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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістра

студента *Резніченка Дмитра Олеговича*

академічної групи *125м-19-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Методика протидії антропогенним загрозам в ІТС «Біржа медичних працівників»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І.			
розділів:				
спеціальний	ст. викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			

Рецензент				

Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.
«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Резніченку Дмитру Олеговичу* **академічної групи** *125м-19-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Методика протидії антропогенним загрозам в ІТС «Біржа медичних працівників»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.2020 № 888-с

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати теоретичні засади дослідження системи захисту інформації та визначити її складові. Охарактеризувати принципи інформаційної безпеки.	25.09.2020
Розділ 2	Виконати аналіз існуючих моделей СІМ. Проаналізувати підходи до проектування СЗІ на базі медичної установи та визначити алгоритм її створення. Зробити розрахунок надійності захисних бар'єрів підприємства та дослідити моделі зловмисника з точки зору ймовірних внутрішніх та зовнішніх загроз.	20.10.2020
Розділ 3	Розробити структурну схему та архітектуру моделі СІМ. Впровадити систему та визначити її ефективність. Розробити інструкції з безпечної експлуатації системи та політики безпеки для медичної установи та медичного працівника.	25.11.2020
Розділ 4	Виконати розрахунок витрат на розробку та впровадження СЗІ на підприємстві. Розрахувати можливі збитки від реалізації атак на підприємство.	05.12.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 01.09.2020р.

Дата подання до екзаменаційної комісії: 11.12.2020р.

Прийнято до виконання _____ Резніченко Д.О.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка складається з: 110 стр., 29 рис., 5 табл., 40 джерел, 4 додатки.

Кваліфікаційна робота на тему «Методика протидії антропогенним загрозам в ІТС «Біржа медичних працівників»» складається зі вступу, чотирьох розділів, висновків, переліку джерел посилання, додатків.

Загальний обсяг роботи становить 110 сторінок. Список джерел посилання складається з 40 найменувань.

Мета роботи - аналіз особливостей розробки та практичної реалізації комплексної системи інформаційного захисту.

Об’єкт дослідження – проектування системи захисту в ІТС «Біржа медичних працівників».

Предмет дослідження – особливості застосування засобів математичного моделювання для реалізації клієнт-орієнтованих систем інформаційного захисту.

У результаті роботи здійснена програмна реалізація комплексної системи захисту в ІТС «Біржа медичних працівників».

Ключові слова: СИСТЕМА МОНІТОРИНГУ, СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ, КІБЕРБЕЗПЕКА, АВТОМАТИЗОВАНА МОДЕЛЬ, ШТУЧНИЙ ІНТЕЛЕКТ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ІНТЕЛЕКТУАЛЬНІ ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ.

РЕФЕРАТ

Пояснительная записка состоит с: 110 стр., 29 рис., 5 табл., 40 источ., 4 прилож.

Квалификационная работа на тему «Методика противодействия антропогенным угрозам в ИТС «Биржа медицинских работников» состоит из вступления, четырёх разделов, выводов, перечня источников, приложений.

Общий объём работы составляет 110 страниц. Список источников состоит из 40 наименований.

Цель работы — анализ особенностей разработки и практической реализации комплексной системы информационной защиты.

Объект исследования — проектирование системы защиты в ИТС «Биржа медицинских работников».

Предмет исследования — особенности применения средств математического моделирования для реализации клиент-ориентированных систем информационной защиты.

В результате работы совершена программная реализация комплексной системы защиты в ИТС «Биржа медицинских работников».

Ключевые слова: СИСТЕМА МОНИТОРИНГА, СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ, КИБЕРБЕЗОПАСНОСТЬ, АВТОМАТИЗИРОВАНАЯ МОДЕЛЬ, ИСКУССТВЕННЫЙ ИНТЕЛЕКТ, ПРОГРАМНОЕ ОБЕСПЕЧЕНИЕ, ИНТЕЛЛЕКТУАЛЬНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ.

ABSTRACT

The explanatory note consists of: 110 p., 29 pic., 5 tabl., 4 s., 40 ap.

Thesis project on «Methods of combating anthropogenic threats in the ITS» Exchange of Medical Workers» consists of an introduction, four sections, conclusions, a list of reference sources, appendices.

The total volume of the work is 110 pages. The list of reference sources consists of 40 names. The purpose of the work is to analyze the features of the development and practical implementation of a comprehensive information security system.

The object of research is the design of the protection system in the ITS «Medical Workers' Exchange».

The subject of research - features of application of means of mathematical modeling for realization of client-oriented systems of information protection.

As a result of work the program realization of complex system of protection in ITS «Exchange of medical workers» is carried out.

Keywords: MONITORING SYSTEM, INFORMATION PROTECTION SYSTEM, CYBER SECURITY, AUTOMATED MODEL, ARTIFICIAL INTELLIGENCE, SOFTWARE PROTECTION,

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АСК - автоматизована система керування;

БД – база даних;

ІІТ – інтелектуальні інформаційні технології;

ІТС – інформаційно-телекомунікаційна система;

ЕОМ – електронно-обчислювальна машина;

ЕОД – електронний обмін даними;

НМ – нейронна мережа;

ПК – персональний комп'ютер;

СЗІ – система захисту інформації;

СІМ – система інтернет-моніторингу;

СУБД – система управління базою даних;

ШІ – штучний інтелект.

ЗМІСТ

ВСТУП

Актуальність дослідження. На сьогоднішнішній стадії розвитку соціуму інформаційні технології стають невід'ємним атрибутом стрімкого зростання актуальності галузей наукової діяльності, що пов'язані з математичним проектуванням процесів. Створення реальних об'єктів дійсності здебільшого супроводжується значними складностями, що формулюються вже на стадії постановки проблеми. Ці складнощі переважним чином є наслідком недосконалості обчислювальних методів та засобів їх реалізації [8, с. 12].

Варто відмітити, що в умовах сучасних трансформаційних явищ кожного дня створюється все більше компаній. В своїй діяльності вони повсякчас використовують сучасні інтелектуальні інформаційні технології, які є основою функціонування інформаційно-телекомунікаційної системи (ІТС) підприємства. Для оптимізації процесів виробничої діяльності такі структури зацікавлені в тому, щоб якомога більше підвищити ефективність функціонування власної системи захисту інформації (СЗІ), в тому числі за допомогою моніторингу інтернет-середовища. В результаті це сприятиме покращенню продуктивності роботи установи в цілому, а також мінімізує ризики проникнення сторонніх ресурсів та витоків конфіденційних даних, на захист яких витрачається багато часу та матеріальних ресурсів. З іншого боку, для управління корпоративними мережами передачі даних надзвичайно важливою видається можливість отримання достовірної інформації про стан програмного забезпечення і про технічний стан устаткування, який підтримує софт. Саме ці вище перелічені проблеми вирішує впровадження електронної системи інтернет-моніторингу в медичній установі (СІМ) [7, с. 56].

Водночас проблема веб-моніторингу гостро стоїть у всіх системах масового електронного користування, оскільки здійснює суттєвий вплив на економічні показники будь-якої організації незалежно від форми власності та виду діяльності. Наслідками неефективної політики в галузі веб-моніторингу

можуть бути як затримки в діяльності установи, так і цілковита втрата конкурентних переваг та рентабельності бізнесу. Альтернативою вирішення проблеми ефективної продуктивності закладу може стати впровадження автоматизованих стратегії інтернет-моніторингу, адже програмне забезпечення для моніторингу веб-середовища позбавляє медичних працівників від спокуси дивитися онлайн-відео та відвідувати соціальні мережі, обмежуючи доступ до сайтів, які керівництво компанії вважає непотрібними чи загрозливими для бізнесу [4, с. 18].

Крім того, електронні СІМ значно покращують загальну якість виробничого процесу. Такі системи дозволяють оперативно отримувати необхідні відомості та моделювати нові методи захисту ІТС медичної установи, здатні внести корективи у режимі реального часу. Результатом використання автоматизованих СЗІ є поліпшення коефіцієнту корисної праці медпрацівників закладу та мінімізація ризиків проникнення сторонніх з інформаційних ресурсів.

Отже, використання методів системного програмування в процесі впровадження клієнт-сервісних програм підвищує ефективність розробки автоматизованого процесу, сприяє зменшенню матеріальних та часових витрат, допомагає отримувати об'єктивні та оперативні дані в режимі он-лайн. Однак, незважаючи на широкий спектр досліджень в цій галузі, все ще залишаються не вирішеними в повному обсязі питання, пов'язані з розробкою методів і алгоритмів моделювання електронних СЗІ в межах функціонування ІТС медичного закладу. Недостатньо чітко описані задачі створення моделей таких систем, а також особливості їх реалізації.

Виходячи з вищенаведеного, наше дослідження особливостей розробки та практичного застосування системи моніторингу веб-середовища з метою забезпечення інформаційного захисту в ІТС «Біржа медичних працівників» є актуальним.

Мета дослідження – аналіз особливостей розробки та практичної реалізації програми моніторингу веб-середовища для ІТС «Біржа медичних працівників».

Для досягнення мети були поставлені наступні завдання:

1. проаналізувати теоретичні засади дослідження системи захисту інформації та визначити її складові;

2. охарактеризувати принципи інформаційної безпеки;

3. розглянути існуючі моделі захисту ІТС;

4. дослідити алгоритм створення СЗІ на прикладі програми моніторингу веб-середовища для ІТС «Біржа медичних працівників»;

5. спроектувати модель СЗІ для заданих умов та перевірити її ефективність;

6. розробити методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних систем під час створення комплексної системи захисту для медичної установи.

Об'єкт дослідження – проектування системи захисту в ІТС «Біржа медичних працівників».

Предмет дослідження – особливості застосування засобів математичного моделювання для реалізації клієнт-орієнтованих систем інформаційного захисту.

Методи дослідження: методи системного аналізу; аналіз наукової літератури; спостереження; абстрагування; узагальнення.

Теоретично - інформаційну базу дослідження склали праці таких науковців, як В. Антонюк, В. Бабак, В. Бурячок, В. Бугаш, Е. Вентцель, В. Глушков, Г. Конохович, В. Комашинський, Ю. Ліпунцов, О. Лотов, О. Малюк, Г. Поспєлов, Л. Растригін, Д. Рутковська, Б. Совєтов, В. Шаньгін, Л. Ясницький та інших.

Наукова новизна одержаних результатів. Результати дослідження пропонують альтернативний метод використання засобів системного

програмування в процесі розробки СЗІ в медичному закладі на прикладі розробки програми моніторингу веб-середовища.

Практичне значення одержаних результатів полягає в тому, що дослідження грунтується на результатах поглибленого вивчення особливостей застосування штучного інтелекту під час проектування комплекної СЗІ для медичної установи.

Апробація результатів дослідження. Результати дослідження були апробовані на кафедрі безпеки інформації та телекомунікацій Національного технічного університету «Дніпровська політехніка».

Публікації. За результатами наукового дослідження опубліковано наукову статтю.

Структура роботи. Кваліфікаційна робота складається зі вступу, трьох розділів, висновків, переліку джерел посилань, додатків. Загальний обсяг роботи становить 84 сторінки. Перелік джерел посилання складається із 40 найменувань.

РОЗДІЛ 1.
ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ І ПОСТАНОВКА ЗАДАЧІ ДОСЛІДЖЕННЯ

1.1. Поняття системи захисту інформації та її складові

Інформаційна безпека -
це практика захисту інформації шляхом зниження інформаційних ризиків. Це частина управління інформаційними ризиками. Зазвичай це включає запобігання або, принаймні, зниження ймовірності несанкціонованого / несанкціонованого доступу
до даних або незаконного використання, розкриття, порушення, видалення, пошкодження, модифікації, перевірки,
записи або знецінення інформації. Сюди також входять дії, спрямовані на зменшення несприятливих наслідків таких інцидентів. Захищена інформація може приймати будь-яку
форму, наприклад, електронну або фізичну, матеріальну (наприклад, паперову) або нематеріальну (наприклад, знання). Основна увага інформаційної безпеки приділяється збалансованої захисту конфіденційності, цілісності і доступності даних при збереженні акценту на ефективної реалізації політики, і все це без зниження продуктивності організації. Це в значній мірі досягається за рахунок структурованого процесу управління ризиками, який включає [11, с. 25]:

- Виявлення інформації та пов'язаних активів,
а також потенційних загроз, вразливостей і впливів;
- Оцінку ризиків;
- Ухвалення рішення про те,
як усувати або обробляти ризики, тобто уникати, пом’якшувати, розділяти або приймати їх;

- Зниження ризику у разі необхідності, вибір або розробка відповідних заходів безпеки та їх впровадження;

- Моніторинг діяльності, внесення коригувань у міру необхідності для вирішення будь-яких проблем, змін і можливостей поліпшення.

Щоб стандартизувати цю дисципліну, вчені і професіонали спільно пропонують рекомендації, політики і галузеві стандарти щодо паролів, антивірусного програмного забезпечення, брандмауера, програмного забезпечення для шифрування, юридичної відповідальності, обізнаності про безпеку і навчання. Ця стандартизація може бути додатково обумовлена широким спектром законів і нормативних актів, які впливають на доступ до даних, їх обробку, зберігання, передачу і знищення. Однак впровадження будь-яких стандартів і керівництв всередині організації може мати обмежений ефект, якщо не буде прийнята культура постійного поліпшення [24, с. 31].

Слід зазначити, що безпека інформації та інформаційних ресурсів з використанням телекомунікаційної системи або пристроїв означає захист інформації, інформаційних систем або книг від несанкціонованого доступу, пошкодження, крадіжки або знищення. При цьому комп'ютерна безпека, кібербезпека або безпека ІІТ (ІТ-безпека) - це захист комп'ютерних систем і мереж від крадіжки або пошкодження їх обладнання, програмного забезпечення або електронних даних, а також від порушення або неправильного напряму послуг, які вони надають.

Отже, сфера інформаційної безпеки стає все більш важливою через все більшу залежність від комп'ютерних систем, Інтернету і стандартів бездротових мереж, таких як Bluetooth і Wi-Fi, а також через зростання «розумних» пристроїв, включаючи смартфони, телевізори та інші пристрою, що становлять «Інтернет речей». Через свою складність, як з політичної, так і

з технологічної точки зору, кібербезпека є однією з основних проблем в сучасному світі.

1.2. Характеристика принципів інформаційної безпеки

На даний час захист інформації та поняття кібербезпеки перетворилося на одне з найактуальніших завдань високотехнологічного суспільства.

Через широке застосування сучасних ІІТ в усіх галузях свого існування соціум стає вкрай вразливим до незначних кібернетичних атак, які все частіше стають ефективним механізмом несилових методів контролю та керування як об'єктами критичної інфраструктури країни, підприємства, так і окремо взятими людьми. З одного боку, кібербезпека являє собою захист від наявних і потенційно небезпечних вразливостей інформаційного впливу, що моделює небезпеку для різноманітних інформаційних структур, програмних та апаратних інструментів, а також морального стану населення. З іншого боку, кібербезпека являє собою систему заходів, направлених на захист ПК, цифрових даних і мереж їх передавання від несанкціонованого доступу та інших дій, що пов'язані з випадковою чи цілеспрямованою маніпуляцією, крадіжками, блокуванням, поломками, знищенням даних чи ресурсів.

Розглянемо принципи інформаційної безпеки. Серед них такі [29, с. 134]:

1. Конфіденційність.

У сфері інформаційної безпеки конфіденційність є тією властивістю, яка не дозволяє розкривати відомості неавторизованих особам, організаціям або процесам. Хоча ці два слова схожі на «конфіденційність», вони не взаємозамінні. Швидше, конфіденційність -

це компонент конфіденційності, який забезпечує захист наших даних від неа вторизованих відвідувачів. Приклади порушення конфіденційності електронн их даних включають крадіжку ноутбука, крадіжку пароля або відправку конф іденційних електронних листів не тим людям.

2. Цілісність.

В інформаційній безпеці цілісність даних означає підтримку і забезпечення точності і повноти даних протягом усього їх життєвого циклу. Це означає, що дані не можуть бути змінені несанкціонованим або нев иявленим чином. Це не те ж саме, що посилальна цілісність в базах даних, хоча її можна розглядати як окремий випадок узгодженості, як це розуміється в класичній моделі обробки транзакцій ACID. Системи інф ормаційної безпеки зазвичай забезпечують цілісність повідомлень поряд з ко нфіденційністю.

3. Доступність.

Щоб будь-яка інформаційна система досягала своєї мети, інформація повинна бути доступна тоді, коли вона необхідна. Це означає, що обчислювальні системи, які використовуютьс я для зберігання і обробки інформації, заходи безпеки, які використовуються для її захисту, і канали зв'язку, що використовуються для доступу до неї, повинні працювати правильно.

Системи високої доступності прагнуть залишатися доступними в будь-який час, запобігаючи перебої в обслуговуванні через перебої в подачі електр оенергії, відмов обладнання і оновлень системи. Забезпечення доступності та кож включає запобігання атак типу «відмова в обслуговуванні», таких як потік вхідних повідомлень в цільову систему, по суті змушує її вимкнутися.

У сфері інформаційної безпеки доступність часто можна розглядати як одну з найбільш важливих частин успішної програми інформаційної безпеки.

В кінцевому підсумку кінцеві користувачі повинні мати можливість виконувати робочі функції; Забезпечуючи доступність, організація здатна відповідати стандартам, яких очікують зацікавлені сторони організації. Це може включати такі теми, як настройки проксі, зовнішній доступ в Інтернет, можливість доступу до загальних дисків і можливість відправки електронних листів. Керівники часто не розуміють технічну сторону інформаційної безпеки і розглядають доступність як просте рішення, але це часто вимагає співпраці багатьох різних організаційних груп, таких як мережеві операції, операції по розробці, реагування на інциденти і управління політиками / змінами.

4. Фіксація авторства.

Згідно із законом невідмова від авторства має на увазі намір виконати свої зобов'язання за контрактом. Це також має на увазі, що одна сторона транзакції не може заперечувати отримання транзакції, а інша сторона не може заперечувати відправку транзакції. Важливо відзначити, що хоча так і технології, як криптографічні системи, можуть допомогти в зусиллях щодо недопущення відмови від авторства, ця концепція за своєю суттю є правовою концепцією, що виходить за рамки сфери технологій. Наприклад, недостатньо показати, що повідомлення відповідає цифрового підпису, підписаної закритим ключем відправника, і, таким чином, тільки відправник міг відправити повідомлення, і ніхто інший не міг змінити його при передачі (цілісність даних). Передбачуваний відправник може в свою чергу продемонструвати, що алгоритм цифрового підпису вразливий або помилковий, або заявити або довести, що його ключ підпису був скомпрометований. Вина за ці порушення може лежати або не лежати на відправника, і такі твердження можуть або не можуть звільняти відправника від відповідальності, але таке твердження зробить

нечинною твердження про те, що підпис обов'язково доводить справжність і цілісність. Таким
чином, відправник може відхилити повідомлення (оскільки автентичність і цілісність є передумовами неспростовності).

Нижче наведемо приклади статистичних даних відносно загроз з боку несанкціонованого доступу до корпоративних мереж та ПК (Рис. 1.1 – 1.3).

На рисунках 1.1 – 1.3 представимо статистику атак за допомогою мережі Інтернет на ПК, джерела атак та кількість реалізованих атак.

Рисунок 1.1- Статистика атак в мережі Інтернет протягом 2014 - 2020 років

Рисунок 1.2 - Джерела атак на ПК

Рисунок 1.3 – Впроваджені системні атаки в мережі OSI

Таким чином, комплексна СЗІ являє собою набір організаційних, інженерно-технічних механізмів, направлених на забезпечення інформаційної безпеки, що упереджує розголошення, виток та несанкціонований доступ до неї. Така сукупність засобів є неодмінним елементом проектування будь-якої СЗІ.

1.2. Постановка задачі дослідження

Метою є проектування комплексної системи інформаційного захисту медичної установи в ІТС «Біржа медичних працівників».

Ставимо перед собою такі завдання:

1. проаналізувати теоретичні засади дослідження системи захисту інформації та визначити її складові;

2. охарактеризувати принципи інформаційної безпеки;

3. розглянути існуючі моделі захисту ІТС;

4. дослідити алгоритм створення СЗІ на прикладі програми моніторингу веб-середовища для ІТС «Біржа медичних працівників»;

5. спроектувати модель СЗІ для заданих умов та перевірити її ефективність;

6. розробити методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних систем під час створення комплексної системи захисту для медичної установи.

Висновки до розділу 1

Підсумовуючи перший розділ, можемо зробити такі висновки:

1. Визначено, що інформаційна безпека - це практика захисту інформації шляхом зниження інформаційних ризиків. Це частина управління інформаційними ризиками.

2. Надано характеристику принципів інформаційної безпеки.

3. Досліджено, що комплексна СЗІ являє собою набір організаційних, інженерно-технічних механізмів, направлених на забезпечення інформаційної безпеки, що упереджує розголошення, виток та несанкціонований доступ до неї. Така сукупність засобів є неодмінним елементом проектування будь-якої СЗІ.

РОЗДІЛ 2.
ОПИС МЕТОДІВ ТА ЗАСОБІВ ВИРІШЕННЯ ЗАДАЧІ

2.1. Огляд та оцінка існуючих моделей

Автоматизовані медичні системи наразі демонструють потенційно смертельні уразливості, включаючи як внутрішньо діагностичне обладнання , так і імплантовані пристрої, включаючи кардіостимулятори та інсулінові помпи. Є багато повідомлень про зломи лікарень і лікарняних організацій, включаючи атаки шкідливих програм, експлойтів Windows XP, вірусів і витоку конфіденційних даних, що зберігаються на серверах лікарень. Враховуючи вищевикладені обставини, розглянемо детальніше існуючі моделі захисту інформації в медичних установах з метою проектування та реалізації коплексної СЗІ в ІТС «Біржа медичних працівників». Для розробки прототипу пропонується застосовувати програму моніторингу веб-середовища в ІТС «Біржа медичних працівників».

Отже, моніторинг являє собою набір науково-технічних, технологічно-організаційних та інших механізмів, що сприяють забезпеченню систематичного контролю (стеження) за станом та тенденціями розвитку різноманітних процесів.

Моніторинг веб-сайту - це процес тестування і перевірки того, що кінцеві користувачі можуть взаємодіяти з веб-сайтом, як очікується [30, с. 144].

Моніторинг веб-сайтів часто використовується підприємствами для забезпечення очікуваного часу безвідмовної роботи, продуктивності і функціональності веб-сайтів.

Компанії з моніторингу веб-сайтів надають організаціям можливість постійно відстежувати роботу веб-сайту або сервера і спостерігати за його реакцією [22].

Моніторинг часто проводиться з декількох місць по всьому світу на конкретному веб-сайті або сервері, щоб виявляти проблеми, пов’язані із загальною затримкою інтернету, проблемами в мережі, і запобігати помилкові спрацьовування, викликані локальними або міжмережевими проблемами. Моніторингові компанії зазвичай повідомляють про це тестиами у вигляді різних звітів, діаграм і графіків.

При виявленні помилки служби моніторингу відправляють оповіщення по електронній пошті, SMS, телефону, пастці SNMP, пейджера, який може містити діагностичну інформацію, таку як маршрут трасування сеті.захват коду HTML-файлу веб-сторінки, знімок екрана веб-сторінки і навіть відео з помилкою веб-сайту.

Ця діагностика дозволяє мережевим адміністраторам і веб-майстрам швидше вирішувати проблеми.

Моніторинг збирає великі дані про продуктивність веб-сайту, такі як час завантаження, час відгуку сервера, продуктивність елементів сторінки, які часто аналізуються і використовуються для подальшої оптимізації продуктивності веб-сайту.

Задачі веб-моніторингу [18, с. 33]:

Моніторинг необхідний для того, щоб забезпечити доступність веб-сайту для користувачів, мінімізувати час простою і оптимізувати продуктивність.

Користувачі, які покладаються на веб-сайт або додаток для роботи або для задоволення, будуть розчаровані або навіть припинять використовувати додаток, якщо воно ненадійно доступно.

Моніторинг може охоплювати багато речей, які повинні функціонувати з додатком, такі як підключення до мережі, записи системи доменних імен, підключення до бази даних, пропускна здатність і ресурси комп’ютера, так і як вільна пам'ять, завантаження процесора, дисковий простір, події, час відповіді і доступність (або час роботи).

Вимірювання доступності та надійності веб-сайту при різних обсягах трафіку часто називають навантажувальним тестуванням.

Моніторинг веб-сайту також допомагає порівняти веб-сайт з показниками конкурентів, щоб визначити, наскільки добре працює сайт. Швидкість сайту також використовується в якості показника для рейтингу в пошукових системах.

Моніторинг веб-сайту може бути використаний для того, щоб провайдери веб-хостингу відповідали своїм угодами про рівень обслуговування.

Більшість веб-хостів надають гарантію безперебійної роботи на 99,9%, і, якщо тривалість роботи менше, то приватним особам може бути відшкодовано надмірне час простою [13, с. 22].

Зверніть увагу, що не всі хости будуть відшкодовувати приватним особам за надмірне час простою, тому необхідно ознайомитися з умовами обслуговування свого хоста.

Більшість платних служб моніторингу веб-сайтів також пропонують функції безпеки, такі як сканування на наявність вірусів і шкідливих програм, яке набуває все більшого значення в міру того, як веб-сайти стають все більш складними і невід'ємними для бізнесу.

Моніторинг сайту може здійснюватися як усередині, так і зовні корпоративного брандмауера. Традиційні рішення по управлінню мережею зосереджені на моніторингу брандмауера, тоді як зовнішній моніторинг продуктивності буде тестувати і відслідковувати проблеми з продуктивністю через магістраль Інтернету, а в деяких випадках аж до кінцевого користувача.

Сторонні рішення для моніторингу продуктивності веб-сайтів можуть відстежувати внутрішні (за брандмауером), зовнішні (орієнтовані на клієнта) або хмарні веб-додатки [24, с. 31].

Внутрішній моніторинг брандмауера здійснюється за допомогою спеціальних апаратних пристроїв, які можуть допомогти вам визначити, чи викликана повільна продуктивність ваших внутрішніх додатків: проектуванням

додатків, внутрішньою інфраструктурою, внутрішніми програмами або підключеннями до загальнодоступного Інтернету.

Зовнішній моніторинг продуктивності також відомий як моніторинг кінцевого користувача або наскрізний моніторинг продуктивності.

Моніторинг реальних користувачів вимірює продуктивність і доступність, з якими стикаються реальні користувачі, діагностує окремі інциденти і відстежує вплив змін.

Типи моніторингу [28, с. 88]:

Користувачі моніторингу веб-сайту (зазвичай мережеві адміністратори, веб-майстри, співробітники веб-служб) можуть відстежувати одну сторінку веб-сайту, але також можуть відстежувати повний бізнес-процес (часто званий багатокроковими транзакціями).

Отже, вирішенням проблеми забезпечення інформаційної безпеки медичної установи може стати впровадження автоматизованої стратегії інтернет-моніторингу в рамках ІТС «Біржа медичних працівників».

Розглянемо програми з відкритим вихідним кодом, які кожен день доводять свою цінність в мережах будь-якого розміру. Від виявлення пристроїв, моніторингу мережевого обладнання та серверів до виявлення тенденцій у функціонуванні мережі, графічного представлення результатів моніторингу і навіть створення резервних копій конфігурацій комутаторів і маршрутизаторів - це безкоштовні утиліти, що дозволяють здійснювати моніторинг мережі та серверів.

1. Cacti.

Спочатку був MRTG (Multi Router Traffic Grapher) - програма для організації сервісу моніторингу мережі та вимірювання даних з плином часу.

Ще в 1990-х, його автор Тобіас Отікер (Tobias Oetiker) вважав за потрібне написати простий інструмент для побудови графіків, що використовує кільцеву базу даних, спочатку використовуваний для відображення пропускної здатності маршрутизатора в локальній мережі. Так, MRTG породив RRDTool, набір утиліт

для роботи з RRD (Round-robin Database, кільцевої базою даних), що дозволяє зберігати, обробляти і графічно відображати динамічну інформацію, таку як мережевий трафік, завантаження процесора, температура і так далі. Зараз RRDTool використовується у величезній кількості інструментів з відкритим вихідним кодом. Cacti - це сучасний флагман серед програмного забезпечення з відкритим вихідним кодом в області графічного представлення мережі, і він виводить принципи MRTG на принципово новий рівень [23, с. 170].

Рисунок 2.1 – Приклад інтерфейсу Cacti

Cacti - це безкоштовна програма, що входить в LAMP-набір серверного програмного забезпечення, яке надає стандартизовану програмну платформу для побудови графіків на основі практично будь-яких статистичних даних. Якщо будь-який пристрій або сервіс повертає числові дані, то вони, швидше за все, можуть бути інтегровані в Cacti.

Існують шаблони для моніторингу широкого спектру обладнання - від Linux- і Windows-серверів до маршрутизаторів і комутаторів Cisco, - в основному все, що спілкується на SNMP (Simple Network Management Protocol, простий протокол мережевого управління).

Існують також колекції шаблонів від сторонніх розробників, які ще більше розширюють і без того величезний список сумісних з Cacti апаратних засобів і програмного забезпечення. Незважаючи на те, що стандартним методом збору даних Cacti є протокол SNMP, також для цього можуть бути використані сценарії на Perl або PHP.

Фреймворк програмної системи вміло розділяє на дискретні екземпляри збір даних і їх графічне відображення, що дозволяє з легкістю повторно обробляти і реорганізовувати існуючі дані для різних візуальних уявлень [25, с. 65].

Крім того, ви можете вибрати певні часові рамки і окремі частини графіків просто клікнувши на них і перетягнувши.Так, наприклад, ви можете швидко переглянути дані за кілька минулих років, щоб зрозуміти, чи є поточна поведінка мережевого обладнання або сервера аномальним, або подібні показники з'являються регулярно.

Використання Network Weathermap, PHP-плагіну для Cacti, дозволить без надмірних зусиль створювати карти власної мережі в реальному часі, що показують завантаженість каналів зв'язку між мережевими пристроями, що реалізуються за допомогою графіків, які з’являються при наведенні покажчика миші на зображення мережевого каналу.

Багато організацій, що використовують Cacti, виводять ці карти в цілодобовому режимі на 42-дюймові РК-монітори, встановлені на стіні, дозволяючи ІТ-фахівцям миттєво відстежувати інформацію про завантаженість мережі і стан каналу.

Таким чином, Cacti - це інструментарій з великими можливостями для графічного відображення та аналізу тенденцій продуктивності мережі, який можна використовувати для моніторингу практично будь-який контрольованої метрики, що подається у вигляді графіка. Дане рішення також підтримує практично безмежні можливості для настройки, що може зробити його занадто складним при певних застосуваннях.

2. Nagios.

Nagios - це що відбулася програмна система для моніторингу мережі, яка вже багато років знаходиться в активній розробці. Написана на мові C, вона дозволяє робити майже все, що може знадобиться системним і мережевим адміністраторам від пакета прикладних програм для моніторингу.

Веб-інтерфейс цієї програми є швидким та інтуїтивно зрозумілим, в той час його серверна частина - надзвичайно надійною [1, с. 144].

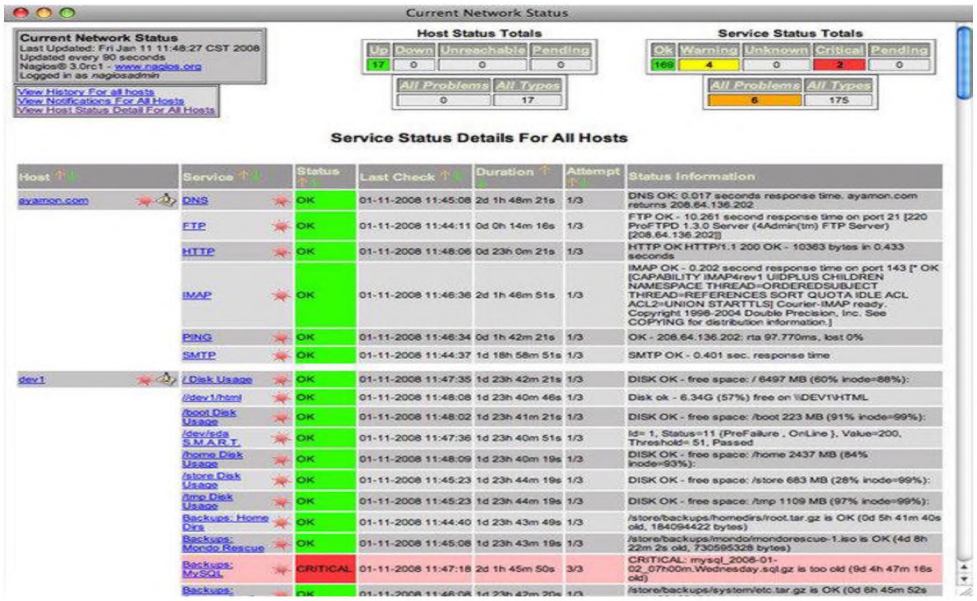


Рисунок 2.2 – Приклад інтерфейсу Nagios

Nagios дозволяє здійснювати постійний моніторинг стану серверів, сервісів, мережевих каналів і всього іншого, що розуміє протокол мережевого рівня IP.

Наприклад, ви можете контролювати використання дискового простору на сервері, завантаженість ОЗУ і ЦП, використання ліцензії FLEXlm, температуру повітря на виході сервера, затримки в WAN і Інтеренет-каналі і багато іншого.

Очевидно, що будь-яка система моніторингу серверів і мережі не буде повноцінною без повідомлень.

У Nagios з цим все в порядку: програмна платформа пропонує настроюється механізм повідомлень по електронній пошті, через СМС та миттєві повідомлення більшості популярних Інтернет-месенджерів, а також схему ескалації, яка може бути використана для прийняття розумних рішень про те, хто, як і при яких обставин повинен бути повідомлений, що при правильному налаштуванні допоможе вам забезпечити багато годин спокійного сну.

Водночас веб-інтерфейс може бути використаний для тимчасового призупинення отримання повідомлень або підтвердження трапилася проблеми, а також внесення заміток адміністраторами.

Крім того, функція відображення демонструє всі контрольовані пристрою в логічному представленні їх розміщення в мережі, з колірним кодуванням, що дозволяє показати проблеми в міру їх виникнення.

Недоліком Nagios є конфігурація, так як її найкраще виконувати за допомогою командного рядка, що значно ускладнює навчання новачків.

Хоча люди, знайомі зі стандартними файлами конфігурації Linux / Unix, особливих проблем випробувати не повинні.

Отже, можливості Nagios величезні, але зусилля по використанню деяких з них не завжди можуть коштувати витрачених на це зусиль.

Переваги системи раннього попередження, що надаються цим інструментом для настільки багатьох аспектів мережі, складно переоцінити.

3. Icinga.

Icinga починалася як відгалуження від системи моніторингу Nagios, але недавно була переписана в самостійне рішення, відоме як Icinga 2.

На даний момент обидві версії програми знаходяться в активній розробці і доступні для використання, при цьому Icinga 1.x сумісна з великою кількістю плагінами і конфігурацією Icinga 2 розроблялася менш громіздкою, з орієнтацією на продуктивність, і більш зручною у використанні.

Вона пропонує модульну архітектуру і багато-дизайн, яких немає ні в Nagios, ні в Icinga 1.

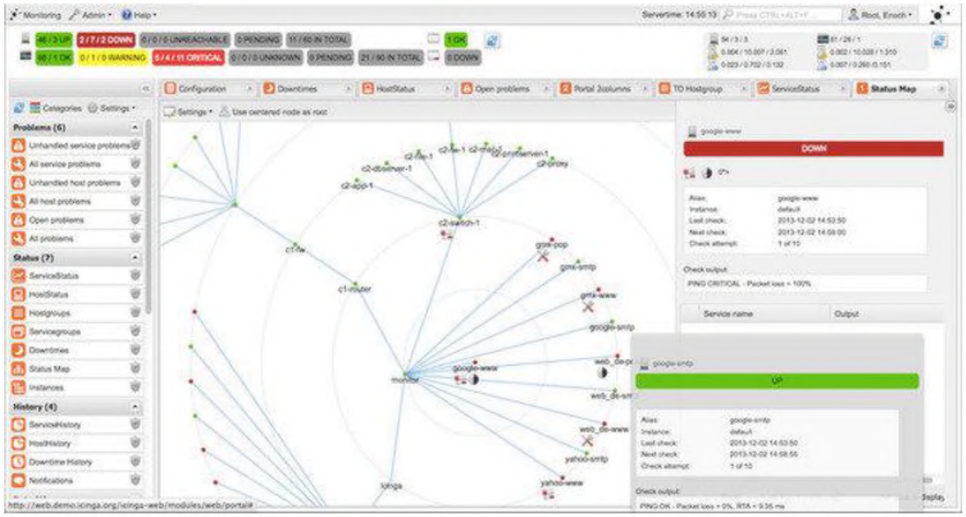


Рисунок 2.3 – Приклад інтерфейсу Icinga

Як і Nagios, Icinga може бути використана для моніторингу за все, що говорить на мові IP, настільки глибоко, наскільки ви можете використовувати SNMP, а також настроюються плагіни і доповнення.

Існує кілька варіацій веб-інтерфейсу для Icinga, але головною відмінністю цього програмного рішення для моніторингу від Nagios є конфігурація, яка може бути виконана через веб-інтерфейс, а не через файли конфігурації.

Для тих, хто вважає за краще управляти своєю конфігурацією поза командного рядка, ця функціональність стане справжнім подарунком.

Icinga інтегрується з безліччю програмних пакетів для моніторингу та графічного відображення, таких як PNP4Nagios, inGraph і Graphite, забезпечуючи надійну візуалізацію вашої мережі.

Крім того, Icinga має розширені можливості звітності.

4. NeDi.

Якщо вам коли-небудь доводилося для пошуку пристроїв у вашій мережі підключатися через протокол Telnet до комутаторів і виконувати пошук по

MAC-адресу, або ви просто хочете, щоб у вас була можливість визначити фізичне розташування певного обладнання (або, що, можливо, ще більш важливо, де воно було розташоване раніше), тоді вам буде цікаво поглянути на NeD [19, с. 54].

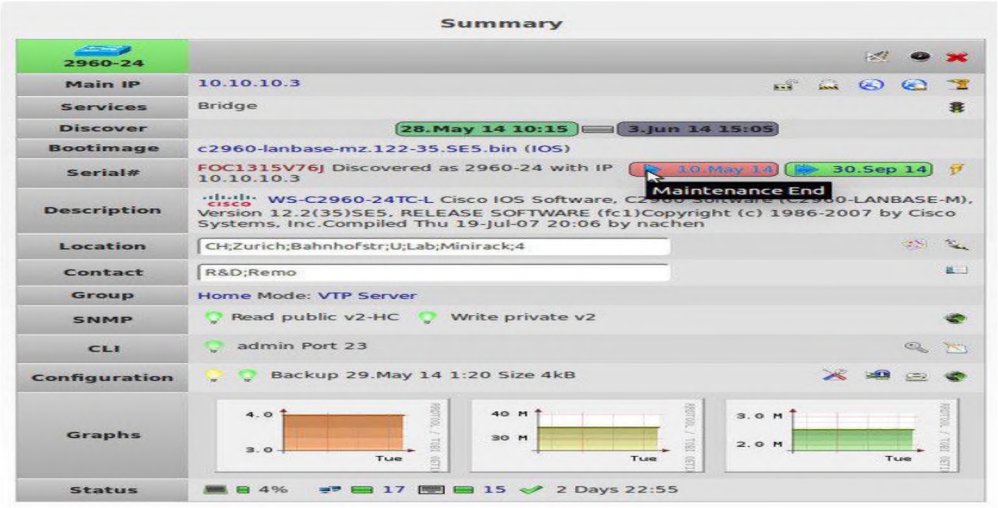


Рисунок 2.4 – Приклад інтерфейсу NeDi

NeDi - це безкоштовне програмне забезпечення, відносить до LAMP, яке регулярно переглядає MAC-адреси і таблиці ARP в комутаторах вашої мережі, каталогізуючи кожне виявлене пристрій в локальній базі даних.

Даний проект не є настільки добре відомим, як деякі інші, але він може стати дуже зручним інструментом при роботі з корпоративними мережами, де пристрої постійно змінюються і переміщаються.

Виявлення запускається процесом cron з заданими інтервалами. Конфігурація проста, з єдиним конфігураційним файлом, який дозволяє значно підвищити кількість налаштувань, в тому числі можливість пропускати пристрої на основі регулярних виразів або заданих меж мережі. NeDi, зазвичай, використовує протоколи Cisco Discovery Protocol або Link Layer Discovery Protocol для виявлення нових комутаторів і маршрутизаторів, а потім підключається до них для збору їхньою інформацією.

Як тільки початкова конфігурація буде встановлена, виявлення пристроїв буде відбуватися досить швидко.

До певного рівня NeDi може інтегруватися з Cacti, тому існує можливість зв'язати виявлення пристроїв з відповідними графіками Cacti.

5. Ntop.

Проект Ntop - зараз для «нового покоління» більш відомий як Ntopng - пройшов довгий шлях розвитку за останнє десятиліття. Але назвіть його як хочете - Ntop або Ntopng, - в результаті ви отримаєте першокласний інструмент для моніторингу мережевого трафіку в парі з швидким і простим веб-інтерфейсом.

Він написаний на C і повністю самодостатній. Ви запускаєте один процес, налаштований на певний мережевий інтерфейс, і це все, що йому потрібно.

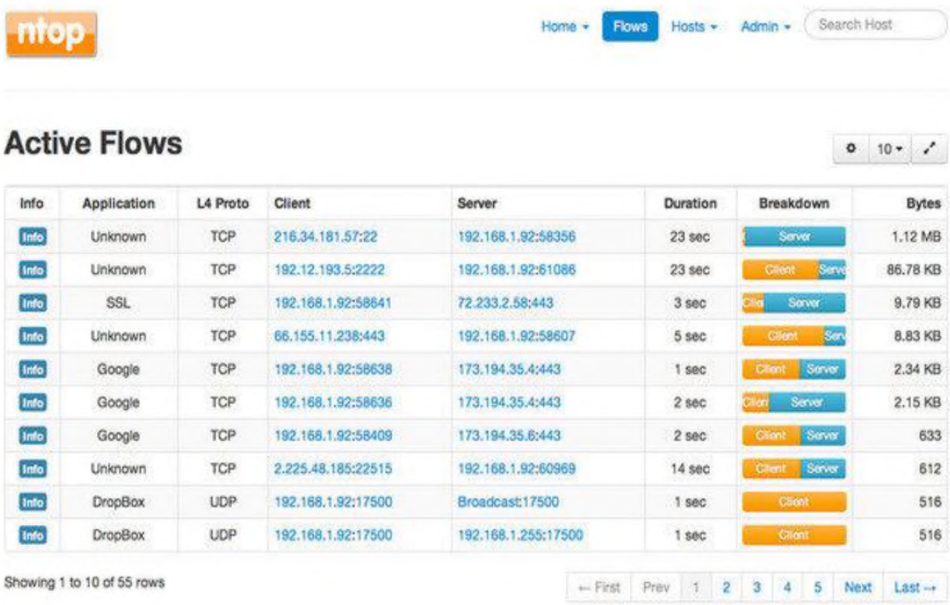


Рисунок 2.5 – Приклад інтерфейсу Ntop

Ntop - це інструмент для аналізу пакетів з легким веб-інтерфейсом, який показує дані в реальному часі про трафік мережі. Інформація про потік даних через хост і про з'єднання з хостом також доступні в режимі реального часу.

Ntop надає легко засвоювані графіки і таблиці, що показують поточний і минулий мережевий трафік, включаючи протокол, джерело, призначення та історію конкретних транзакцій, а також хости з обох кінців.

Крім того, в наявності вражаючий набір графіків, діаграм і карт використання мережі в реальному часі, а також модульну архітектуру для величезної кількості надбудов, таких як додавання моніторів NetFlow і sFlow.

Тут навіть можна знайти Nbox - апаратний монітор, який вбудовує в Ntop.

Крім того, Ntop включає API-інтерфейс для скриптового мови програмування Lua, який може бути використаний для підтримки розширень. Ntop також може зберігати дані хоста в файлах RRD для здійснення постійного збору даних.

Одним з найбільш корисних застосувань Ntopng є контроль трафіку в конкретному місці.

Наприклад, коли на вашій карті мережі частина мережевих каналів підсвічені червоним, але ви не знаєте чому, ви можете за допомогою Ntopng отримати щохвилинний звіт про проблемний сегменті мережі і одразу дізнатися, які хости відповідальні за проблему.

Користь від такого контролінгу мережі складно переоцінити, а отримати її дуже легко.

По суті, ви можете запустити Ntopng на будь-якому інтерфейсі, який був налаштований на рівні комутатора, для моніторингу іншого порту або VLAN. От і все.

6. Zabbix.

Zabbix - це повномасштабний інструмент для мережевого і системного моніторингу мережі, який об’єднує декілька функцій в одній веб-консолі.

Він може бути налаштований для моніторингу та збору даних з різних серверів і мережевих пристроїв, забезпечуючи обслуговування і моніторинг продуктивності кожного об'єкта [33, с. 170].

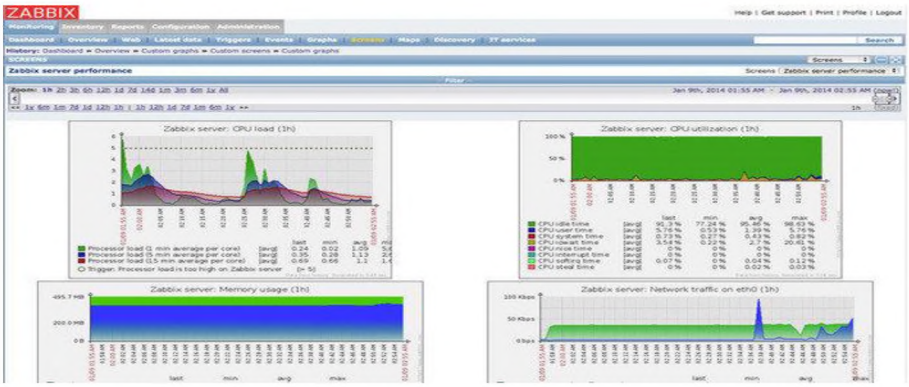


Рисунок 2.6 – Приклад інтерфейсу Zabbix

Zabbix дозволяє робити моніторинг серверів і мереж за допомогою широкого набору інструментів, включаючи моніторинг гіпервізора віртуалізації і стеків веб-додатків. В основному, Zabbix працює з програмними агентами, запущеними на контрольованих системах. Але це рішення також може працювати і без агентів, використовуючи протокол SNMP або інші можливості для здійснення моніторингу.

Zabbix підтримує VMware і інші Гіпервізор віртуалізації, надаючи докладні дані про продуктивність гипервизора і його активності. Особлива увага також приділяється моніторингу серверів додатків Java, веб-сервісів і баз даних.

Хости можуть додаватися вручну або через процес автоматичного виявлення. Широкий набір шаблонів за замовчуванням застосовується до найбільш поширеним варіантам використання, таким як Linux, FreeBSD і Windows-сервера; широко-використовувані служби, такі як SMTP і HTTP, а також ICMP і IPMI для докладного моніторингу апаратної частини мережі.

Крім того, призначені для користувача перевірки, написані на Perl, Python або майже на будь-якому іншому мовою, можуть бути інтегровані в Zabbix.

Zabbix дозволяє налаштовувати панелі моніторингу та веб-інтерфейс, щоб сфокусувати увагу на найбільш важливих компонентах мережі. Відомості та ескалації проблем можуть грунтуватися на настроюються діях, які застосовуються до хостів або групам хостів. Дії можуть навіть налаштовуватися

для запуску віддалених команд, тому якийсь ваш сценарій може запускатися на контрольованому хості, якщо спостерігаються певні критерії подій.

Програма відображає у вигляді графіків дані про продуктивність, такі як пропускна здатність мережі та завантаження процесора, а також збирає їх для настроюються систем відображення.

Крім того, Zabbix підтримує настроюються карти, екрани і навіть слайд-шоу, що відображають поточний статус контрольованих пристроїв. Zabbix може бути складним для реалізації на початковому етапі, але розумне використання автоматичного виявлення і різних шаблонів може частково полегшити труднощі з інтеграцією.

На додаток до встановлюваного пакету, Zabbix доступний як віртуальний пристрій для декількох популярних гіпервізора.

7. Observium.

Observium - це програма для моніторингу мережевого обладнання та серверів, яке має величезний список підтримуваних пристроїв, що використовують протокол SNMP. Як програмне забезпечення, що відноситься до LAMP, Observium відносно легко встановлюється і налаштовується, вимагаючи звичайних установок Apache, PHP і MySQL, створення бази даних, конфігурації Apache і тому подібного [38, с. 17].

Він встановлюється як власний сервер з виділеною URL-адресою.

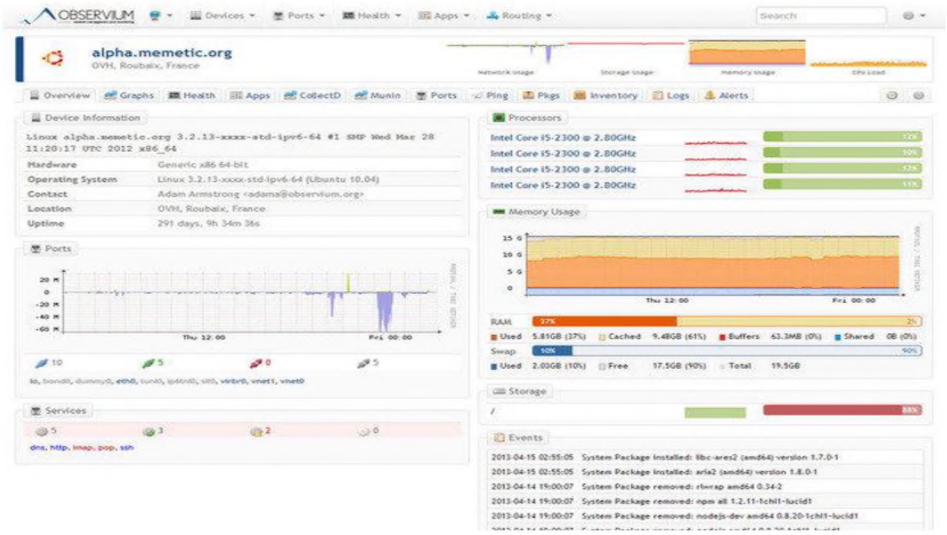


Рисунок 2.7 – Приклад інтерфейсу Observium

Observium поєднує в собі моніторинг систем і мереж з аналізом тенденцій продуктивності. Він може бути налаштований для відстеження практично будь-яких показників.

Можна увійти в графічний інтерфейс і почати додавати хости і мережі, а також задати діапазони для автоматичного виявлення і дані SNMP, щоб Observium міг досліджувати навколишні його мережі і збирати дані по кожній виявленій системі.

Observium також може виявляти мережеві пристрої через протоколи CDP, LLDP або FDP, а віддалені агенти хоста можуть бути розгорнуті на Linux-системах, щоб допомогти в зборі даних.

Все ця зібрана інформація доступна через легкий у використанні призначений для користувача інтерфейс, який надає просунуті можливості для статистичного відображення даних, а також у вигляді діаграм і графіків. Ви можете отримати будь-що: від часу відгуку ping і SNMP до графіків пропускної здатності, фрагментації, кількості IP-пакетів.

В залежності від пристрою, ці дані можуть бути доступні аж для кожного виявленого порту.

Що стосується серверів, то для них Observium може відобразити інформацію про стан центрального процесора, оперативної пам'яті, сховища даних, свопу, температури. З журналу подій Ви також можете включити збір даних і графічне відображення продуктивності для різних сервісів, включаючи Apache, MySQL, BIND, Memcached, Postfix і інші.

Observium відмінно працює як віртуальна машина, тому може швидко стати основним інструментом для отримання інформації про стан серверів і мереж. Це відмінний спосіб додати автоматичне виявлення і графічне представлення в мережу будь-якого розміру.

8. Internet Access Monitor.

Це програма моніторингу використання веб-середовища. За статистикою, найбільш типовим способом виходу в Інтернет для сучасних організацій є використання спеціальних програм-шлюзів (proxy servers), що дозволяють розділити єдине Інтернет-підключення між усіма співробітниками офісу.

Аналізуючи лог файли, створювані даними програмами, Internet Access Monitor дозволяє швидко і просто видавати звіти про те хто, коли і які сайти відвідував.

Також програма покаже, що саме більшу частину часу робив співробітник - читав тексти, розглядав картинки, слухав музику або дивився кліпи.

Програма вміє створювати такі види звітів [23, с. 53]:

- Розподіл трафіку по користувачам;
- Розподіл трафіку по IP адресам;
- Розподіл трафіку по сервісів;
- Розподіл трафіку по протоколах;
- Розподіл трафіку по типу даних

  - картинки,
  - відео,
  - тексти,
  - музика;

- Розподіл трафіку за програмами, використовуваними користувачами;
- Розподіл трафіку по часу доби;
- Розподіл трафіку по днях тижня;
- Розподіл трафіку по датах і місяцях;
- Розподіл трафіку по сайтам, за якими ходив користувач;
- Помилки авторизації в системі;
- Входи і виходи із системи;

а також ще цілий ряд звітів.

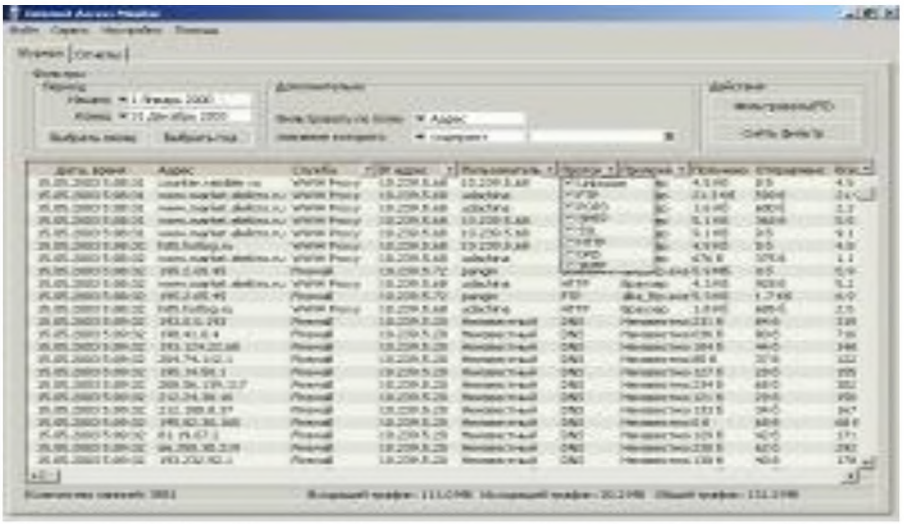


Рисунок 2.8 – Приклад програми Internet Access Monitor

Отже, на сьогоднішній день існує велика кількість моделей для моніторингу веб-середовища, проте багато з них мають труднощі відносно програмної реалізації та обмеженого функціоналу.

2.2. Підходи до проектування системи та алгоритм її створення

Повноцінна розробка нового програмного рішення є доволі ресурсовитратною та вимагає залучення додаткових фахівців, що неухильно тягне за собою надмірні витрати часу. Вищевикладені вимоги можуть бути реалізовані в рамках існуючих програмних продуктів. В даному проекті раціональніше за все буде використовувати вже наявні системи.

Впровадження готового рішення дозволить скоротити час, оскільки відсутні етапи розробки та налагодження програми.

Таким чином, поставлена задача зводиться до вибору системи (Комплексу систем), що задовольняє заданим вимогам.

Принцип роботи системи побудований на архітектурі клієнт-сервер. Клієнтська частина даної автоматизованої системи функціонує в фоновому режимі.

З заданим тимчасовим інтервалом клієнтська частина проводить перевірку стану обладнання і за запитом відсилає отримані дані на сервер.

Попередньо необхідно упевнитися, що для впровадження обраної системи присутні всі пакети, необхідні для серверного програмного забезпечення, тобто LAMP. Необхідні компоненти: - Apache - MySQL - PHP Для їх інсталяції можна використовувати системну команду apt-get
(aptitude):

– % sudo apt-get install apache2

– % sudo apt-get install libapache2-mod-php5

– sudo apt-get install mysql-server

– sudo apt-get install mysql-client

– sudo apt-get install php5-mysql

Проведення попередніх випробувань:

Після проведення підготовчих дій можлива установка обраної системи моніторингу обладнання - GLPI:

– sudo apt-get install glpi

В процесі установки з'явиться вікно налаштування бази даних для системи (Рис. 2.9).

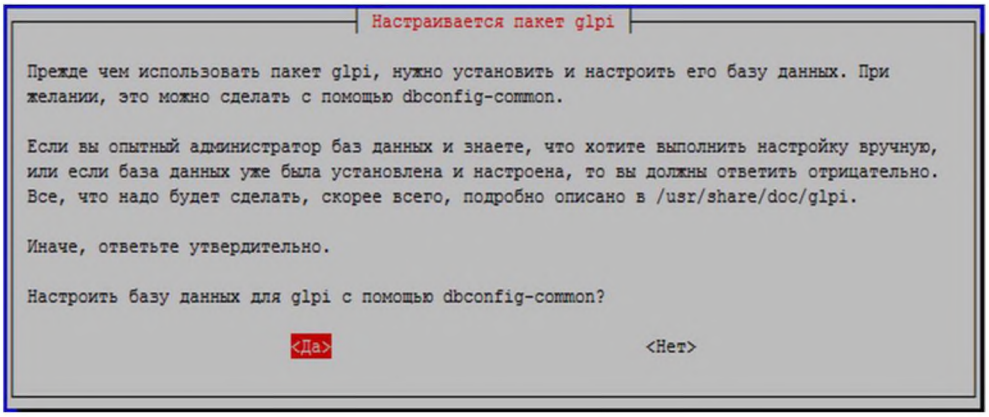


Рисунок 2.9 – Вікно налаштування бази даних

Вхід в веб-інтерфейс.

Тепер можна увійти в веб-інтерфейс системи GLPI. Для цього необхідно в браузері ввести:

– http://10.0.4.123/glpi/

З'явиться запит на введення імені користувача і пароля для аутентифікації в веб-інтерфейсі. Далі відбувається процес налаштування користувачів.

Спочатку необхідно налаштувати відповідні права доступу і права управління на профіль адміністратора. Для цього в розділі адміністрування створюється новий користувач (Рис. 2.10).

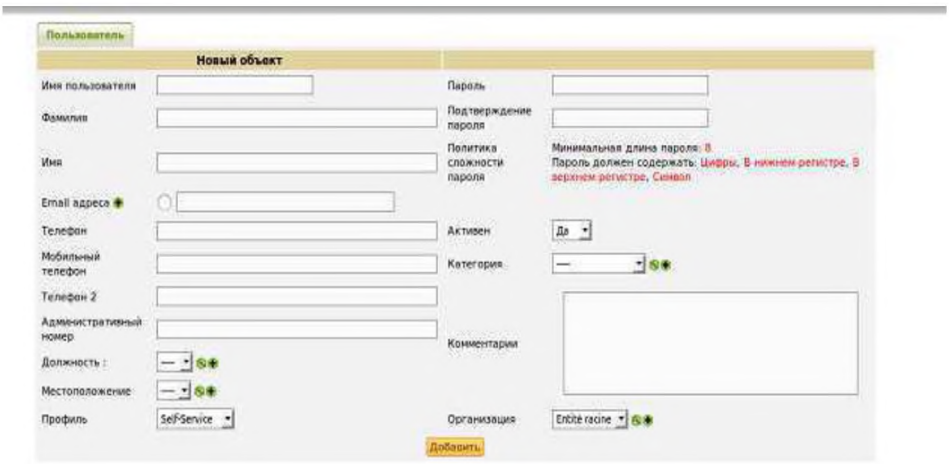


Рисунок 2.10 – Створення нового користувача

Налаштування груп користувачів.

З метою структурування обладнання необхідно ввести групи, які будуть являти собою повний список підрозділів (відділів) організації.

У розділі Адміністрування / Групи додається новий користувач (Рис. 2.11).

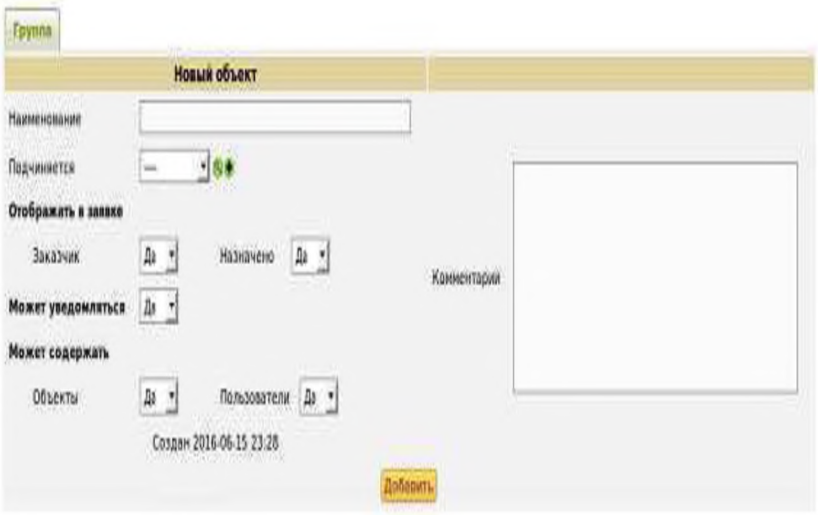


Рисунок 2.11 – Створення нової групи користувачів

Отже, для програмної реалізації системи моніторингу веб-середовища нами було обрано програму Zabbix, яка являє собою повномасштабний інструмент для мережевого і системного моніторингу мережі, який об'єднує декілька функцій в одній веб-консолі.

2.3. Розрахунок надійності захисних бар'єрів

В сучасних медичних установах впроваджується системи передачі даних, а також їх зберігання. Це дозволяє оптимізувати виробничий процес та реалізовувати нові автоматизовані системи. Із збільшенням цифрових технологій збільшується кількість загроз збоку конкурентів, виходу із ладу програм, набирає загрозливих масштабів шпигунство. Для зменшення цих

загроз варто пердметніше проаналізувати всі види загроз та спроектувати заходи щодо забезпечення інформаційної безпеки в медичному закладі. Тому варто охарактеризувати проникнення зловмисника на територію підприємства. Необхідні дані віднесемо до наступних пунктів.

1. параметри СІЗ передачі інформації медичної установи:

a) Надійність існуючих СІЗ в закладі:

b) Інтенсивність відмови компонентів СІЗ установи: 1 раз в 365 діб

c) Період профілактичних робіт: 182 діб;

d) Тривалість виконання робіт: 8 діб;

e) Тривалість відновлення системи сигналізації після пошкодження: 12 год.;

Зведено вартість даних, що зберігаються в межах медичної установи (табл. 2.1)

Таблиця 2.1

Вартість інформації яка зберігається у приміщеннях

№ кімнати	1	2	3	4	5	6	Усього
Вартість (грн.)	600	2200	2500	3000	2000	500	10800

Час необхідний для подолання бар'єра захисту (табл. 2.2)

Таблиця 2.2

Необхідний період часу для подолання захисних бар'єрів

№ кімнати	Назва захисного бар'єра						
	Вікна (решітки)		Двері				Вхідні двері
	1	2	1	2	5	4	
1			16	19	20	19	28
2	20		16	13			
3	21		13				
4	20		19				
5			20				
6	23		19				

Час реакції охорони на проникнення та видалення зловмисника (табл. 2.3).

Таблиця 2.3

Час реакції охорони на проникнення зловмисника

№ кімнати	1	2	3	4	5	6
Час (хв.)	3	4	6	6	5	4

2.4. Аналіз моделі поведінки зловмисника (внутрішні та зовнішні)

Для розрахунку необхідно зробити топологічний план приміщення медичної установи та нанести на нього вірогідності проникнення зловмисника та реакції охорони. Топологічний план є елементом приміщення медичної установи, що охороняється, і зв'язки між ними, визначаючи можливості переходу з одного елемента в інший або проникнення з зовнішнього середовища. Модель побудуємо на підставі плану приміщення який наведений на рис 2.12. Таким чином топологічна модель приміщення являє собою графу, вершини якої відповідають кімнатам медичної установи, а зв'язки між ними відповідають можливості переходу зловмисника між ними. Кожному захисному елементу простору протиставляють стан зловмисника у процесі здійснення злочину.

A_i – заходження зловмисника у певному приміщені.

A_0 – стан коли зловмисник знаходиться поза охороняємим об'єктом. Проникнення в установу можна здійснити по декільком шляхам – через головний вхід та через вікна. Двері медичної установи оснащені датчиками сигналізації та замками. Вікна оснащені металевими решітками та сигналізацією. Спрацювання сигналізації відображається на пульті керування охорони. На основі даних таблиці 2 та моделі приміщення побудуємо топологічну модель медичної установи у вигляді графу. Шлях, який обирає зловмисник. залежить від багатьох факторів таких як ціль проникнення, наявні

засоби захисту, технічна оснастка зловмисника. В умовах невизначеності відносно вибору зловмисника початку шляху проникнення приймемо вірогідність вибору того чи іншого напряму дії рівними.

Далі розрахуємо доступ до окремих топологічних елементів.

Для моделювання та розрахунку будемо використовувати математичну програму Mathcad15. Проведемо розрахунок вірогідності знаходження зловмисника у кожному з приміщень медичного закладу. Для цього виконаємо наступні розрахунки у програмі Mathcad 15. Зведемо значення вірогідності та інтенсивності проникнення в таблицю (Табл.2.4).

Таблиця 2.4

Значення вірогідності та інтенсивності проникнення

I -- приміщення	J -- приміщення	λ	$P_{\lambda}(i) := \lambda_i \cdot \Delta t$
0	1	0.036	0.044
0	2	0.05	0.061
0	3	0.048	0.059
0	4	0.05	0.061
0	6	0.043	0.053
1	2	0.063	0.077
1	4	0.053	0.065
1	5	0.05	0.061
1	6	0.053	0.065
2	1	0.063	0.077
2	3	0.077	0.094
3	2	0.077	0.094
4	1	0.053	0.065
5	1	0.05	0.061
6	1	0.053	0.065

Знайдемо інтенсивність проникнення зловмисника у певний топологічний елемент медичної установи на основі даних таблиці 2.4 до таблиці 2.5. Використаємо для проектування Mathcad 15.

Задамо час, що необхідний зловмиснику для проникнення та час реакції охорони. Також врахуємо можливість того що зловмисник може швидше проникнути на територію тому додамо деякі елементи управління за допомогою яких будемо регулювати час як для охорони так і для зловмисника. За

допомогою двох регуляторів «w» та «h» ми можемо змінити час для охорони та зловмисника.

Виходячи з отриманих часових характеристик, можемо знайти інтенсивність проникнення та реакції охорони. Отримавши значення інтенсивностей знайдемо час переходу зловмисника з одного приміщення до іншого.

$$\Delta t := \frac{1}{\sum_{i=0}^{14} \lambda(i)}$$

$$\Delta t = 0.261$$

Для подальшого розрахунку нам потрібно знайти вірогідність реакції охорони та зловмисника.

$$P_\lambda(i) := \lambda(i) \cdot \Delta t$$

$$P_\mu(j) := \mu(j) \cdot \Delta t$$

Таблиця 2.5

Матриця станів

	A_0	A_1	A_2	A_3	A_4	A_5	A_6
A_0	1	1	1	1	1	0	1
A_1	1	1	1	0	1	1	1
A_2	1	1	1	1	0	0	0
A_3	1	0	1	1	0	0	0
A_4	1	1	0	0	1	0	0
A_5	1	1	0	0	0	1	0
A_6	1	1	0	0	0	0	1

$$i := 0..4$$

$$Pd_0 := \sum_i P_\lambda(i) = 0.2$$

$$j := 0 \qquad i := 5..8$$

$$Pd_1 := P_\mu(j) + \left(1 - P_\mu(j)\right)\cdot\left(\sum_i P_\lambda(i)\right) = 0.317$$

$j := 1 \qquad i := 9..10$

$$Pd_2 := P_\mu(j) + \left(1 - P_\mu(j)\right)\cdot\left(\sum_i P_\lambda(i)\right) = 0.268$$

Для подальших розрахунків складемо матрицю вектору початкових станів.

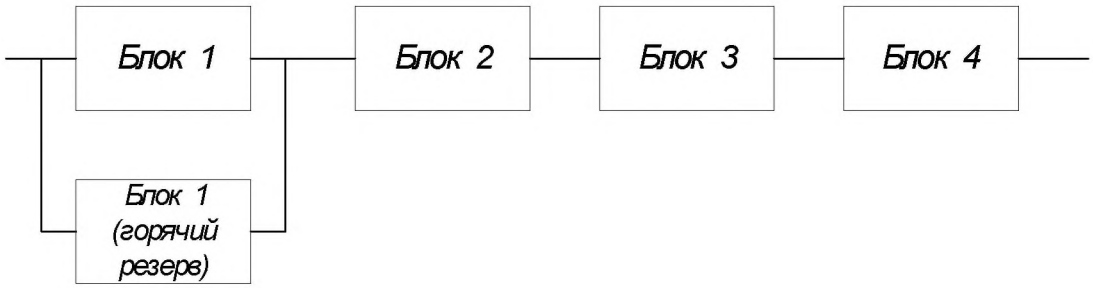
$j := 2 \qquad i := 11$

$$M := \left(1 - Pd_0 \;\; P_\mu(0) \;\; P_\mu(1) \;\; P_\mu(2) \;\; P_\mu(3) \;\; P_\mu(4) \;\; P_\mu(5)\right)$$

$$Pd_3 := P_\mu(j) + \left(1 - P_\mu(j)\right)\cdot P_\lambda(i) = 0.168$$

Далі розрахуємо надійність системи сигналізації медичної установи.

$j := 3 \qquad i := 12$ Структурна схема для розрахунку надійності окремої гілки системи сигналізації медичної установи. Розіб'ємо її на чотири блоки (рис.2.12):



$$Pd_4 := P_\mu(j) + \left(1 - P_\mu(j)\right)\cdot P_\lambda(i) = 0.106$$

Рисунок 2.12 - Блок схема сигналізації медичної установи

$j := 4 \qquad i := 13$

$$Pd_5 := P_\mu(j) + \left(1 - P_\mu(j)\right)\cdot P_\lambda(i) = 0.102$$

- Блок 1 – датчики.

$j := 5 \qquad i := 14$

- Датчик відкриття дверей

$$Pd_6 := P_\mu(j) + \left(1 - P_\mu(j)\right)\cdot P_\lambda(i) = 0.126$$

- Датчик руху

- Блок 2 – лінія зв'язку, по яким передається сигнал от датчиків на центральний пульт;
- Блок 3 – пульт охоронної сигналізації;
- Блок 4 – блок живлення;

Використовуючи данні на початку розділу, знайдемо інтенсивності безвідмовної роботи комплексу.

В результаті отримуємо інтенсивність роботи кожного блоку. Побудуємо графіки інтенсивності відмов кожного елемента.

Глибина контролю датчика рівна 0 (q_1=0), оскільки датчик не контролюється, а будь яка відмова лінії зв'язку, пульта охоронної сигналізації та блока живлення визначається автоматично, тому значення глибини їх контролю можуть прирівняні до одиниці.

Побудуємо графік залежності глибини контролю від часу (рис. 2.13).

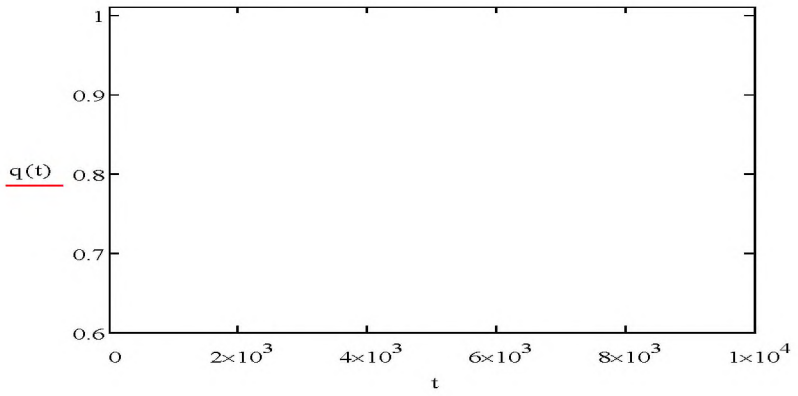


Рисунок 2.13 - Залежність глибини контролю комплексу від часу

Далі розрахуємо коефіцієнти готовності та коефіцієнта простою системи.

Використовуючи вище отримані дані оцінимо коефіцієнт готовності системи охороною сигналізації та розглянемо шляхи його підвищення за рахунок вибору оптимального періоду проведення профілактичних робіт.

Глибина контролю датчика рівна 0 (q_1=0), оскільки датчик не контролюється, а будь яка відмова лінії зв'язку, пульта охоронної сигналізації та

блока живлення визначається автоматично, тому значення глибини їх контролю можуть прирівняні до одиниці. Інтенсивність відмов комплексу визначається по наступним формулам. Профілактичні роботи у приміщені проводяться 2 рази на рік, тоді випливає і інтенсивність профілактичних робіт рівна:

$$L_{p0} := \frac{2}{24 \cdot 365} = 2.283 \times 10^{-4}$$

Визначимо показники системи до моменту початку профілактичних робіт. Час напрацювання до початку профілактичних робіт буде становити:

$$T_{p0} := \frac{1}{L_{p0}} = 4380$$

$$q_1 := 0 \qquad q_2 := 1$$

$$q(t) := \frac{q_1 \cdot \lambda_1(t) + q_2 \lambda_2(t) + q_2 \cdot \lambda_3(t) + q_2 \cdot \lambda_4(t)}{\lambda_1(t) + \lambda_2(t) + \lambda_3(t) + \lambda_4(t)}$$

Визначаємо інтенсивність профілактичних робіт для кожного з компонентів комплексу:

$$\lambda 2\left(T_{p0}\right) := \frac{\left[\frac{d}{dT_{p0}}\left(1 - p_2\left(T_{p0}\right)\right)\right]}{p_2\left(T_{p0}\right)}$$

$$\lambda 2\left(T_{p0}\right) = 5.708 \times 10^{-5}$$

$$\lambda 3\left(T_{p0}\right) := \frac{\left[\frac{d}{dT_{p0}}\left(1 - p_3\left(T_{p0}\right)\right)\right]}{p_3\left(T_{p0}\right)}$$

$$\lambda 3\left(T_{p0}\right) = 1.142 \times 10^{-4}$$

$$\lambda 4\left(T_{p0}\right) := \frac{\left[\frac{d}{dT_{p0}}\left(1 - p_4\left(T_{p0}\right)\right)\right]}{p_4\left(T_{p0}\right)}$$

$$\lambda 4\left(T_{p0}\right) = 3.805 \times 10^{-5}$$

Встановимо параметри системи технічного обслуговування. Профілактичні роботи проводяться на протязі 8 годин, тоді можна визначити інтенсивність обслуговування:

$$M_p := \frac{1}{8}$$

У випадку наявності неполадок комплексу систему ремонтують на протязі 1,5 діб, тоді інтенсивність відновлення становить:

$$M_b := \frac{1}{36}$$

Визначаємо склад аналізованих станів комплексів:

H_0 – робочий стан;

H_1 – стан контролюємої відмови;

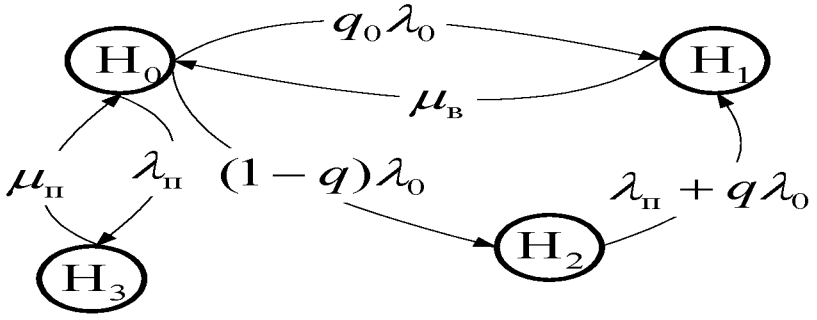
$$\lambda 1\left(T_{p0}\right) := \frac{\left[\frac{d}{dT_{p0}}\left(1 - p_1\left(T_{p0}\right)\right)\right]}{p_1\left(T_{p0}\right)}$$

$$\lambda 1\left(T_{p0}\right) = 6.447 \times 10^{-5}$$

H_2 – стан неконтролюємої відмови;

H_3 – стан проведення профілактичних робіт;

Складемо діаграму, яка моделює поведінку системи з урахування процесів технічного обслуговування.



З отриманого графу визначимо коефіцієнт готовності та простою.

Інтенсивність обслуговування всього комплексу та глибину контролю в період обслуговування.

$$\lambda 0\left(T_{p0}\right) := \frac{\left[\frac{d}{dT_{p0}}\left(1 - P\left(T_{p0}\right)\right)\right]}{P\left(T_{p0}\right)}$$

$$q0\left(T_{p0}\right) = 0.765$$

$$q0\left(T_{p0}\right) := \frac{q_1 \cdot \lambda_1\left(T_{p0}\right) + q_2 \lambda_2\left(T_{p0}\right) + q_2 \cdot \lambda_3\left(T_{p0}\right) + q_2 \cdot \lambda_4\left(T_{p0}\right)}{\lambda_1\left(T_{p0}\right) + \lambda_2\left(T_{p0}\right) + \lambda_3\left(T_{p0}\right) + \lambda_4\left(T_{p0}\right)}$$

$$\lambda 0\left(T_{p0}\right) = 2.738 \times 10^{-4}$$

Визначимо оптимізаційний період профілактичних робіт.

Оптимальна інтенсивність та період профілактичних робіт при заданих параметра обслуговування та очікування буде рівним:

$$a1\left(T_{p0}\right) := \frac{q_1 \cdot \lambda_1\left(T_{p0}\right) + q \lambda_2\left(T_{p0}\right) + q \cdot \lambda_3\left(T_{p0}\right) + q \cdot \lambda_4\left(T_{p0}\right)}{\lambda_1\left(T_{p0}\right) + \lambda_2\left(T_{p0}\right) + \lambda_3\left(T_{p0}\right) + \lambda_4\left(T_{p0}\right)}$$

$$a1\left(T_{p0}\right) = 0.765$$

$$L_p := \sqrt{\lambda_{k1}\left(T_{p0}\right)} \cdot \sqrt{M_p} \cdot \sqrt{1 - a1\left(T_{p0}\right)} = 0.003$$

$$T_p := \frac{1}{L_p} = 352.27$$

$$K_{p0} := 1 - \frac{1}{1 + \frac{L_p}{M_p} - \frac{\lambda_{k1}\left(T_{p0}\right)}{L_p} + \frac{\lambda_{k1}\left(T_{p0}\right) \cdot a1\left(T_{p0}\right)}{L_p} + \frac{\lambda_{k1}\left(T_{p0}\right)}{M_b}}$$

$$K_{p0} = 0.01$$

$$K_{g0} := 1 - K_{p0}$$

$$K_{g0} = 0.99$$

Отримані значення періода профілактичних робіт дорівнюють 353 годинам. При цьому оптимальний коефіцієнт простою 0,052, а коефіцієнт готовності 0,948.

Далі розрахуємо потенційні втрати та отримаємо значення збитку до та після оптимізації. Результати оптимізації представимо у вигляді рисунку 2.14.

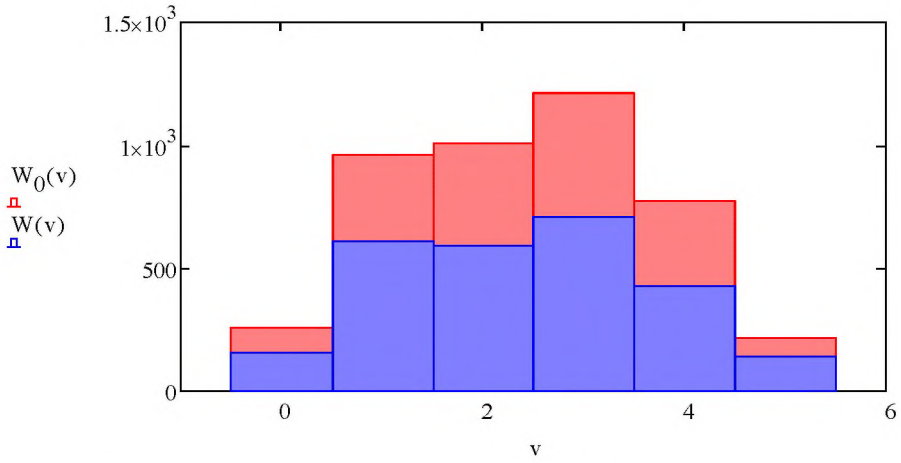


Рисунок 2.14 - Графік збитку по втраті інформації в кожному приміщенні медичної установи

Знайдемо коефіцієнт корисного використання системи захисту інформації:

$$W_0 := \sum_v W0(v)$$

$$W := \sum_v W(v)$$

$$W = 2.635 \times 10^3$$

$$K := \frac{W_0}{W} = 1.68$$

$$W_0 = 4.428 \times 10^3$$

Тобто після оптимізації системи ми можемо знизити ризик на 1,68 разів .

Розглянутий метод дозволяє проаналізувати будь-яке приміщення медичної установи та провести оптимізацію його системи охорони та проаналізувати можливі втрати інформації.

Варто додати, що IoT - всі ці пристрої та обладнання, що підключається до Інтернету і один до одного в мережі медичної установи- створили нові можливості для кіберзлочинців. Ніхто не хоче, щоб хакер проник в їх мережу IoT. Розглянемо кілька сценаріїв розвитку подій.

1. Проблема: VPNFilter може встановлювати шкідливе ПО на пристрої та системи, підключені до маршрутизатора медичної установи, - обладнання, що забезпечує зв'язок між підключеними пристроями та Інтернетом. Це може зробити маршрутизатор закладу непрацездатним. Він також може збирати інформацію, що проходить через маршрутизатор медичної установи. І це може заблокувати мережевий трафік і вкрасти паролі АСУ медичним закладом.

Рішення: у Symantec є безкоштовний онлайн-інструмент, який допоможе перевірити, чи не впливає VPNFilter на маршрутизатор ІТС «Біржа медичних працівників».

2. Проблема: кіберзлочинці можуть скористатися наявними можливостями пристроїв IoT ІТС «Біржа медичних працівників».

Вищеокреслені приклади показують, що кіберзлочинці можуть діяти локально і глобально. Вони можуть проникнути у пристрої IoT медичного закладу, щоб заподіяти йому шкоди. Або вони можуть використовувати пристрої інших АСУ для запуску широкої атаки.

Безпека зазвичай не є головним пріоритетом для виробників пристроїв IoT. Їх погана практика низької якості безпеки може включати в себе наступне [39]:

- відсутність захисту системи, яка надає комп'ютерній системі різні засоби захисту і робить її більш безпечною;
- відсутність механізму оновлення програмного забезпечення, який може створювати уразливості;

• використання стандартних паролей, які можуть використовувати хакери.

Запропонуємо декілька рішень відносно підвищення захисту СІЗ медичної установи в рамках ІТС «Біржа медичних працівників» [40]:

1. Унікальна назва роутера.

2. Використання надійного методу шифрування для Wi-Fi.

3. Налаштування гостьової мережі.

4. Зміна імена користувачів та паролей за замовчуванням.

5. Використання надійних унікальних паролей для мереж Wi-Fi та облікових записів пристроїв.

7. Відключення зайвих функцій.

8. Постійне оновлення програмного забезпечення.

9. Проведення аудиту пристроїв IoT, які вже перебувають у мережі.

10. Застосування двократної аутентифікації.

11. Уникнення публічних мереж Wi-Fi.

12. Недопущення простоїв роботи системи.

Таким чином, для максимально ефективного використання переваг від реалізації ІТС «Біржа медичних працівників» слід звести до мінімуму ризики від його впровадження, а для цього варто забезпечити безпеку функціонування ІТС «Біржа медичних працівників»

Висновки до розділу 2

Підсумовуючи другий розділ, можемо зробити такі висновки:

1. Розглянуто існуючі моделі СІМ та визначені найбільш ефективні з точки зору пріоритезації для оптимізації в межах медичних установ.

2. Проаналізовано підходи до проектування СЗІ на базі медичної установи та визначено алгоритм її створення.

3. Зроблено розрахунок надійності захисних бар'єрів та досліджено моделі поведінки зловмисника з точки зору ймовірних внутрішніх та зовнішніх загроз СЗІ в рамках ІТС «Біржа медичних працівників».

РОЗДІЛ 3.
ПРАКТИЧНА РЕАЛІЗАЦІЯ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В ІТС «БІРЖА МЕДИЧНИХ ПРАЦІВНИКІВ»

3.1. Розробка структурної схеми та архітектури моделі

Для проектування структурної схеми та архітектури CIM конкретизуємо задачі дослідження. Задачі включають в себе:

1. Моделювання програмної роботи системи для моніторингу веб-середовища в рамках створення комлексної СЗІ в медичній установі на базі додатку ІТС «Біржа медичних працівників».

2. Розробку структурної бази даних системи, що проектується.

3. Сворення інтерфейсу системи.

4. Проектування програмного забезпечення моделі CIM.

5. Проведення тестування всіх структурних елементів розробленої моделі.

Визначимо галузі практичного застосування розробленого продукту.

Отже, програма може використовуватись в:

- державних установах;
- комерційних установах.

Наступним етапом формалізуємо постановку задач дослідження.

Оскільки підготовчі етапи впровадження вже проведені на стадії впровадження основної системи, можна відразу ж перейти до установки програмного забезпечення.

Установка Zabbix-server.

Для інсталяції серверної частини системи моніторингу мережі також необхідно встановити сервер БД MySQL і утиліту для управління

– sudo apt-get install mysql-server

– sudo apt-get install mysql-client

Але дана дія пропускається, так як воно було виконано при інсталяції системи моніторингу обладнання.

Для їх інсталяції допоміжної системи можна використовувати системну команду apt-get (aptitude):

- apt-get install zabbix-server-mysql

Налаштовується база даних для встановлюваної системи за допомогою dbconfig-common (Рис. 3.1).

Рисунок 3.1 - Вікно налаштування бази даних

Далі налаштовуються права доступу до створеної базою даних (Рис. 3.2).

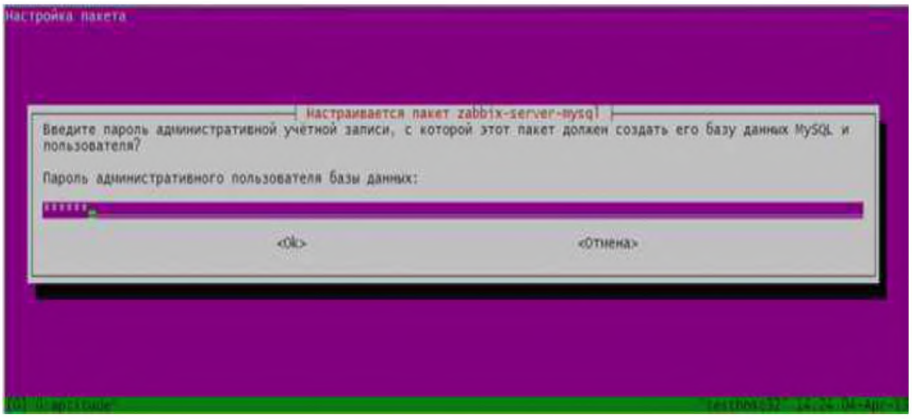


Рисунок 3.2 – Вікно налаштування прав доступу до бази

Наступним дією вказується спеціальний пароль для програми для zabbix-server (Рис. 3.3).

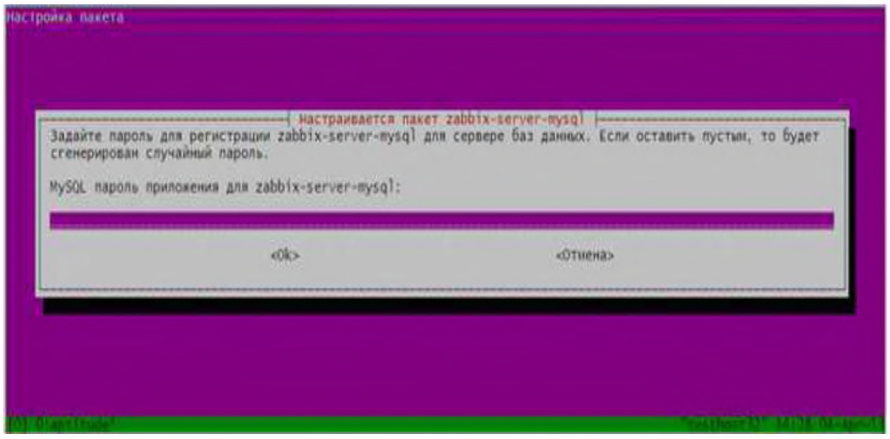


Рисунок 3.3 – Вікно налаштування паролю

Установка веб-інтерфейсу.

Встановлюється веб-сервер системи:

- apt-get install lighttpd

Далі встановлюється інтерпретатор PHP:

- apt-get install php5-cgi

Також потрібно встановити сканер портів:

- apt-get install nmap

Останнім кроком встановлюється веб-інтерфейс Zabbix:

- apt-get install zabbix-frontend-php

Після даної операції виконується запит на вибір типу бази даних для веб-інтерфейсу (Рис. 3.4). Вибирається MySQL.

Рисунок 3.4 – Вікно налаштування типу БД

Вказується пароль бази даних для веб-інтерфейсу (Рис. 3.5).

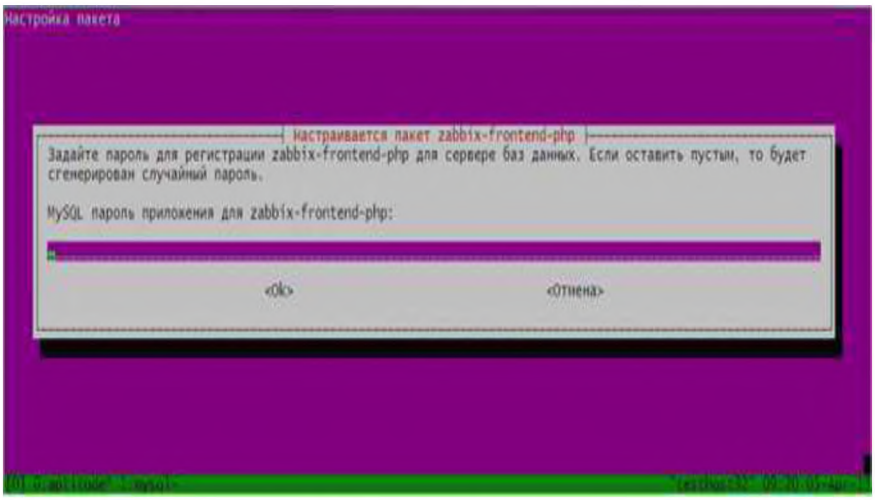


Рисунок 3.5 – Вікно налаштування паролю

Тепер можна увійти в веб-інтерфейс системи Zabbix. Для цього необхідно в в браузері ввести:

- http://10.0.4.123/zabbix/

3.2. Впровадження системи та перевірка її ефективності

З’явиться перша сторінка помічника установки веб-інтерфейсу (Рис. 3.6).

Рисунок 3.6 - Перша сторінка помічника установки веб-інтерфейсу

Сторінка з перевіркою вимог програмного забезпечення (Рис. 3.7).

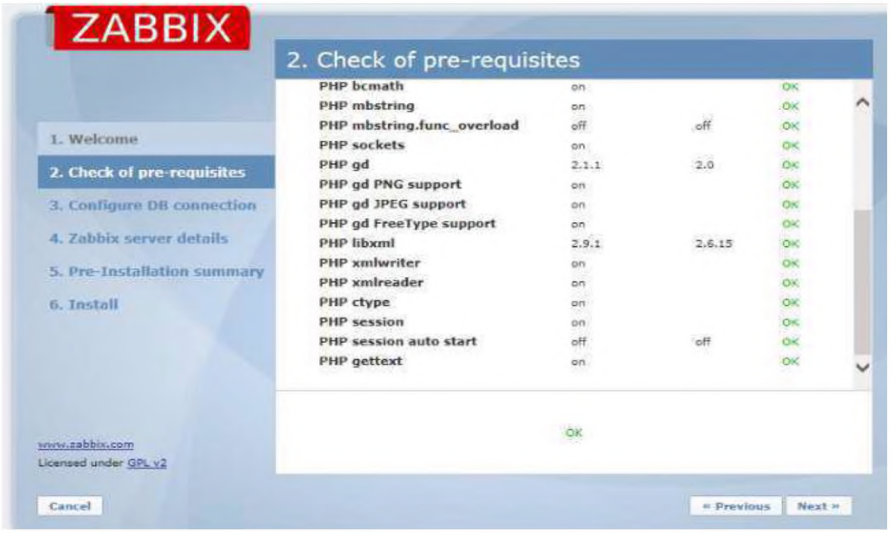


Рисунок 3.7 – Перевірка вимог ПЗ

Наступним кроком вказуються деталі для підключення до бази даних (Рис. 3.8).

Рисунок 3.8 – Підключення до БД

Вказуються додаткові налаштування серверу (Рис. 3.9).

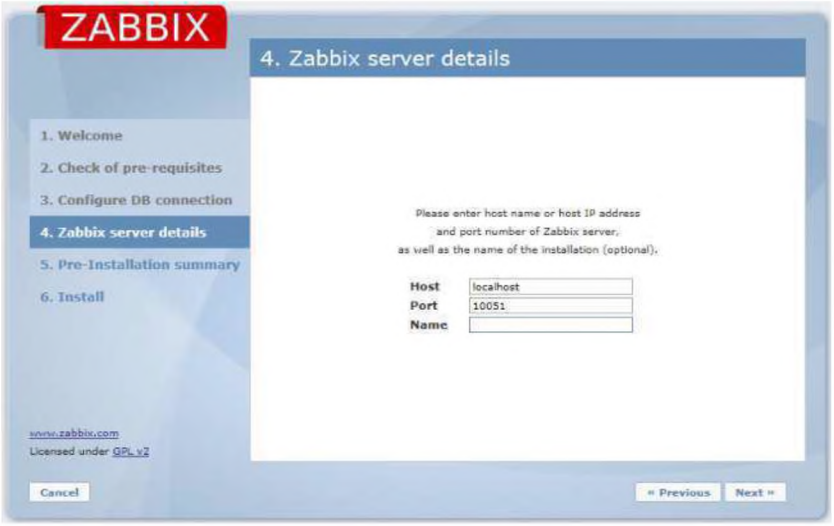


Рисунок 3.9 – Вікно налаштування серверу

І останнім пунктом показується результат всіх попередніх налаштувань (Рис. 3.10).

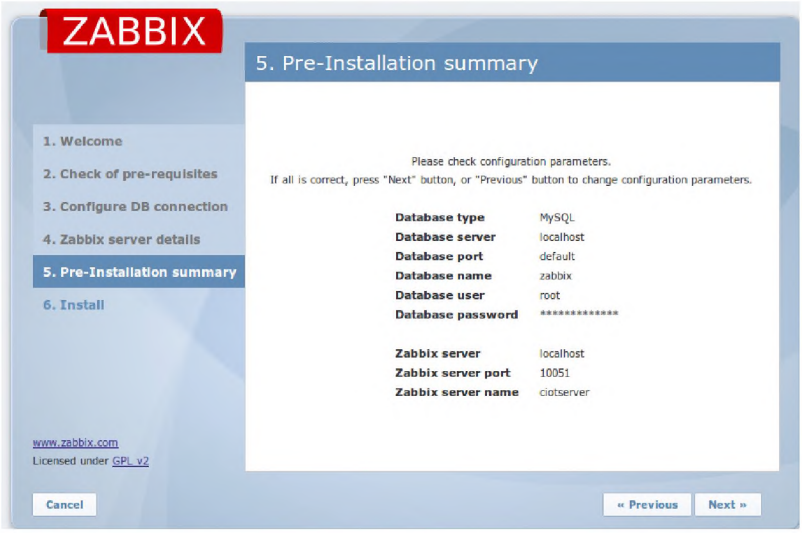


Рисунок 3.10 – Вікно результату налаштувань

З’явиться запит на введення імені користувача і пароля для входу в веб-інтерфейс (Рис. 3.11).

Рисунок 3.11 - Вікно аутентифікації системи Zabbix

Дана форма свідчить про успішну установку автоматизованої системи.

Представимо інфраструктуру дільниці медичного закладу, де реалізовується спроектована модель CIM, у вигляді рисунку 3.12.

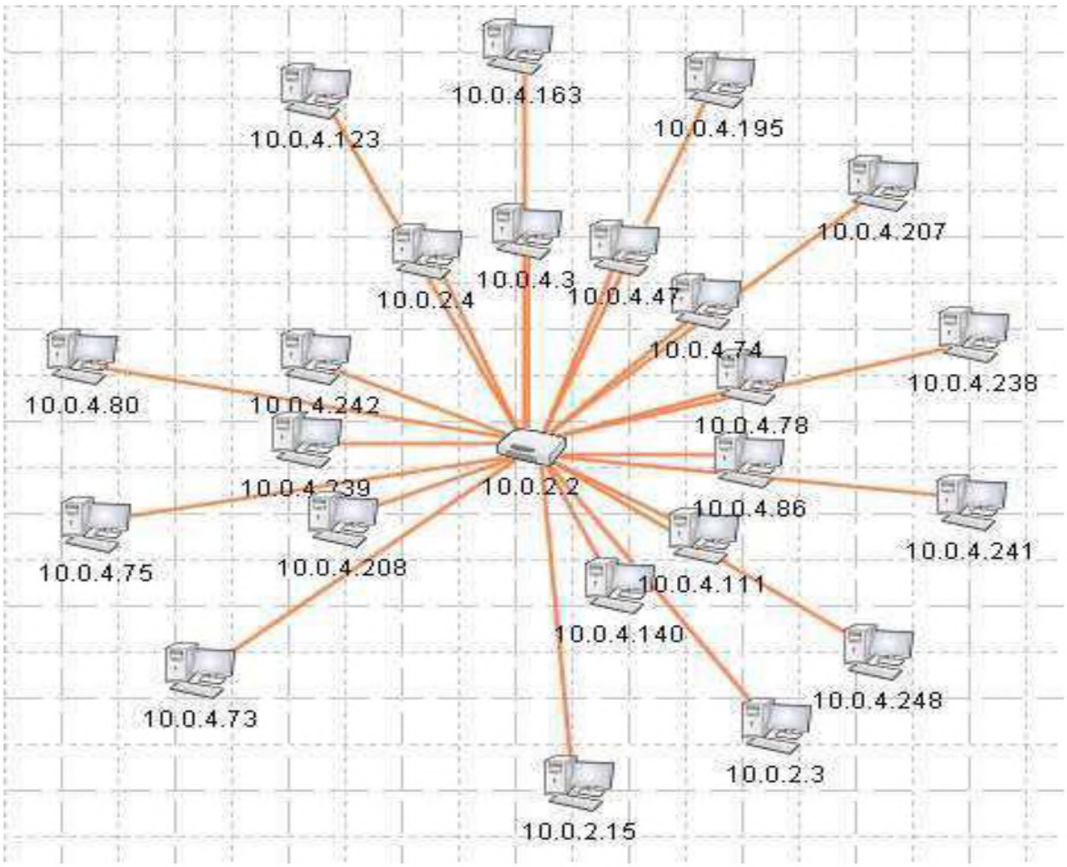


Рисунок 3.12 - Інфраструктура дільниці медичного закладу, де реалізовується спроектована модель СІМ

Далі в рамках перевірки ефективності реалізації СІМ розглянемо потреби у впровадженні системи в медичній установі. В ході роботи центру були виявлені труднощі при обліку обладнання.

З кожним днем кількість обладнання збільшується.

Необхідно постійно підтримувати обладнання в справному стані: контролювати поточний стан обладнання, враховувати термін служби обладнання, швидко знаходити несправні компоненти.

Лавиноподібне збільшення числа технічних засобів, тягне за собою ускладнення процесу проведення обліку.

Перевірка, як правило, проводиться пасивно, тобто при ремонті обладнання, або при плановій інвентаризації.

Таким чином, проблеми з обладнанням і програмним забезпеченням виявляються тільки при виникненні серйозних проблем у користувачів.

Все це веде в першу чергу до постійного погіршення якості пропонованих послуг і підвищення навантаження на системних адміністраторів і службу технічної підтримки користувачів. З ростом клієнтської бази, і, як наслідок, числа активного обладнання, виникла необхідність оперативного відстеження стану технічного обладнання в цілому і окремих її елементів.

У відповідності зі сформованою ситуацією, було вирішено впровадити систему, здатну вирішити поставлені завдання.

Також проаналізуємо вимоги до структури та функціонування системи:

Функціонування серверної частини в режимі - 24 годин на день, 7 днів на тиждень (24х7) за винятком профілактичних робіт;

У профілактичному режимі система повинна забезпечувати можливість проведення наступних робіт:

- технічне обслуговування;

- усунення аварійних ситуацій.

Загальний час проведення профілактичних робіт не повинна перевищувати 5% від загального часу роботи системи в основному режимі.

Також можливий аварійний режим функціонування системи.

Характеризується відмовою одного або декількох компонентів програмного або апаратного забезпечення.

Вимогою до надійності системи є наявність джерела безперебійного або резервного живлення, щоб уникнути втрати даних при відключенні електроживлення.

В якості основного інтерфейсу роботи в системі повинен бути використаний веб-інтерфейс.

Функціональні вимоги.

У системі повинні бути реалізовані наступні функції:

- облік і моніторинг комп'ютерів в мережі;

- збір статистики, список і технічних параметрів обладнання;

- віддалене управління комп'ютерами, що знаходяться в мережі;

- вести довідники пристроїв, властивостей і атрибутів пристроїв, термінів випуску, періодів обслуговування;

- проводити інвентаризацію комп'ютерів, периферійного обладнання;

Вимоги до апаратних і програмних засобів

Потрібно оперативна пам'ять не менше 512 МБ оперативної пам'яті і 80 ГБ вільного місця на жорсткому диску.

Програмне забезпечення повинно працювати на наступних платформах: Debian 4.0 і вище, Madriva 10.2 і вище, Fedora 13 і вище, Ubuntu 7.10 і вище.

Вимоги до лінгвістичного забезпечення

- для організації діалогу системи з користувачем повинен застосовуватися призначений для користувача веб-інтерфейс;

- все прикладне програмне забезпечення системи для організації взаємодії з користувачем повинно використовувати українську або англійську мови.

Деталізуємо специфікацію програмного забезпечення системи.

1. Призначення і цілі створення системи.

Система призначена для моніторингу програмного забезпечення і обладнання в межах комерційної установи, зокрема для таких завдань:

- можливість моніторингу обладнання та програмного забезпечення;

- автоматизація процесу контролю над обладнанням (Наявність / працездатність);

- можливість негайного зворотного зв'язку після отримання повідомлень про помилки на обладнанні.

Цілі створення системи

Цілями створення системи моніторингу є:

- скорочення трудових і тимчасових витрат персоналу;

- забезпечення збору і первинної обробки інформації;

- підвищення якості (повноти, точності, достовірності, своєчасності, узгодженості) інформації.

2. Характеристика об'єкта автоматизації.

Замовником є установа, основні цілі якого – це створення якісного ПЗ та надання ІТ-послуг.

3. Вимоги до системи.

Вимоги до структури та функціонування системи.

- Обсяг технічних засобів не менше 500 найменувань.
- Кількість користувачів не менше 180 чоловік.
- Додаток типу клієнт-сервер;
- Клієнтська частина реалізується в товстому клієнті.

Вимоги до способів і засобів зв'язку для інформаційного обміну між компонентами системи.

В основному режимі система повинна забезпечувати:

- роботу користувачів в режимі

- 24 годин на день, 7 днів на тиждень (24х7) за винятком профілактичних робіт;

- функціонування серверної частини в режимі

- 24 годин на день, 7 днів на тиждень (24х7) за винятком профілактичних робіт;

- виконання своїх функцій;

- збір, обробка та завантаження даних;

- зберігання даних, надання даних.

У профілактичному режимі система повинна забезпечувати можливість проведення наступних робіт:

- технічне обслуговування;

- усунення аварійних ситуацій.

Загальний час проведення профілактичних робіт не повинна перевищувати 5% від загального часу роботи системи в основному режимі.

Також можливий аварійний режим функціонування системи.

Характеризується відмовою одного або декількох компонентів програмного або апаратного забезпечення.

Вимоги до надійності і безпеки.

Вимоги до надійності Вимогою до надійності системи є наявність джерела безперебійного або резервного живлення, щоб уникнути втрати даних при відключенні електроживлення.

Надійність і цілісність даних повинна забезпечуватися вбудованими механізмами, а також резервним копіюванням даних.

Резервне копіювання виконується адміністратором системи. Надійність системи повинна характеризуватися такими значеннями показників надійності:

- Система повинна зберігати працездатність і забезпечувати відновлення своїх функцій при виникненні таких ситуацій:

- ймовірність апаратного збою в системі при нормальних умовах 168 годин функціонування - не більше 0,05;

- тривалість відновлення працездатного стану системи - не більше 6 годин;

- середній термін служби апаратного забезпечення системи - не менше 7 років.

Система повинна зберігати працездатність і забезпечувати відновлення своїх функцій при збоях в системі електропостачання апаратної частини.

Для цього робочі місця і сервер системи забезпечені джерелами безперебійного живлення.

Вимоги до безпеки.

Всі технічні рішення, які будуть використані при розробці даної системи, повинні відповідати чинним нормам і правилам техніки безпеки і пожежної безпеки.

Забезпечення безпеки при роботі з технічними засобами:

- технічне забезпечення повинно мати відповідні сертифікатами та засобами захисту;

- місця розташування обладнання повинні відповідати умовам експлуатації даних технічних засобів;

- площа на одне робоче місце ЕОМ для користувачів повинна бути обрана відповідно до СНиП;

- система електроживлення повинна забезпечувати захисне відключення при перевантаженнях і коротких замиканнях в ланцюгах навантаження, а також аварійне ручне відключення.

Вимоги до ергономіки.

Система повинна забезпечувати зручний для кінцевого користувача інтерфейс, який відповідає наступним функціям:

- система повинна мати інтуїтивно зрозумілий і нескладний для сприйняття інтерфейс;

- інтерфейси сторінок додатку повинні бути типізовані;

- повинно бути забезпечено наявність локалізованого (російськомовного або англомовного) інтерфейсу користувача;

• при виникненні системних помилок на екран монітора адміністратора має виводитися повідомлення з найменуванням помилки.

• при виникненні помилок в результаті дій користувача на екран користувача повинно виводитися повідомлення про помилку.

Взаємодія обслуговуючого персоналу з програмним забезпеченням системи має здійснюватися через графічний інтерфейс. Введення / висновок даних системи і відображення результатів повинні виконуватися в інтерактивному режимі. Інтерфейс повинен забезпечувати зручний доступ до основних функцій і операцій системи. Меню також має відображати технічний стан системи.

Вимоги до експлуатації, технічного обслуговування, ремонту і зберігання компонентів системи.

Для нормальної експлуатації даної АС повинно бути забезпечено безперебійне живлення ПЕОМ.

При експлуатації системи повинна бути забезпечена необхідна температура і вологість повітря.

У повітрі не повинно бути агресивних речовин, що викликають корозію.

Розміщення обладнання і технічних засобів повинно відповідати вимогам техніки безпеки, санітарним нормам і вимогам пожежної безпеки.

Вимоги до захисту інформації від несанкціонованого доступу.

Для захисту інформації від несанкціонованого потрібно розмежування доступу до системи або призначеного для користувача інтерфейсу, для цього у кожного користувача повинна бути своя обліковий запис.

Визначення прав користувачів здійснює адміністратор системи.

З метою забезпечення цілісності програмних засобів і оброблюваної інформації необхідно забезпечити використання коштів захисту.

Вимоги до збереження інформації при аваріях.

Програмне забезпечення системи повинно автоматично відновлювати своє функціонування при коректному перезапуску апаратних засобів.

Повинна бути передбачена можливість організації резервного копіювання. Також при відключенні електроенергії автоматично зберігати (без втрат) останні дані.

Вимоги до захисту від впливу зовнішніх впливів.

Система повинна мати можливість функціонування при коливаннях напруги електроживлення в межах, встановлених виробниками апаратних засобів.

Система повинна мати можливість функціонування в діапазоні допустимих температур навколишнього середовища, встановлених виробниками апаратних засобів.

Система повинна мати можливість функціонування в діапазоні допустимих значень вологості навколишнього середовища, встановлених виготовлювачами апаратних засобів.

Система повинна мати можливість функціонування в діапазоні допустимих значень вібрацій, встановлених виробником апаратних коштів.

Вимоги до патентної чистоти.

Патентна чистота системи повинна бути забезпечена відносно України та країн СНД.

Вимоги до функцій, виконуваних системою.

В системі повинні бути реалізовані наступні функції:

- облік і моніторинг комп'ютерів в мережі;

- збір статистики, список і технічних параметрів обладнання;

- віддалене управління комп'ютерами, що знаходяться в мережі;

- вести довідники пристроїв, властивостей і атрибутів пристроїв, термінів випуску, періодів обслуговування;

- проводити інвентаризацію комп'ютерів, периферійного обладнання.

Вимоги до видів забезпечення.

Вимоги до математичного забезпечення.

Вимоги до інформаційного забезпечення .

Інформаційне забезпечення повинно забезпечувати:

- єдиний методологічний підхід до організації даних;

- узгоджені формати представлення даних, що виключає дублювання інформації.

Вимоги до лінгвістичного забезпечення.

– для організації діалогу системи з користувачем повинен застосовуватися призначений для користувача веб-інтерфейс;

- все прикладне програмне забезпечення системи для організації взаємодії з користувачем повинно використовувати українську або англійську мови.

Все прикладне програмне забезпечення системи для організації взаємодії з користувачем повинно використовувати українську мову.

Вимоги до програмного забезпечення системи.

Програмне забезпечення повинно працювати на наступних платформах:

- для клієнтської частини: OS MS Windows XP і вище, Debian 4.0 і вище, Madriva 10.2 і вище, Fedora 13 і вище, Ubuntu 7.10 і вище;

- для серверної частини ОС CentOS 6.2 і вище

Вимоги до метрологічного забезпечення (не пред'являються).

Вимоги до організаційного забезпечення.

Основними користувачами системи є адміністратори медичного закладу та медичні працівники.

Забезпечує експлуатацію системи адміністратори.

Склад співробітників кожніого відділу визначається штатним розписом, яке, в разі необхідності, може змінюватися.

У разі профілактичних робіт адміністратори повинні проінформувати всіх користувачів (із зазначенням точного часу і тривалості) про перехід її в профілактичний режим.

Порядок контролю і приймання системи.

Попередні випробування виконуються після проведення розробником налагодження і тестування поставляються програмних і технічних засобів системи і подання ним відповідних документів про їх готовність до випробувань. а також після ознайомлення персоналу з експлуатаційною документацією.

Робота завершується оформленням акту прийому в дослідну експлуатацію.

В результаті дослідної експлуатації системи визначають фактичні значення кількісних і якісних характеристик АС, готовність персоналу до роботи в умовах функціонування АС, фактична ефективність АС, відбувається коригування (при необхідності) документації.

За результатами дослідної експлуатації складають акт про завершенні робіт по перевірці системи в режимі дослідної експлуатації, з висновком про можливість пред'явлення системи на приймальні випробування.

Загальні вимоги до приймання робіт по стадіях.

Випробування представляють процес перевірки відповідності АС вимогам ТЗ.

Для перевірки виконання заданих функцій АС встановлюються приймально-здавальні випробування по кожному етапу та по проекту в цілому відповідно до вимог ТЗ.

Після задоволення всіх вимог даного ТЗ проект вважається завершеним.

Вимоги до складу та змісту робіт з підготовки об'єкта автоматизації до введення системи в дію.

В ході виконання проекту на об'єкті автоматизації потрібно виконати роботи з підготовки до введення системи в дію. при підготовці до введення в експлуатацію системи повинні бути проведені комплекс заходів:

- забезпечити придатність приміщень і робочих місць користувачів системи відповідно до вимог, викладених у цьому ТЗ,

- забезпечити присутність користувачів на навчанні роботі з системою, проведеної центром.

Вимоги до складу та змісту робіт з підготовки об'єкта автоматизації до введення системи в дію, включаючи перелік основних заходів і їх виконавців, повинні бути уточнені на стадії підготовки робочої документації і за результатами експлуатації.

3.3. Інструкції з безпечної експлуатації системи

Перерахуємо принципи успішного моніторингу веб-середовищем медичної установи:

1. Централізоване керування.

Першим етапом є створення централізованої системи моніторингу. Якщо існує бажання почати використовувати безкоштовне рішення, слід переконатися, що буде знайдена безкоштовна версія корпоративного програмного забезпечення, яка забезпечить необхідну потужність і надійність.

2. Відповідальність делегата.

На ранніх етапах проекту корпоративного моніторингу часто трапляється, що менеджер сервера створить систему моніторингу, яка буде стежити за серверами і не бути захопленою зненацька користувачами і менеджерами вищого рівня. Потім менеджер сервера вирішує також контролювати частини мережі. Це привертає увагу членів групи мережі, які відразу ж вступають в масовий рух, тому що вони розуміють цінність проактивного моніторингу мережі. Велика частина роботи і відповідальності за управління новою системою корпоративного моніторингу сконцентрована в невеликій кількості досить високопоставлених співробітників IT-відділу. Тому виникає необхідність у делегуванні повноважень.

3. Поточне обслуговування.

Старші IT-фахівці повинні довести систему моніторингу підприємства до зрілості, а потім якомога швидше скинути з себе відповідальність за її поточне обслуговування. Через спеціальні навички, якими володіють адміністратори

серверів і мереж, важливо, щоб вони зберігали деяку ступінь залученості в довгострокове управління системою моніторингу, але їм не потрібно брати участь в повсякденних операціях.

Моніторинг медичної установи не є технічно складним і, ймовірно, навіть не цікавий для старших IT-співробітників. Одним з побічних ефектів наявності спеціалізованої групи моніторингу, що спостерігає за підприємством, є те, що члени команди познайомляться з закладом. Вони дізнаються, які мережеві посилання зазвичай зайняті. Вони будуть розрізняти закономірності в рівнях трафіку і доступності сервера. І найголовніше, вони дізнаються, коли речі «просто виглядають неправильно».

Багато корпоративних інструменти моніторингу мережі дозволяють користувачам бачити, які типи трафіку знаходяться на певному мережевому каналі. Для цього необхідно, щоб агенти були встановлені або на мережевому обладнанні, або на серверах. Однак, якщо ця інфраструктура є, група моніторингу мережі може зайняти активну позицію для виявлення активних атак на мережу і сервери. Великі сплески необробленого мережевого трафіку або SMTP-трафіку, що надходить з сервера, який зазвичай не відправляє електронну пошту, є прикладами того, що щось могло піти не так. Група моніторингу мережі може виявити таку ситуацію, і команда мережевого управління дозволить її, перш ніж вона стане проблемою, з якою стикається клієнт.

Таким чином, варто доручити щоденний моніторинг підприємства фахівцям. Важливо, щоб членам групи моніторингу медичної установи були надані максимально широкі можливості. Делегування відповідальності призводить до виконання завдань тими співробітниками, які з найбільшою ймовірністю виконають свою роботу.

3. Розподілення інформації.

Останнім еволюційним кроком в успішному моніторингу медичної установи є поширення доступу до системи моніторингу іншим відділам і

організаціям всередині компанії. Звичайно, це може здатися суперечливим, враховуючи, що першим кроком була централізація. Різниця в тому, що у вас є централізоване управління, тому тепер ви хочете розподілити доступ. Мета полягає в тому, щоб знайти синергію між різними відділами клієнтів і командами. Наприклад, більш технічно складні команди, такі як WebOps або адміністратори баз даних, будуть досить добре знати свої системи, щоб мати можливість самостійно виявляти проблеми і, сподіваюся, вирішувати їх самостійно.

4. Доступ.

Одним з ключів до успішного розподілу доступу до корпоративної системи моніторингу є забезпечення того, щоб різні зацікавлені сторони мали доступ, який їм потрібен, без додаткового функціоналу. Адміністраторам баз даних не має сенсу стежити за веб-серверами, але мало б сенс дати їм деяку інформацію про стан базової мережі, оскільки це впливає на доступність їх серверів баз даних. Точно так же, для управління, ймовірно, не потрібна детальна мережева карта підприємства, тільки та, яка містить основні основні сервери і орієнтовані на клієнта сервери. Важливо, щоб всі зацікавлені сторони, які мають доступ до системи моніторингу, розуміли, що в разі виявлення проблеми необхідно дотримуватися комунікаційного шляху.

Крім того, в цілях забезпечення безпеки спроектованої системи рекомендується налаштувати допоміжну систему моніторингу мережі. Нижче представимо етапи такого налаштування.

1. Налаштування профілю користувача

За замовчуванням для входу в веб-інтерфейс системи необхідно використовувати Login name (ім'я користувача) admin і Password (пароль) zabbix. Тому необхідно відразу змінити ці налаштування, щоб уникнути несанкціонованого доступу до системи.

Ця установка знаходиться у закладці Profile в правому верхньому кутку сторінки. На сторінці, USER

PROFILE: Zabbix Administrator необхідно натиснути кнопку Password і задати новий пароль.

А також для подальшого зручності змінюється мова веб-інтерфейсу на українську.

2. Додавання вузлів мережі

Для того, щоб сервер кожні півгодини сканував заданий діапазон IP-адрес на наявність таких робочих станцій, додавав знайдені робочі станції в групу вузлів потрібно створити правило, слідуючи якому сервер буде отримувати необхідні дані.

За замовчуванням правило Local network вже є в списку правил виявлення, однак його параметри не відповідають необхідним для наявної мережі вимогам. Для зміни конфігурації правила виявлення Local network слід зайти в розділ Налаштування / Виявлення та перейти за посиланням Local network в стовпці Ім'я. На сторінці необхідно задати діапазон IP-адрес значення, відповідне конфігурації мережі, і частоту виконання правила.

Для створення забезпечення додавання вузлів мережі, необхідно в розділі «налаштування дії», створити нову дію. На сторінці «налаштування дій» слід задати ім’я дії, видалити текст,що міститься в полях Тема за замовчуванням і Повідомлення за замовчуванням, а також задати умови дії і виконувані операції.

Як умова вибирається створене раніше правило виявлення.

Далі варто проаналізувати ефективність впровадження комплексу систем. В результаті тестування виявлено потребу в такого далекого управлінні ПК, що дозволить істотно прискорити роботу відділу та максимально ефективно використовувати впроваджений комплекс програмних коштів.

Як засіб віддаленого доступу вирішено використовувати VNC.

VNC (або Virtual Network Computing) - це система віддаленого доступу, яка дозволяє підключитися до робочого столу віддаленого сервера. VNC спрощує управління файлами, програмним забезпеченням і настройками віддаленого сервера.

Установка середовища робочого столу і VNC-сервера Для початкової настройки сервера VNC необхідно використовувати команду vncserver, яка створить безпечний пароль:

- vncserver

Команда vncserver завершить установку VNC, створивши стандартні конфігураційні файли і необхідну серверу інформацію про з'єднання.

Налаштування VNC-сервера.

Для початку задаються команди, які VNC-сервер повинен виконувати при запуску. Ці команди знаходяться в файлі конфігурації xstartup.

Після установки VNC-сервер за замовчуванням запускається на порту 590x,

який називається display port (порт дисплея) і де x - це порт дисплея, який задається як 5900 + x (за замовчуванням це порт 5901).

VNC дозволяє запускати кілька примірників на портах (як: 2, 3 і т.д.).

Перш ніж приступити до налаштування файлу xstartup, создайем його резервну копію:

- mv ~ / .vnc / xstartup ~ / .vnc / xstartup.bak

Тепер можна редагувати файл xstartup в nano:

- nano ~ / .vnc / xstartup

Внесіть в нього такі команди, які будуть автоматично виконуватися під час запуску або перезапуску VNC-сервера:

#! / Bin / bash xrdb $ HOME / .Xresources startxfce4 &

Перша команда в файлі (xrdb $ HOME / .Xresources) говорить фреймворку GUI VNC-сервера читати файл .Xresources.

Друга команда просто запускає графічне ПЗ для зручного управління сервером.

Щоб переконатися, що сервер VNC зможе коректно використовувати новий

файл, необхідно зробити його виконуваним:

- sudo chmod + x ~ / .vnc / xstartup

Створення файлу сервісу VNC

Для зручності управління створимо додатковий модуль сервісу, який дозволить запускати, зупиняти і перезапускати VNC-сервер в міру необхідності.

Необхідно внести зміни в файл сервісу в /etc/init.d за допомогою консольного текстового редактора nano:

- sudo nano /etc/init.d/vncserver

Перший блок даних необхідний для оголошення деяких загальних налаштувань VNC (наприклад, імені користувача і дозволу дисплея).

```
#! / Bin / bash
PATH = "$ PATH: / usr / bin /"
export USER = "user"
DISPLAY = "1"
DEPTH = "16"
GEOMETRY = "1024x768"
OPTIONS = "- depth $ {DEPTH} -geometry $ {GEOMETRY}: $ {DISPLAY}
localhost "
. / Lib / lsb / init-functions
```

Далі задаємо команди для управління новим сервісом.

Наступний блок коду включає команду, необхідну для запуску сервера VNC, і її зворотний зв'язок (ключове слово команди start).

```
case "$ 1" in
start)
log_action_begin_msg "Starting vncserver for user '$ {USER}' on
localhost: $ {DISPLAY} "
su $ {USER}
-c "/ usr / bin / vncserver $ {OPTIONS}" ;;
```

Наступний блок створює ключове слово команди stop, яке дозволяє зупинити VNC-сервер.

```
stop) log_action_begin_msg
"Stopping vncserver for user '$ {USER}'
on localhost: $ {DISPLAY} "
su $ {USER} -c "/ usr / bin / vncserver -kill:
$ {DISPLAY}" ;;
```

Заключний блок коду створює ключове слово команди restart, яка, по суті, є комбінацією двох попередніх команд:

```
restart)
$ 0 stop
$ 0 start;
esac
exit 0
```

Щоб мати можливість використовувати щойно створені команди, необхідно зробіть скрипт сервісу виконуваним:

- sudo chmod + x /etc/init.d/vncserver

Використовувати сервіс можна, задавши наступні команди:

- sudo service vncserver start
- sudo service vncserver stop
- sudo service vncserver restart

Запропонуємо декілька рекомендацій відносно підвищення ефективності застосування СІЗ в медичному закладі, в тому числі з точки зору її кібербезпеки та напрямків зниження загроз інформаційної безпеки у високоорганізованих системах:

1. Аналіз і тестування пропонованого до використання програмного забезпечення з метою перевірки забезпечення захисту від специфічних загроз для систем подібного типу.

2. Забезпечення контролю за діями обслуговуючого персоналу систем «Біржа медичних працівників», який повинен включати поділ режимів доступу, збереження інформації про проведені операції, введених, що скачали і

переданих даних, автоматичне блокування команд, які створюють небезпеку збою функціонування окремого обладнання або всієї системи.

3. Забезпечення контролю за діями користувачів системи «Біржа медичних працівників» з метою запобігання можливих проблем з функціонуванням обладнання, даними і інформаційним обміном.

4. Запобігання несанкціонованого доступу до обладнання, баз даних, каналам зв'язку системи «Біржа медичних працівників», що має включати в себе цілий комплекс заходів. Одним з найважливіших напрямків при цьому є криптографічні методи захисту інформації.

3.4. Політика безпеки для медичного працівника

При роботі з інформаційними ресурсами медичної установи кожний медичний працівник повинен:

- забезпечувати, виходячи зі своїх можливостей і спеціальних обов'язків щодо забезпечення безпеки інформації ІТС «Біржа медичних працівників», захист від несанкціонованого доступу до інформації системи, до якої він має санкціонований доступ в силу своїх службових обов'язків;
- ні в якій формі не брати участь у процесах несанкціонованого доступу до інформації, що належить іншим працівникам і службам;
- ні в якій формі не використовувати дані, що стали йому відомими в силу виконання своїх функціональних обов'язків, інформацію не за прямим призначенням;
- при порушенні встановлених правил доступу іншими співробітниками повідомляти про це безпосередньому начальнику, відповідальним адміністраторам ІТС «Біржа медичних працівників» або до Служби безпеки медичної установи.

Ремонтні та профілактичні регламентні роботи повинні проводитися тільки уповноваженими особами експлуатаційної служби за погодженням з керівником медичної установи, в якій встановлено комп'ютерне обладнання. Порядок зняття, перенесення, модифікації апаратної конфігурації

встановлюється Регламентом проведення такого роду робіт і здійснюється тільки уповноваженими особами експлуатаційної служби.

При роботі в автоматизованій інформаційній системі медичної установи медичні працівники зобов'язані:

1. зберігати в таємниці паролі доступу до ІТС «Біржа медичних працівників»;

2. надійно зберігати фізичні ключі (ідентифікатори) доступу;

3. періодично змінювати особисті паролі, якщо це передбачено регламентом управління доступом до ІТС «Біржа медичних працівників»;

4. при випадковому отриманні (збій механізмів захисту, аварії, недбалість персоналу) доступу до чужої конфіденційної інформації припинити будь-які дії в системі і негайно повідомити в Службу безпеки й адміністраторові системи ІТС «Біржа медичних працівників» медичної установи;

5. повідомляти в службу безпеки й адміністраторові системи медичної установи про відомих каналах витоку, способи і засоби обходу або руйнування механізмів захисту.

При роботі в автоматизованій інформаційній системі медичної установи ІТС «Біржа медичних працівників» медпрацівникам забороняється (крім особливо обумовлених випадків):

- записувати в будь-якому доступному вигляді або вимовляти вголос відомі користувачеві паролі;

- реєструватися і працювати в системі під чужим ідентифікатором і паролем;

- передавати ідентифікатори і паролі кому б то не було;

- залишати без контролю робоче місце протягом сеансу роботи;

- дозволяти проводити будь-які дії з закріпленим за користувачем комплектом програмно-апаратних засобів іншим особам;

- несанкціоновано змінювати або знищувати дані чи програми в мережі або на зовнішніх (відчужуваних) носіях;

- залишати без контролю носії критичної інформації ІТС «Біржа медичних працівників»;

- використовувати комп'ютерну техніку в неробочий час не за прямим призначенням;

- займатися дослідженням обчислювальної мережі;

- ігнорувати системні повідомлення і попередження про помилки;

- несанкціоновано встановлювати на автоматизовані робочі місця будь-які додаткові програмні і апаратні компоненти та пристрої;

- копіювати на знімні носії будь-яке програмне забезпечення та файли даних;

- використовувати для передачі інформації обмеженого доступу не призначені для цього кошти і канали зв'язку.

3.5. Політика безпеки для медичної установи

Впровадження організаційних заходів в медичній установі не вимагає великих матеріальних витрат, але їх ефективність підтверджена життям і часто недооцінюється потенційними жертвами. Відзначимо їх одну відмінну особливість у порівнянні з технічними засобами: організаційні заходи ніколи не стають провокуючим фактором агресії. Вони застосовуються до зіткнення зі зловмисником. Використовуючи досвід багатьох організацій в області проектування СЗІ, відзначимо, що організаційні заходи включають в себе створення концепції інформаційної безпеки в рамках функціонування автоматизованої системи комплексного захисту ІТС «Біржа медичних працівників», а також:

- складання посадових інструкцій для користувачів та медичного персоналу;

- створення правил адміністрування компонентів інформаційної системи, обліку, зберігання, розмноження, знищення носіїв інформації, ідентифікації користувачів;

- розробку планів дій у разі виявлення спроби несанкціонованого доступу до інформаційних ресурсів системи «Біржа медичних працівників», виходу з ладу засобів захисту, виникнення надзвичайної ситуації;
- навчання правилам інформаційної безпеки користувачів.

Дотримання основних принципів і простих правил дозволить запобігти втраті інформації, а разом з цим і можливий матеріальний, моральний збиток, фінансові втрати.

У разі необхідності, в рамках проведення організаційних заходів може бути створена служба інформаційної безпеки медичного закладу, режимно-пропускний відділ, проведена реорганізація системи діловодства та зберігання документів.

При присвоєнні категорій критичності інформації, слід врахувати наступні моменти:

- Критична інформація і вихідні дані систем, що містять критичну інформацію, повинні мати відповідні категорії критичності.
- Надмірне засекречування інформації може призвести до невиправданих додаткових витрат у компанії.
- Вихідним даними інформаційних систем, що містить критичну інформацію, повинен бути присвоєно відповідний рівень критичності. Цей рівень критичності повинен відображати категорію критичності найбільш уразливої інформації у вихідних даних.

Наприклад, в межах медичної установм вводяться такі рівні категорій критичності інформації: загальнодоступно, конфіденційно, суворо конфіденційно, таємно.

Медичним працівниками суворо забороняється розголошувати будь-яку інформацію вище рівня конфіденційно.

1) Загальнодоступної інформацією є інформація, вже опублікована в засобах масової інформації.

Рішення про надання статусу загальнодоступно приймає керівництво медичної установи.

Висновки до розділу 3

Підсумовуючи третій розділ, можемо зробити такі висновки:

1. Розроблено структурну схему та архітектуру моделі CIM для ІТС «Біржа медичних працівників».

2. Спроектовано модель роботи системи та структуру бази даних, розроблено інтерфейс програмного додатку, розроблено електронну CIM.

3. Розроблено інструкції з безпечної експлуатації системи.

4. Проаналізовано політику безпеки для медичного працівника та для медичної установи в цілому.

РОЗДІЛ 4.
ЕКОНОМІЧНИЙ РОЗДІЛ

Метою цього розділу є обґрунтування економічної доцільності проектування та впровадження системи захисту інформації на комерційному підприємстві. Для досягнення поставленої мети необхідно здійснити наступні розрахунки:

- капітальні витрати на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов’язані з виготовленням апаратури, приладів, програмного забезпечення;

- річні експлуатаційні витрати на утримання і обслуговування об'єкта проектування;

- річний економічний ефект від системи захисту інформації на комерційному підприємстві;

- показники економічної ефективності впровадження системи захисту інформації на комерційному підприємстві.

4.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

4.1.1. Визначення витрат на створення програмних засобів захисту інформації

4.1.1.1 Визначення трудомісткості розробки та впровадження системи захисту інформації на підприємстві

Визначення трудомісткості розробки та опрацювання засобів резервування даних на підприємстві здійснюється, виходячи з тривалості кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації:

$$t = t_{тз} + t_{в} + t_{а} + t_{п} + t_{алг} + t_{впр} + t_{р} + t_{пол}, \text{ годин}, \qquad (4.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на проектування комплексної системи інформаційного захисту медичної установи, $t_{тз}$ = 8 год.;

$t_в$ – тривалість вивчення ТЗ, літературних джерел за темою тощо, $t_в$=16 год.;

$t_а$ – тривалість аналізу існуючих моделей захисту ІТС, $t_а$= 16 год.;

$t_п$ – тривалість складання моделі порушника, $t_п$= 16 год.;

$t_{алг}$ – тривалість розробки структурної схеми та архітектури прототипу, $t_{алг}$= 24 год.;

$t_{впр}$ – тривалість впровадження системи та перевірка її ефективності, $t_{впр}$= 24 год.

$t_р$ – тривалість складання моделі ризику, $t_р$= 16 год.;

$t_{пол}$ – тривалість розробки політик безпеки для медичного працівника та установи, $t_{пол}$= 24 год.;

Тоді:

$t = t_{тз} + t_в + t_а + t_п + t_{алг} + t_{впр} + t_р + t_{пол}$ = 8+16+16+16+24+24+16+24=144 год.

4.1.1.2 Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту ***Кпз*** складаються з витрат на заробітну плату виконавця програмного забезпечення ***Ззп*** і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК ***Змч***:

$$K_{пз} = З_{зп} + З_{мч}\,. \qquad (4.2)$$

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

$$З_{зп} = t \cdot З_{пр}, \quad \text{грн.}, \qquad (4.3)$$

де t – загальна тривалість створення ПЗ, годин;

Зпр – средньогодинна заробітна плата з нарахуваннями, грн./годину.

За формулою (4.3) визначається заробітна плата виконавця з урахуванням середньогодинної заробітної плати з нарахуваннями у розмірі 107,50 грн./годину.

$$З_{зп} = 144 \cdot 107{,}50 = 15480 \text{ грн.},$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = t_{опр} \cdot C_{мч} + t_{д \cdot} c_{мч}, \text{ грн.}, \quad (4.4)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

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

Вартість машинного часу для налагодження програми на ПК визначається за формулою (4.4):

$$З_{мч} = 7{,}25 \cdot 2{,}85 + 2 \cdot 2{,}85 = 26{,}93 \text{ грн.}$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$С_{мч} = Р \cdot t_{нал} \cdot С_е + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн.}, \quad (4.5)$$

де P – встановлена потужність ПК (P = 0,8 кВт);

C_e – тариф на електричну енергію (C_e = 1,64 грн./кВт за годину);

$Ф_{зал}$ – залишкова вартість ПК на поточний рік ($Ф_{зал}$ = 3997 грн.);

H_a – річна норма амортизації на ПК (H_a = 0,1 частки одиниці);

$H_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення ($H_{апз}$ = 0,2 частки одиниці);

$K_{лпз}$ – вартість ліцензійного програмного забезпечення ($K_{лпз}$ = 0 грн.);

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня ($F_р$ = 1920 годин).

Вартість 1 години машинного часу ПК визначається за формулою (4.5):

$$С_{мч} = 0{,}8 \cdot 1 \cdot 1{,}64 + \frac{3997 \cdot 0{,}1}{1920} + \frac{0 \cdot 0{,}2}{1920} = 1{,}73 грн.$$

Витрати на створення програмного продукту $К_{пз}$ визначаються за формулою (4.2)

$$К_{пз} = 15480+26{,}93=15506{,}93 \text{ грн.}$$

Залишкова вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання.

Визначена таким чином вартість створення програмного забезпечення *Кпз* є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи інформаційної безпеки.

Вартість використання програми Zabbix є безкоштовною.

Таким чином, капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} , \qquad (4.6)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки ($К_{пр}$=15506,93 грн.);

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), ($К_{зпз}$ = 0.);

Капітальні витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки визначаються за формулою (4.6):

$$К = 15506{,}93 \text{ грн}$$

4.2 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак} , \quad \text{грн.} \qquad (4.7)$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в}$ = 0);

$С_к$ - витрати на керування системою в цілому обчислюються за формулою (4.8);

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак}$ = 0 грн.).

Витрати на керування системою інформаційної безпеки ($С_к$) складають:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос}, \text{ грн.} \quad (4.8)$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н$ = 0 грн.).

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій.

Амортизації програмне забезпечення не підлягає. Таким чином, річні амортизаційні відрахування за прямолінійним методом нарахування складуть:

$$С_а = 0 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (4.15)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного системного адміністратора на місяць складає 15000 грн. Додаткова заробітна плата –8% від основної заробітної плати. Отже,

$$С_з = 15000*12 + 15000*12*0,08= 194400 \text{ грн.}$$

З 01.01.2016 року ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 194400*0,22 = 42768 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (4.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р = 0,8 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою (4.16):

$$С_{ел} = 0,8*1920*1,64 = 2519,04 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат -1% ($С_{тос}$ = 15506,93*0,01=155 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються за формулою (4.8):

$$С_к = 194400 + 42768 + 2519,04 + 155 = 239\ 842,04 грн.$$

Річні поточні витрати на функціонування системи інформаційної безпеки визначаються за формулою (3.9):

С = 239 842,04 грн.

4.3 Оцінка можливого збитку від атаки на вузол або сегмент мережі

4.3.1 Оцінка величини збитку

Для розрахунку вартості збитку застосовуємо спрощену модель оцінки.

Необхідні вхідні дані для розрахунку:

де $t_п$ – час простою вузла внаслідок атаки ($t_п$ = 12 годин);

$t_в$ – час відновлення після атаки персоналом ($t_в$ = 8 годин);

$t_{ві}$ – час повторного введення загубленої інформації співробітниками атакованого сегменту мережі ($t_{ві}$ = 7 годин);

$З_о$ – заробітна плата обслуговуючого персоналу ($З_о$ = 9000 грн. на місяць);

$З_с$ – заробітна плата співробітників атакованого вузла ($З_с$ = 11000 грн. на місяць);

$Ч_о$ – чисельність обслуговуючого персоналу ($Ч_о$ = 2 особи);

$Ч_с$ – чисельність співробітників атакованого сегменту мережі ($Ч_с$ = 2 особи);

О – обсяг продажів атакованого сегменту мережі, (О = 260000 грн. на рік);

$П_{зч}$ – вартість заміни устаткування або запасних частин, ($П_{зч}$ = 0 грн.);

I – число атакованих вузлів (I = 3);

N – середнє число атак на рік (N = 30).

Упущена вигода від простою атакованого вузла становить:

$$U = П_п + П_в + V, \quad (4.10)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла, грн.;

$П_в$ – вартість відновлення працездатності сегмента мережі, грн.;

V – втрати від зниження обсягу продажів за час простою атакованого вузла, грн.

Упущена вигода від простою атакованого вузла визначається за формулою (4.10):

$$U = 681,82 + 761,37 + 3375 = 4818,19 \text{ грн.},$$

Втрати від зниження продуктивності співробітників атакованого сегмента мережі являють собою втрати їхньої заробітної плати за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} \cdot t_п \ , \quad (4.11)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить F = 176 годин).

Втрати від зниження продуктивності співробітників атакованого сегмента мережі визначаються за формулою (4.18):

$$П_п = \frac{11000}{176} \cdot 12 = 750 \text{ грн.},$$

Витрати на відновлення працездатності сегмента мережі включають кілька складових:

$$П_в = П_{ві} + П_{пв} + П_{зч}, \quad (4.12)$$

де $П_{ві}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення сегмента мережі, грн.;

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

Витрати на відновлення працездатності сегмента мережі визначаються за формулою (4.12):

$$П_в = 397,73 + 363,64 = 761,37 \text{ грн.},$$

Витрати на повторне введення інформації $П_{ві}$ розраховуються, виходячи з розміру заробітної плати співробітників атакованого сегмента мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ві}$:

$$П_{ві} = \frac{\sum Зс}{F} \cdot t_{ві} . \quad (4.13)$$

Витрати на повторне введення інформації визначаються за формулою (4.13):

$$П_{ві} = \frac{11000}{176} \cdot 7 = 437,50 \text{ грн.}$$

Витрати на відновлення сегмента мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу:

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в . \quad (4.14)$$

Витрати на відновлення сегмента мережі визначаються за формулою (4.14):

$$П_{пв} = \frac{9000}{176} \cdot 8 = 409,09 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого сегмента мережі визначаються виходячи із середньогодинного обсягу продажів типового підприємства і сумарного часу простою атаковано сегмента мережі:

$$V = \frac{o}{Fp} \cdot (t|п + t_в + t_{ві}) \text{ , грн.} \quad (4.15)$$

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

Втрати від зниження очікуваного обсягу продажів типового підприємства визначаються за формулою (4.15):

$$V = \frac{260000}{2080} \cdot (12 + 8 + 7) = 3375 \text{ грн.},$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе:

$$B = \sum\sum U = 3*30*4818,19=433637,1 \text{ грн} \qquad (4.16)$$

4.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = \text{В} \cdot R - C \text{ грн.}, \qquad (4.17)$$

де В – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (95%);

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

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і визначається за формулою (4.17):

$$E= 433637,1*0,95 – 239\ 842,04 = 172113,21 \text{ грн.}$$

4.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

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

$$\text{ROSI} = \frac{E}{K}, \quad \text{частки одиниці,} \tag{4.18}$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

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

Коефіцієнт повернення інвестицій ROSI визначається за формулою (4.18): $\text{ROSI} = \frac{172113,21}{15506,93} = 11,1$, частки одиниці,

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (N_{\text{деп}} - N_{\text{інф}})/100), \tag{4.19}$$

де $N_{\text{деп}}$ – річна депозитна ставка, (11 %);

$N_{\text{інф}}$ – річний рівень інфляції, (4,1%).

Розрахункове значення коефіцієнта повернення інвестицій визначається за формулою (4.19):

$$11,1 > (11 - 4,1)/100 = 11,1 > 0,069.$$

Термін окупності капітальних інвестицій T_o визначається за формулою (4.20) та показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_o = \frac{К}{Е} = \frac{1}{\text{ROSI}} = \frac{1}{11,01} = 0,1, \quad \text{років.} \tag{4.20}$$

4.4 Висновки до розділу 4

Результатом проведеної роботи в даному розділі є обґрунтування економічної доцільності проектування та впровадження системи захисту інформації на комерційному підприємстві..

Розраховані капітальні витрати, які складають 15506,93 грн., поточні витрати на експлуатацію системи інформаційної безпеки, що становлять 239

842,04 грн. Визначена величина економічного ефекту складає 172113,21 грн. Коефіцієнт повернення інвестицій складає 11,1 та швидкість повернення - 0,1 року.

Аналіз проведених розрахунків дозоляє зробити висновок про економічну доцільність впровадження системи захисту інформації на комерційному підприємстві.

ВИСНОВКИ

Підсумовуючи загальний зміст дослідження, можемо констатувати наступне:

1. Для оптимізації процесів виробничої діяльності медичні установи зацікавлені в тому, щоб якомога більше підвищити автоматизаційні можливості моніторингу власних інтернет-продуктів. В результаті це сприятиме покращенню продуктивності роботи закладу в цілому, а також мінімізує ризики проникнення сторонніх ресурсів та витоків конфединційних даних, на захист яких витрачається багато часу. З іншого боку, для управління корпоративними мережами передачі даних надзвичайно важливою видається можливість отримання достовірної інформації про стан програмного забезпечення і про технічний стан устаткування, який підтримує софт медичної установи. Саме ці проблеми вирішує впровадження електронної системи інтернет-моніторингу (CIM).

2. Інформаційна безпека - це практика захисту інформації шляхом зниження інформаційних ризиків. Це частина управління інформаційними ризиками. Зазвичай це включає запобігання або, принаймні, зниження ймовірності несанкціонованого / несанкціонованого доступу до даних або незаконного використання, розкриття, порушення, видалення, пошкодження, модифікації, перевірки, записи або знецінення інформації. Сюди також входять дії, спрямовані на зменшення несприятливих наслідків таких інцидентів. Захищена інформація може приймати будь-яку форму, наприклад, електронну або фізичну, матеріальну (наприклад, паперову) або нематеріальну (наприклад, знання). Основна увага інформаційної безпеки приділяється збалансованої захисту конфіденційності, цілісності і доступності даних при збереженні акценту на ефективної реалізації політики, і все це без зниження

продуктивності організації. Це в значній мірі досягається за рахунок структурованого процесу управління ризиками, який включає:

- Виявлення інформації та пов'язаних активів, а також потенційних загроз, вразливостей і впливів;

- Оцінку ризиків;

- Ухвалення рішення про те, як усувати або обробляти ризики, тобто уникати, пом’якшувати, розділяти або приймати їх;

- Зниження ризику у разі необхідності, вибір або розробка відповідних заходів безпеки та їх впровадження;

- Моніторинг діяльності, внесення коригувань у міру необхідності для вирішення будь-яких проблем, змін і можливостей поліпшення.

3. На даний час захист інформації та поняття кібербезпеки перетворилося на одне з найактуальніших завдань високотехнологічного суспільства. Через широке застосування сучасних ІІТ в усіх галузях свого існування соціум стає вкрай вразливим до незначних кібернетичних атак, які все частіше стають ефективним механізмом несилових методів контролю та керування як об’єктами критичної інфраструктури країни, підприємства, так і окремо взятими людьми. З одного боку, кібербезпека являє собою захист від наявних і потенційно небезпечних вразливостей інформаційного впливу, що моделює небезпеку для різноманітних інформаційних структур, програмних та апаратних інструментів, а також морального стану населення. З іншого боку, кібербезпека являє собою систему заходів, направлених на захист ПК, цифрових даних і мереж їх передавання від несанкціонованого доступу та інших дій, що пов’язані з випадковою чи цілеспрямованою маніпуляцією, крадіжками, блокуванням, поломками, знищенням даних чи ресурсів.

4. Моніторинг веб-ресурсів часто використовується медичними установами для забезпечення очікуваного часу безвідмовної роботи, продуктивності і функціональності веб-сайтів. Компанії з моніторингу веб-сайтів надають медичним установам можливість постійно відстежувати роботу

веб-сайту або сервера і спостерігати за його реакцією. Моніторинг часто проводиться з декількох місць по всьому світу на конкретному веб-сайті або сервері, щоб виявляти проблеми, пов'язані із загальною затримкою інтернету, проблемами в мережі, і запобігати помилкові спрацьовування, викликані локальними або міжмережевими проблемами. Моніторингові компанії зазвичай повідомляють про це тестиами у вигляді різних звітів, діаграм і графіків. При виявленні помилки служби моніторингу відправляють оповіщення по електронній пошті, SMS, телефону, пастці SNMP, пейджера, який може містити діагностичну інформацію, таку як маршрут трасування мережі, захват коду HTML-файлу веб-сторінки, знімок екрана веб-сторінки і навіть відео з помилкою веб-сайту медичної установи.

5. Автоматизовані медичні системи наразі демонструють потенційно смертельні уразливості, включаючи як внутрішньо діагностичне обладнання , так і імплантовані пристрої, включаючи кардіостимулятори та інсулінові помпи. Є багато повідомлень про зломи лікарень і лікарняних організацій, включаючи атаки шкідливих програм, експлойтів Windows XP, вірусів і витоку конфіденційних даних, що зберігаються на серверах лікарень. Враховуючи вищевикладені обставини, розглянемо детальніше існуючі моделі захисту інформації в медичних установах з метою проектування та реалізації коплексної СЗІ в ІТС «Біржа медичних працівників». Для розробки прототипу пропонується застосовувати програму моніторингу веб-середовища в ІТС «Біржа медичних працівників».

6. Розроблено та впроваджено модель системи моніторингу веб-середовища для ІТС «Біржа медичних працівників» та розроблено методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних програм.

Таким чином, були виконані наступні задачі дослідження:

- проаналізувано теоретичні засади дослідження системи захисту інформації та визначити її складові;

- охарактеризовано принципи інформаційної безпеки;

- розглянуто існуючі моделі захисту ІТС;

- досліджено алгоритм створення СЗІ на прикладі програми моніторингу веб-середовища для ІТС «Біржа медичних працівників»;

- спроектовано модель СЗІ для заданих умов та перевірити її ефективність;

- розроблено методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних систем під час створення комплексної системи захисту для медичної установи.

7. Економічні підрахунки підтвердили доцільність впровадження системи захисту інформаціїї на комерційному підприємстві.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Антонюк В. С. Методологія наукових досліджень: [Текст] : навч. посіб./ В.С. Антонюк, Л. Г. Полонський, В. І. Аверченков, Ю. А. Малахов. – К.: НТУУ «КПІ», 2015. – 286 с.

2. Бабак В. П. Інформаційна безпека та сучасні мережеві технології : Англо-українсько-російський словник термінів / В. П. Бабак, О. Г. Корченко. – Київ : Издательство НАУ, 2003. – С. 230-255.

3. Бурячок В. Л., Толюпа С. В., Аносов А. О., Козачок В. А., Лукова-Чуйко Н. В. Системний аналіз та прийняття рішень в інформаційній безпеці: підручник. / В. Л. Бурячок, С. В.Толюпа, А. О. Аносов, В. А.Козачок, Н.В. Лукова-Чуйко / – К.:ДУТ, 2015. – 345 с.

4. Бурячок В. Л.Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. [Підручник]. / В. Л. Бурячок, Г.М.Гулак, В.Б. Толубко. – К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. – 449 с.

5. Богуш В.М., Кудін А.М. Інформаційна безпека від А до Я: 3000 термінів і понять. - К.: МОУ, 1999. - 456 с.

6. Бугайский К. Проблемы построения систем информационной безопасности //"Information Security/ Информационная безопасность" – 2008. – № 2. – С. 5-9.

7. Бугров Ю. Г. Системные основы оценивания и защиты информации: Учеб. пособие / Воронеж: Воронеж. гос. техн. ун-т, 2005. - 354 с.

8. Вентцель Е. С. Теорія ймовірностей: Учеб. для вузів. - 6-е вид. стер. - М.: Высш. шк., 1999. – С. 12-54.

9. Глушков В. М., Амосов Н. М., Артеменко И. А. Энциклопедия кибернетики. Том 2. Киев, - 1974. – С. 33-54.

10. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ООО «ТИД «ДС». 2001. – 688 с.

11. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. - М.: Горячая линия - Телеком, 2000. - С. 26-120.

12. Измалкова С.А., Тарасов А.В. Принципы построения эффективной системы информационной безопасности // Управление общественными и экономическими системами. – 2006. – № 2. – С. 3-12.

13. Конохович Г. Ф. Захист інформації в телекомунікаційних системах. – МК Прес Київ 2005. – 288 с.

14. Комашинский В. И. Смирнов Д. А. Внедрение в нейро-информационные технологии. / В. И. Комашинский, Д. А. Смирнов - СПб, 1999. – С. 33-48.

15. Корченко О. Г. Англо-українсько-російський словник із тлумаченнями щодо безпеки інформації в комп'ютерних мережах. - Київ: Вид.-во КМУГА.- С. 348-453.

16. Липунцов Ю. П. Управление процессами. М: Компания АйТи, 2003. – С. 33-42.

17. Лотов А. В., Поспелова И. И. Многокритериальные задачи принятия решений: учеб. пособие. М.: МАКС Пресс, 2008. – С. 77-89.

18. Малюк А. А., Пазизин С.В., Погожин Н.С. Введение в защиту информации в автоматизированных системах. – М.: Горячая линия-Телеком, 2001. – 148 с.

19. Нечаев М. Правовые и организационные основы комплексных систем защиты информации // Корпоративные системы. – 2008. – №2. – С. 54-57.

20. Поспелов Г. С Искусственный интеллект - основа новой информационной технологии - М.: Высшая школа, 1988 – С. 129-154.

21. Растригин Л. А., Эйдук Я. Ю. Адаптивные методы многокритериальной оптимизации // Автоматика и телемеханика. 1985. - № 1. - С. 5-26.

22. Системи автоматизації діяльності організації [Електронний ресурс] - Режим доступу: http://www.in-line.ru/solutions/business_appl.

23. Советов Б. Я. Информационные технологии / Б.Я. Советов, В.В Цехановский - М.: Высшая школа, 2005 – С. 55-63.

24. Скулиш Є. Д. Засоби аналізу та оцінка ризиків інформаційної безпеки / Є. Д. Скулиш, О. Г. Корченко, Ю. І. Горбенко, С. В. Казмирчук // Інформаційна безпека. Людина, суспільство, держава – 2011. – №3 (7). – С. 31-48.

25. Тархов Д. А. Нейронные сети. Модели и алгоритмы. – М.: Радиотехника, 2010. – С. 65-70.

26. Типове положення про службу захисту інформації в автоматизованій системі [Текст] : НД ТЗІ 1.4-001. - 2000. - Чин. 2000.12.04. - К. : ДСТСЗІ СБ України, 2000. - С. 4-30.

27. Терехов В. А., Єфімов Д. В., Тюкин И. Ю. Нейромережні системи керування. - 1-е. - Высшая школа, 2002. - С. 180-184.

28. Уосермен Ф. Нейрокомп'ютерна техніка: Теорія і практика. Переклад українською І. Ю. Юрчак, 2001. – С. 88-94.

29. Уфимцев Ю.С. Методика информационной безопасности / Уфимцев Ю. С., Буянов В. П., Ерофеев Е. А. и др. – М.: Издательство «Экзамен», 2004. – 544 с.

30. Чипига, А. Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2017. - С. 144-167.

31. Черноруцкий И. Г. Методы принятия решений [Текст] / И.Г. Черноруцкий.– СПб.: БХВ-Петербург, 2005. – С. 388-395.

32. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. – М.: Форум, 2018. – С. 67-88.

33. Ясницкий Л. Н. Введення в штучний інтелект. - 1-е. - Издательский центр «Академия», 2005. - С. 170-176.

34. Dewitt David J , Gray Jim. Parallel database systems: the future of high performance database systems. Communications of the ACM, Volume 35, Number 6, June, 1992. – P. 12-26.

35. Guttman Antonin. R - trees: a dynamic index structure for spatial searching. ACM SIGMOD International Conference on Management of Data, 1984. – P. 43-52.

36. Magic Quadrant for Data Warehouse and Data Management Solutions for Analytics.URL:https://www.gartner.com/doc/reprints?id=12ZFVZ5B&ct=160225&st=s

37. Moghaddam B. and Pentland A. «Probabilistic Visual Reconition for Object Recognition», Trans. IEEE Pattern Analysis and Machine Intelligence, July 1997. – P. 696–710.

38. Salamon J. A Dataset and Taxonomy for Urban Sound Research / J. Salamon, C. Jacoby, J. Bello. // 22nd ACM International Conference on Multimedia, Orlando USA. – 2014. - P. 17–44.

39. Richard C. Larson. Perspectives on Queues: Social Justice and the Psychology of Queueing. – INFORMS, 1987 – P. 895-905.

40. Rouse Margaret. Real - time analytics. – 2016. URL: http://searchcrm.techtarget.com/definition/real-time-analytics.

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	4	
5	А4	1 Розділ	7	
6	А4	2 Розділ	32	
7	А4	3 Розділ	28	
8	А4	4 Розділ	12	
9	А4	Висновки	4	
10	А4	Перелік джерел посилання	4	
11	А4	Додаток А	1	
12	А4	Додаток Б	1	
13	А4	Додаток В	1	
14	А4	Додаток Г	1	
15	А4	Додаток Д	5	
16	А4	Додаток Е	1	

ДОДАТОК Б. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Розділ 4.doc

11 Висновки.doc

12 Перелік джерел посилання.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

16 Додаток Д.doc

17 Додаток Е.doc

17 Презентація.pptx

ДОДАТОК В. ВІДГУКИ КЕРІВНИКІВ РОЗДІЛІВ

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу магістра на тему:
студента групи 125м-19-1
Резніченко Дмитро Олегович

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, чотирьох розділів, висновків, переліку посилань та додатків, розташованих на 110 сторінках та містить 29 рисунків, 5 таблиць, 40 джерел та 6 додатків.

Актуальність теми полягає в необхідності підвищення рівня захищеності інформації в ІТС медичного закладу.

Зміст та структура кваліфікаційної роботи дозволяють розкрити поставлену тему повністю.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота виконана самостійно. У роботі було проведено аналіз існуючих моделей СІМ. Розроблено та впроваджено модель системи моніторингу веб-середовища для ІТС «Біржа медичних працівників» та розроблено методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних програм.

Це підтверджує самостійність обробки даних, практичні рекомендації та висновки.

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому кваліфікаційна робота задовольняє усім вимогам і може бути допущена до захисту, а його автор Резніченко Д.О. заслуговує на оцінку «_____».

Керівник спец. част.
ст. викл. кафедри БІТ В.І. Мєшков

ДОДАТОК Д. ЛІСТИНГ КОДУ

```
from collections import Counter
import pandas as pd
import string
from nltk.tokenize import TweetTokenizer
from nltk.corpus import stopwords
from nltk import pos_tag
import re
from sklearn.base import BaseEstimator, TransformerMixin
from sklearn.feature_extraction import DictVectorizer
from sklearn.feature_extraction.text import TfidfVectorizer, TfidfTransformer
from sklearn.feature_extraction.text import CountVectorizer
from nltk.stem.snowball import SnowballStemmer
from sklearn.pipeline import Pipeline, FeatureUnion
from preprocessor import preProcessSerie
import pickle
from sklearn.svm import SVC
from sklearn.model_selection import cross_val_score, KFold
def preProcessor(tweet):

                                    emoji_pattern = re.compile("["

u"\U0001F600-\U0001F64F"
u"\U0001F300-\U0001F5FF"
u"\U0001F680-\U0001F6FF"
u"\U0001F1E0-\U0001F1FF"
"]+", flags=re.UNICODE)
tweet = str(emoji_pattern.sub(r'', str(tweet)))
pal = tokenizer_1.tokenize(str(tweet))
urls = re.compile(r'.http[s]?://(?:[a-zA-Z]|[0-9]|[$-_@.&+]|[!*\(\),]|(?:%[0-
9a-fA-F][0-9a-fA-F]))+')
line = urls.sub('', str(tweet))
ht = re.compile(r'http.')
bar = re.compile(r'//*')
punctuation = set(string.punctuation)
stoplist = stopwords.words('english')
pr = ["rt","@","http","https","'s",'...', 'english', 'translation',')':', '. .', '..']
pal = [stemmer.stem(str(i)) for i in pal if i not in pr
if i not in stoplist if i not in punctuation
if not bar.search(i) if not ht.search(i)
if not i.isdigit() if not i.startswith('#')]
tweet = pal
```

```
return tweet
tokenizer_1 = TweetTokenizer(preserve_case=False, reduce_len=True,
strip_handles = True)
tokenizer_2 = TweetTokenizer(preserve_case=False, reduce_len=True,
strip_handles = False)
stemmer=SnowballStemmer("english")
listwords = []
                                    ngrams_featurizer = Pipeline([
('count_vectorizer', CountVectorizer(ngram_range=(1, 3), encoding='ISO-
8859-1',
analyzer=preProcessor)),
('tfidf_transformer', TfidfTransformer())
])
isis = pd.read_csv('isisfanboy.csv')
about = pd.read_csv('aboutisis.csv')
isis = isis[:17392]
about = about[:17392]
dataframe = pd.concat([isis, about])
X = dataframe['tweets'].values.astype('U')
y = dataframe['radical'].values
class POS(BaseEstimator, TransformerMixin):
def stats(self, tweet):
tokens = tokenizer_1.tokenize(str(tweet))
tagged = pos_tag(tokens, tagset='universal')
counts = Counter(tag for word, tag in tagged)
total = sum(counts.values())
pos_fts = {
'PRON': 0, 'NUM': 0,
'NOUN': 0, 'ADJ': 0,
'CONJ': 0, 'ADP': 0,
'VERB': 0, 'ADV': 0
                                    }
pos = dict((tag, float(count) / total) for tag, count in counts.items())
for key in pos:
pos_fts[key] = pos[key] if key in pos_fts else None
return pos_fts
def transform(self, data, y=None):
dataproc = preProcessSerie(data)
result = [self.stats(tweet) for tweet in dataproc]
return result
```

```
def fit(self, data, y=None):
return self
class Hashtags(BaseEstimator, TransformerMixin):
listwords = []
def fit(self, X, y=None):
return self
def notinlist(self, item, list_hashtags):
return False if item not in list_hashtags else True
def get_hashtags(self, tweet, list_hashtags):
list_hashtags = pickle.load(open("hashtags.pkl", "rb"))
return list_hashtags
def hashtags(self, tweet, all_hashtags, result_list):
all_hashtags_dict = dict((ht, 0) for ht in all_hashtags)
sent = tokenizer_2.tokenize(str(tweet))

                                        for term in sent:

all_hashtags_dict[term]=1 if term in all_hashtags else None
result_list.append(all_hashtags_dict)
return (result_list)
def transform(self, data):
dataproc = preProcessSerie(data)
list_ = []
result_list = []
list_ht = [self.get_hashtags(tweet, list_) for tweet in data]
result_list = [self.hashtags(tweet, list_ht, result_list) for tweet in dataproc]
return result_list
class NER(BaseEstimator, TransformerMixin):
def fit(self, X, y=None):
return self
def notinlist(self, item, list_ner):
return False if item not in list_ner else True
def get_ner(self, dataproc, list_ner):
list_ner = pickle.load(open("ner.p", "rb"))
return list_ner
def ner(self, tweet, all_ner_list, ner_s, result_list):
all_ner_dict = dict((entity, 0) for entity in all_ner_list)
words = tokenizer_2.tokenize(str(tweet))

                                        for i in words:

for k in all_ner_dict:
all_ner_dict[k] = 1 if i.lower() == k[0] and i.lower() in ner_s else None
result_list.append(all_ner_dict)
```

```
return (result_list)
def transform(self, data):
dataproc = preProcessSerie(data)
list_ner = []
result_list = []
ner_s = []
list_ner = self.get_ner(dataproc, list_ner)
[ner_s.append(k[0]) for k in list_ner]
for tweet in dataproc:
result_list = self.ner(tweet, result_list)
print(result_list[0])
return result_list
class Sentiment(BaseEstimator, TransformerMixin):
def fit(self, data, y=None):
return self
def transform(self, data, y=None):
sentiments = pickle.load(open("sentiments.pkl", "rb"))
list_sntms = []
for tweet in data:
if tweet != "nan":
try:
                                    print(tweet, sentiments[tweet])
tweetsent = sentiments[tweet]
list_sntms.append(tweetsent)
except:
list_sntms.append("NONE")
else:
list_sntms.append("NONE")
return list_sntms
pipelinesvm = Pipeline([
('features',
FeatureUnion([
('words', TfidfVectorizer(encoding='utf-8', analyzer=preProcessor)),
('ngrams', ngrams_featurizer),
('pos_stats', Pipeline([
('pos_stats', POS()),
('vectors', DictVectorizer())
])),
('ner', Pipeline([
('ner_recogniser', NER()),
('vectors', DictVectorizer())
])),
```

```
('hashtags', Pipeline([
('gethashtags', Hashtags()),
('vect', DictVectorizer())
])),
('sentiments', Pipeline([
('getsentiments', Sentiment()),
('vector', TfidfVectorizer(encoding='utf-8'))
]))

                                                    ])),

('clf', SVC(C=10, gamma= 1, kernel='rbf', probability=True)
)
])
cv = KFold(2, shuffle=True, random_state=33)
print(cv)
#
print(type(X.shape[0]))
scores = cross_val_score(pipelinesvm, X, y, cv=cv)
print("Scores in every iteration", scores)
print("Accuracy: %0.2f (+/- %0.2f)" % (scores.mean(), scores.std() * 2))
pipelinesvm.fit(X,y)
pickle.dump(pipelinesvm, open('model1.pkl', 'wb'))
pipelinesvm = pickle.load(open('model1.pkl', 'rb'))
print("Enter tweet to be classified")
tweet = input()

                                    print(pipelinesvm.predict([tweet]))
```

ДОДАТОК Е. РЕЗУЛЬТАТ ПЕРЕВІРКИ КВАЛІФІКАЦІЙНОЇ РОБОТИ НА ПЛАГІАТ