутність таких документів може спричини використання обмежуваних дій, щодо підприємства або навіть спричини його повне закриття через небезпеку витоку інформації про персональні дані населення, на які воно має право таємниці.

Також не менш важливим є і той факт, що при використанні політик безпеки, нормативних документів та навчання персоналу роботі на комп’ютеризованих робочих місцях зменшує ризик злому або витоку інформації з підприємства. Тобто це свідчить про те, що підприємство, яке чітко сформувало регламент роботи на таких робочих місцях та використовує певні мережеві політики безпеки, що це являється дійсним методом забезпечення мережевої системи безпеки.

Завданнями впровадження політик безпеки є:

— мінімізація ризиків інформаційної безпеки;

— захист інформації на підприємстві;

— забезпечення стабільної роботи підприємства.

Політики безпеки використовуються у всіх аспектах діяльності підприємства, пов’язаних з мережевими системами.

Але й такі політики безпеки повинні суворо дотримуватися персоналом. Якщо з апаратно-програмними рішеннями питань виникає небагато, як

використання білих списків веб-ресурсів, то вже нормативні документи, які їх регламентують, повинні бути не лише наявні на підприємстві, а і дотримуватися персоналом. Написання таких політик безпеки має бути чітко регламентоване та сформульоване. Використання нечітко сформованих нормативних документів політики безпеки може спричини великі проблеми у роботі не лише мережі підприємства, а і у роботі підприємства в цілому. Скажімо простий список з кількох пунктів, що «можна» і «не можна» роботи на робочому місці може зменшити ризик підхоплення шкідливого програмного забезпечення, втрати конфіденційної інформації, втрати паролів, тощо. Але такий список, який чомусь на підприємстві затвердили як політику безпеки, може спричинити чималі проблеми у роботі підприємства. Для прикладу є перелік відповідних usb-портів, які можна використовувати, але для роботи працівнику потрібно більше, ніж є у затвердженій політиці безпеки, або є налаштовано білий список веб-ресурсів на який працівник може зайти і використовувати у своїй роботі, але йому прийшло посилання, яке є легітимним, але порушує політики безпеки, відповідно для подальшої роботи він повинен звертатися до системного адміністратора у кращому випадку, у гіршому до тих, хто затвердив такий документ.

На підприємстві КНП «Дубівська лікарня» було запропоновано використання наступних політик безпеки.

У першу чергу мають бути чітко сформовані пункти у посадових обов’язків кожної штатної одиниці, яка працює, або має доступ до комп’ютеризованого робочого міста, що стосується мережевої безпеки. У таких пунктах має бути відображена чітко сформульоване завдання працівника, яке він буде виконувати на комп’ютеризованому робочому місці. Це потрібно зробити у посадових обов’язках кожної посади. Повинна бути призначена відповідна посада, або посади, що будуть відповідати за виконання цих пунктів. Кожна посада має мати чітко описані обов’язки, а також регламентована.

Тобто потрібно виконати наступні пункти:

— детально та чітко сформовані умови прийому на роботу, тобто працівник повинен затвердити та підписати трудовий договір, у

якому буде встановлено його обов’язки та відповідальність при роботі на комп’ютеризованому робочому місці. Так як підприємство є медичним закладом, тобто працює з конфіденційною інформацією населення, то має буту чітко сформована згода на зобов’язання щодо нерозголошення цієї інформації. У контракті мають бути описані заходи, які будуть прийняті по відношенню до працівника у разі невиконання вимог;

— обов’язки за підтримку інформаційної безпеки мають бути включені у посадові інструкції кожного працівника підприємства;
— персонал з певною періодичністю має проходити навчання з інформаційної безпеки;
— якщо якийсь працівник був звільнений, то потрібно унеможливити для нього спроби входу до мережі підприємства.

Для кожного працівника підприємства зробити навчання по наступним питанням:

— зберігання паролів у спеціалізованих програмах;
— можливі загрози при передачі даних автентифікації у мережі підприємства особам, які не пов’язані з підприємством;
— загрози зберігання інформації на власних пристроях, а саме: небезпеки пов’язані з санкціонованою чи випадковою передачею третім особам;
— про необхідність використання власного користувацького профілю на комп’ютеризованому робочому місці;
— про правила поведінки при роботі на комп’ютеризованому робочому місці у разі необхідності залишити його на будь-який термін.

Такі правила повинен виконувати кожен працівник. Також потрібно не забувати про необхідність введення нових правил, коригування попередніх, які можуть бути потрібні при подальшому збільшенні досвіду роботи працівників на комп’ютеризованих робочих системах.

Для роботи з електронною системою охорони здоров’я кожен, хто з нею працює, повинен не тільки вносити дані до медичної інформаційної системи, а і підписувати ці дані використовуючи кваліфікований електронний підпис.

Відповідно закону України «Про електронні довірчі послуги» від 7.11.2018: «Кваліфікований електронний підпис чи печатка вважається таким, що пройшов перевірку та отримав підтвердження, якщо: під час перевірки за допомогою кваліфікованого сертифіката електронного підпису чи печатки отримано підтвердження того, що особистий ключ, який належить підписувачу чи створювачу електронної печатки, зберігається в засобі кваліфікованого електронного підпису чи печатки.»

Такий пункт у законі України зобов’язує використання кваліфікованих електронних підписів на відповідних засобах кваліфікованого електронного підпису. До таких засобів відносять: токени, хмарні сервіси та смарт-картки. Смарт-картки містять спеціально інтегральну схему, яка містить кваліфікований електронний підпис. Для використання таких карток потрібно мати спеціальне обладнання: так звані пристрої для читання смарт-карток. Використання хмарних сервісів, які пропонують можливість формування кваліфікованого електронного підпису, є досить ефективним рішенням для підприємства, але несе за собою необхідність оплати підписки для його зберігання, що пропонують таку можливість. Використання токену як засіб кваліфікованого електронного підпису є також ефективним рішенням для цього. Токен — це певний пристрій, що має у собі відповідний криптографічний модуль, який забезпечує неможливість копіювання, видалення, доступу до кваліфікованого електронного підпису, що зберігається на ньому. Він виконаний у формі звичайного USB-носія та для роботи з ним потрібне лише відповідне програмне забезпечення, яке є безкоштовним.

Рекомендовано серйозно поставитися до цього закону та ввести на підприємстві використання токенів у якості засобу кваліфікованого електронного підпису. Регламентувати чіткі постанови, щодо роботи з ним та унеможливити винесення такого пристрою за межі підприємства.

Також до політик безпеки потрібно визначити і правила використання фізичних пристроїв. Основними правила є:

- комп’ютеризовані робочі місця мають бути розташовані у захищених зонах;
- захищені зони повинні бути оснащені відповідними засобами контролю, які будуть забезпечувати доступ до них лише уповноваженого персоналу;
- для зберігання документів, які відносяться до службових, носіїв інформації з ними, мають використовуватися певні приміщення, які обладнані сейфами або металевими шафами;
- усі точки доступу, через які може бути здійснений несанкціонований доступ до приміщень де зберігаються документи, або носії інформації з ними, мають бути ізольованими;
- електропостачання, водопостачання, каналізація, опалення, вентиляція повинні забезпечувати стабільну роботи мережі підприємства;
- усі носії інформації, які використовуються повторно, мають бути відповідним чином форматовані, щоб при втраті таких носіїв інформації унеможливити метод відновлення всіх документів, що були колись на даному носії;
- процедуру відповідного видалення всіх документів, ліцензійного програмного забезпечення потрібно проводити і з обладнанням, яке будуть виводити з експлуатації;
- будь-яке обладнання, документи, програмне забезпечення при необхідності переміщення за межі підприємства має мати за собою письмовий дозвіл керівництва;
- документи або носії інформації, що містять службову таємницю або маю іншу конфіденційну інформацію, мають зберігатися у сейфах або металевих шафах. Якщо ж вони були потрібні у роботі, то після

її завершення мають бути переміщені назад до сейфів або металевих шаф;

— всі документи, що друкуються мають бути переміщені з лотка принтера або багатофункціонального пристрою одразу після завершення друку.

Такі політики стосуються безпеки фізичних пристроїв та комп'ютеризованих робочих місць, які використовуються у мережі підприємства. Ці політики безпеки забезпечують виключення випадкової втрати інформації, як усередині підприємства, так і за його межами.

Мають бути впроваджені політики безпеки, що стосуються і прав доступу користувачів у мережі. Вони мають бути чітко сформульованими:

— рівень повноважень користувача повинен відповідати поставленим для нього завданням;

— має бути створений офіційний список всіх користувачів, які мають змогу працювати у мережі підприємства;

— має бути негайним зміна або блокування доступу до мережі працівників, що змінили посаду, звільнилися з підприємства;

— найбільші права доступу мають мати конкретні особи, що працюють з мережею і тільки вони;

— має бути впровадження паролів для користувачів, які знають тільки вони, що використовуються для автентифікації користувачів у мережі;

— необхідно уникати передачі паролів стороннім особам, у тому числі і іншому персоналу, який не має на це регламентованих повноважень;

— паролі, які використовуються за замовчуванням, повинні бути негайно змінені після першого входу;

— необхідно впровадити регламентований період, через який користувач мережі має змінити пароль до свого акаунту;

3.2 Програмно-апаратні засоби для побудови захищеності системи

Ключовими елементами при побудові захищеної мережі є: апаратні та програмні засоби.

Апаратні засоби є необхідними для забезпечення безперервної та правильної роботи мережі.

Серед переліку мережевого обладнання є MikroTik RB951Ui-2HnD, який є непоганим рішенням основного шлюзу між глобальною мережею Інтернет та мережею підприємства. Серед його властивостей є можливість тонкої конфігурації міжмережевого екрану. Також ми бачимо у цьому переліку і маршрутизатори TP-LINK841N. Вони не є кращим вибором для того, щоб використовувати на підприємстві, але вони є досить дешевим вибором для розгортання мережі.

Тому необхідно забезпечити можливості зміни кількості комп’ютеризованих робочих місць та додаткового обладнання. Тому є необхідною забезпечення можливості зміни параметрів захисту, що використовуються у мережі підприємства для внесення туди більшої кількості комп’ютеризованих робочих місць. Це створює необхідність побудови такої мережі, яка дозволить вносити зміни без повної переробки мережі. Прикладом пристроїв, які можна ввести для такої задачі, є міжмережеві екрани від компанії Huawei.

Але можна використати і вже наявний MikroTik RB951Ui-2HnD, у якому достатньо правильно налаштувати міжмережевий екран. Цього буде достатньо для повноцінної роботи підприємства.

Також потрібно брати до уваги таку річ як сумісність пристроїв у мережі. Деякі пристрої можуть бути складними у налаштуванні у парі з іншими, що може призвести до помилок у роботі, неправильної роботи всієї мережі та постійних апаратних та програмних збоїв.

Необхідно врахувати і той факт, що кожен працівник може використовувати свої власні пристрої для роботи, це можуть бути ноутбуки,

планшети, телефони. Тому робити повністю закриту мережу є недоречним у такому підприємстві, адже електронна система охорони здоров’я якраз поставила за мету, що кожен лікар може через свій девайс переглянути історію хвороби пацієнта без необхідності постійно перебувати за комп’ютеризованим робочим місцем.

Апаратні засоби захисту мережі являють собою різні пристрої з різною архітектурою та призначенням, але кожен з них містить власне програмне забезпечення, що виконує операції покладені на ці апаратні засоби захисту.

Перевагою апаратних засобів є надійність за рахунок того, що вони є вузькоспеціалізованими і виконують тільки ті функції, які покладені тільки на них.

Відповідно для забезпечення збереження інформації та для продовження роботи на всіх комп’ютеризованих робочих місцях потрібно встановити джерела безперебійного живлення. Такі джерела зможуть вберегти робочі комп’ютери від проблем пов’язаних з раптовим відключенням електроенергії та допоможуть зберегти зміни у робочих документах, що дозволить не втратити прогрес роботи та збереже цілісність файлів. Одним з досить хороших та відносно недорогих джерел безперебійного живлення є LogicPower LPM-525VA-P, який має змогу живити комп’ютеризоване робоче місце з потужністю до 525 Вт протягом 30 хвилин, яких вистачить для повного і правильного завершення роботи.

Також потрібно забезпечити працівників хорошими засобами кваліфікованих електронних підписів.

Пропонується використовувати електронний ключ «Алмаз-1К». До його особливостей відноситься легке використання та зрозуміле програмне забезпечення для роботи з ним. Конструктивно він виглядає як малогабаритний USB-пристрій, який має програмний CCID-інтерфейс. Даний засіб реалізує наступні криптографічні алгоритми та протоколи:

— шифрування за ДСТУ ГОСТ 28147:2009;

— гешування за ГОСТ 34.311-95;

— протокол розподілу ключових даних Діффі-Гелмана у групі точок еліптичної кривої (довжина ключа до 571 біту).

Його апаратна реалізація забезпечує захищеність процесу виконання криптографічних перетворень та унеможливлює доступ до особистих ключів з боку апаратно-програмного середовища. Зберігання особистих ключів та інших ключових даних здійснюється у внутрішньому постійному запам’ятовуючому пристрої електронного ключа.

На сьогоднішній день різні компанії також пропонують використання програмних рішень для забезпечення безпеки мережі.

Неможливо спрогнозувати перевірку кожного носія інформації, адже вони часто міняються (мається на увазі флешки, диски, тощо), що може призводити до можливості проникнення у систему шкідливого програмного забезпечення. Тому рекомендується на кожному комп’ютеризованому робочому місці використовувати антивірусне програмне забезпечення.

Найпопулярнішим антивірусним засобом являється антивірусна програма Avast. Але для потреб підприємства краще підходить антивірусна програма від компанії ESET. Вибір на дане антивірусне забезпечення впав через високу ефективність у протидії шкідливому програмному забезпеченню. Він надає комплексний захист, який включає у себе такі функції: перевірку файлів, захист перегляду веб-ресурсів, захист від фішингових посилань, шифрування дисків з інформацією, вбудовану систему протидії вторгнення. Також є доступні додаткові рівні захисту, наприклад, захист від витоків даних. Для всіх комп’ютеризованих робочих місць рекомендовано використовувати ESET PROTECT Enterprise.

При користуванні браузерів часто виповзають реклами з посиланнями на фішингові сайти, або сайти з сумнівною репутацією. Одним з найбільш частих порушень правил безпеки є перехід користувачем на такий сайт. Тому варто встановити браузерне розширення, яке запобігає показу такої реклами. Найчастіше для цього використовуються розширення Adblock та Adguard.

Для підприємства рекомендується використання розширення Ghostery. Його особливостями є відкритий програмний код, блокує сторонні скрипти на сайті, які займаються трекінгом даних користувача, часто та автоматично оновлюється та має можливість створення білих списків веб-сервісів, на яких можна використовувати сторонні скрипти.

Для забезпечення безпечного зберігання паролів не варто використовувати паперові носії. Вони можуть легко загубитися або бути зіпсовані. Також неможна і виключати можливість того, що такі паперові носії можуть бути викрадені. Тому рекомендується використовувати менеджери паролів, де є можливість зберігання паролів у захищеному форматі. Рекомендується використовувати програму Keeper. До його переваг можна віднести генерування надійних паролів, їх автоматичне введення.

Розділ 4. БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Ергономічні аспекти безпеки життєдіяльності

Важливою проблемою ергономіки є сумісність людини з машинами, механізмами. Тому основне завдання ергономіки – вивчення зв'язків між елементами системи ЛМС, розробка методів сумісності основного її компонента — людини з іншими середовищами та машинами, технікою.

Завдання ергономіки:

- розробка основ проектування діяльності людини-оператора з врахування специфіки експлуатації технічних систем та факторів навколишнього середовища;
- вивчення закономірностей взаємодії людини з технічними системами та навколишнім середовищем;
- формування принципів побудови системи ЛМС та алгоритмів дії у них людини-оператора;
- розробка перспективних форм праці людини і пов'язаних з нею технічних систем, факторів навколишнього середовища;
- розробка методів дослідження, проектування та експлуатації системи ЛМС, які забезпечують безпеку людини, ефективність праці.

Основним об'єктом ергономіки є система ЛМС. Проблемами взаємодії людини та машини займається також інженерна психологія, яка вивчає закономірності процесів інформаційної взаємодії людини у системі ЛМС.

У системі ЛМС завжди є 3 елементи: предмет праці, засоби праці та суб'єкт праці. Найменшою цільною одиницею, де наявні вказані елементи, є місце праці.

Місце праці – це зона, де відбувається трудова діяльність людини. Місце праці обладнане засобами відображення інформації, органами керування та допоміжним обладнанням.

Організацією місця праці називається проведення системи заходів щодо його обладнання засобами та предметами праці і їх розташуванням у визначеному порядку з метою досягнення:

— оптимізації умов трудової діяльності;

— безпеки праці;

— максимальної ефективності;

— комфортності роботи людини.

До робочого місця ставляться такі вимоги:

— достатній робочий простір, який дає змогу працюючій людині здійснювати необхідні рухи та переміщення;

— достатні фізичні, зорові та слухові зв'язки між людиною та обладнанням, а також між людьми під час виконання спільного трудового завдання;

— необхідний рівень освітлення;

— наявність необхідних засобів захисту;

— оптимальне розташування робочих місць, а також безпечні та достатні проходи для працюючих людей.

При організації робочого місця враховують основні антропометричні дані людини. Найважливішою характеристикою робочого місця є зона досягнення моторного поля.

Моторне поле – це простір робочого місця, в якому розміщені органи керування та інші технічні засоби, в якому людина здійснює рухові дії для виконання робочого завдання.

Ергономіка виробила конкретні вимоги до антропометричних показників обладнання.

Характеристика пульта:

— загальна висота: "сидячи" – 1650мм, "стоячи" – не більше ніж 1300 мм;

— висота розміщення органів керування для положення "сидячи" 530 – 104 мм, стоячи - 1000 - 1500 мм.

Характеристики крісла:

— форма сидіння-квадратна;

— форма спинки - прямокутна вгнута;

— розмір сидіння - 400х400 мм, спинки - 300х120 мм;

— кут нахилу сидіння назад - 50 - 60°;

— кут нахилу спинки - 50 - 100°;

Розміри вільного місця для ніг:

— висота - не менше 600 мм;

— ширина - не менше 500 мм;

— глибина - не менше 400 мм.

Досягнення органів керування по горизонталі – півколо радіусом 600 мм. Встановлені також відстань між органами керування, їх розміри, зусилля переміщення, величина переміщення, напрямок переміщення.

Для операторів, які працюють з екранами дисплеїв та інших індикаторів, можуть бути рекомендовані такі режими праці та відпочинку.

Тривалість безперервної праці не повинна перевищувати 4-6 год. В іншому випадку працездатність через втому зору раптово знижується. Наприклад, оператор, який стежить за екраном індикатора, найуважніше працює протягом перших 30 хв чергування. А далі, внаслідок втоми зорового аналізатора, кількість помилок зростає май же в два рази та залишається незмінною до кінця другої години. Потім спостерігається нове зростання кількості помилок через загальну втому оператора. Тому для підтримки високої ефективності праці може бути рекомендований 30-хвилинний період чергування з наступною 30-хвилинною перервою.

Отже, основним завданням ергономіки є забезпечення ефективної взаємодії людини і техніки, щоб перейти від техніки безпеки до безпечної техніки, яку ми використовуємо як у виробничій, так і побутовій сферах. Це один з основних напрямків ергономіки.

4.2 Психологічні чинники небезпеки

Виділяють комплекс чинників, що збільшують індивідуальну схильність людини до небезпеки. Це особливості темпераменту, функціональні зміни в організмі, дефекти органів відчуття, незадоволення даним видом діяльності.

Несприятливий характер діяльності (значні фізичні та розумові зусилля, незручна робоча поза, високий темп праці, нервово-емоційні перевантаження, перенапруга слухових та зорових аналізаторів, несумісність робочого місця, засобів праці, антропометричних даних людини) призводять до підвищеної фізичної та нервової втоми, яка послаблює психіку, знижує швидкість та точність орієнтації, притупляє пильність та увагу, порушує сприйняття.

Афектні стани (афект — вибух емоцій) можуть виникнути внаслідок виробничих невдач, під впливом образи. У стані афекту у людини розвивається емоційне звуження обсягу свідомості. Можуть спостерігатися різкі рухи, агресивні та руйнівні дії.

Вживання легких стимуляторів допомагає у боротьбі з сонливістю і може сприяти підвищенню працездатності на короткий період. Вживання ж активних стимуляторів на відповідальних роботах здатне викликати негативний ефект — погіршується самопочуття, зменшується швидкість реакції. Використання транквілізаторів, які діють заспокійливо та запобігають розвитку неврозів, може знижувати психічну активність, уповільнювати реакцію, викликати апатію та сонливість.

Чинники, що тимчасово підвищують індивідуальну імовірність наразитись на небезпеку.

Недосвідченість ж є одним із найважливіших факторів при безпеці роботи. Практичний досвід є безумовно важливим чинником, що підвищує безпеку праці. Він, до того ж, впливає на загальну поведінку працівника на робочому місці, що проявляється у високому темпі, ритмі, інтенсивності роботи.

Необережність — це чинник, який підвищує імовірність наразити на небезпеку в певний момент часу не лише самого працівника, а й цілий виробничий колектив.

Втома з точки зору безпеки життєдіяльності є досить значним чинником. Як правило розрізняють фізіологічну та психічну втому.

Психічна втома виявляється такими явищами:

— зниженням сприйняття подразників, в результаті чого окремі подразники людина взагалі не сприймає, а інші сприймає лише з певним запізненням;
— зниження здатності концентрувати увагу;
— сповільненням мислення, яке, окрім того, певною мірою втрачає критичність, гнучкість, широту;

Таким чином, психічні стани, що виникають внаслідок раптових емоційних впливів, характеру діяльності, психічної втоми підвищують індивідуальну імовірність наразитись на небезпеку: з одного боку людина стає тимчасово необережною через відповідний психічний стан, а з іншого – втрачає пильність і впевненість в рухах.

4.3 Висновок до розділу безпека життєдіяльності та основи охорони праці

В четвертому розділі кваліфікаційної роботи висвітлено питання БЖД та ОП із застосуванням для практичної роботи.

В першому пункті описано значення ергономічних проблем в трудовій діяльності людини. Вжито заходи пов’язані із зручністю та збереженням концентрації уваги користувача.

Другий пункт досліджує дію психологічних чинників на організм людини та методи зменшення небезпек. При виконанні кваліфікаційної роботи було оцінено дію негативних психологічних чинників.

ВИСНОВКИ

Отже, на основі проведеної роботи з побудови мережевої системи безпеки на базі КНП «Дубівська лікарня» можна зробити наступні висновки:

1. Базуючись на теоретичних засадах поняття мережевої безпеки можна дати йому наступне визначення — це заходи, які направлені на захист мережі від несанкціонованого доступу, навмисного втручання у її роботу, випадкового або цільового руйнування її компонентів. Основними джерелами загроз для роботи підприємства є: техногенні, антропогенні та стихійні джерела. До найбільш можливих типів атак, які можуть бути спрямовані на підприємство можна віднести: шкідливе програмне забезпечення, фішинг, міжсайтовий скриптінг. До основних елементів створення системи мережевої безпеки відносяться: міжмережеві екрани та антивірусне програмне забезпечення.

2. КНП «Дубівська лікарня» є закладом охорони здоров’я, який надає послуги медичної допомоги населенню. Під час проведення огляду підприємства було виявлено застарілі політики безпеки та відсутність адміністрування засобів захисту мережі та комп’ютеризованих робочих місць. Після огляду підприємства, його локальної мережі, наявного обладнання та аналізу отриманої інформації було сформовано завдання, які можна поділити на два етапи: формування політик безпеки та побудова мережевої безпеки на основі програмно-апаратних засобів.

3. Політикою безпеки прийнято вважати набір вимог, правил, обмежень, рекомендацій, які регламентовані нормативними документами на підприємстві та спрямовані на досягнення достатнього захисту мережевої системи для нормальної роботи підприємства. На даному підприємстві політика безпеки була застаріла та недостатньо охоплювала питання роботи персоналу з комп’ютеризованим робочим місцем, носіями інформації, медичними інформаційними системами. Тому мною запропоновано додання пунктів у посадових обов’язках працівників, які б регламентували їхні обов’язки на комп’ютеризованому робочому місці та чітко ставили вимоги щодо роботи у

мережі підприємства; проведення регулярного навчання персоналу; використання правил, щодо зберігання носіїв інформації.

Створено рекомендації щодо поліпшення мережевої безпеки підприємства: закупівля джерел безперебійного живлення LogicPower LPM-525VA-P, налаштування міжмережевого екрану на основі маршрутизатора MikroTik RB951Ui-2HnD, використання «Алмаз-1К» у якості засобу кваліфікованого електронного підпису; реалізація програмного захисту за допомогою антивірусного програмного забезпечення ESET PROTECT Enterprise, розширення для браузера Ghostery, менеджера паролів Keeper.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "What is Network Security? Poda myre". [Електронний ресурс] — Режим доступу: https://www.forcepoint.com/cyber-edu/network-security Дата доступу: 03.03.2022
2. Simmonds, A.; Sandilands, P.; van Ekert, L. An Ontology for Network Security Attacks. Broadway, NSW 2007, С. 317–323
3. A Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco. [Електронний ресурс] — Режим доступу: http://newsroom.cisco.com/dlls/2008/ts_010208b.html?sid=BAC-NewsWire Дата доступу 03.03.2022
4. "Understanding Denial-of-Service Attacks". [Електронний ресурс] — Режим доступу: https://www.us-cert.gov/ncas/tips/ST04-015 Дата доступу 04.03.2022
5. Prince, Matthew (25 April 2016). "Empty DDoS Threats: Meet the Armada Collective" [Електронний ресурс] — Режим доступу: https://blog.cloudflare.com/empty-ddos-threats-meet-the-armada-collective/ Дата доступу 04.03.2022
6. Lockhart, Andrew (2007). Network security hacks. O'Reilly. С. 184
7. "A Security Approach to Prevent ARP Poisoning and Defensive tools" [Електронний ресурс] — Режим доступу: https://www.researchgate.net/publication/282568321 Дата доступу 05.04.2022
8. Grossman, Jeremiah (July 30, 2006). "The origins of Cross-Site Scripting (XSS)" [Електронний ресурс] — Режим доступу: http://jeremiahgrossman.blogspot.com/2006/07/origins-of-cross-site-scripting-xss.html Дата доступу: 06.04.2022
9. "SQL Injection Attacks & Prevention: Complete Guide". [Електронний ресурс] — Режим доступу: https://www.appsecmonkey.com/blog/sql-injection-attack-and-prevention/ Дата доступу 07.04.2022

10. Szor, Peter. The Art of Computer Virus Research and Defense. Boston 2005 С. 285
11. Chapman, D. and Zwicky, E. Internet Security Firewalls. O'Reilly, Sebastopol, Calif., 1995. С. 92
12. Гатчин Ю. А., Сухостат В. В. Теория информационной безопасности и методология защиты информации. — СПб.: СПбГУ ИТМО, 2010. — 98 с.
13. Макаренко С. И. Информационная безопасность: учебное пособие для студентов вузов. — Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. — 372 с.
14. Ергономічні принципи безпеки [Електронний ресурс] – Режим доступу: https://pidru4niki.com/12281128/bzhd/ergonomichni_printsipi_bezpeki l – Дата доступу: 01.06.2022
15. Психологічні чинники небезпеки [Електронний ресурс] – Режим доступу: https://subject.com.ua/safety/bezpeka/30.html – Дата доступу: 01.06.2022
16. Про електронні довірчі послуги: Закон України від 05.10.2017 №2155-VIII.