Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Трубчанінова Данила Ігоровича*

академічної групи *125-20-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо–професійною програмою *Кібербезпека*

на тему *Системи забезпечення захисту інформації в інформаційно-комунікаційній системі ТОВ «N1 Clinic»*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	доц. Ткач М.О.			
розділів:				
спеціальний	доц. Ткач М.О.			
економічний	доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2024

ЗАТВЕРДЖЕНО:

завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«____» _____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Трубчанінову Д.І.*** **академічної групи** ***125-20-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації _____

за освітньо–професійною програмою ***Кібербезпека***

на тему ***Системи забезпечення захисту інформації в інформаційно-комунікаційній системі ТОВ «N1 Clinic»***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 23.05.2024 р. № 469-с

Розділ	Зміст	Термін виконання
Розділ 1	Визначити стан питання, провести обстеження ІКС, розробити модель порушника та аналіз кіберзагроз	20.03.2024
Розділ 2	Провести оцінку існуючих елементів політики безпеки, обгрунтувати модель безпеки, розробити елементи політики безпеки та встановити заходи реалізації	15. 05.2024
Розділ 3	Виконати техніко-економічне обгрунтування доцільності запровадження політики безпеки підприємтсва	20.06.2024

Завдання видано _____ Ткач М.О.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 01.04.2024р.

Дата подання до екзаменаційної комісії: 01.07.2024р.

Прийнято до виконання _____ Трубчанінов Д.І.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 76 с. 1 рис., 7 табл., 4 додатки, 8 джерел

Об'єкт дослідження являє собою інформаційну інфраструктуру організації, яка здійснює медичну діяльність.

Метою роботи є підвищенні рівня безпеки інформаційних систем організації завдяки вдосконаленню існуючої комплексної системи захисту медичного закладу.

Методи розробки: спостереження, порівняння, аналіз, опис.

В першому розділі було проаналізовано нормативно-правову базу, стандарти та методології у сфері кібербезпеки. Також було розглянуто структуру підприємства ТОВ «N1 Clinic» і проведено загальний аналіз об'єкта дослідження.

У спеціальній частині було проаналізовано основні методи захисту інформації, розглянуто моделі порушника та загроз, зокрема проведено оцінку потенційного зловмисника та аналіз загроз медичній інформації. Було розглянуто профіль захищеності та програмне забезпечення для захисту організації, а також проведено обстеження існуючої системи захисту інформації та вдосконалено її методом впровадження нового програмного забезпечення.

В економічному розділі визначено економічну доцільність розробки та впровадження рекомендацій для проведення ідентифікації інформаційних активів. Проведено розрахунок капітальних (фіксованих) витрат, поточних (експлуатаційних) витрат, загального збитку від атаки на ІТС та загального ефекту від впровадження рекомендацій.

Практична значимість дослідження полягає у можливості подальшого застосування отриманих результатів роботи медичними компаніями для розробки та впровадження ефективних комплексних заходів захисту інформації.

Наукова новизна роботи полягає в дослідженні питання забезпечення комплексної інформаційної безпеки в організації, яка здійснює медичну діяльність.

ІНФОРМАЦІЙНА БЕЗПЕКА, КОМПЛЕКСНА СИСТЕМА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, КРИТИЧНА ІНФОРМАЦІЙНА ІНФРАСТРУКТУРА, ПІДПРИЄМСТВО, МЕДИЧНА ОРГАНІЗАЦІЯ, МЕДИЧНА ДІЯЛЬНІСТЬ, ТОВ «N1 CLINIC».

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматичні робочі місця;

БФП – багатофункціональний пристрій;

ДТЗС – допоміжні технічні засоби і системи;

ЗЗІ – засоби захисту інформації;

ІБ – інформаційна безпека;

ІС – інформаційна система;

КІІ – критична інформаційна інфраструктура;

КСІБ – комп'ютерна система інформаційної безпеки;

ЛМ – локальна мережа;

МІС – медична інформаційна система;

НСД – несанкціонований доступ;

ПД – персональні дані;

СКУД – система контролю та управління доступом;

ТЗ – технічні засоби.

ЗМІСТ

ВСТУП

Актуальність дослідження. Вдосконалення інформаційних технологій та безперервність процесу інформатизації є характерною особливістю розвитку сучасного суспільства. Інтеграція ІТ–технологій у всі сфери життєдіяльності людей призвела до необхідності створення інформаційної інфраструктури, здатної забезпечити цілісність та безпеку конфіденційних даних. Враховуючи повсюдне впровадження передових технологій у різні галузі суспільства, виникають проблеми інформаційної безпеки (ІБ) організацій, які з кожним роком стають все більш складними та різноплановими.

Не стала винятком і сфера надання медичних послуг, оскільки у цій області дуже гостро постає питання інформаційної безпеки. В результаті інтеграції високотехнологічного обладнання та інформаційних систем (ІС) у всі галузі та організації охорони здоров'я у зв'язку з розширенням спектру медичних послуг, проблема захисту інформації набула особливої актуальності та значущості, викликавши необхідність розробки та впровадження інноваційних рішень щодо забезпечення інформаційної безпеки медичних установ.

Проблематика дослідження полягає в необхідності збільшення рівня захищеності інформації в медичних установах за рахунок забезпечення комплексної інформаційної безпеки в умовах безперервного зростання кількості загроз, способів їх реалізації, а також вимог державних законів та інших нормативних документів щодо обробки даних на суб'єктах критичної інформаційної інфраструктури.

Об'єктом дослідження є інформаційна інфраструктура організації, яка здійснює медичну діяльність.

Предметом дослідження є методи вдосконалення системи інформаційної безпеки організації, яка здійснює медичну діяльність.

Мета роботи полягає у підвищенні рівня безпеки інформаційних систем організації через удосконалення комплексної системи захисту медичного закладу. Для досягнення зазначеної мети слід вирішити такі завдання:

1. Дослідити теоретичні аспекти питання забезпечення інформаційної безпеки критичних інформаційних інфраструктур за допомогою аналізу існуючих підходів та принципів.

2. Провести аналіз методів забезпечення інформаційної безпеки критичної інформаційної інфраструктури.

3. Провести аналіз діяльності та дослідити поточний рівень інформаційної безпеки систем організації, яка здійснює медичну діяльність.

4. Провести аналіз вразливостей та загроз інформаційній безпеці об'єктів критичної інформаційної інфраструктури організації, яка здійснює медичну діяльність.

5. Розробити моделі порушника та актуальних загроз безпеці об'єктів критичної інформаційної інфраструктури організації, яка здійснює медичну діяльність.

6. Категорувати існуючі об'єкти критичної інформаційної інфраструктури організації, яка здійснює медичну діяльність.

7. Удосконалити існуючу систему захисту організації, яка здійснює медичну діяльність, за рахунок підбору оптимального комплексу заходів та використання методів інформаційної безпеки у відповідності до Закону України № 2163–VIII «Про основні засади забезпечення кібербезпеки України».

Методологічною основою дослідження є сукупність методів наукового пізнання, що використовуються для досягнення поставленої мети:

1. Вивчення та аналіз наукової літератури.

2. Системний аналіз та моделювання.

3. Методи індукції та дедукції.

Наукова новизна роботи полягає в тому, що дослідження питання забезпечення комплексної інформаційної безпеки в організації, яка здійснює медичну діяльність, реалізується в контексті безпеки критичних інформаційних інфраструктур.

Теоретична значимість полягає у можливості застосування одержаних результатів у дослідженнях та роботах, присвячених різним аспектам забезпечення безпеки об'єктів критичної інформаційної інфраструктури.

Практична значимість дослідження полягає у можливості подальшого застосування отриманих результатів роботи комерційними медичними компаніями для розробки та впровадження ефективних комплексних заходів щодо захисту інформації, спроектованих з урахуванням положень та вимог державних законів та інших нормативно–правових документів у галузі обробки даних суб'єктів інформаційних інфраструктур з високою вразливістю (критичних об'єктів медичної галузі).

1 СТАН ПИТАННЯ ТА ПОСТАНОВКА ЗАДАЧІ

1.1 Актуальність питання

Масштабність та неоднорідність інформаційних структур підприємств медицини та охорони здоров'я призводить до високої вразливості інформаційних систем медичних установ. Менш захищеними в кінцевому результаті виявляються цілі структури, а не окремо взяті вузли, що пов'язано з підвищенням складності інструментів та засобів програмно–апаратного забезпечення компаній, а також з певними вадами самих інформаційних технологій.

Чинні норми законів та інших керівних документів вимагають забезпечення комплексного інформаційного захисту медичних установ як об'єктів інформатизації, що є актуальною проблемою на сьогоднішній день. Головною метою впровадження комплексного підходу у сфері інформаційної захищеності установ охорони здоров'я виступає забезпечення доступності та високого ступеня безпеки оброблюваних даних та захисту інформації, що використовується в рамках передбачених законодавством заходів від несанкціонованого втручання третіх осіб.

Відсутність ефективного захисту, розробленого на основі комплексного підходу до забезпечення інформаційної безпеки, веде до виникнення великої кількості загроз, пов'язаних з розкраданням або знищенням персональних даних (ПД) – ключової інформації про співробітників і пацієнтів медичних організацій, а також порушує штатний порядок роботи самої установи. У деяких ситуаціях збої у функціонуванні інформаційних систем обертаються значними фінансовими втратами, а в окремих випадках можуть стати причиною заподіяння шкоди життю та здоров'ю людей. Наприклад, некоректна робота діагностичного обладнання призводить до отримання недостовірних результатів аналізів, а збої в медичній апаратурі несуть небезпеку для життя та здоров'я пацієнтів. Виходячи з цього можна зробити висновок, що проведення досліджень у сфері підвищення захисту інформаційної структури медичних організацій необхідні як для забезпечення безпеки ІС суб'єктів охорони здоров'я, так і для пацієнтів, які отримують будь–який вид медичної допомоги, включаючи консультативну.

В даний час активно ведуться дослідження питань захисту інформації та вивчення захищеності інформаційної інфраструктури медичних установ у контексті реалізації різного виду атак. Однак питанню забезпечення комплексної інформаційної безпеки організацій, що здійснюють медичну діяльність, у контексті вивчення критичних інформаційних інфраструктур (КІІ) майже не присвячено наукових робіт через недавнє затвердження в 2021 році Закону України № № 1882–IX «Про критичну інфраструктуру» [1].

Вивчити проблему підвищення надійності інформаційних систем медичної сфери, знайти способи забезпечення безпечного функціонування інформаційної структури та звести до мінімуму ризик зовнішніх і внутрішніх загроз є як ніколи актуальним завданням. З цією метою необхідно впровадити механізм підвищення захищеності ІС шляхом розробки та реалізації заходів, спрямованих на забезпечення комплексного захисту інформації установ.

Відштовхуючись від актуальності та наявної проблеми, можна дійти висновку про необхідність проведення дослідницьких робіт у напрямку забезпечення комплексної інформаційної безпеки в організаціях, які здійснюють медичну діяльність.

1.2 Аналіз об’єкта дослідження

1.2.1 Структура підприємства та його склад

У рамках цієї роботи ключовий інтерес представляє діяльність досліджуваної організації ТОВ «N1 Clinic», що надає широкий спектр ортопедичних та травмалогічних медичних послуг у місті Дніпрі з 2023 року.

Робочі місця співробітників клініки розміщено на території організації за адресою м. Дніпро, вул. Сімферопольська, буд. 2М. Будівля, в якій розташована клініка, є 3–поверховою будовою, на першому поверсі якої з окремим входом розташована рецепція клініки, кабінети медичних спеціалістів, а також процедурні та масажні кабінети, спортивний зал та кімнати персоналу. На другому поверсі також знаходиться рецепція, палати для пацієнтів, кабінети лікарів та столова.

ТОВ «N1 Clinic» дозволяє пацієнтам записатися на прийом до низки лікарів та медичних спеціалістів, зокрема хірургічного напрямку:

1. Ортопед–травматолог.
2. Стоматолог.
3. Ортодонт.

2. Пластичний хірург.

3. Щелепно–лицьовий хірург.

Виходячи з наданої інформації про спектр медичної діяльності ТОВ «N1 Clinic», насамперед сформуємо узагальнений перелік процесів та послуг даної клініки:

1. Надання медичних послуг та медичної допомоги.
   - Амбулаторна медична консультативна та лікувальна допомога.
   - Відновне лікування.
   - Діагностична медична допомога.
   - Високотехнологічна медична допомога.
2. Проведення досліджень, клінічних випробувань, оглядів.
3. Діяльність, пов'язана з використанням джерел іонізуючого випромінювання (ультразвукове дослідження).
4. Роздрібна торгівля товарами особистої гігієни та загального споживання.
5. Бухгалтерський облік.
6. Обслуговування ІТ–інфраструктури.
7. Робота зі зверненнями клієнтів.

На рисунках 1 і 2 Додатка Б представлені схеми приміщень з урахуванням, у яких розміщуються співробітники організації ТОВ «N1 Clinic».

На даний момент у всіх приміщеннях медичної організації встановлено засоби пожежної та охоронної сигналізацій. На вікнах приміщень першого поверху сталеві грати відсутні. У робочий час в приміщення службової частини організації пропускний режим за допомогою системи контролю та управління доступом (СКУД) не забезпечується. У неробочий час приміщення закриваються на замок та ставляться на сигналізацію, яка виведена на пульт охорони. Усі автоматичні робочі місця (АРМ) користувачів об'єднані у локальну мережу (ЛМ) з виходом до Інтернету. Топологія локальної мережі організації ТОВ «N1 Clinic» представлена

на рисунках 1 та 2 у Додатку Г. Ця топологія відображає основні структурні елементи мережевої інфраструктури клініки.

1.2.2 Інформація підприємства та інформаційні потоки

У рамках забезпечення комплексної інформаційної безпеки в організації першим кроком слід визначити, які дані використовуються в інформаційних системах клініки.

Інформаційна система компанії оперує персональними даними та відомостями, що належать до лікарської таємниці.

Якщо відомості, що стосуються лікарської таємниці відносно просто виявити, то питання виявлення та організації захисту особистих даних значно складніше.

Закон України № 2297–VI "Про захист персональних даних" від 1 червня 2010 р. визначає, що персональні дані – це будь–які відомості, які так чи інакше, стосуються будь–якої фізичної особи. Іншими словами, персональні дані є будь–якою інформацією, що відноситься до певної або визначається на підставі такої інформації фізичній особі (суб'єкту персональних даних). Дані про пацієнтів – це особисті відомості, що містять дані про події та обставини життя пацієнта, що допускають розпізнання його особи. До таких відомостей відносять біометрію, що представляє параметри суб'єкта, а саме групу крові, ріст, колір очей, вагу, аналіз дезоксирибонуклеїнової кислоти (ДНК) тощо. [2]

Сюди відносять і дані, які можна отримати з фото– або відеоматеріалів з людиною.

Особисті дані працівників клініки застосовують для оформлення договірних відносин із наймачем у межах дії Трудового законодавства.

Обробка персональних даних пацієнтів та співробітників медичної організації ТОВ «N1 Clinic» здійснюється з використанням інформаційних систем, в яких операції з обробки персональних даних можна визначити наступним переліком: збір, запис, систематизація, накопичення, зберігання, уточнення (оновлення, зміна), вилучення, використання, передача (поширення, надання, доступ), блокування, знеособлення, видалення, знищення персональних даних.

Режим обробки персональних даних в інформаційних системах клініки розрахований на відносно невелику кількість користувачів. Усі компоненти інформаційних систем обробки персональних даних ТОВ «N1 Clinic» розташовані одному об'єкті обчислювальної техніки всередині контрольованої зони (КЗ) (рисунок 1 і 2 Додатка Б). У роботі інформаційних систем обробки персональних даних клініки використовуються такі технічні засоби:

1. Сервер, який обробляє персональні дані.

2. Автоматизовані робочі місця (робочі станції користувачів).

3. Мережеве устаткування, що у передачі персональних даних всередині інформаційної системи персональних даних.

4. Лінії допоміжних технічних засобів і систем (ДТЗС).

5. Принтери та багатофункціональні пристрої (БФП).

6. Знімні носії інформації.

1.3 Висновки

Таким чином, у цьому розділі було проведено дослідження діяльності та організаційної структури медичної організації ТОВ «N1 Clinic», що включає вивчення загальної інформації про організацію, аналіз технічної та програмної архітектури, а також існуючих інформаційних систем та даних, що обробляються у досліджуваній клініці. Первинний аналіз показав, що поточний рівень безпеки даних можна оцінити як незадовільний. Справа в тому, що в компанії немає мінімально необхідних інженерних засобів захисту (наприклад, решіток на вікнах), чіткої документації щодо порядку отримання доступу до персональних даних та лікарської таємниці, а також прописаного ступеня відповідальності за розголошення такої інформації. Разом з тим, у приміщеннях медичної організації ТОВ «N1 Clinic» немає системи контролю управління доступу, що також є неприпустимим у рамках забезпечення доступу різних категорій персоналу (адміністративного та управлінського, а також виконавського рівнів). У подальшій роботі слід точніше визначити поточний рівень інформаційної безпеки відповідно до Постанови №518 "Про затвердження Загальних вимог до кіберзахисту об’єктів критичної інфраструктури" за допомогою проведення виявлення та категорування

об'єктів критичної інформаційної інфраструктури, виявлення критичних процесів, проведення аналізу актуальних загроз та інших заходів, що дозволяють визначити конкретні вимоги до комплексу заходів та методів, які забезпечують комплексну систему інформаційну безпеки медичної організації ТОВ «N1 Clinic». [3]

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз основних методів захисту інформації

Способи та інструменти забезпечення інформаційної безпеки критичної інформаційної інфраструктури є набором програмно–апаратних засобів, етичних та юридичних норм, спрямованих на протидію зловмисникам та мінімізації потенційної шкоди власників інформаційного комплексу та користувачів інформації.

Класифікацію методів забезпечення інформаційної безпеки критичної інформаційної інфраструктури в контексті організації підходу до забезпечення безпеки описано нижче.

В рамках даної роботи ключовий інтерес становлять організаційні, програмно–апаратні (технічні) та фізичні методи забезпечення інформаційної безпеки критичної інформаційної інфраструктури.

До організаційних методів забезпечення інформаційної безпеки критичної інформаційної інфраструктури належать:

- Організація роботи з персоналом.
- Організація внутрішнього та прохідного режиму та охорони.
- Організація роботи з носіями інформації.
- Комплексне планування заходів щодо захисту інформації.
- Організація аналітичної роботи та контролю.

Правові методи забезпечення інформаційної безпеки критичної інформаційної інфраструктури включають:

- Патентний захист.
- Закон про виробничі секрети.
- Ліцензійні угоди та контракти.
- Закон про авторське право.

Організаційно–правове забезпечення є багатоаспектним поняттям, що включає закони, рішення, нормативи та правила. Серед організаційно–правових методів забезпечення інформаційної безпеки критичної інформаційної інфраструктури є:

- Визначення підрозділів та осіб, відповідальних за організацію забезпечення інформаційної безпеки критичної інформаційної інфраструктури.
- Розробка та впровадження нормативно–правових, керівних та методичних матеріалів (документів) щодо забезпечення інформаційної безпеки критичної інформаційної інфраструктури.
- Встановлення заходів відповідальності за порушення правил захисту інформації.
- Урегулювання порядку вирішення спірних та конфліктних ситуацій з питань забезпечення інформаційної безпеки критичної інформаційної інфраструктури.

Під техніко–математичною стороною організаційних та правових методів організації інформаційної безпеки мається на увазі комплекс технічних засобів, математичних способів, прототипів та програмних додатків, за сприяння яких дотримуються всі положення та правила, необхідні для правового поділу прав та відповідальності щодо порядку поводження з інформацією, що охороняється.

Ключовими з цих положень вважають наступні:

- Закріплення на документі індивідуальних ідентифікаторів (підписів) осіб, які виготовили документ та (або) відповідальні за нього.
- Закріплення (за потреби) на документі індивідуальних ідентифікаторів (підписів) осіб, які ознайомилися із змістом документу.
- Можливість непомітної (без залишення слідів) зміни змісту інформації особами з дозволом на доступ до неї.
- Закріплення факту будь–якого (як неузгодженого, і дозволеного) копіювання захищуваної інформації.

Під правовими аспектами організаційно–законодавчих методів забезпечення інформаційної безпеки критичної інформаційної інфраструктури об'єктів розуміється сукупність законів та інших законів, з яких досягаються такі цілі:

1. Неухильний обов'язок дотримання всіма особами всіх правил захисту інформації.

2. За недотримання норм захисту узаконюються міри відповідальності.
3. Техніко–математичні вирішення питань організаційно–законодавчого забезпечення захисту інформації також узаконюються (набувають юридичної сили)
4. Процесуальні процедури вирішення ситуацій, що складаються у процесі діяльності системи захисту, також узаконюються.

Способи організації інформаційної безпеки на фізичному рівні — це набір певних підходів із застосуванням різних пристроїв різних типів пристосувань, і навіть приладів, які створюють перешкоди у ході роботи зловмисників.

До фізичних засобів належать: механічні, електричні, радіотехнічні прилади обмеження чи заборони несанкціонованого доступу (НСД), переміщення грошей, матеріалів та інших можливих видів протиправних процесів.

Для розмежування доступу та фізичного захисту організації прийнято використовувати наступні методи:

1. Спостереження та охорона території, на якій розміщено об'єкти критичної інформаційної інфраструктури.
2. Контроль та охорона будівель та внутрішніх приміщень.
3. Охорона інформації, обладнання.
4. Контрольований доступ до будівель та внутрішніх приміщень.

Фізичні засоби забезпечення інформаційної безпеки критичної інформаційної інфраструктури можна поділити на три категорії:

1. Засоби запобігання.
2. Засоби виявлення.
3. Системи ліквідації небезпек.

Загалом усі засоби фізичного захисту об'єктів критичної інформаційної інфраструктури можна поділити на такі групи:

1. Охоронні та охоронно–пожежні системи
2. Охоронне телебачення.
3. Охоронне освітлення
4. Засоби фізичного захисту.

До засобів фізичного захисту належать:

1. Огородження та фізична ізоляція.
2. Замикаючі пристрої.
3. Системи розмежування доступу.

До систем розмежування доступу належать:

1. Системи, що використовують різноманітні карти та картки, на яких міститься кодована або відкрита інформація про власника.
2. Системи розпізнавання за відбитками пальців
3. Системи розпізнавання за голосом
4. Системи розпізнавання за почерком.
5. Система розпізнавання з геометрії рук.

Відповідно до вимог українського законодавства, для об'єктів критичної інформаційної інфраструктури впроваджено організаційні заходи та технічні засоби забезпечення безпеки в залежності від їх значимості та ідентифікованих загроз безпеці інформації.

Надалі слід визначити актуальні загрози інформаційної безпеки для об'єктів критичної інфраструктури медичної організації ТОВ «N1 Clinic». Метою аналізу загроз безпеки інформації є визначення можливих способів реалізації (виникнення) загроз безпеки інформації та наслідків їх реалізації (виникнення) з урахуванням складу користувачів та їх повноважень, програмних та програмно–апаратних засобів, взаємозв'язків компонентів значущого об'єкта, взаємодії з іншими об'єктами критичної інформаційної інфраструктури, інформаційними системами, автоматизованими системами управління, інформаційно–телекомунікаційними мережами, і навіть особливостей функціонування значного об'єкта.

Аналіз загроз безпеки інформації повинен включати:

1. Виявлення джерел загроз безпеки інформації та оцінку можливостей (потенціалу) зовнішніх та внутрішніх порушників;

2. Аналіз можливих вразливостей значного об'єкта та його програмних, програмно–апаратних засобів;

3. Визначення можливих способів (сценаріїв) реалізації (виникнення) загроз безпеці інформації;

4. Оцінку можливих наслідків від реалізації (виникнення) загроз безпеці інформації.

2.2 Моделі порушника та модель загроз

2.2.1 Оцінка потенційного зловмисника

Реалізація загрози безпеці можлива внаслідок утворення каналу реалізації між джерелом загрози та носієм даних. З погляду наявності законного доступу до об'єктів критичної інфраструктури медичної організації ТОВ «N1 Clinic» всі порушники поділяються на дві групи:

1. Зовнішні порушники.
2. Внутрішні порушники.

До зовнішніх зловмисників належать фізичні особи, які не мають законного доступу до ресурсів об'єктів критичної інфраструктури медичного закладу, та реалізують загрози за допомогою несанкціонованого доступу. Для організації такими можуть бути:

1. Кримінальні структури.
2. Зловмисники чи зовнішні суб'єкти.
3. Конкуруючі організації.
4. Несумлінні розробники та постачальники.
5. Колишні співробітники.

До внутрішніх зловмисників належать фізичні особи, які мають доступ до об'єктів критичної інфраструктури медичної організації ТОВ «N1 Clinic», у тому числі самі працівники медичних установ. До внутрішніх зловмисників в організації можуть належати:

1. Адміністратори об'єктів критичної інфраструктури медичної організації та адміністратори безпеки.
2. Користувачі об'єктів критичної інфраструктури медичної організації.

3. Співробітники, які мають санкціонований доступ у службових цілях до приміщень, у яких розміщено ресурси об'єктів критичної інфраструктури медичної організації, але не мають права доступу до ресурсів.
4. Обслуговуючий персонал.

У зв'язку з тим, що вхід до офісного приміщення закривають із застосуванням сучасних надійних дверей, а всі приміщення оснащені сигналізацією, виведеною на диспетчерський пульт охоронної організації, це не становить значного інтересу в рамках цієї роботи.

Як метод удосконалення комплексної системи забезпечення інформаційної безпеки щодо таких порушників необхідно реалізувати встановлення залізних грат на вікна приміщень.

Враховуючи специфіку діяльності медичної організації, важливо звернути увагу на внутрішніх зловмисників.

Наприклад, інсайдери можуть передати персональні дані пацієнтів зловмисникам.

Іншими словами, внутрішніми зловмисниками інформаційної безпеки медичних установ є співробітники самої організації, які є легальними учасниками процесів медичної організації, а також персонал, який обслуговує апаратно–програмні комплекси або допущений до них відповідно до своїх службових обов'язків.

Імовірність заподіяння шкоди є вищою, відповідно до кваліфікації, яку має співробітник, що на вищому рівні ієрархії інформаційної інфраструктури організації він знаходиться і чим до більшого обсягу електронних інформаційних ресурсів має доступ тим більшу небезпеку може становити для організації.

Головна мета, яку ставить внутрішній зловмисник, полягає у отриманні контролю над електронними інформаційними ресурсами медичної організації, включаючи засоби їх обробки, зберігання та надання, на найвищому доступному йому рівні.

Можна виділити такі ознаки класифікації внутрішнього зловмисника інформаційних систем медичних установ:

1. Досвід та знання у професійній сфері.
2. Доступні ресурси, необхідні виконання службових завдань.
3. Сфера функціональної діяльності.
4. Наявність мотивації дій.

Зазвичай порушники класифікуються за рівнем їх можливостей (тобто за тим параметром, який їм надає наявна у ТОВ «N1 Clinic» інфраструктура).

Виділяється чотири рівні таких можливостей. Сам поділ і категоризація зловмисників мають ієрархічний характер. Інакше кажучи, попередні рівні містять деяку частину наступних.

У ТОВ «N1 Clinic» важлива роль має відводитися адміністраторам інформаційної системи та її інструментів, а також фахівцям з ІБ.

Вони мають найвищий пріоритет доступу, розуміють вразливості, знають необхідні заходи захисту: як превентивні, так і імпульсні.

Ці співробітники у своїй роботі використовують не тільки звичайне та загальнодоступне обладнання, а й, за потреби, спеціалізоване.

Важливо розуміти, що від цієї категорії персоналу залежить інформаційна безпека всієї клініки.

Потрібні особливі процедури, коли йде добір, відбір та прийом спеціалістів на посади цього типу.

Не варто забувати і про те, що періодично повинен контролюватись поточний зріз діяльності інформаційних адміністраторів.

Логічний висновок – максимально ймовірні порушники потенційно відносяться до перших трьох рівнів класифікації порушників безпеки.

Вони мають доступ (хоч і різного рівня допуску) до закритих приміщень та програмно–технічних засобів ТОВ «N1 Clinic».

Варто відстежувати соціальне становище та матеріальну забезпеченість цієї групи персоналу, оскільки вони можуть спричинити порушення законодавства країни для отримання певної особистої винагороди.

Категорії порушників, специфікації моделі порушника та модель внутрішнього порушника наведені у табл. 2.1, 2.2 – 2.6 та 2.7 відповідно [4].

Таблиця 2.1 – Категорії порушників, визначених у моделі

Позначення	**Визначення категорії**	**Рівень загроз**
	Внутрішні по відношенню до ІТС	
ПВ1	Технічний персонал, який обслуговує будови та приміщення (електрики, прибиральники тощо), в яких розташовані компоненти ІТС	1
ПВ2	Персонал, який обслуговує технічні засоби ІТС (інженери, техніки)	2
ПВ3	Користувачі (оператори) ІТС	2
ПВ4	Адміністратори ІТС, співробітники служби захисту інформації	3
ПВ5	Співробітники служби безпеки установи та керівники різних рівнів	4
	Зовнішні по відношенню до ІТС	
ПЗ1	Відвідувачі (запрошені з будь–якого приводу)	1
ПЗ2	Представники організацій, що взаємодіють з питань технічного забезпечення (енерго–, тепло–, водопостачання тощо)	2
ПЗ3	Хакери	3
ПЗ4	Агенти конкурентів або закордонних спецслужб «під прикриттям»	4

Таблиця 2.2 – Специфікація моделі порушника за мотивами здійснення порушень

Позначення	**Визначення категорії**	**Рівень загроз**
М1	Безвідповідальність	1
М2	Самоствердження	2
М3	Корисливий інтерес	3
М4	Професійний обов’язок (ПЗ4)	4

Таблиця 2.3 – Специфікація моделі порушника за рівнем кваліфікації та обізнанності щодо ІТС

Позначення	Визначення категорії	Рівень загроз
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами ІТС	1
К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	2
К3	Володіє високим рівнем знань у галузі програмування та обчислювальної техніки, проектування та експлуатації ІТС	3
К4	Знає структуру, функції й механізми дії засобів захисту інформації в ІТС, їх недоліки та можливості	4

Таблиця 2.4 – Специфікація моделі порушника за показником можливостей використання засобів та методів подолання систем захисту

Позначення	Визначення категорії	Рівень загроз
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документи на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікації інформації та компонентів ІТС	2
З3	Використовує лише штатні засоби та недоліки систему захисту для її подолання (несанкціоновані дії з використанням дозволених засобів), а також компактні машинні носії інформації, які може бути приховано та пронесено крізь охорону	3
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки інформації	4

Таблиця 2.5 – Специфікація моделі порушника за часом дії

Позначення	**Визначення категорії**	**Рівень загроз**
Ч1	Під час повної бездіяльності ІТС з метою відновлення та ремонту	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування та модернізації	2
Ч3	Під час функціонування ІТС (або компонентів системи)	3
Ч4	Як у процесі функціонування ІТС, так і під час призупинки компонентів системи	4

Таблиця 2.6 – Специфікація моделі порушника за місцем дії

Позначення	**Визначення категорії**	**Рівень загроз**
Д1	Усередині приміщень, але без доступу до технічних засобів ІТС	1
Д2	З робочих місць користувачів (операторів) ІТС	2
Д3	З доступом у зону зберігання баз даних, архівів тощо	3
Д4	З доступом у зону керування засобами забезпечення безпеки ІТС	4

Таблиця 2.7 – Модель внутрішнього порушника політики безпеки інформації

Категорія поршушника «ПВ»	Мотив порушення	Рівень обізнаності щодо ІТС	Можливості щодо подолання захисту	Можливості за часом дії	Можливості за місцем дії	**Сума загроз**
Служба безпеки	М1	К1	З1	Ч4	Д3	**14**
Адміністратор ІТС	М1	К4	З1	Ч4	Д4	**17**
Користувач	М1	К2	З1	Ч3	Д2	**11**
Технік ІТС	М1	К2	З1	Ч4	Д3	**12**
Електрик	М1	К1	З1	Ч1	Д1	**8**
Прибиральник	М1	К1	З1	Ч4	Д1	**9**

2.2.2 Аналіз вразливостей та загроз медичній інформаційній системі

Модель загроз безпеки інформації може розроблятися для кількох значущих об'єктів, що мають однакові цілі створення та архітектуру, а також типові загрози безпеці інформації. У зв'язку з тим, що всі виявлені об'єкти критичної інформаційної інфраструктури входять до складу єдиної локальної мережі, представленої в Додатку В, визначимо найактуальніші загрози для всіх виявлених об'єктів критичної інформаційної інфраструктури медичної організації ТОВ «N1 Clinic», результати будуть розміщенні у таблиці 1 Додатка Г. За результатами аналізу в подальшій роботі буде проведено оцінку можливих наслідків від реалізації загроз безпеці інформації та категорії об'єктів критичної інформаційної інфраструктури з метою подальшої розробки організаційно–технічних заходів, спрямовані на блокування та нейтралізацію виявлених загроз безпеці інформації [7].

На сьогоднішній день можна виділити значну кількість різних видів загроз безпеці ТОВ «N1 Clinic». Аналіз наукових джерел показує, що виникнення загроз має або природний, або штучний характер.

До природних загроз безпеці інформаційної системи відносять такі фактори, що спричинені об'єктивними обставинами. Вони не залежать від людини і з'являються по збігу деяких несприятливих обставин. Штучні ж, навпаки, заздалегідь продумані певним колом осіб або виявляються внаслідок ненавмисної недбалості людини.

Говорячи про цілі зловмисників, які здатні завдати шкоди інформаційній безпеці інфраструктури ТОВ «N1 Clinic», можна виділити такі:

1. Отримання для передачі або розголошення даних про пацієнтів, які підпадають під категорію лікарської таємниці.
2. Доступ до закритих даних усередині інформаційної системи клініки або у відповідних приміщеннях з метою подальшого порушення.
3. Спроби збити нормальний ритм роботи інформаційної системи: її цілісність, достовірність інформації, що зберігається.

На підставі проведеного дослідження системи інформаційної безпеки ТОВ «N1 Clinic», а також виявлених факторів можливих порушень можна зробити висновок, що основні проблеми випливають із розподіленості (нецентралізованості) та відкритості частини компонентів та об'єктів системи. Далі описано найбільш актуальні та вразливі місця передбачуваних атак на підсистеми інформаційної інфраструктури медичного закладу.

Відповідно, в рамках дослідження зроблено припущення, що основною та найбільш затребуваною проблемою є аналіз вразливостей інформаційного характеру. Сюди насамперед входять технічні загрози. Вони виявлені всіх рівнях системи та інфраструктури досліджуваного об'єкта – ТОВ «N1 Clinic».

Незважаючи на захищеність інформації, що передається через IP–протокол, назвати його застосування в медичній організації виправданим не можна. Такі відомості легко перехопити, а також неможливо гарантувати однозначну їх доставку. Система (у разі відповідного наміру зловмисників високого рівня) схильна до атак вірусів, спаму, навмисного навантаження на мережу (DDoS) з метою виведення її з ладу на певний проміжок часу. Слід зупинитися докладніше на ймовірно можливих загрозах:

1. Аналіз мережевого трафіку між модулями інформаційної системи клініки.

Цей захід проводиться з метою отримання відомостей, що передаються каналами зв'язку, вивчення архітектури системи безпеки ТОВ «N1 Clinic», виявлення її топології. Головне завдання – отримання тієї інформації, що циркулює в реальному часі.

2. Зміна даних, що передаються каналами зв'язку всередині ІС клініки.

Порушник, який отримав доступ до механізмів передачі інформації, цілком здатний не просто скористатися ними, а й цілеспрямовано змінити. Таким чином він внесе елементи дезінформації та зможе здійснити певний вплив на дані.

3. Перехоплення сеансу взаємодії.

Загроза передбачає заміну сесії, поточного сеансу. Спочатку здійснюється аутентифікація користувача, підтвердження його повноважень, рівня доступу до елементів інформаційної інфраструктури ТОВ «N1 Clinic». Зловмисник у відповідь

перемикає потік даних на новий канал, а поточний, легітимний сеанс розривається. За фактом замість реального уповноваженого користувача в систему впроваджується порушник.

Також, якщо зломщик використовував проксі–сервера або пірингові мережі, то визначити його IP–адресу буде неможливо (оскільки вона виявиться підробленою). Отже, виходить, що усередині організації не застосовується обмеження доступу виходячи з лімітованого спектра адрес. Такий стан справ ускладнюється ще й тим, що порушник здатний запустити в систему черв'яка, шкідливу програму, а то й зовсім зробити спам–розсилку користувачам (ті, відреагувавши на прохання адміністратора, можуть ще більше погіршити ситуацію – відправити зловмиснику додаткові дані).

4. Парольні атаки (брутфорс).

Отримання паролів ключових користувачів інформаційної системи у ТОВ «N1 Clinic» може суттєво розширити можливості зломщиків. Механізми такої дії відомі: автоматичний перебір, підміна адрес, сніффінг (підслуховування) тощо.

5. Атака через мережеві порти.

Оскільки у роботі системи використовується широкий набір програмних засобів, вони пов'язані між собою певними портами. Їх багато, вони ніяк не екрануються і фактично неможливо заздалегідь передбачити номер порту, з якого буде здійснена атака. Виходить, що їх повністю виключити неможливо. Причина в тому, що в ТОВ «N1 Clinic» застосовується велика кількість компонентів, а вони, у свою чергу, мають вразливості.

6. Фрод (шахрайство у сфері інформаційних технологій).

Основна мета застосування операції фроду – отримання закритої інформації (комерційної таємниці, персональних відомостей) для подальшого перепродажу зацікавленим особам (конкурентам, органам контролю тощо). Інструментом для здійснення фроду здатний стати будь–який циркуляр інформації на фізичному рівні (радіоканал, бездротова мережа, оптоволоконне з'єднання). Щоб запобігти такому зловмисницькому діянню важливо постійно стежити за потоками інформації всередині системи. У випадку ТОВ «N1 Clinic» це неможливе на поточний момент

(обладнання постачальників послуг зв'язку несумісне). Проблему необхідно осмислити і терміново змінити ситуацію.

7. DOS – атаки.

Ще один інструмент в руках шахраїв. Вони цілком спроможні порушити роботу інформаційної інфраструктури ТОВ «N1 Clinic».

Атаки подібного роду загрожують негативними проявами на рівні всієї системи інформації медичного закладу. Вони можуть продукуватись як зниженням якості обслуговування основної категорії користувачів, так і втратою доступу всіма учасниками мережі. Важливо відзначити і те, що успішно проведена атака на один з об'єктів інфраструктури може негативно позначитися на роботі інших модулів. Для медичного закладу таке неприпустимо.

Більше того, успішна реалізація DDoS заходу щодо лише одного компонента системи ТОВ «N1 Clinic» здатна обернутись зупиненням всієї мережі чи, в кращому випадку, окремої ділянки. Інфраструктура не зможе виконувати свої функції певний час.

8. Атаки типу «IP–спуфінг».

Оскільки для обміну даними між пристроями інформаційної інфраструктури медичної організації ТОВ «N1 Clinic» необхідна мережа, то відомості передаються IP–адресами.

Для порушника – це ще один із способів здійснити свої наміри. «IP–spoofing» – наукове визначення зазначеної дії.

Мета зломщика – видати себе за «свого», незалежно від того, де він зараз перебуває фізично (всередині клініки чи за її межами).

Для цього він здійснює заміну IP–адрес.

Так як для здійснення спуфінгу необхідний певний діапазон адрес, він спочатку повинен його дізнатися.

До списку можуть входити як внутрішні IP–адреси, так і зовнішні, які мають право авторизації у рамках системи ТОВ «N1 Clinic».

Порушник може мати інструменти, які будують потік IP–пакетів таким чином, ніби вони виходять від легітимних компонентів або користувачів системи.

Фактично, він обриває зв'язок одного з учасників системи (той може і не помітити подібної обставини з низки причин), займає його місце та отримує можливість користуватися даними організації або їх змінювати.

Внаслідок реалізації «IP–спуфінгу» зловмисник завдає певних (за деяких обставин значних) збитків клініці. Основні способи представлені далі:

1. Доступ до інформації, що охороняється (комерційна, лікарська таємниці, персональні відомості), яка передається всередині системи між компонентами інфраструктури.
2. Заміна інформації на більш вигідну для порушника або внесення коректив для дезінформації та зниження ефективності системи.
3. Впровадження чужорідних елементів та об'єктів в інформаційну інфраструктуру медичної організації ТОВ «N1 Clinic».

Отже, можна дійти певного висновку. Об'єкти інформаційної інфраструктури ТОВ «N1 Clinic» знаходяться під загрозою впливу певного кола зовнішніх і внутрішніх чинників.

Розробка запобіжних заходів інформаційної безпеки – важливе завдання установи.

2.3 Профіль захищеності

Сьогодні безпека вже не обмежується встановленням окремого пристрою і має бути забезпечена на рівні кожного пакету, сервісу або компонента об'єкта критичної інформаційної інфраструктури. Засоби захисту інформації (ЗЗІ) повинні бути розподілені по всьому робочому середовищу об'єкта критичної інформаційної інфраструктури та підтримувати такі умови:

1. Доступність та надійність сервісів.

2. Безперервність ділової активності.

3. Заданий рівень обслуговування та ефективності роботи системи [4].

Створення надійно захищених об'єктів критичної інформаційної інфраструктури є всеосяжною дилемою, що включає в себе:

1. Забезпечення конфіденційності інформації, яка зберігається, обробляється та передається каналами зв'язку.

2. Забезпечення контролю доступу до інформаційних ресурсів об'єктів критичної інформаційної інфраструктури відповідно до повноважень користувачів, а також цілісність та ідентифікація інформації, що зберігається та передається.

3. Запобігання витоку інформації, що циркулює в об'єктах критичної інформаційної інфраструктури.

4. Виключення несанкціонованого доступу до інформації при її зберіганні та обробці в об'єктах критичної інформаційної інфраструктури, а також запобігання програмним впливам або їх наслідкам, що викликають спотворення інформації або її знищення.

5. Реалізацію необхідних організаційно–технічних заходів щодо забезпечення інформаційної безпеки об'єктів критичної інформаційної інфраструктури.

З метою організації безпеки розробляються та впроваджуються комплексні системи забезпечення безпеки, які є сукупністю організаційних та інженерно–технічних заходів, спрямованих на забезпечення захисту інформації від розголошення, витоку та несанкціонованого доступу. Основні вимоги до комплексної системи захисту критичної інформаційної інфраструктури можна перерахувати в наступному переліку:

1. Розробка на основі положень та вимог існуючих законів, стандартів та нормативно–методичних документів щодо забезпечення інформаційної безпеки.

2. Використання комплексу програмно–технічних засобів та організаційних заходів для захисту системи.

3. Надійність, продуктивність, конфігурованість.

4. Економічна доцільність.

5. Виконання всіх етапів життєвого циклу обробки інформації.

6. Можливість удосконалення.

7. Забезпечення розмежування доступу до конфіденційної інформації з відволіканням порушника на неправдиву інформацію (забезпечення не тільки пасивного, а й активного захисту).

8. Взаємодія з незахищеними системами за встановленими для цього правилами розмежування доступу.

9. Забезпечення проведення обліку та розслідування випадків порушення безпеки інформації.

10. Можливість оцінки ефективності її застосування.

Безпека стає критично важливою характеристикою роботи суб'єктів критичної інформаційної інфраструктури та відіграє найважливішу роль. Забезпечення комплексної безпеки має бути реалізовано насамперед шляхом переходу від традиційного реактивного підходу до поетапного проактивного підходу, зменшуючи кількість існуючих вразливостей, покращуючи показники часу реакції та ефективність придушення атак.

Таким чином, принципи забезпечення комплексної безпеки критичної інформаційної інфраструктури можна визначити у наступному переліку:

1. Законність.

2. Пріоритет на користь запобігання комп'ютерним атакам.

3. Системність (розробка алгоритмів, враховуючи також зовнішні чинники).

4. Комплексність.

5. Безперервність захисту.

6. Розумна достатність (економічна ефективність).

7. Гнучкість управління та застосування.

8. Відкритість алгоритмів та механізмів захисту.

9. Простота застосування захисних заходів та засобів.

10. Превентивність.

11. Участь уповноважених органів виконавчої влади на належному рівні [7].

У межах наведеного дослідження щодо організації системної інформаційної безпеки проблемних інформаційних структур треба брати до уваги основні правила усунення загроз інформаційній безпеці:

1. Запобігання. Здійснення захисних заходів щодо попередження відомих небезпек. Ліквідація небезпек передбачає використання ряду інструментів, що включають як типові, так і покращені варіанти програмного забезпечення, спеціалізованих міжмережевих екранів або інших аналогів для розмежованого доступу до системи.

2. Моніторинг. Щоб визначати реальні чи потенційні ризиковані поведінкові дії користувачів, необхідно здійснювати процедуру моніторингу. Вона дозволяє, особливо у вразливих областях, передбачати небезпеку.

3. Важливо поділяти причини виникнення загроз та конфліктів в інформаційній системі. Вони можуть мати або цілеспрямований характер (навмисні дії зловмисників), або бути результатом помилок. У першому випадку слід виявляти джерело загрози та блокувати його, у другому – мінімізувати випадкові зміни даних системи через неуважність, непроінформованість чи недбалість користувачів. Необхідно фіксувати та відстежувати атаки, аналізувати логи журналів та мережевих екранів (брандмауерів).

4. Заходи у відповідь. Якщо виявлено спробу несанкціонованого втручання у інформаційну систему, потрібне оперативне (зазвичай – в режимі реального часу) втручання. Всі кроки повинні бути опрацьовані заздалегідь, щоб не гаяти час, який потім здатний вилитися в суттєві збитки.

2.4 Критерії конфіденційності

Функціональні критерії захищеності інформації можна розділити на чотири окремі групи, кожна з яких включає детальний опис вимог до послуг, що забезпечують захист від загроз одного із чотирьох типів.

1. Конфіденційність. Загрози, що відносяться до несанкціонованого ознайомлення з інформацією, становлять загрози конфіденційності.

2. Цілісність Загрози, що відносяться до несанкціонованої модифікації інформації, становлять загрози цілісності.

3. Загрози, що відносяться до порушення можливості використання комп'ютерних систем або оброблюваної інформації, становлять загрози доступності.

4. Ідентифікація і контроль за діями користувачів, а також керованість комп'ютерною системою становлять предмет послуг спостереженості і керованості.

Крім функціональних критеріїв, що дозволяють оцінити наявність послуг безпеки в комп'ютерній системі, існують ще й критерії гарантій, що дозволяють оцінити коректність реалізації послуг. Критерії гарантій включають вимоги до

архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації. [4].

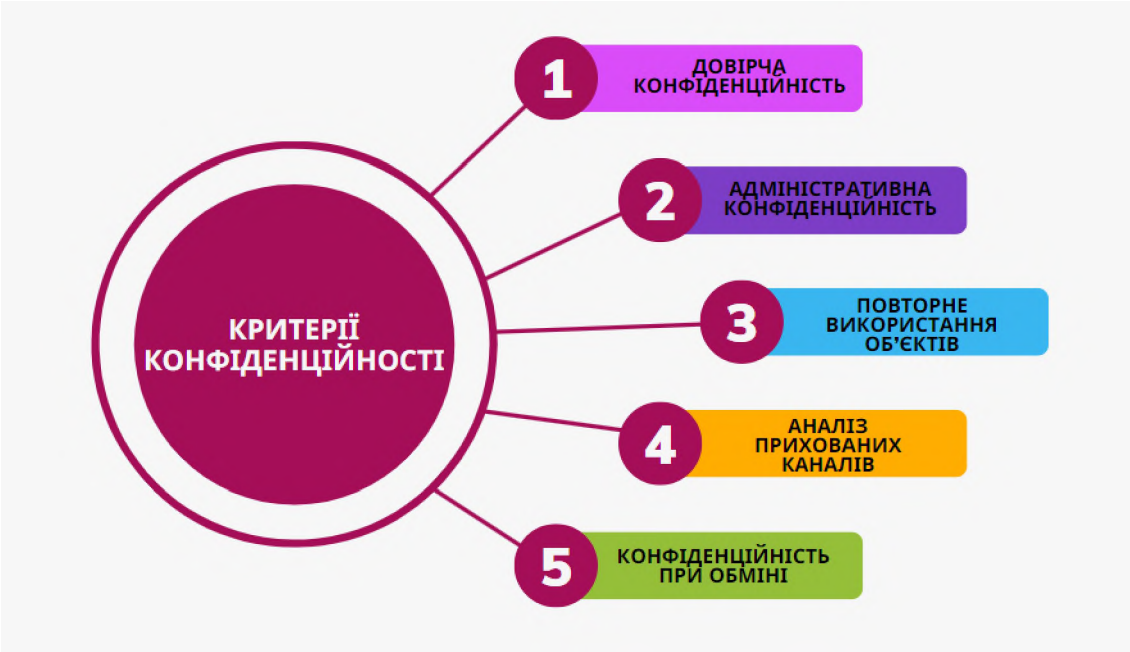

Рис. 2.1 – Схема критеріїв конфіденційності

У цій роботі розглядаються виключно критерії конфіденційності, оскільки основною метою є забезпечення захисту інформації.

Конфіденційність забезпечується наступними послугами:

1. Довірча конфіденційність.
2. Адміністративна конфіденційність.
3. Повторне використання об'єктів.
4. Аналіз прихованих каналів.
5. Конфіденційність при обміні.

Довірча конфіденційність дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування та описані у табл. 1 Додатку Г.

Адміністративна конфіденційність дозволяє адміністратору або спеціально авторизованому користувачу керувати потоками інформації від захищених об'єктів

до користувачів. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості управління та описані у табл. 2 Додатку Г.

Повторне використання об'єктів дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу та описані у табл. 3 Додатку Г.

Аналіз прихованих каналів виконується з метою виявлення і усунення потоків інформації, які існують, але не контролюються іншими послугами. Рівні даної послуги ранжируються на підставі того, чи виконується тільки виявлення, контроль або перекриття прихованих каналів та описані у табл. 2.4 Додатку В.

Конфіденційність при обміні дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ранжируються на підставі повноти захисту і вибірковості керування та описані у табл. 5 Додатку Г.

2.5 Програмне забезпечення для захисту інформації

На сьогоднішній день у ТОВ «N1 Clinic» використовуються технічні засоби сучасного зразка. Підсистему технічного забезпечення медичної організації, що досліджується, можна визначити наступним переліком:

1. Технічні засоби збору, реєстрації, накопичення, обробки, відображення, розмноження, доставки, збереження та забезпечення безпеки інформації.

2. Комп’ютери різних моделей, серверні та мережеві пристрої, оргтехніка.

3. Телекомунікаційна техніка та засоби зв’язку.

4. Загальносистемна документація, що включає державні, галузеві та корпоративні стандарти з технічного забезпечення.

5. Спеціалізована документація, що містить методичні матеріали по всіх етапах проектування, розробки, впровадження, супроводу та застосування технічних та технологічних засобів.

6. Нормативно–довідкова документація для виконання технічного забезпечення.

Технічні характеристики апаратного забезпечення повністю відповідають потребам співробітників та лікарів організації ТОВ «N1 Clinic» при вирішенні їх трудових функцій та завдань. АРМ мають різну конфігурацію, але мають такі мінімальні вимоги:

1. Процесор із частотою не менше 2.6 ГГц.
2. Оперативна пам'ять не менше 3 Гб.
3. Роздільна здатність монітора не менше 1280x1024 пікс.
4. Відеокарта щонайменше 1024 МБ.
5. Мережева карта.
6. Операційна система Windows 7 або нова.

Також до апаратного забезпечення входять джерела безперебійного живлення, які у разі короткочасних збоїв напруги дозволяють працювати із системою не менше десяти хвилин після відключення електрики. Для роботи мережі поліклініки використовується один мережевий комутатор.

До локальної мережі організації «N1 Clinic» входять 29 автоматизованих робочих місць працівників. Для адміністрування мережі використовується наступне серверне обладнання HP ProLiant ML30 Gen9, яке змонтоване в адміністративному підрозділі організації.

Для реалізації друку та сканування в локальній мережі підключено 18 БФП Brother DCP–7057WR, підключених до USB роз'єму

Існує розділення прав доступу для забезпечення доступу до ресурсів мережі. Кожному працівнику надано унікальне ім’я (логін) пароль, необхідні для входу в систему. Крім цього, для кожного користувача заведена окрема папка до якої має доступ він та адміністратор мережі. Існує спільна папка, необхідна обмінюватись даними між працівниками компанії.

На даний момент у медичній організації ТОВ «N1 Clinic» використовуються різні програмні продукти. Модель інформаційної інфраструктури клініки містить програмні продукти MS Office, 1С для підприємства (Бухгалтерія, Зарплата і

управління персоналом, CRM, Аналітика тощо), MS Office, та інше спеціалізоване програмне забезпечення, яке потрібне для виконання основної діяльності клініки.

В управлінні адміністративного відділу клініки ТОВ «N1 Clinic» також є інформаційний сайт (https://n1clinic.com.ua/), що дозволяє клієнтам віддалено ознайомитися з діяльністю та послугами медичної організації.

Встановлене програмне забезпечення на робочих станціях визначено специфікою діяльності співробітника, за яким закріплено робоче місце. Незважаючи на трудові функції співробітника, за яким закріплено робоче місце на сервер і робочу станцію, встановлено загальне програмне забезпечення:

1. Стандартний набір програми Microsoft Office: Word, Excel.
2. Як основний браузер використовується Google Chrome.
3. Для віддаленої технічної підтримки користувачів встановлено AnyDesk.
4. В якості антивірусу встановлено стандартний Microsoft Defender Antivirus.

Для автентифікації користувачів та управління доступом до ресурсів мережі на сервері організації використовується Active Directory.

Окремо варто зазначити, що на сервері ТОВ «N1 Clinic» встановлена операційна система Windows Server 2012. Ця операційна система використовується у сучасних обчислювальних мережах для організації серверів, оскільки вона має відмінну функціональність, високу швидкість роботи, а також підтримку необмеженої кількості підключень. Захист серверу відсутній, тому в майбутньому потрібно впровадити захист від спуфінгу. Оскільки без належного захисту сервер залишається вразливим до атак, цю вимогу треба виконати терміново.

2.6 Обстеження системи захисту інформації в ТОВ «N1 Clinic»

Система захисту інформації клініки має критично важливе значення для забезпечення конфіденційності, цілісності та доступності медичних даних. В ході обстеження системи захисту інформації в ТОВ «N1 Clinic» було визначено кілька критичних недоліків та областей, які в терміновому порядку потребують покращення.

1. В клініці відсутні належні засоби мережевого захисту, такі як міжмережеві екрани (фаєрволи) та системи виявлення та запобігання вторгнень (IDS/IPS).

2. Сервери не забезпечені належним антивірусним програмним забезпеченням та системами моніторингу і управління подіями (SIEM), що ставить під загрозу безпеку зберігання та обробки медичних даних.

3. Відсутні засоби резервного копіювання, що може призвести до втрати важливої інформації у разі виникнення інциденту.

4. Система управління обліковими записами та доступом забезпечує лише помірний рівень ідентифікації та автентифікації користувачів.

5. Захист серверних приміщень, робочих станцій та іншого обладнання забезпечений на помірному рівні, що включає лише базові заходи фізичного нагляду персоналом.

6. Відсутні чіткі правила визначення рівнів доступу для різних категорій персоналу, що призводить до неконтрольованого доступу до конфіденційної інформації.

7. Відсутні детальні процедури реагування на інциденти безпеки, що ускладнює оперативне вирішення проблем та розслідування інцидентів.

8. Відсутній регулярний аналіз вразливостей, що не дозволяє своєчасно виявляти та усувати слабкі місця в системі захисту.

9. Відсутні системи моніторингу для виявлення аномалій та потенційних інцидентів у режимі реального часу.

10. Не проводяться регулярні внутрішні та зовнішні аудити для оцінки відповідності системи захисту вимогам законодавства та стандартам безпеки.

2.7 Впровадження нових та вдосконалення існуючих методів та систем ЗІ

Забезпечення комплексної безпеки є необхідною умовою безпечного функціонування будь–якої медичної установи як суб'єкта критичної інфраструктури. Необхідний рівень безпеки повинен забезпечуватись за рахунок організаційних, технічних, а також інженерних заходів та методів захисту.

З метою відповідності нормативним документам комплексна система забезпечення інформаційної безпеки медичної організації ТОВ «N1 Clinic» повинна:

1. Запобігати несанкціонованому доступу до інформації та/або передачі її третім особам, які не мають права на доступ до інформації.

2. Забезпечувати своєчасне виявлення фактів несанкціонованого доступу до інформації.

3. Забезпечувати запобігання можливості несприятливих наслідків порушення порядку доступу до інформації.

4. Забезпечувати недопущення впливу на технічні та програмні засоби обробки інформації, внаслідок яких порушується їхнє функціонування.

5. Забезпечувати негайне відновлення інформації, модифікованої чи знищеної внаслідок несанкціонованого доступу до неї.

6. Забезпечувати постійний контроль забезпечення рівня захищеності інформації.

7. Забезпечувати захист інформації під час її передачі інформаційно–телекомунікаційними мережами.

8. Забезпечувати застосування сертифікованих за вимогами безпеки інформації засобів захисту.

9. Забезпечувати захист інформації під час експлуатації іншої інформаційної системи.

10. Забезпечувати обов'язковість обліку й реєстрації дій та ідентифікації учасників, пов'язаних з обробкою персональних даних в інших інформаційних системах.

11. Забезпечувати дотримання наступних організаційних заходів формування вимог щодо захисту інформації, що міститься в іншій інформаційній системі:

- розробка та впровадження системи (підсистеми) захисту інформації іншої інформаційної системи;
- мінімізація складу оброблюваних персональних даних, необхідні рішення покладених інші інформаційні системи задач;
- декларування та відповідність порядку обробки персональних даних цілям їх обробки;

- визначення інформаційного запиту як переважного способу отримання в інших інформаційних системах відомостей про об'єкт (суб'єкт) персональних даних;
- зберігання персональних даних в електронному вигляді в інформаційних системах за місцем виникнення таких даних.

12. Відповідати вимогам щодо забезпечення цілісності, стійкості функціонування та безпеки інформаційних систем загального користування, затвердженим Міністерством цифрової трансформації України, а також вимогам, затвердженим Службою безпеки України та Держспецзв'язком [7].

Заходи, виконання яких необхідне для забезпечення безпеки медичної організації ТОВ «N1 Clinic», визначаються конкретними законодавчими документами. При визначенні заходів слід враховувати можливі загрози, пов'язані з відповідною категорією об'єкта та рівнем потенціалу джерела, а також співвідношення категорії значущості та необхідного класу засобів захисту інформації.

У рамках вдосконалення комплексної системи забезпечення інформаційної безпеки медичної організації ТОВ «N1 Clinic» необхідно також вносити відповідні зміни до політики інформаційної безпеки, що є найважливішим документом у системі управління інформаційною безпекою медичного закладу. Політика ІБ має повністю відповідати вимогам міжнародного стандарту ISO 27002 [5] та державним стандартам України, таким як ДСТУ ISO/IEC 27001 [6].

Заходи та методи забезпечення безпеки інформації виявлених значущих об'єктів критичної інфраструктури ТОВ «N1 Clinic» мають бути спрямовані на нейтралізацію зазначених у пункті 2.2 загроз безпеки інформації.

У першу чергу необхідно забезпечити наявність грат на вікнах приміщень, що захищаються, і співробітника служби безпеки, який організує облік осіб, допущених до приміщень медичного закладу, та оперативно відреагує на спрацювання охоронної сигналізації, коли це буде потрібно. Разом з тим, такий співробітник, за потреби, повинен відстежувати пересування сторонніх осіб по

території, що захищається за допомогою внутрішнього та зовнішнього відеоспостереження.

Система контролю управління доступом медичної організації ТОВ «N1 Clinic» має містити низку предметних зон, що дозволяють зіставляти функціональні обов'язки співробітника та категорію значущості об'єктів критичної інфраструктури, яких співробітник може отримати доступ. Доцільно включити до облікової форми такі зони:

1. Зона штатних функціональних обов'язків працівника, під час реалізації яких використовуються значні об'єкти критичної інфраструктури (відповідно до затвердженої посадової інструкції).

2. Зона змін та доповнень, внесених до функціональних обов'язків працівника. Такий підхід дозволить не лише доповнити захист периметра об'єктів критичної інформаційної інфраструктури, а й організувати ешелонований захист систем. Аналіз здійснюється порівнянням змісту записів у зонах та індексів відомих співробітнику, тобто. ведеться пошук невідповідності.

Водночас необхідно реалізувати програмно–апаратний захист значущих об'єктів критичної інформаційної інфраструктури ТОВ «N1 Clinic». З метою організації ідентифікації та аутентифікації користувачів, процесів і пристроїв, що ініціюються, а також інших аспектів ідентифікації та аутентифікації слід використовувати системи захисту інформації від несанкціонованого доступу. Така система дозволить забезпечити управління обліковими записами користувачів, поділ повноважень (ролей) користувачів, призначення мінімально необхідних прав та привілеїв та інші аспекти управління доступом.

Для захисту інформаційної безпеки медустанови варто вдатися до наступних пунктів та запровадити:

1. Комплекс організаційних заходів та методів забезпечення інформаційної безпеки критичної інфраструктури медичного закладу. Організаційні заходи відіграють значну роль у створенні надійного механізму захисту об'єктів критичної інфраструктури ТОВ «N1 Clinic». До поточного моменту здійснено заходи навчального характеру. Співробітникам було проведено інструктаж про заходи

безпеки, захист даних, ймовірні дії у разі виявлення неполадок або збоїв в інформаційній системі. Це дозволяє говорити про те, що загальний рівень інформаційної безпеки у ТОВ «N1 Clinic» зростає. Водночас здійснюється контроль обізнаності персоналу про загрози безпеці інформації та правила безпечної роботи. Однак у положеннях про підрозділи та посадові інструкції керівників та співробітників медичної організації ТОВ «N1 Clinic» пункти про відповідальність за передачу, а також розголошення чи втрату атрибутів розмежування доступу не передбачено. На сьогоднішній день у відповідність до Закону України "Про захист персональних даних" № 2297–VI вже розроблено в медичній організації ТОВ «N1 Clinic» деякі політики ідентифікації та аутентифікації, аудиту безпеки, політику управління доступом, захисту носіїв інформації, політику про антивірусний захист, забезпечення цілісності та доступності, а також низку інших політик безпеки. У частині проведення аудиту безпеки нарікань немає – аудит проводиться на періодичній основі сторонньою організацією, в рамках якого відбувається інвентаризація інформаційних ресурсів, реєстрація подій безпеки, моніторинг безпеки, а також перевіряється реагування на збої під час реєстрації подій безпеки. Серед організаційних заходів щодо захисту виявлених значущих об'єктів критичної інфраструктури ТОВ «N1 Clinic» необхідно опрацювати докладніше наступні напрямки:

- порядок роботи з носіями інформації та мобільними пристроями;
- захист інформації від несанкціонованого доступу;
- порядок роботи адміністратора безпеки;
- порядок та правила використання паролів користувачів;
- розміщення технічних засобів (окремо приділити увагу щодо розміщення пристроїв виведення інформації, щоб унеможливити несанкціонований перегляд).

2. Комплекс програмно–апаратних заходів та методів забезпечення інформаційної безпеки в частині технічного та фізичного захисту.

На поточний момент встановлено охоронну та пожежну сигналізацію, двері зачиняються на замок, проте організація безпеки контрольованої зони відповідною

службою забезпечена не повністю. Усі точки входу/виходу та в'їзду/виїзду з будівлі медичного закладу, в яких функціонують значні об'єкти критичної інфраструктури, обладнані системою контролю та управління доступом, системами оповіщення та відеомоніторингу, проте не обладнані постами охорони та турнікетами, а на вікнах кабінетів не встановлені грати.

Водночас існуюча система не передбачає розмежування предметних зон, що дозволяють зіставляти функціональні обов'язки працівників та категорію значущості об'єкта критичної інформаційної інфраструктури. За результатами раніше проведеного аналізу, перерахуємо необхідні програмно–апаратні засоби значущих об'єктів критичної інфраструктури наступним списком:

– засіб захисту інформації від НСД;
– антивірусний засіб;
– засіб аналізу захищеності.

Організаційні заходи щодо розміщення ТЗ у медичній організації ТОВ «N1 Clinic», розроблені у цій роботі:

1. Усі технічні засоби значних об'єктів критичної інфраструктури перебувають у приміщеннях межах контрольованих зон.

2. Передбачено організаційні заходи, які створюють обмеження для несанкціонованого доступу до технічних засобів значимих об'єктів критичної інфраструктури (режим доступу до приміщень, порядок допуску до роботи з технічними засобами, опечатування корпусів та місць підключення периферійних пристроїв до основних технічних засобів обробки).

3. Передбачені організаційні заходи, які створюють обмеження для несанкціонованого доступу до АРМ (режим доступу до приміщень, порядок допуску до роботи з АРМ).

4. Передбачено організаційні заходи, що створюють обмеження для несанкціонованого доступу до ЗЗІ (визначено порядок допуску до роботи із ЗЗІ, визначено порядок їх використання).

5. При розміщенні технічних засобів, які використовують ЗЗІ, враховано рекомендації для цих засобів.

6. Розташування технічних засобів, встановлених для виведення інформації, що захищається, на друк, реалізовано з урахуванням проблеми візуального перегляду особами, які не мають допуску до цієї інформації.

Усі знімні носії медичної організації ТОВ «N1 Clinic», що знаходяться на зберіганні та в обігу, повинні враховуватися в Журналі обліку носіїв. Кожен носій із записаними даними повинен мати етикетку, на якій вказується мітка знімного носія та гриф.

Користувачі значимих об'єктів критичної інфраструктури для виконання робіт отримують окремий знімний носій від адміністратора безпеки. При його отриманні вносяться відповідні записи до журналу обліку.

У приміщеннях, що містять ТЗ або інші компоненти значущих об'єктів критичної інфраструктури, не допускається використання мобільних пристроїв.

Адміністратор безпеки медичної організації ТОВ «N1 Clinic» призначається на найвищому рівні, якщо є необхідність, то на середньому та нижньому рівнях.

Адміністратор безпеки повинен мати знання з налаштування та використання засобів захисту інформації, які застосовуються до об'єктів критичної інфраструктури, відповідно до документації, яка входить у їх поставку, а також до вимог і виписок із заключень, які визначають порядок їх використання.

Адміністратор безпеки веде журнали обліку роботи користувачів та друку користувачами документів, ідентифікаторів та паролів доступу користувачів до ТЗ, ідентифікаторів та паролів доступу адміністратора до ТЗ, врахування несправностей та спроб реалізації загроз безпеці.

Адміністратор інформаційної безпеки контролює дотримання політики безпеки та дотримання відповідних наказів. Також на нього покладено обов'язок за контролем виконання заходів щодо забезпечення захисту інформації та саме він здійснює резервне копіювання та відновлення програмного забезпечення при різних збоях чи позаштатних ситуаціях.

При використанні паролів у об'єктах критичної інфраструктури ТОВ «N1 Clinic» необхідно дотримуватись таких правил:

1. Паролі необхідно змінювати з установленою періодичністю відповідно до вимог організаційно–розпорядчого документа.

2. Пароль повинен мати не менше 6 символів і містити буквені та цифрові символи.

3. Обов'язкове застосування індивідуальних паролів.

4. Застосування групових паролів не допускається.

5. Для запобігання повторному використанню паролів необхідно вести облік (запис паролів) за попередні 12 місяців.

При використанні паролів необхідно ввести заборону на наступні дії: використання свого ПІБ, дати народження, прізвиська собаки тощо в якості паролю; використання легко обчислюваних поєднань символів та навіть загальноприйнятих скорочень як пароль.

2.8 Документообіг ТОВ «N1 Clinic»

Документообіг медичної організації ТОВ «N1 Clinic» – це процес створення, зберігання, передачі та знищення документів, які пов’язані не тільки з медичними, але й з адміністративними аспектами діяльності клініки. Невід’ємними складовими є медична документація, фінансові документи, а також внутрішні розпорядження та кореспонденція.

Для оформлення нового працівника на роботу необхідно подати наступні оригінали документів:

- Трудова книжка
- Медична книжка та пройдений медогляд
- Заповнена особова справа, включаючи автобіографію
- Довідка з пенсійного фонду
- Довідка з наркологічного диспансеру
- Довідка про несудимість
- Заява про прийом на роботу
- Згода на обробку персональних даних
- Фотографії

А також наступні копії:

- Паспорт
- Закордонний паспорт (за наявності)
- Ідентифікаційний код платника податків (РНОКПП)
- Диплом про освіту та додатки до диплому
- Довідка МСЕК про особу з інвалідністю (при наявності інвалідності)
- Свідоцтво про шлюб (за наявності)
- Свідоцтво про народження дітей віком до 18 років (за наявності)
- Військовий квиток або приписне свідоцтво (для військовозобов'язаних осіб)
- Сертифікати, посвідчення про категорію та звання доктора/професора
- Посвідчення про проходження курсів

З діяльності ТОВ «N1 Clinic» перелік персональних даних пацієнтів визначається наступним чином та включає в себе:

- Договір про надання медичних послуг.
- Медичну довідку, заключення лікаря.
- Журнал відмов у госпіталізації.
- Медичну карта амбулаторного хворого.
- Результати лабораторних та інструментальних досліджень.
- Протоколи лікування та медичні історії хвороби.
- Дані про проведені інтервенції та маніпуляції.
- Направлення на консультації до інших фахівців.
- Виписку з історії хвороби після госпіталізації.
- Інформацію про проведені вакцинації та профілактичні щеплення.
- Рентгенівські знімки та інші результати функціональних досліджень.
- Персональні дані для зв'язку: адресу проживання, номери телефонів, електронну пошту.
- Страхові документи та інформація про страхові поліси.

- Інформація про наявність алергічних реакцій та інші особливості пацієнта.
- Фінансову інформацію: рахунки на оплату медичних послуг, чеки, квитанції.
- Дані про контактних осіб, у разі екстрених ситуацій.
- Заяви на отримання медичних послуг або відмову від них.
- Документи, що підтверджують особу (паспорт, ідентифікаційний код).
- Записи розмов та консультацій з лікарями.
- Анкети та опитувальники, заповнені пацієнтами при зверненні до клініки.
- Дані про попередні медичні обстеження та лікування в інших медичних закладах.
- Згоду на обробку персональних даних відповідно до законодавства.

Копії персональних документів працівників, а також інші паперові документи повинні зберігатись в металевому висувному ящику під надійним замком. А після звільнення працівника чи закінчення терміну зберігання документів всі копії, заяви та інші пов’язані документи обов’язково мають знищуватись шредером. Саме приміщення бухгалтерії, де зберігаються всі документи, потрібно обладнати сигналізацією.

Система документообігу ТОВ «N1 Clinic» інтегрована з Медичною інформаційною системою (МІС) «Doctor Eleks EHealth», тому у клініці забезпечено єдиний інформаційний простір.

Документи, що регламентують організаційні заходи щодо захисту виявлених значущих об'єктів критичної інфраструктури медичної організації ТОВ «N1 Clinic», можна визначити наступним переліком:

- перелік співробітників, які мають допуск до роботи з виявленими значимими об'єктами;
- положення про захист значимих об'єктів критичної інфраструктури медичного закладу;

– наказ про виділення приміщень для захисту значимих об'єктів критичної інфраструктури медичного закладу;

Документи, що регламентують технічні заходи щодо захисту важливих об'єктів критичної інфраструктури медичної організації ТОВ «N1 Clinic», можна визначити таким переліком:

– план заходів щодо забезпечення захисту інформації;
– план дій у позаштатних ситуаціях;
– журнал обліку та зберігання носіїв;
– акт встановлення засобів захисту інформації;
– акт списання та знищення електронних носіїв;
– акт знищення документів

2.9 Якісні зміни в моделі загроз

У даному розділі було визначено оптимальний комплекс програмно–апаратних заходів та методів забезпечення інформаційної безпеки в частині технічного та фізичного захисту інформації.

Антивірусний захист має забезпечувати захист самих об'єктів КІІ, а також електронної пошти, інших сервісів та програм, а також мати оновлення баз даних ознак шкідливих комп'ютерних програм. На сьогоднішній день одним із найкращих антивірусних засобів є антивірус Bitdefender Business Security;

Цей «антивірус» дозволяє ефективно виявляти і видаляти вже наявне шкідливе ПЗ, а також забезпечує онлайн–безпеку та захист навіть від найскладніших вірусів.

В якості файрволу необхідно обирати саме той, який забезпечує надійний контроль трафіку в мережі, тому вибір було зупинено на pfSense. Цей міжмережевий екран моніторить і керує доступом користувачів до ресурсів, ідентифікує та автентифікує користувачів, контролює їхні права доступу і мінімізує можливі ризики втрати конфіденційності. Також він забезпечує захист від шкідливих програм і недозволених дій в мережі, використовуючи комплексні механізми безпеки.

Elastic Stack (ELK) – це інтегрована система управління інформаційною безпекою (SIEM), що забезпечує моніторинг в режимі реального часу, а також проводить аналіз подій і виявлення загроз для ефективного контролю безпеки мережі.

Wazuh – це система виявлення і запобігання вторгнень (NIDS), яка аналізує мережевий трафік для ідентифікації атак і аномалій за допомогою різноманітних сигнатур та правил.

Спільно ці інструменти забезпечують потужні засоби для виявлення, аналізу та реагування на потенційні загрози інформаційної безпеки в мережі ТОВ «N1 Clinic».

Також критично важливим є введення резервного копіювання даних, оскільки в медичних установах зберігається значна кількість конфіденційних пацієнтських інформаційних даних, а резервні копії дозволяють запобігати їх втратам в разі аварій або кібератак і забезпечують швидке відновлення робочих процесів та безперебійну роботу установи.

У таблиці 2.13 наведено заходи захисту з метою нейтралізації виявлених загроз значимих об'єктах критичної інформаційної інфраструктури медичної організації ТОВ «N1 Clinic».

Таблиця 2.13 – Заходи захисту інформації з метою нейтралізації виявлених загроз об'єктам КІІ ТОВ «N1 Clinic»

Назва загрози	Заходи щодо протидії загрозі	
	Технічні та фізичні	Організаційні
Загрози значимим об'єктам критичної інформаційної інфраструктури шляхом фізичного доступу		
Крадіжка, модифікація, знищення інформації	SIEM Elastic Stack (ELK); NIDS Wazuh, система контролю управління доступом, співробітник СБ, засоби фізичного запобігання проникненню	Інструкції персоналу, зобов'язання про нерозголошення, розміщення ТЗ відповідно до політики безпеки, обмеження використання зовнішніх носіїв, встановлення

		сертифікованого ПЗ
Несанкціоноване відключення засобів захисту	SIEM Elastic Stack (ELK); NIDS Wazuh, система контролю управління доступом, співробітник СБ, засоби фізичного запобігання проникненню	Дотримання порядку доступу до роботи з ЗЗІ, дотримання порядку використання паролів
Загроза впровадження агентів до персоналу системи	—	Первинна та періодична перевірка співробітників (аудит безпеки)
Загроза розголошення, передачі чи втрати атрибутів розмежування доступу	—	Інструкції персоналу, зобов'язання про нерозголошення, дотримання порядку використання паролів
Загроза виведення з ладу підсистем забезпечення функціонування мережі	Система контролю керування доступом, співробітник СБ, засоби фізичного запобігання проникненню	Інструкції персоналу
Загроза несанкціонованого використання терміналів користувачів, що мають унікальні фізичні характеристики (номер робочої станції в мережі, фізична адреса, адреса в системі зв'язку тощо)	Система контролю керування доступом, співробітник СБ, засоби фізичного запобігання проникненню	Інструкції персоналу, зобов'язання про нерозголошення, розміщення ТЗ відповідно до політики безпеки, обов'язкова ідентифікація користувачів
Загрози значимих об'єктів критичної інформаційної інфраструктури із застосуванням програмних та програмно–апаратних засобів		
Загроза впровадження програмних "закладок" та "вірусів"	Файрвол pfSense; Антивірус Bitdefender Business Security; SIEM Elastic Stack (ELK); NIDS Wazuh	Інструкції персоналу, обмеження використання зовнішніх носіїв, ведення Журналу обліку носіїв та використання мережі

		Інтернет, встановлення сертифікованого ПЗ
Загроза незаконного отримання паролів та інших реквізитів розмежування доступу з подальшим їх використанням	Файрвол pfSense; NIDS Wazuh	Інструкції персоналу, періодична зміна паролів, обмеження використання зовнішніх носіїв, встановлення сертифікованого ПЗ, дотримання порядку використання паролів
Загроза реалізації прихованого каналу передачі	Файрвол pfSense; Антивірус Bitdefender Business Security; SIEM Elastic Stack (ELK);	Первинна та періодична перевірка співробітників СБ
Загроза перехоплення конфіденційної інформації через мережу	Файрвол pfSense; SIEM Elastic Stack (ELK); NIDS Wazuh	Інструкції персоналу

На основі проведеного захисту від найпоширеніших загроз КІІ можна визначити наступні якісні зміни в моделі загроз:

- Підвищення відповідальності персоналу
- Посилення контролю за доступом
- Удосконалення технічних заходів захисту
- Запровадження системи моніторингу і аналізу подій

Ці зміни сприяли підвищенню рівня безпеки та захисту критичної інформаційної інфраструктури в клініці ТОВ «N1 Clinic» та зменшили потенційні вразливості і покращили реакцію на майбутні можливі кіберзагрози.

3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Вступ

Метою економічного розділу є техніко-економічне підтвердження доцільності запровадження запропонованих у проекті рішень. Зокрема, аналізується економічна ефективність впровадження системи інформаційної безпеки в контексті захисту інформаційних активів ТОВ «N1 Clinic». Економічна доцільність впровадження системи інформаційної безпеки включає аналіз капітальних і поточних витрат, оцінку можливих збитків від кіберзагроз, а також розрахунок загального ефекту від впровадження запропонованих заходів. Розробка політики безпеки інформації та її впровадження вимагають значних інвестицій, але ці витрати виправдані за рахунок зменшення ризику витоку конфіденційної інформації та підвищення рівня довіри пацієнтів.

Проведений аналіз дозволяє визначити економічну ефективність запропонованих заходів, що є важливим етапом для прийняття управлінських рішень у сфері інформаційної безпеки. Результати економічного аналізу допоможуть обгрунтувати інвестиції в інформаційну безпеку та забезпечити стабільний розвиток клініки в умовах сучасних кіберзагроз.

3.2 Розрахунок капітальних витрат

3.2.1 Визначення витрат на розробку політики безпеки інформації

3.2.1.1 Визначення трудомісткості розробки політики безпеки інформації

$$t = t_{\text{тз}} + t_{\text{в}} + t_{\text{а}} + t_{\text{вз}} + t_{\text{озб}} + t_{\text{овр}} + t_{\text{д}},$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень із забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

Розробка технічного завдання вимагає детального аналізу існуючих інформаційних систем, перевірки на відповідність вимогам безпеки, а також узгодження завдання з керівництвом та відповідними підрозділами. Під час виконання дипломної роботи на цей етап було витрачено 40 годин. Таким чином, $t_{тз} = 40$ годин.

Концепція безпеки включає в себе розробку стратегічних напрямків, політик і процедур, спрямованих на забезпечення інформаційної безпеки. Сюди відноситься аналіз ризиків, вибір методологій та визначення необхідних ресурсів. В ході виконання дипломної роботи на цей етап було витрачено 60 годин. Таким чином, $t_в = 60$ годин.

Аналіз ризиків передбачає ідентифікацію потенційних загроз, оцінку їх впливу та ймовірності, а також визначення способів їх мінімізації. Цей процес передбачає збір і аналіз даних, проведення опитувань та консультацій. В межах виконання дипломної роботи на виконання цього етапу було витрачено 70 годин. Таким чином, $t_а = 70$ годин.

Визначення вимог до заходів, методів та засобів захисту включає деталізацію технічних та організаційних заходів, необхідних для досягнення потрібного рівня безпеки. Цей етап тісно пов'язаний із попередніми та передбачає ретельний розгляд різних можливих рішень. Під час виконання дипломної роботи на цей процес було витрачено 30 годин. Таким чином, $t_{вз} = 30$ годин.

Вибір основних рішень із забезпечення безпеки інформації базується на визначених вимогах та включає оцінку різних технологічних та процедурних опцій, з урахуванням їхньої вартості, ефективності та відповідності специфічним потребам організації. В ході виконання дипломної роботи на цей етап було витрачено 20 годин. Таким чином, $t_{озб} = 20$ годин.

Етап організації виконання відновлювальних робіт та забезпечення неперервного функціонування організації включає розробку планів відновлення після інцидентів, тестування цих планів, а також заходи для забезпечення безперервності бізнес–процесів. Важливою умовою є те, що цей процес є комплексною роботою, яка вимагає участі декількох відділів. В межах виконання

дипломної роботи на виконання цього етапу було витрачено 50 годин. Таким чином, $t_{овр}$ = 50 годин.

Документальне оформлення включає в себе написання, редагування та узгодження таких документів як політики безпеки, інструкції та нормативні акти. Процес роботи з документами вимагає не лише уваги до деталей, а й забезпечення того, що всі документи відповідають вимогам організації та чинного законодавства. Під час виконання дипломної роботи на цей процес було витрачено 30 годин. Таким чином, $t_{д}$ = 30 годин.

Підставивши всі значення в формулу, отримаємо:

$$t = 40 + 60 + 70 + 30 + 20 + 50 + 30 = 300 \text{ годин}$$

Отже, загальна трудомісткість становить 300 годин.

3.2.1.2 Розрахунок витрат на створення політики безпеки інформації

Витрати на розробку політики безпеки інформації $К_{рп}$ складаються із витрат на заробітну плату спеціаліста з інформаційної безпеки $З_{зп}$ і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації $З_{мч}$:

$$К_{рп} = З_{зп} + З_{мч}$$

Заробітна плата виконавця враховує основну і додаткову заробітню плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) і визначається за формулою:

$$З_{зп} = t \times З_{іб},$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуванням, грн/годину

В попередніх розрахунках було отримано значення загальної трудомісткості, яке становить 300 годин.

Середньогодинна заробітна плата спеціаліста з інформаційної безпеки становить 70 грн/год.

Підставивши ці дані в формулу, отримаємо:

$$З_{зп} = 300 \times 70 = 21\,000 \text{ грн},$$

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$Змч = t \times Смч,$$

де t – трудомісткість розробки політики безпеки інформації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК грн/година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \times t_{нал} \times С_е + \frac{Ф_{зал} \times Н_а}{F_р} + \frac{К_{лпз} \times Н_{апз}}{F_р},$$

де P – встановлена потужність ПК, кВт;

C_e – тариф на електричну енергію, грн/кВт·год;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн;

H_a – річна норма амортизації на ПК, частки одиниці;

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$K_{лпз}$ – витрати на ліцензійне програмне забезпечення;

F_p – річний фонд робочого часу (за 40–годинного робочого тижня F_p = 1920)

В роботі спеціаліста з інформаційної безпеки використовується ноутбук Lenovo B50–30. Вольт–амперна характеристика цього ноутбука становить 20V ≈ 2.25A. Потужність слід обрахувати за наступною формулою:

$$W = A \times V,$$

де A – сила струму, A;

V – напруга, В.

$$W = 2.25 \times 20 = 45$$

Таким чином, потужність ПК становить 45 Вт, що еквівалентно 0.045 кВт.

Згідно постанови №632 Кабінету Міністрів України від 31.05.2024 ціна на електроенергію становит 4,32 грн/кВт·год.

Даний ноутбук було придбано та введено в експлуатацію в червні 2021 року. Первісна вартість ПК на той момент становила 7000 грн. Строк корисного використання – 5 років. Загальний термін використання об’єкта на даний момент становить 36 місяців. Накопичена амортизація обраховується наступним чином:

(7000 × 36) ÷ (5 × 12) = 4200 грн. Таким чином, залишкова вартість ПК на поточний рік становить 7000 – 4200 = 2800 грн.

Річна норма амортизації обчислюється як частка від первісної вартості, розділеної на строк користного використання: 7000 ÷ 5 = 1 400 грн. Таким чином, річна норма амортизації на ПК становить 20% або 1 400 грн.

В ході роботи було запропоновано впровадити нове ліцензійне програмне забезпечення, а саме:

1. PfSense – безкоштовно
2. Elastic Stack (ELK) – безкоштовно
3. Wazuh – безкоштовно (йде як доповнення до ELK)
4. Bitdefender Business Security: 2 786 грн на рік (за одну ліцензію), 27 863 грн на рік (за десять ліцензій);

Отже, у вартість ліцензійного програмного забезпечення організації входить лише річна підписка на ативірус, що коштує 27 863 грн. Місяць використання ліцензійного програмного забезпечення обійдеться майже в 2 325 грн.

Так як підписка на ліцензійне програмне забезпечення купується щороку, то в такому випадку річна норма амортизації дорівнює 1 (або 100%), оскільки вся вартість ліцензії списується тільки в той рік, коли вона була сплачена.

Вартість 1 години машинного часу ПК становить:

$$С_{мч} = 0.045 \times 300 \times 4.32 + \frac{2800 \times 0.2}{1920} + \frac{27863 \times 1}{1920} = 73 \text{ грн}$$

Таким чином, вартість машинного часу для розробки політики безпеки інформації на ПК становить: $Зм_{ч} = 300 \times 73 = 21\,900$ грн.

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки обчислюються за формулою:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}$$

Вартість розробки проекту та політики інформаційної безпеки для організації ТОВ «N1 Clinic» була безкоштовною, оскільки проходила в межах практики і була включена в заробітню плату. Залучення зовнішніх консультантів в ході виконання роботи не відбувалось. Таким чином, $К_{пр} = 0$ та $К_{пз} = 0$.

Вартість закупівель ліцензійного програмного забезпечення була прописана раніше та становить 27 863 грн. $К_{зпз}$ = 27.8 тис. грн.

Вартість закупівлі апаратного забезпечення та допоміжних матеріалів складається з оновлення маршрутизаторів на ASUS RT–AX53U AX1800 (вартість одного – 2400 грн, було оновлено 2 шт) та заміни конекторів мережевих кабелів (200 грн), а також встановлення брандмауера Cisco Secure Access Control System (його вартість була врахованна до вартості ПЗ). Таким чином, $К_{аз}$ = 5 тис. грн.

Витрати на навчання технічних фахівців і обслуговуючого персоналу були поділені на два етапи, оскільки внутрішні тренінги були проведені розробником проекту та були оплачені йому надбавкою до заробітньої плати в сумі 2 тис. грн., а спеціалістами компанії CyberLab було проведено одноденний курс для групи з 10 осіб вартістю 10 000 грн. $К_{навч}$ = 12 тис. грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки включають в себе:

1. Встановлення системи контролю керування доступом (СКУД)
   - Автономний Host Dahua DH–ASI1201A – 2285 грн (6 шт)
   - Вартість монтажу одного контролера – 2000 грн
2. Встановлення датчику руху (Ajax MotionProtect) в серверну кімнату разом з монтажем коштувала 3000 грн.
3. Для встановлення та налогодження ПЗ та системи ІБ було запрошено спеціалістів служби ІБ з компанії CyberLab. Процес встановлення та налаштування загалом зайняв 10 годин, що коштувало 10 000 грн.

Цей етап був найдорожчим – $К_{н}$ = 89 тис. грн.

Таким чином, капітальні витрати становлять:

$$К = 0 + 27.8 + 0 + 5 + 12 + 89 = 133.8 \text{ тис. грн}$$

3.3 Розрахунок річних експлуатаційних витрат

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки визначаються за формулою: $С = С_{в} + С_{к} + С_{ак}$

де $С_{в}$ – витрати на Upgrade–відновлення й модернізацію системи інформаційної безпеки;

$C_к$ – витрати на керування системою в цілому;

$C_{ак}$ – витрати, викликані активністю користувачів системи інформаційної безпеки.

Витрати на Upgrade–відновлення й модернізацію системи включають в себе оновлення програмного забезпечення, апаратні оновлення, додаткові модулі безпеки тощо. Оскільки організація ТОВ «N1 Clinic» невелика, то ці витрати становлять 15 000 грн. $C_в$ = 15 тис. грн.

Витрати на керування системою інформаційної безпеки складаються з наступних компонентів:

1. Витрати на навчання адміністративного персоналу й кінцевих користувачів $C_н$
2. Річний фонд амортизаційних відрахування $C_а$
3. Річний фонд заробітної плати інженерно–технічного персоналу $C_з$
4. Вартість електроенергії $C_е$
5. Витрати на залучення сторонніх організацій $C_о$
6. Витрати на технічне й організаційне адміністрування та сервіс $C_{тос}$
7. Витрати, викликані активнісю користувачів системи інформаційної безпеки $C_{ак}$

Обчислюється за формулою $C_к = C_н + C_а + C_з + C_{єв} + C_е + C_{ел} + C_о + C_{тол}$.

Навчання адміністративного персоналу забезпечується курсами підвищення кваліфікації, а навчання кінцевих користувачів планується проводити один раз на рік. Курси для адміністративного персоналу коштують 10 000 грн для навчання однієї особи, а курси для навчання кінцевих користувачів роботі з ПЗ проводяться для групи та коштують 10 000 грн за групу з 10 осіб. Адміністративний персонал складається з двох осіб, а кінцевих користувачів є 20. Навчання адмінперсоналу буде коштувати організації 20 000 грн і навчання всіх кінцевих користувачів також 20 тис. грн на рік. Отже, $C_н$ = 40 тис. грн.

Річний фонд амортизаційних відрахування $C_а$ дорівнює вартості закупівель підписок на послуги ліцензійного програмного забезпечення на рік (оскільки в такому випадку амортизація дорівнює 100%). $C_а$ = 27.8 тис. грн.

Річний фонд заробітної плати інженерно–технічного персоналу складається з основної та додаткової заробітньої плати та обчислюється за формулою:

$$С_з = З_{осн} + З_{дод},$$

де Зосн, Здод – основна і додаткова заробітня плата відповідно.

Основна заробітня плата визначається, виходячи з місячного посадового окладу та становить 11 200 грн, а додаткова заробітна плата – в розмірі 8–10% від основної заробітної плати та складається з 1120 грн. $С_з$ = 12 320 грн.

Розмір єдиного соціального внеску (ЄСВ) становить 22%. Таким чином, $С_{єв}$ = 2 710 грн.

Вартість електроенергії, що споживається апаратурою системи інформаційної безпеки протягом року, визначається за формулою:

$$С_{ел} = P \times F_p \times С_е,$$

де P – встановлена потужність апаратури інформаційної безпеки, кВт;

F_p – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки);

$С_е$ – тариф на електроенергію, грн/кВт·годин

Система безпеки включає в себе наступну апаратуру:

- Сервер, що споживає 0.7 кВт за годину
- 1 датчик руху, який споживає 0.01 кВт
- Мережеві комутатори, кожен з яких споживає 0.1 кВт
- Система зберігання даних, яка споживає 1 кВт.

Таким чином, P = 1.81 кВт.

Оскільки робочий час системи інформаційної безпеки працює безперебійно (24 години на тиждень), то річний фонд робочого часу F_p становить 8064.

Тариф на електроенергію було описано раніше, тому $С_е$ = 4.32 грн/ кВт·годин.

$$С_{ел} = 1.81 \times 8064 \times 4.32 = 63\,054 \text{ грн}$$

Витрати на залучення сторонніх організацій для виконання обслуговування та навчання обслуговуючого персоналу було описано раніше. Загалом ці витрати становлять 22 тис. грн. $С_о$ = 22 тис. грн

Витрати на технічне й організаційне адміністрування та сервіс становлять 2% від вартості капітальних витрат. Таким чином, $С_{тос}$ = 2 920 грн.

Таким чином, витрати на керування системою інформаційної безпеки становлять: $С_к = 143\,031$ грн.

Витрати, викликані активністю користувачів системи ІБ включають такі вагові частки витрат:

– Пряма допомога й додаткові налаштування 11%
– Робота з даними 15%

Ці витрати загалом становлять 26% від сукупної вартості системи інформаційної безпеки, а зокрема:

– Пряма допомога й додаткові налаштування коштують 14 718 грн
– Робота з даними коштує 20 070 грн

Що загалом становить $С_{ак}$ = 34 788 грн.

Таким чином, річні експлуатаційні витрати на функціонування системи інформаційної безпеки $С$ становлять 192 819 грн.

3.4 Оцінка величини збитку від атаки на корпоративну мережу

Можна виділити 4 основні види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

1. Порушення конфіденційності ресурсів КСІБ;
2. Порушення цілісності ресурсів КСІБ;
3. Порушення доступності ресурсів КСІБ;
4. Порушення автентичності ресурсів КСІБ.

Для розрахунку вартості потенційного збитку застосовується спрощена модель оцінки.

Оскільки організація ТОВ «N1 Clinic» відносно невелика, то час простою вузла або сегмента корпоративної мережі внаслідок атаки становить близько 10 годин, а час відновлення після атаки персоналом, що обслуговує корпоративну мережу складає майже 16 годин. Таким чином $t_п$ = 10 год, а $t_в$ = 16 год.

Час повторного введення загубленої інформації співробітниками атакованого вузла/сегмента корпоративної мережі, оскільки резервне копіювання відсутнє, становить 48 годин. Отже, $t_{ви}$ = 48 год.

Заробітна плата обслуговуючого персоналу становить 11 200 грн на місяць, а заробітна плата співробітників атакованого вузла/сегмента корпоративної мережі – 9500 грн. Таким чином, $З_о$ = 11 200 грн, а $З_с$ = 9500 грн.

Чисельність обслуговуючого персоналу (системних адміністраторів) складає 2 особи, а чисельність співробітників потенційно можливого атакованого вузла/сегмента корпоративної мережі становить 20 осіб. *Таким чином,* $Ч_о$ = 2 особи, а $Ч_с$ = 20 осіб.

Обсяг продажів атакованого вузла/сегмента корпоративної мережі в середньому вартує 1 700 000 грн у рік. Таким чином, $О$ = 1 млн. 700 тис. грн.

У випадку вдалої атаки на вузол, вартість заміни встаткування чи запасних частин буде коштувати в середньому 35 000 грн. Таким чином, $П_{зч}$ = 35 тис. грн

Оскільки в організації наявний тільки один сервер, який відповідає за всі функції ТОВ «N1 Clinic» та лише 2 основних сегмента мережі, які забезпечують інтернет-зв'язок та доступ до зовнішніх ресурсів, то число атакованих вузлів або сегментів корпоративної мереж в такому випадку становить . Таким чином, $І$ = 3.

Медичні установи часто стають об'єктом кібератак через наявність чутливої інформації про пацієнтів. За статистичними даними, маленькі та середні організації зазнають від однієї до кількох десятків атак на рік, залежно від захищеності та активності в мережі. Тому можна припустити, що середня кількість атак на рік становить 6. Але варто пам'ятати, що кількість успішних атак може бути меншою та залежить від захищеності та активності в мережі. Таким чином, N = 6.

Втрачена вигода від простою атакованого вузла або сегмента корпоративної мережі обчислюється за формулою:

$$U = П_п + П_в + V,$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (перевстановлення системи, зміна конфігурацій та інше), грн

V – вартість від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн

Втрати від зниження продуктивності співпробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки обчислюється за формулою:

$$П_п = \frac{\sum З_с}{F} \times t_п \text{ або } П_п = \frac{З_с}{F} \times t_п \times Ч_с,$$

де F – місячний фонд робочого часу (при 40-годинному робочому тижні становить 176 год)

Всі дані були обчислені раніше, тому лишається лише підставити їх у відповідну формулу.

$$П_п = \frac{9500}{176} \times 10 \times = 10\,795 \text{ грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових: $П_в = П_{ви} + П_{пв} + П_{зч}$,

де $П_{ви}$ – витрати на повторне введення інформації, грн

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співпробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$: $П_{ви} = \frac{\sum З_с}{F} \times t_{ви}$ або $П_{ви} = \frac{З_с}{F} \times t_{ви} \times Ч_с$,

Всі дані були обчислені раніше, тому лишається лише підставити їх у відповідну формулу.

$$П_{ви} = \frac{9500}{176} \times 48 \times 20 = 51\,818 \text{ грн}$$

Витрати на відновлення вузла або сегмента корпоративної мережі Ппв визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о}{F} \times t_в \text{ або } П_{пв} = \frac{З_о}{F} \times t_в \times Ч_о,$$

Всі дані були обчислені раніше, тому лишається лише підставити їх у відповідну формулу.

$$П_{пв} = \frac{11200}{176} \times 16 \times 2 = 2\,036 \text{ грн}$$

Таким чином, $П_в = 51\,818 + 2\,036 + 35\,000 = 88\,854$ грн

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі визначаються виходячі із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \times (t_п + t_в + t_{ви}),$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

Всі дані були обчислені раніше, тому лишається лише підставити їх у відповідну формулу.

$$V = \frac{1\,700\,000}{2080} \times (2 + 3 + 5) = 8\,173 \text{ грн}$$

Втрачена вигода від простою атакованого вузла або сегмента корпоративної мережі становить $U = 10\,795 + 88\,854 + 8\,173 = 107\,822$ грн.

Загальний збиток від атаки на вузол або сегмент корпоративної мережі обчислюється за формулою $B = \sum_i \sum_n U$.

Оскільки вузлів та сегментів в мережі є 3, то загальний збиток від атаки на вузол або сегмент корпоративної мережі буде $В = 107\,822 \text{ грн} \times 3 = 323\,466$ грн.

3.5 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B - C,$$

де В – загальний збиток від від атаки на вузол або сегмент корпоративної мережі, тис. грн;

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн

$$E = 323\,466 - 192\,819 = 130\,647$$

3.6 Визначення та аналіз показників економічної ефективності

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Але якщо мова йде про інформаційну безпеку, то говорять не про прибуток, а про запобігання можливих втрат від атаки на вузол або сегмент корпоративної мережі, а отже:

$$ROSI = \frac{E}{K},$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, тис. грн

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн

$$ROSI = \frac{130\ 647}{133\ 000} = 0.98$$

Оскільки організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань), то в якості Ен приймається бажана норма прибутковості альтернативних варіантів вкладень коштів К з урахуванням інфляції.

Формула для перевірки економічної доцільності проекту:

$$ROSI > \frac{N_{\text{деп}} - N_{\text{інф}}}{100},$$

де $N_{деп}$ – річна депозитна ставка (15%);

$N_{інф}$ – річний рівень інфляції (8.5%).

$$ROSI > 0.065$$

3.7 Висновок про економічну доцільність

Запропонована в даному проекті система інформаційної безпеки виявилась економічно доцільною для організації ТОВ «N1 Clinic». Так як ROSI 0.98 є значно більшим, ніж коефіцієнт ефективності 0.065, то даний проект є економічно доцільним, оскільки він генерує достатньо високий відсоток повернення від інвестицій в інформаційну безпеку, що вказує на його ефективність з фінансової точки зору. ROSI на рівні 0.98 підтверджує, що кожна інвестована одиниця валюти приносить більше, ніж одиниця витрат, що свідчить про високий рівень віддачі від

інвестицій в захист інформації. Цей показник підтверджує не лише стратегічну важливість впровадження запропонованих заходів для забезпечення безпеки, а й їхню фінансову доцільність, забезпечуючи баланс між витратами на захист та потенційними втратами від можливих кібератак або інших інцидентів.

ВИСНОВКИ

В даній роботі було проведено дослідження питання забезпечення інформаційної безпеки критичної інформаційної інфраструктури, на підставі якого можна зробити висновок про певний перелік вразливостей та загроз інформаційної безпеки стосовно медичних організацій. В ході роботи було проаналізовано ключові аспекти та визначено принципи забезпечення безпеки критичної інформаційної інфраструктури, на підставі чого було зроблено висновок щодо необхідності підвищення захищеності критичних інформаційних інфраструктур, зокрема медичного закладу.

Також в роботі було виявлено критичні процеси, визначено об'єкти критичної інформаційної інфраструктури медичної організації ТОВ «N1 Clinic», проведено оцінку факторів активності потенційного зловмисника, а також розроблено модель загроз безпеки об'єктів критичної інфраструктури медичного закладу. За результатом проведеного аналізу було проведено оцінку категорій значущих об'єктів критичної інформаційної інфраструктури ТОВ «N1 Clinic», у відповідність до Закону України № 1882-IX «Про критичну інфраструктуру» від 16.11.2021 р. та Постанова № 518 «Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 р.

На підставі проведеного категорування та постанови було запропоновано проект вдосконалення комплексної системи забезпечення інформаційної безпеки медичної організації ТОВ «N1 Clinic». Запропонований проект містить оптимальні й економічно вигідні комплекси організаційних, технічних та програмно-апаратних заходів та методів забезпечення інформаційної безпеки, впровадження яких дозволяє нейтралізувати виявлені актуальні загрози безпеці медичної організації ТОВ «N1 Clinic».

Таким чином в результаті роботи було досліджено організаційно-правовий та інженерно-технічний напрями забезпечення інформаційної безпеки, підібрано заходи та методи забезпечення комплексної безпеки з метою нейтралізації визначених загроз.

Отримані результати можуть бути використані державними та комерційними медичними організаціями для проектування сучасних комплексних систем захисту інформації, які враховують вимоги постанови № 518, а також інших нормативних документів щодо обробки даних на суб'єктах критичної інформаційної інфраструктури.

ПЕРЕЛІК ПОСИЛАНЬ

1. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX : станом на 21 черв. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/1882-20

2. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2297-17

3. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури : Постанова Каб. Міністрів України від 19.06.2019 р. № 518 : станом на 7 верес. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/518-2019-п

4. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Чинний від 1999-04-28. Вид. офіц. Київ : ДСТСЗІ СБ України, 1999. 60 с.

5. ISO/IEC 27002:2005. ЗВІД ПРАВИЛ ДЛЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ. Вид. офіц. Київ : НАЦ. БАНК УКРАЇНИ, 2010. 139 с.

6. ДСТУ ISO/IEC 27001:2023. Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги. На заміну ДСТУ ISO/IEC 27001:2015 ; чинний від 2023-08-22. Вид. офіц. ДП «УкрНДНЦ», 2023.

7. Правове забезпечення кібербезпеки критичної інформаційної інфраструктури України / М. Ковалів та ін. Траєкторія науки: міжнародний електронний науковий журнал. 2021. Т. 7, № 4.

8. Присяжнюк М., Марущак А. Організаційно-правові основи забезпечення кібербезпеки : Навч. посіб. Київ : Ліра К, 2023. 320 с.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	1	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	3	
5	А4	Стан питання. Постановка задачі	6	
6	А4	Спеціальна частина	36	
7	А4	Економічний розділ	14	
8	А4	Висновки	2	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	2	
12	А4	Додаток В	1	
13	А4	Додаток Г	4	

ДОДАТОК Б. Схема організації ТОВ «N1 Clinic»

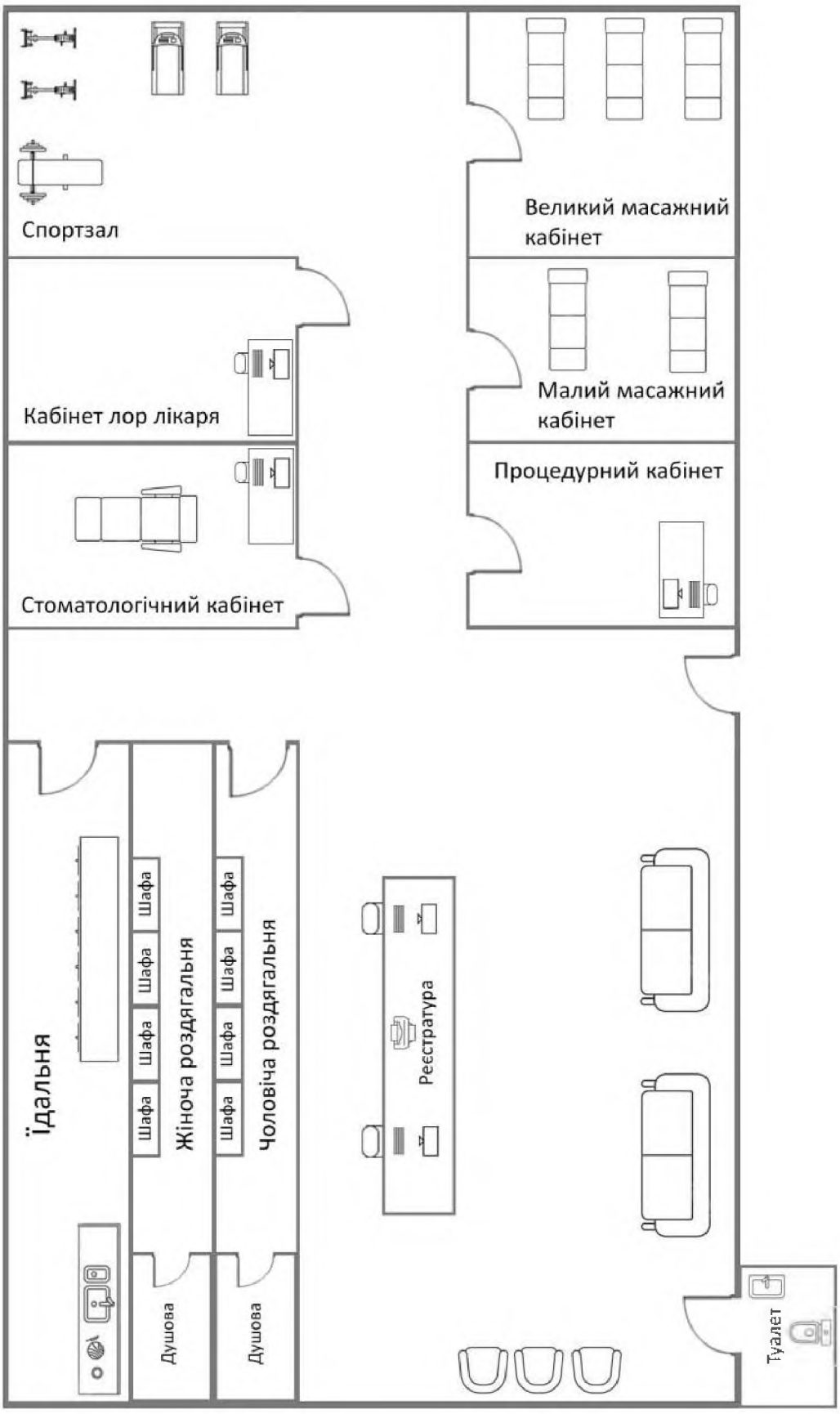

Рис. 1 – Схема першого поверху організації ТОВ «N1 Clinic»

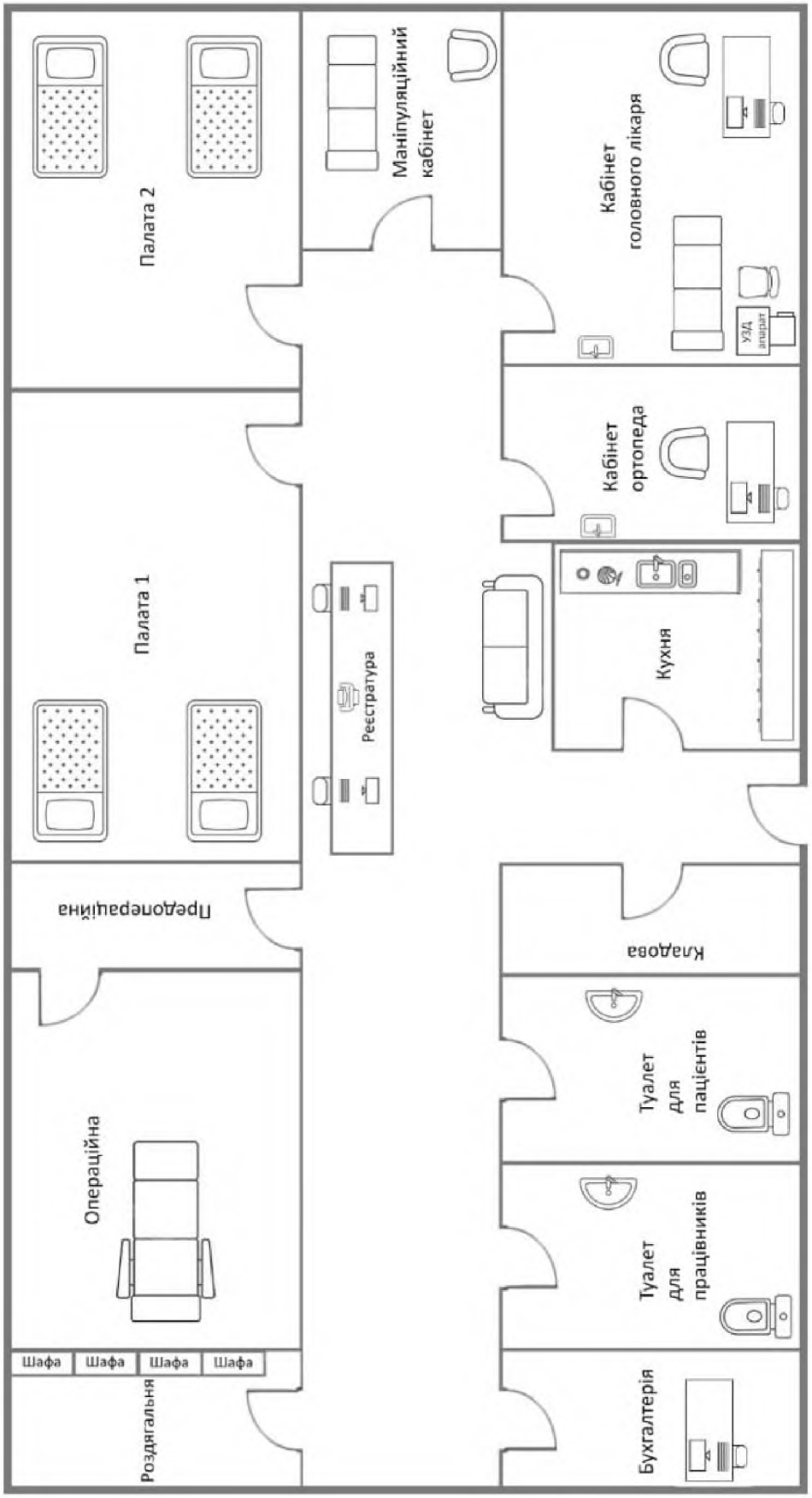

Рис. 2 – Схема першого поверху організації ТОВ «N1 Clinic»

ДОДАТОК В. Топологія локальної мережі організації ТОВ «N1 Clinic»

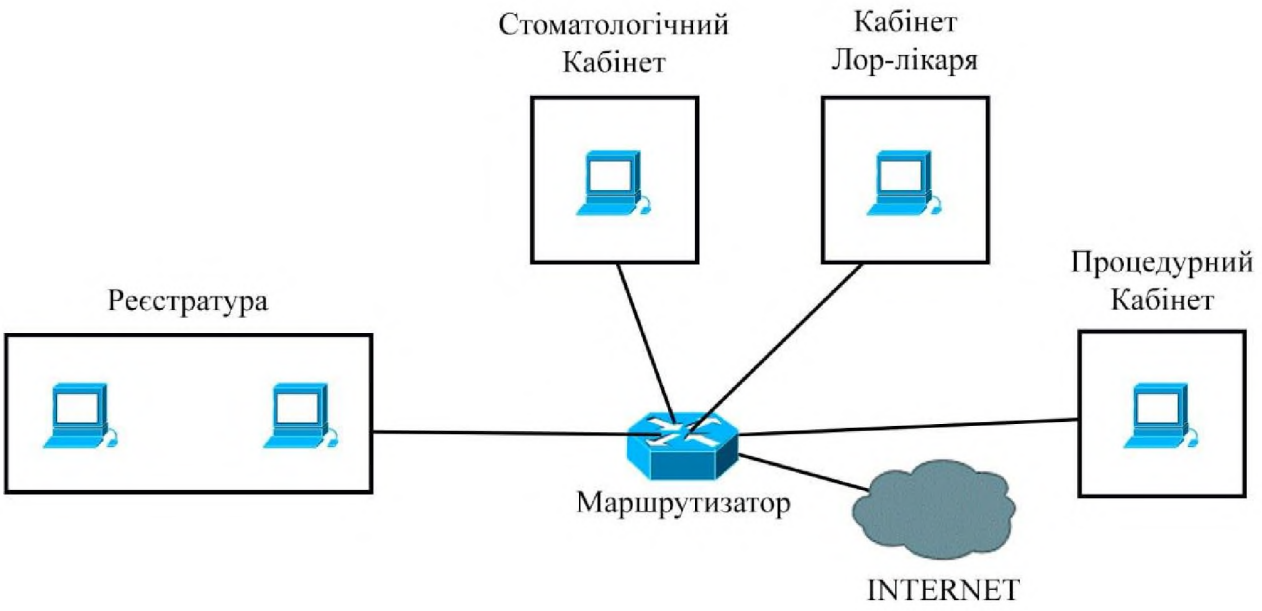

Рис. 1 – Топологія локальної мережі першого поверху організації ТОВ «N1 Clinic»

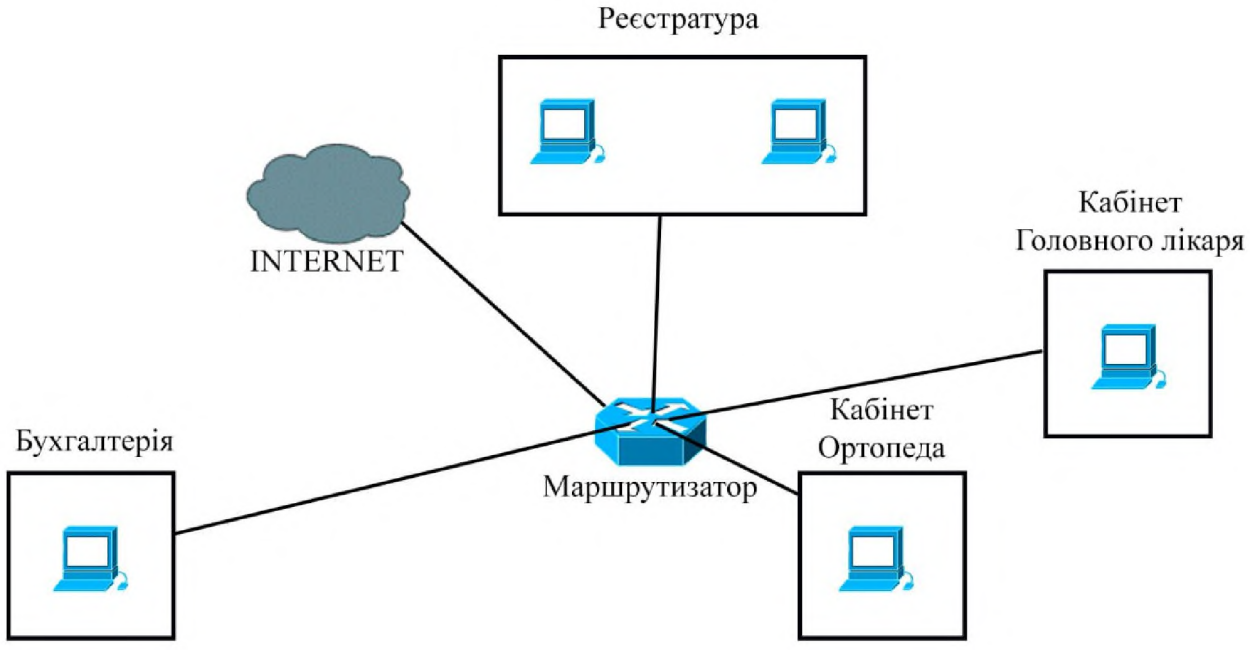

Рис. 5 – Топологія локальної мережі другого поверху організації ТОВ «N1 Clinic»

ДОДАТОК Г. Критерії конфіденційності

Таблиця 1 – Довірча конфіденційність

<table>
<tr><th>КД–1
Мінімальна довірча конфіденційність</th><th>КД–2
Базова довірча конфіденційність</th><th>КД–3
Повна довірча конфіденційність</th><th>КД–4
Абсолютна довірча конфіденційність</th></tr>
<tr><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика довірчої конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу до об'єкта повинні оброблятися КЗЗ на підставі атрибутів доступу користувача, що ініціює запит, і об'єкта</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати користувачу можливість для кожного захищеного об'єкта, що належить його домену, визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td>—</td><td colspan="3">КЗЗ повинен надавати користувачу можливість для кожного процесу, що належить його домену, визначити
конкретних користувачів і/або групи користувачів, які мають право ініціювати процес — конкретних користувачів (і групи користувачів), які мають, а також тих, що не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватись в момент його створення або ініціалізації.
Як частина політики довірчої конфіденційності повинні бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НИ–1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО–1, НИ–1</td></tr>
</table>

Таблиця 2 – Адміністративна конфіденційність

<table>
<tr><th>КА–1
Мінімальна адміністративна конфіденційність</th><th>КА–2
Базова адміністративна конфіденційність</th><th>КА–3
Повна адміністративна конфіденційність</th><th>КА–4
Абсолютна адміністративна конфіденційність</th></tr>
<tr><td colspan="2">Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна визначати множину об'єктів КС, до яких вона відноситься</td><td colspan="2">Політика адміністративної конфіденційності, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС</td></tr>
<tr><td colspan="4">КЗЗ повинен здійснювати розмежування доступу на підставі атрибутів доступу</td></tr>
<tr><td>процесу і захищеного об'єкта</td><td colspan="2">користувача і захищеного об'єкта</td><td>користувача, процесу і захищеного об'єкта</td></tr>
<tr><td colspan="4">Запити на зміну прав доступу повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або від користувачів, яким надані відповідні повноваження</td></tr>
<tr><td colspan="4">КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити</td></tr>
<tr><td>конкретні процеси і/або групи процесів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта</td><td>конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td><td>конкретних користувачів і процеси (і групи користувачів і процесів), які мають, а також тих, які не мають права одержувати інформацію від об'єкта</td></tr>
<tr><td rowspan="2">—</td><td colspan="3">КЗЗ повинен надавати можливість адміністратору або користувачу, що має відповідні повноваження, для кожного процесу через керування належністю користувачів і процесів до відповідних доменів визначити</td></tr>
<tr><td>конкретних користувачів і/або групи користувачів, які мають право ініціювати процес</td><td colspan="2">конкретних користувачів (і групи користувачів), які мають, а також тих, які не мають права ініціювати процес</td></tr>
<tr><td colspan="4">Права доступу до кожного захищеного об'єкта повинні встановлюватися в момент його створення або ініціалізації. Як частина політики адміністративної конфіденційності мають бути представлені правила збереження атрибутів доступу об'єктів під час їх експорту та імпорту</td></tr>
<tr><td colspan="2">НЕОБХІДНІ УМОВИ: НО–1, НИ–1</td><td colspan="2">НЕОБХІДНІ УМОВИ: КО–1, НО–1, НИ–1</td></tr>
</table>

Таблиця 3 – Повторне використання об'єктів

КО–1 **Повторне використання об'єктів**
Політика повторного використання об'єктів, що реалізується КЗЗ, повинна відноситись до всіх об'єктів КС Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, встановлені для попереднього користувача або процесу права доступу до даного об'єкта повинні бути скасовані Перш ніж користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об'єкт, вся інформація, що міститься в даному об'єкті, повинна стати недосяжною
НЕОБХІДНІ УМОВИ: НЕМАЄ

Таблиця 4 – Аналіз прихованих каналів

КК–1 **Виявлення прихованих каналів**	**КК–2** **Контроль прихованих каналів**	**КК–3** **Перекриття прихованих каналів**
Повинен бути виконаний аналіз прихованих каналів		
Всі приховані канали, які існують в апаратному і програмному забезпеченні, а також в програмах ПЗП, повинні бути документовані Має бути документована максимальна пропускна здатність кожного знайденого прихованого каналу, одержана на підставі теоретичної оцінки або вимірів Для прихованих каналів, які можуть використовуватися спільно, повинна бути документована сукупна пропускна здатність		Всі (затверджена підмножина) знайдені під час аналізу приховані канали повинні бути усунені
—	КЗЗ повинен забезпечувати реєстрацію використання затвердженої підмножини знайдених прихованих каналів	
НЕОБХІДНІ УМОВИ: КО–1, Г–3	НЕОБХІДНІ УМОВИ: КО–1, НР–1, Г–3	НЕОБХІДНІ УМОВИ: КО–1, Г–3

Таблиця 5– Конфіденційність при обміні

<table>
<tr><th>КВ–1
Мінімальна конфіденційність при обміні</th><th>КВ–2
Базова конфіденційність при обміні</th><th>КВ–3
Повна конфіденційність при обміні</th><th>КВ–4
Абсолютна конфіденційність при обміні</th></tr>
<tr><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати множину об'єктів і інтерфейсних процесів, до яких вона відноситься</td><td colspan="2">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна відноситись до всіх об'єктів і існуючих інтерфейсних процесів</td></tr>
<tr><td colspan="4">Політика конфіденційності при обміні, що реалізується КЗЗ, повинна визначати рівень захищеності, який забезпечується механізмами, що використовуються, і спроможність користувачів і/або процесів керувати рівнем захищеності</td></tr>
<tr><td colspan="4">КЗЗ повинен забезпечувати захист від безпосереднього ознайомлення з інформацією, що міститься в об'єкті, який передається</td></tr>
<tr><td>—</td><td colspan="3">Запити на призначення або зміну рівня захищеності повинні оброблятися КЗЗ тільки в тому випадку, якщо вони надходять від адміністраторів або користувачів, яким надані відповідні повноваження</td></tr>
<tr><td>—</td><td colspan="3">Запити на експорт захищеного об'єкта повинні оброблятися передавальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
—
і приймальника об'єкта</td></tr>
<tr><td>—</td><td colspan="3">Запити на імпорт захищеного об'єкта повинні оброблятися приймальним КЗЗ на підставі атрибутів доступу інтерфейсного процесу
—
і джерела об'єкта</td></tr>
<tr><td colspan="2">—</td><td colspan="2">Представлення захищеного об'єкта має бути функцією атрибутів доступу інтерфейсного процесу, самого об'єкта, а також його джерела і приймальника</td></tr>
<tr><td colspan="3"></td><td>Політика конфіденційності при обміні повинна включати опис інформації , яку можливо отримати шляхом сумісного аналізу ряду одержаних об'єктів Повинен бути виконаний аналіз прихованих каналів обміну. Всі знайдені приховані канали обміну і максимальна пропускна здатність кожного із них мають бути документовані. Повинна бути забезпечена реєстрація використання затвердженої підмножини знайдених прихованих каналів, їх часткове перекриття або усунення</td></tr>
<tr><td>НЕОБХІДНІ УМОВИ: НЕМАЄ</td><td>НО–1</td><td>НО–1, НВ–1</td><td>НО–1, НВ–1, НР–1, Г–3</td></tr>
</table>