МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук

«____»_____ 2020 р.

МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Удосконалений модуль обробки інцидентів порушення інформаційної безпеки СУІБ

Автор: А.В. Дзюбенко

Науковий керівник: доц. Н.К. Гулак

Нормоконтролер: асист.

Київ 2020

ВСТУП

Актуальність. 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.

Варто відмітити, що в умовах сучасних трансформаційних явищ кожного дня створюється все більше компаній. Для оптимізації процесів виробничої діяльності такі підприємства зацікавлені в тому, щоб якомога більше підвищити ефективність функціонування інформаційної системи захисту підприємства (СЗП), в тому числі за допомогою моніторингу власних інтернет-середовища. В результаті це сприятиме покращенню продуктивності роботи підприємства 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 управління інформаційною безпекою (СУІБ).

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 фірми, так і цілковита втрата конкурентних переваг та рентабельності бізнесу. Альтернативою вирішення проблеми ефективної продуктивності компанії може стати впровадження автоматизованих стратегії

інтернет-моніторингу, адже програмне забезпечення для моніторингу веб-середовища позбавляє співробітників від спокуси дивитися онлайн-відео та відвідувати соціальні мережі, обмежуючи доступ до сайтів, які керівництво компанії вважає непотрібними чи загрозливими для бізнесу [17].

Крім того, електронні СУІБ значно покращують загальну якість виробничого процесу. Такі системи дозволяють оперативно отримувати необхідні відомості та моделювати нові методи, здатні внести корективи у режимі реального часу. Результатом використання автоматизованих СУІБ є поліпшення коефіцієнту корисної праці працівників компанії та мінімізація ризиків проникнення сторонніх з інформаційних ресурсів [3, с. 33].

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 СЗП. 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 підприємства є актуальним.

Метою роботи є розробка програмного продукту для удосконалення модуля обробки інцидентів порушення інформаційної безпеки СУІБ.

Для досягнення поставленої мети вирішуються такі **задачі:**

- аналіз теоретичних засад дослідження системи моніторингу веб-середовища;
- визначення переваги та недоліки наявних СУІБ;
- проектування моделі СУІБ для заданих умов;

- розробка програмного продукту для моніторингу веб-середовища на підприємстві.

Об’єктом дослідження є процес захисту інформації в ІКС.

Предметом дослідження є особливості застосування інформаційних технологій для реалізації системи інформаційного захисту.

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

Наукова новизна одержаних результатів. Результати дослідження пропонують альтернативний метод використання засобів системного програмування в процесі розробки СЗП на прикладі розробки удосконаленого модулю обробки порушень СУІБ на підприємстві.

Практичне значення одержаних результатів полягає в тому, що дослідження ґрунтується на результатах поглибленого вивчення особливостей застосування штучного інтелекту під час проектування інформаційної системи захисту на підприємстві.

Апробація. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- «Прикладні наукові розробки - 2020», 25.07.2020 р. – 30.07.2020 р., Чехія.
- «Наука та інновації – 2020», 07.10.2020 р. – 15.10.2020 р., Польща.

РОЗДІЛ 1.
ВІДОМОСТІ ПРО ОБ'ЄКТ РОЗРОБКИ

1.1. Загальна характеристика об'єкта дослідження

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.

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 [5].

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 [8]:

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 [9, с. 33].

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 [14, с. 200].

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 [22, с. 388]:

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).

Існує два основних типи моніторингу сайту, а саме:

1. Синтетичний моніторинг (активний моніторинг),

2. Пасивний моніторинг (реальний моніторинг).

Отже, вирішення проблеми ефективної продуктивності компанії може стати впровадження автоматизованих стратегії інтернет-моніторингу.

1.2. Постановка задачі дослідження

Метою є проектування модулю обробки порушень СУІБ на підприємстві.

Ставимо перед собою такі завдання:

1. проаналізувати теоретичні засади дослідження системи моніторингу веб-середовища;

2. визначити переваги та недоліки наявних СІМ;

3. дослідити алгоритм створення програми для моніторингу веб-середовища;

4. спроектувати модель СІМ для заданих умов;

5. розробити методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних програм.

Висновки до першого розділу

Підсумовуючи перший розділ, можемо зробити такі висновки:

1. Визначено, що 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-середовища необхідний для того, щоб забезпечити доступність веб-сайту для користувачів, мінімізувати час простою і оптимізувати продуктивність.

2. З’ясовано, що 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.

РОЗДІЛ 2.
ОПИС МЕТОДІВ ТА ЗАСОБІВ ВИРІШЕННЯ ЗАДАЧІ

2.1. Огляд та оцінка існуючих моделей

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].

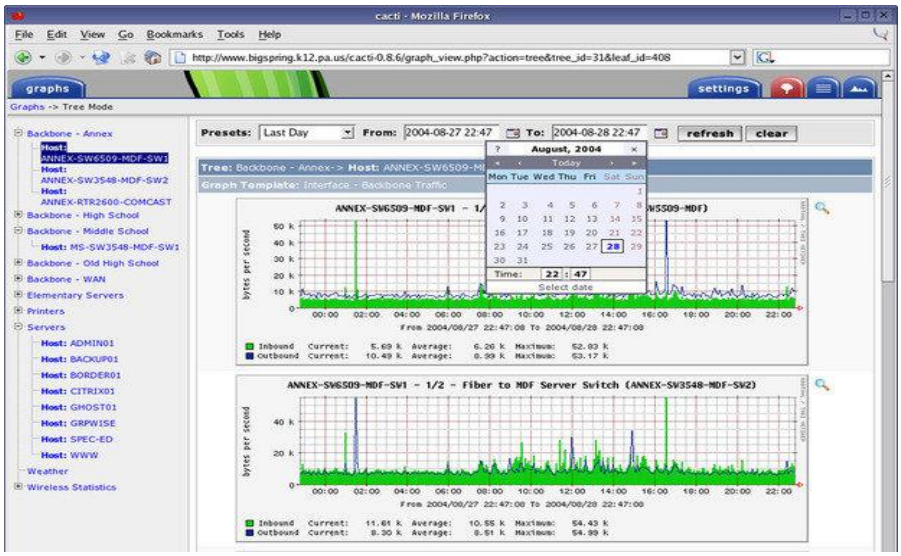

Рисунок 2.1 – Приклад інтерфейсу Cacti

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 [3, с. 33].

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 IT-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 [4].

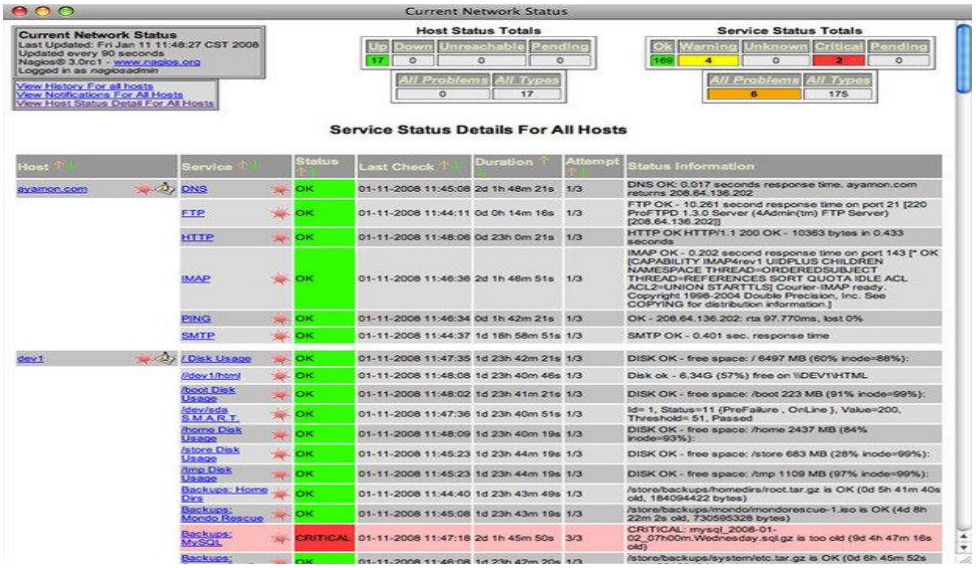

Рисунок 2.2 – Приклад інтерфейсу Nagios

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 [6].

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.

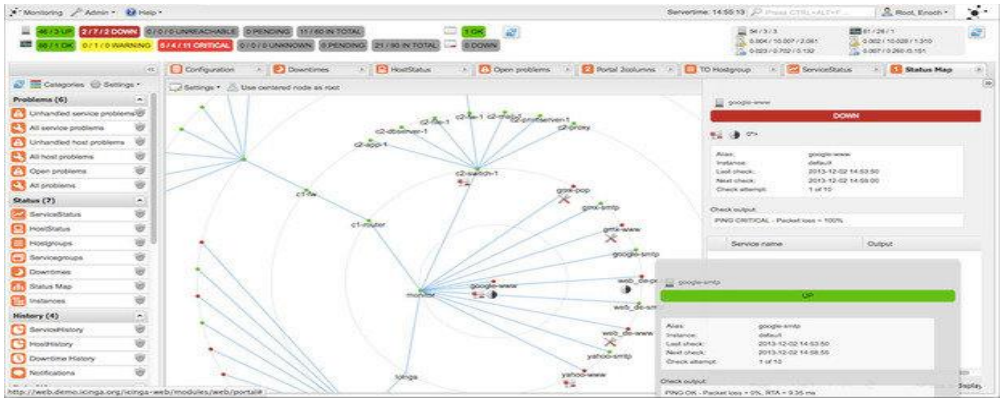

Рисунок 2.3 – Приклад інтерфейсу Icinga

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 [7].

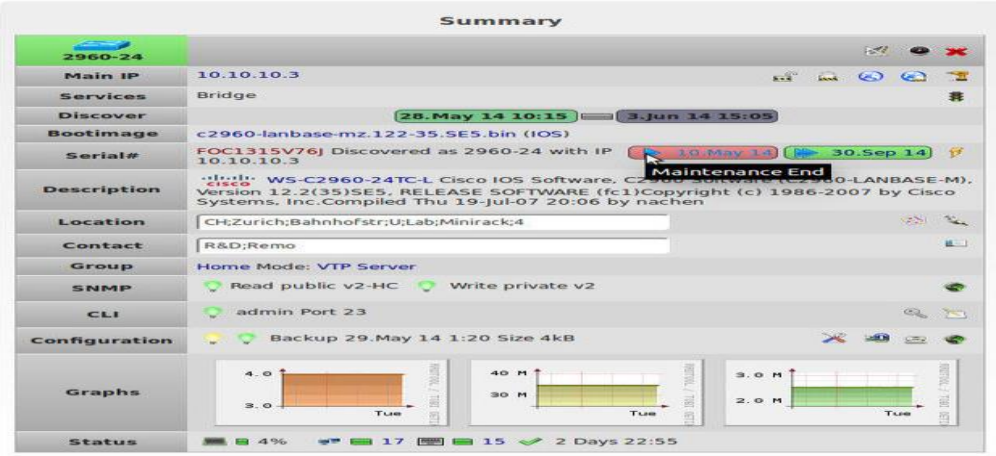

Рисунок 2.4 – Приклад інтерфейсу NeDi

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 [8].

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.

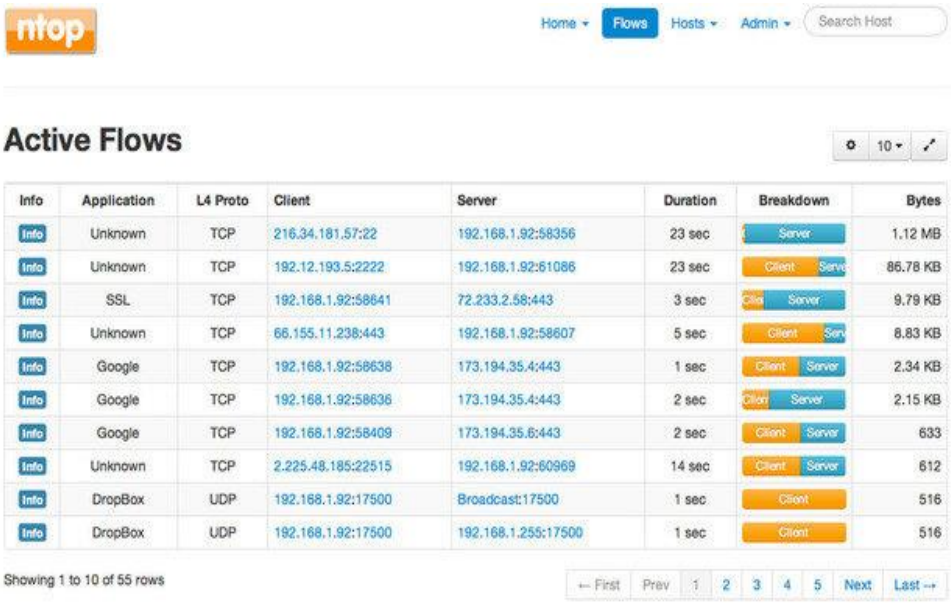

Рисунок 2.5 – Приклад інтерфейсу Ntop

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 [9].

Крім того, ви знайдете 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 ви навіть зможете 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 [11, с. 77].

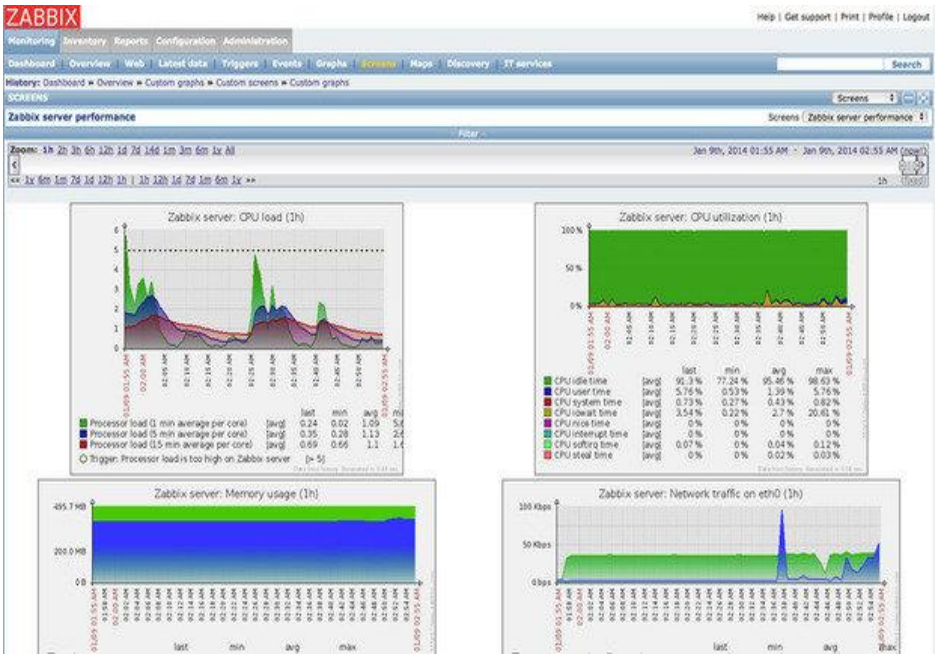

Рисунок 2.6 – Приклад інтерфейсу Zabbix

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 [12, с. 129].

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 [20, с. 180].

Він встановлюється як власний сервер з виділеною URL-адресою.

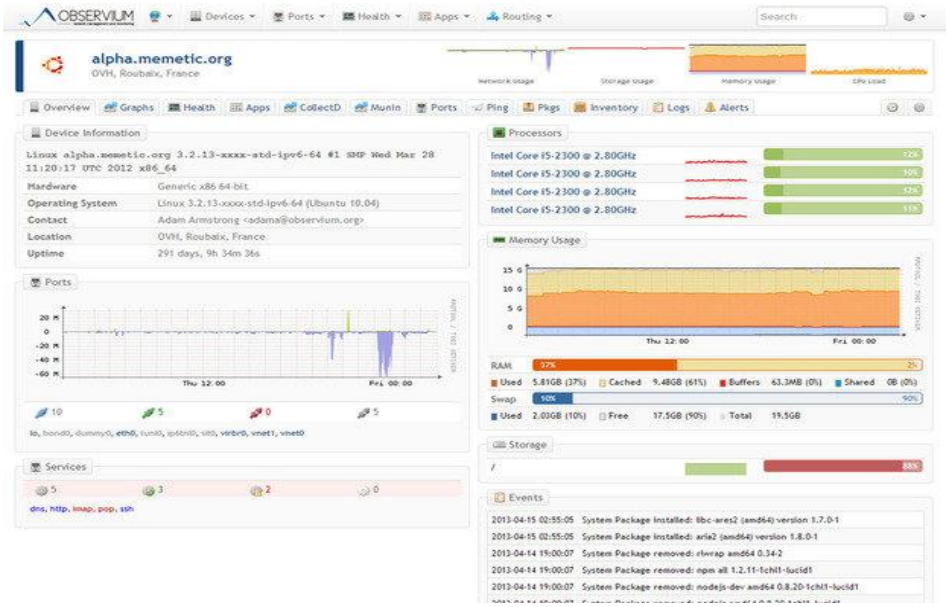

Рисунок 2.7 – Приклад інтерфейсу Observium

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 [7].

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 [4]:

- 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.

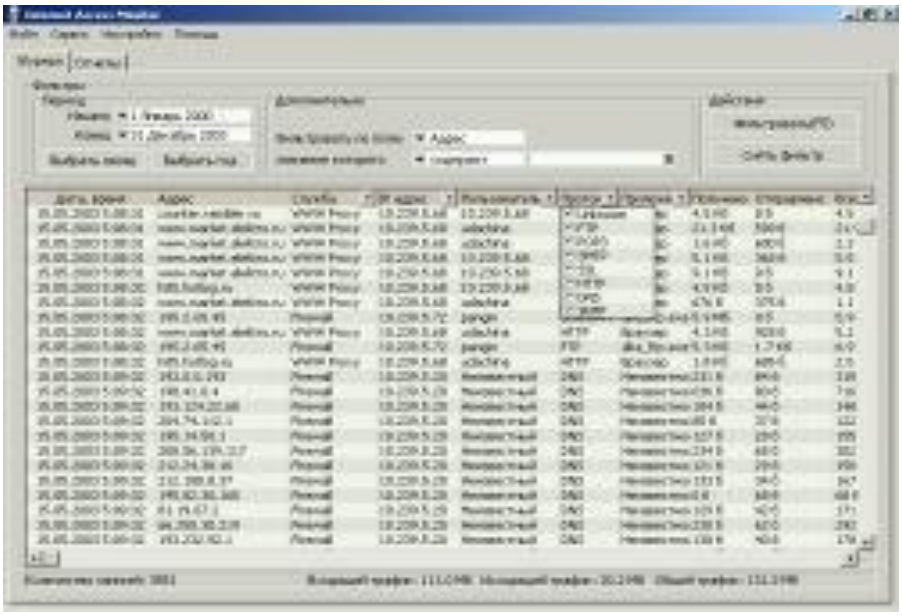

Рисунок 2.8 – Приклад програми Internet Access Monitor

Отже, на сьогоднішній день існує велика кількість моделей для моніторингу веб-середовища, проте багато з них має 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 раціональнішеза 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 [8].

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)

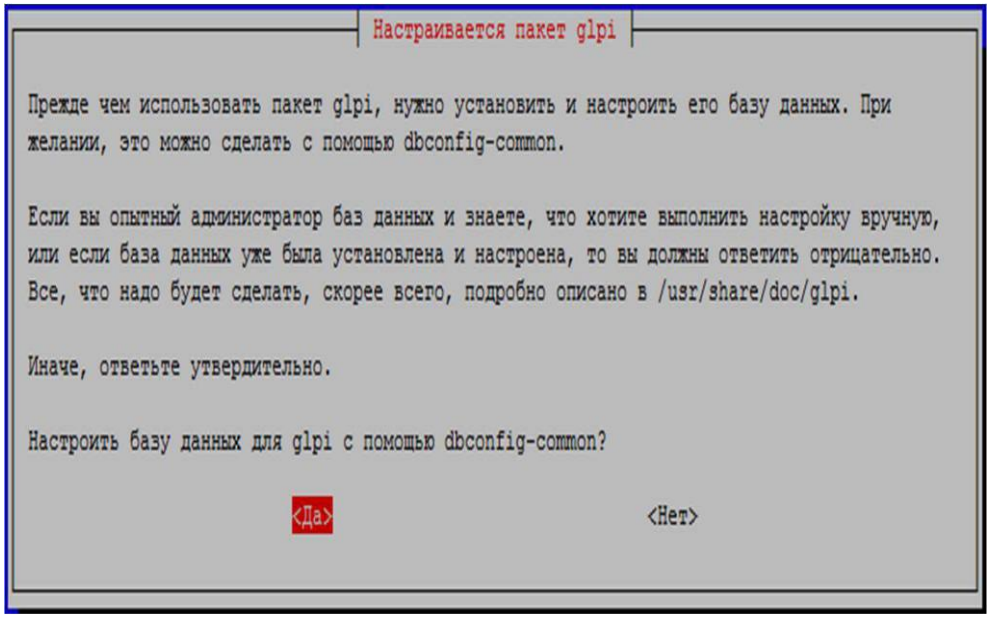

Рисунок 2.9 – Вікно налаштування бази даних

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).

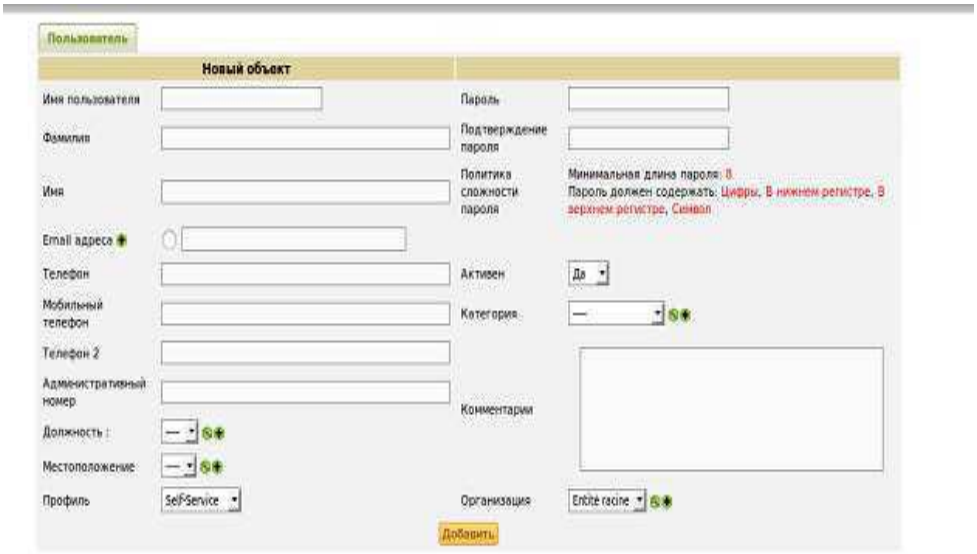

Рисунок 2.10 – Створення нового користувача

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).

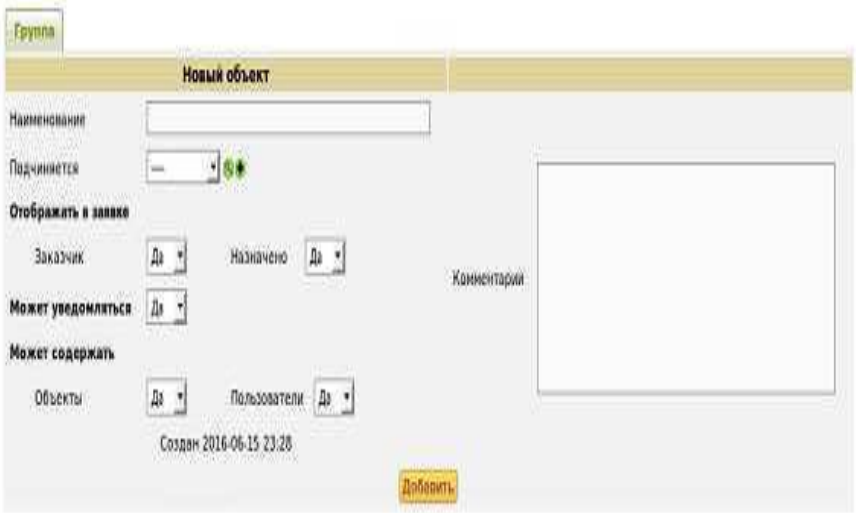

Рисунок 2.11 – Створення нової групи користувачів

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.

Висновки до другого розділу

Підсумовуючи другий розділ, можемо зробити такі висновки:

1. Розглянуто існуючі моделі CIM та визначені найбільш ефективні з точки зору пріоритезації для оптимізації в межах комерційних структур.

2. Проаналізовано підходи до проектування CIM та визначено алгоритм її створення.

РОЗДІЛ 3.
АНАЛІЗ РЕЗУЛЬТАТІВ ТА ПРАКТИЧНА РЕАЛІЗАЦІЯ ПРОГРАМИ

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.

2. Розробку структурної бази даних системи, що проектується.

3. Створення 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 бази даних (Рис. 3.2).

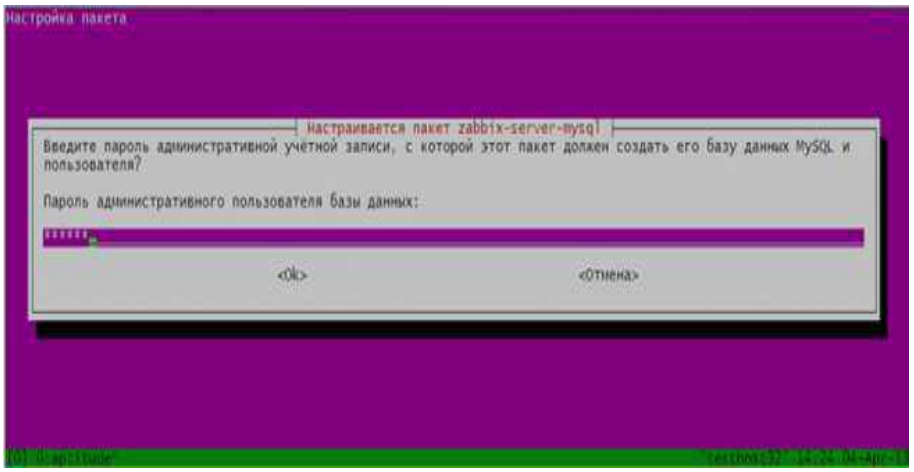

Рисунок 3.2 – Вікно налаштування прав доступу до бази

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

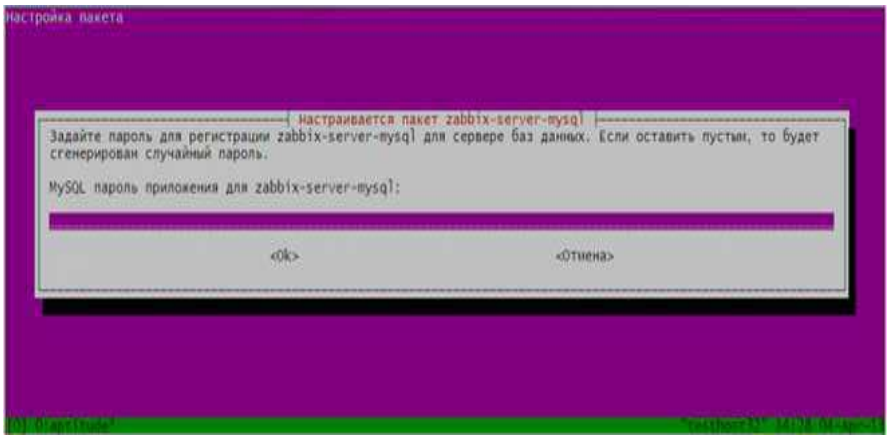

Рисунок 3.3 – Вікно налаштування паролю

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).

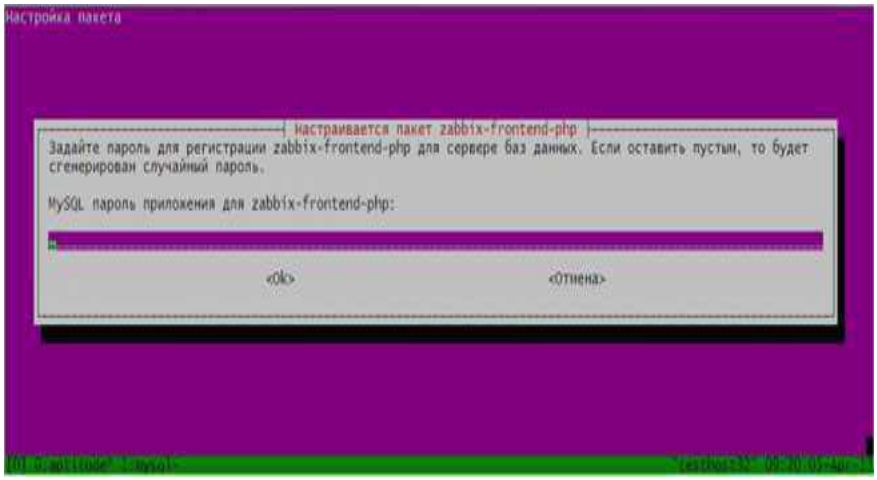

Рисунок 3.5 – Вікно налаштування паролю

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

- http://10.0.4.123/zabbix/

3.2. Впровадження програми 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).

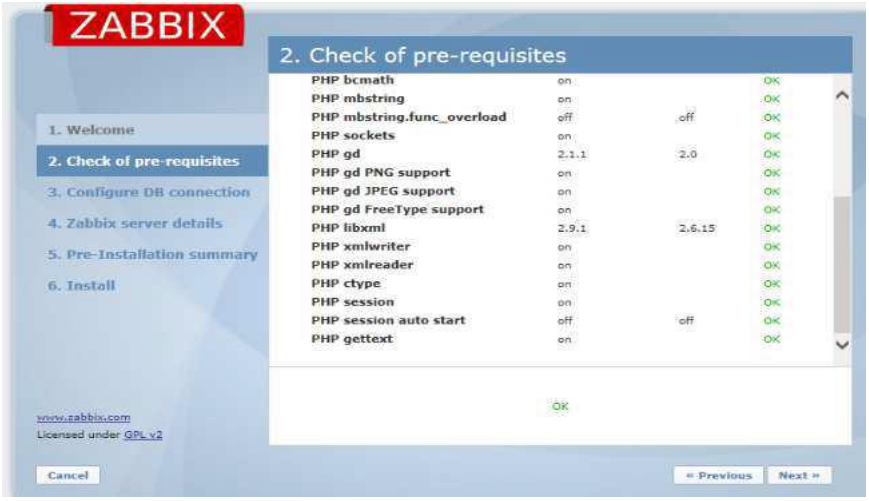

Рисунок 3.7 – Перевірка вимог ПЗ

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

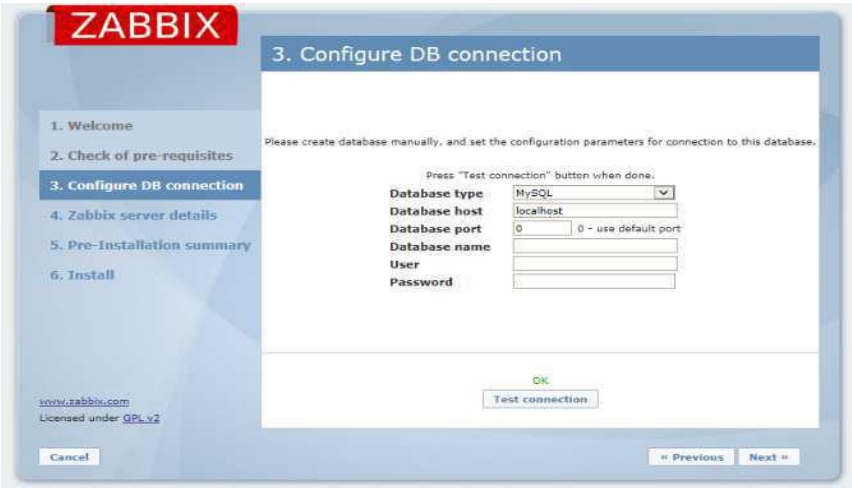

Рисунок 3.8 – Підключення до БД

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.

Дана форма свідчить про успішну установку автоматизованої системи.

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

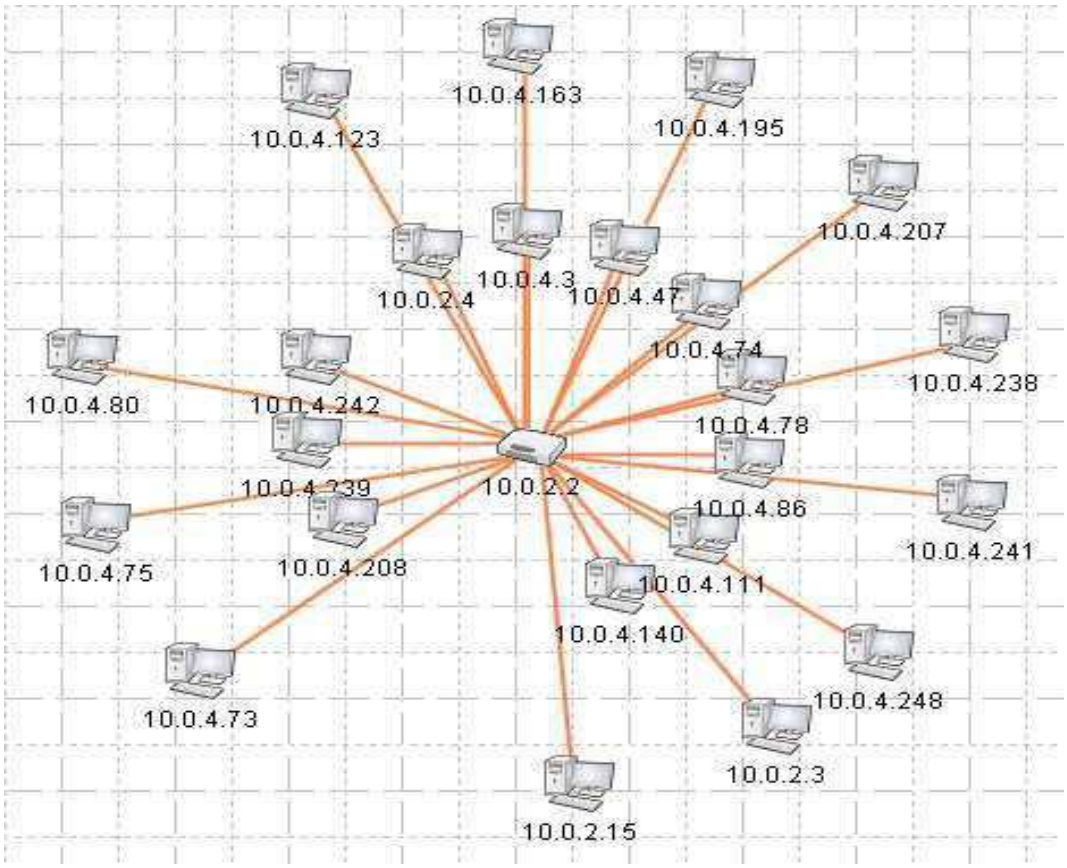

Рисунок 3.12 - Інфраструктура дільниці підприємства, де реалізовується спроектована модель CIM

Далі в рамках перевірки ефективності реалізації CIM розглянемо потреби у впровадженні системи на підприємстві. 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 співробітники бібліотечного фонду та читачі.

Забезпечує експлуатацію системи адміністратори.

Склад співробітників кожного 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. Пропозиції щодо успішного функціонування системи

Перерахуємо принципи успішного моніторингу веб-середовищем компанії:

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 підприємства 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 підприємством. 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 підприємства 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 підприємства 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

Висновки до третього розділу

Підсумовуючи третій розділ, можемо зробити такі висновки:

1. Розроблено структурну схему та архітектуру моделі CIM для підприємства.

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

3. Запропоновано практичні рекомендації щодо успішного функціонування системи.

РОЗДІЛ 4.

ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Даний розділ присвячений ідентифікації потенційних небезпек, аналізу та оцінюванню ризиків, а також розробці заходів щодо підвищення виробничої безпеки під час професійної діяльності працівників, які займаються створенням веб-сайту інтернет-магазину одягу.

Розділ розроблено відповідно до:

1. Закону України «Про охорону праці» від 16.10.2020 р.

2. Кодексу законів про працю України від 25.10.2020 р;

3. Постанови КМУ «Про порядок проведення атестації робочих місць за умовами праці» від 28.10.2016 р.

4. Наказу ДСНС України «Про загальні вимоги стосовно забезпечення роботодавцями охорони праці працівників» від 25.01.2012 р.

5. Типової інструкції з охорони праці для ІТ - фахівців.

1. Постановка завдання

Об’єктом обстеження на предмет визначення небезпек та аналізу ризиків є ІТ-підприємство Kozak Group. Компанія «Kozak Group» - це талановита і висококваліфікована команда професіоналів, що спеціалізується на розробці веб-сайтів і різних типів веб-орієнтованого програмного забезпечення. На сьогоднішній день компанія розробляє програмне забезпечення та обслуговує малі та середні підприємства по всьому світу, включаючи США, Австралію, Іспанію, Францію, Німеччину.

В даний час компанія має два офіси, розташованих на території України в Києві та Запоріжжі.

Сайт компанії знаходиться за адресою: https://kozak-group.com.

Метою проведення даного аналізу є визначення небезпек, аналізу можливих ризиків та аварій, а також та їх наслідків на підприємстві, з урахуванням наступних чинників:

- умов праці на підприємстві;
- значень параметрів виробничої діяльності підприємства;
- конструкційних особливостей, фактичного стану устаткування об'єкту обстеження, умови його експлуатації;
- технічних і організаційних можливостей в цілому по запобіганню переходу аварійної ситуації в аварію і локалізації наслідків аварії, що відбулася.

Аналіз був проведений на підставі даних, одержаних при вивченні законодавчо-нормативної документації, що регламентує вимоги безпеки, а також проектної і експлуатаційно-технічної документації, наданої керівництвом компанії Kozak Group.

2. Аналізування ризику

При великих масштабах виробництва зростає ймовірність і ступінь небезпеки виникнення вибухів і пожеж на підриємстві. Аналіз статистичних даних по багатьох країнах світу показує, що розміри щорічних матеріальних збитків від пожеж і вибухів у всіх технічно розвинених країнах мають тенденцію до неухильного зростання. При цьому збільшуються розміри матеріальних збитків від кожного окремого випадку - вибуху або пожежі, тому аналізування ризику виникнення можливих небезпек в межах ІТ-компанії здатне упередити чи мінімізувати виникнення аварійних ситуацій.

Аналіз ризику включає в себе аналіз і дослідження інформації про ризик на об'єкті. Аналіз ризику дозволяє визначити вхідні дані процесу загальної оцінки ризику, допомагає в прийнятті рішень щодо необхідності обробки ризику, а також допомагає вибрати відповідні стратегії і методи обробки ризику в межах ІТ-компанії. Аналіз ризику включає аналіз ймовірності і наслідків ідентифікованих

небезпечних подій з урахуванням наявності та ефективності застосовуваних методів управління. Дані про ймовірність подій і їх наслідки використовують для визначення рівня ризику.

Отже, представимо структурований перелік потенційних небезпек та джерел ризику на підприємстві «Kozak Group».

Таблиця 4.1

Структурований перелік потенційних небезпек та джерел ризику на підприємстві «Kozak Group»

№ з/п	Найменування потенційної небезпеки	Джерело
1. Потенційні небезпеки та джерела ризику при нормальному режимі функціонування об'єкту		
1.1	Підвищена запиленість і загазованість повітря робочої зони	На робочому місці працівників (шкідливий пил від кулерів ПК)
1.2	Підвищена або знижена температура повітря робочої зони	Обслуговування криогенного обладнання
1.3.	Підвищена або знижена вологість повітря робочої зони	Тепловиділення від центральних процесорів
1.4	Підвищений рівень статичної електрики, що досягає небезпечних рівнів	Під час перепаду температур на рабочому місці
1.5	Відсутність або нестача природного світла у світлий час доби	Вимоги до облаштування робочого місця працівника
1.6	Підвищена яскравість світла, що характеризує зорову роботу	Мерехтіння зображення при неправильній роботі монітора
1.7	Знижена контрастність, що характеризує зорову роботу	Неправильна робота монітору
1.8	Фізичне перевантаження:	
1.8.1	надмірне статичне перевантаження: - тривала багатогодинна (8 годин і більше) праця в одноманітному напруженому положенні; - мала рухова активність при значних локальних динамічних навантаженнях кістково-м'язового апарату кистей рук.	Умови праці на робочому місці працівника
1.8.2	Нервово-психічні перевантаження, що супроводжують трудову діяльність: - часте прийняття відповідальних рішень в умовах дефіциту часу; - безпосередній контакт із людьми різних типів темпераменту; - навантаження на елементи зорової системи;	Праця програмістів пов'язана з монотонністю

	- монотонність праці.	
2. Потенційні небезпеки та джерела ризику в умовах виникнення надзвичайної ситуації		
2.1 Надзвичайні ситуації техногенного характеру		
2.1.1	Пожежа у будівлі чи комунікаціях	Вихід з ладу пристроїв електроживлення
2.1.2	Вибух у будівлі чи комунікаціях	Під час пожежі обладнання
2.2 Надзвичайні ситуації соціального характеру		
2.2.1	Вчинення психічного впливу на людину (мобінг, булінг, шантаж)	Тиск з боку керівництва або колективу
2.2.2	Вчинення фізичного впливу на людину (нанесення побоїв)	Тиск з боку керівництва або колективу

3. Оцінювання ризику

В Україні для оцінки ризику та декларування безпеки об’єктів підвищеної небезпеки була розроблена Методика визначення ризиків та їх прийнятних рівнів для декларування безпеки об’єктів підвищеної небезпеки затверджена Наказом Міністерства праці та соціальної політики України № 637 від 04.12.2002 р. Методика включає аналіз небезпеки та умов виникнення аварій, оцінку ризику виникнення аварій, аналіз умов і оцінку ймовірності розвитку аварій, оцінку ймовірності наслідків аварій.

Отже, визначимо вірогідність реалізації небажаної події за умови впливу джерел небезпеки на досліджуваному об’єкті за формулою нижче згідно даних табл. 4.1:

$$P_d = 1 - \prod (1 - P_i)$$

де і – фактори, що обумовлюють потенційну небезпеку;

Рі – вірогідність реалізації і -ї небезпеки.

Для визначення вірогідності використовуємо наступну шкалу (табл. 4.2).

Таблиця 4.2

Аналізування джерел небезпеки компанії «Kozak Group»

№ з/п	Найменування потенційної небезпеки	*Pa*	*Q*	*R*
1	Підвищена запиленість і загазованість повітря робочої зони	5	1	5

2	Підвищена або знижена температура повітря робочої зони	7	5	35
3	Підвищена або знижена вологість повітря робочої зони	7	5	35
4	Підвищений рівень статичної електрики, що досягає небезпечних рівнів	8	2	16
5	Відсутність або нестача природного світла у світлий час доби	8	1	8
6	Підвищена яскравість світла, що характеризує зорову роботу	7	3	21
7	Знижена контрастність, що характеризує зорову роботу	7	2	14
8	Фізичне перевантаження:			
8.1	надмірне статичне перевантаження: - тривала багатогодинна (8 годин і більше) праця в одноманітному напруженому положенні; - мала рухова активність при значних локальних динамічних навантаженнях кістково-м’язового апарату кистей рук.	8	2	16
8.2	Нервово-психічні перевантаження, що супроводжують трудову діяльність: - часте прийняття відповідальних рішень в умовах дефіциту часу; - безпосередній контакт із людьми різних типів темпераменту; - навантаження на елементи зорової системи; - монотонність праці.	8	3	21
9	Пожежа у будівлі чи комунікаціях	7	9	63
10	Вибух у будівлі чи комунікаціях	5	10	50
11	Вчинення психічного впливу на людину (мобінг, булінг, шантаж)	6	2	12
12	Вчинення фізичного впливу на людину (нанесення побоїв)	6	3	18

Отже, як бачимо за результатами аналізування небезпеки компанії «Kozak Group» згідно розрахованим даним табл. 4.2, найбільш ймовірними та небезпечними загрозами є: пожежа у будівлі чи комунікаціях, вибух у будівлі чи комунікаціях, підвищена або знижена температура повітря робочої зони, Підвищена або знижена температура повітря робочої зони.

4. Обробляння ризику компанії «Kozak Group»

Важливим напрямом стосовно визначення професійної придатності фахівців з інформаційних технологій є проведення психофізіологічної експертизи відповідно до 5 статті Закону України «Про охорону праці».

Робота з комп'ютерами нового покоління характеризується певним психофізіологічними перенавантаженнями, втомою зорового аналізатора, гіпокінезією, відсутність диференційованих норм праці при роботі з новою комп'ютерною технікою в залежності від віку, статі, категорії зорової роботи, режимів праці і відпочинку (протягом робочого дня, тижня, щорічного режиму відпусток).

Все це потребує розробки нових нормативно-правових актів з регламентації праці та відпочинку фахівців IT-індустрії і стандартів підприємств, центрів комп'ютерної техніки, центрів інформаційних технологій, сучасних комп'ютерних класів.

Особлива роль з точки зору збереження та відновлення здоров'я працюючих в комп'ютерні' галузі належить попереднім та періодичним наглядам з подальшої психофізіологічної експертизи і встановленням професійної придатності при роботі з комп'ютерами нового покоління, який супроводжується виникненням певних факторів професійного ризику електротравматизму при їх ремонті та обслуговуванні. В цьому зв'язку необхідне запровадження експертизи на предмет безпечної експлуатації ПЕОМ, тобто офіційне підтвердження фактичних параметрів електробезпеки, їх відповідності вимогам нормативної документації фахівців, які проводять таку експертизу повинні пройти навчання і перевірку знань відповідно до вимог ДНАОП 0.00-8.20-99. За результатами експертизи повинні прийматися рішення про відповідність ПЕОМ нормам безпеки, терміни чергової експертизи, оформлюються протоколи вимірювань і випробувань, проведені у разі потреби розрахунки та експертний висновок.

Для підвищення розумової працездатності то зорової роботи повинна здійснюватися ергономічна оптимізація в рамках системи «оператор-термінал», яка

сприятиме результативній фізичній та інтелектуальний працездатності і відновленню психосоматичного здоров’я фахівців ІТ-індустрії.

Заслуговує на увагу зарубіжний досвід створення у приміщеннях та в зоні їх розміщення на територіях підприємств спеціальних візуальних комфортних умов та забезпечення вимог виробничої естетики, дотримання норм рівнів виробничого шуму та акустичної тиші за межами офісу. Також дуже важливим є використання в офісних приміщеннях та кабінетах психофізіологічного розвантаження функціональної музики, яка сприяє попередженню перевтоми і підтриманню необхідного рівня розумової працездатності фахівців комп’ютерної галузі.

В цьому напрямі заслуговує на увагу створення при великих центрах інформаційних технологій кімнат (кабінетів) психофізіологічного розвантаження працівників галузі (на 5 місць).

Зарубіжний досвід охорони праці при використанні новітніх інформаційних технологій та сучасного комп’ютерного обладнання передбачає з метою попередження наслідків монотонної праці, підвищення рівня рухової активності і покращення розумової працездатності фахівців ІТ-індустрії під час технологічних перерв участь у спеціальних облаштованих приміщеннях необхідним спортивним інвентарем та різними тренажерами відповідних фізичних вправ, індивідуальних тренінгових завдань відповідно до віку, статі та категорії зорової роботи. Такий підхід дозволяє зняти надлишкове психофізіологічне перевантаження, підвищити працездатність центральної нервової системи, попередити перевтому зорового аналізатора. Показана ефективність проведення різноманітних за своєю спрямованістю вправ робітників цієї галузі (приблизно на 5-30%).

Всі наведені заходи щодо вдосконалення охорони праці фахівців ІТ-індустрії повинні контролюватися службою охорони праці та комісією з охорони праці підприємства «Kozak Group».

Особливе значення у соціальному захисті цієї категорії працівників належить прийняття комплексного договору, який може забезпечити фахівців додатковими пільгами та компенсаціями.

5. Висновки

Аналіз умов праці ІТ-фахівців підприємства «Kozak Group» свідчить про наявність та можливий вплив наступних шкідливих та небезпечних чинників: шуму; несприятливого мікроклімату (тепловиділення, високі температури при нагріві центральних процесорів та блоків живлення та низькі – при проведенні ремонтних робіт та обслуговування криогенного обладнання квантових комп'ютерів; іонізуючі і неіонізуючі випромінювання (рентгенівське, інфрачервоне, електромагнітне ВЧ і СВЧ діапазону, статичної електрики); недостатнє штучне та природнє освітлення; візуальні фактори: надмірна яскравість, контрастність, мерехтіння зображення, відблиски тощо. Враховуючи, що для забезпечення роботи квантових комп'ютерів потрібна напруга понад 1000В, проведення з ними роботи потребує відповідних заходів електробезпеки та здійснення психофізіологічної експертизи.

Для підвищення ефективності системи управління охорони праці (СУОП) підприємства «Kozak Group» дуже важлива роль належить формуванню і розвитку інформаційної культури ІТ-фахівців компанії, яка впливає на удосконалення інформаційного контуру сучасних підприємств, дозволяє створювати надійні прогнози щодо стану умов праці, показників здоров'я та працездатності, виробничого травматизму і професійної захворюваності, визначати політику розвитку підприємств, установ та організацій на основі різноманітних стратегій охорони праці (інноваційні, маркетингові, інвестиційні, фінансові, технологічні, диверсифікаційні). Поряд з інформаційною культурою важливо використовувати в рамках СУОП «трикутник» її складових: правову (8,1 за 10-бальною шкалою), організаційну (8,0), управлінську (7,5).

З метою вдосконалення охорони праці фахівців з сучасних інформаційних технології розроблені системні заходи з правової оптимізації, соціального захисту працівників, діагностики їх професійної придатності, необхідності обґрунтування диференційованих норм праці при роботі з новою комп'ютерною технікою в

залежності від віку, статі, категорії зорової роботи, режимів праці та відпочинку (протягом робочого дня, тижня, щорічного режиму відпустки).

Для підвищення ефективності розумової працездатності та зорової роботи повинне здійснюватися ергономічна оптимізація в рамках системи «оператор-термінал», яка сприятиме результативній фізичній та інтелектуальний працездатності і відновленню психосоматичного здоров'я фахівця ІТ-індустрії. В цьому напрямі заслуговує на увагу створення при великих центрах інформаційних технологій кімнат (кабінетів) психофізіологічного розвантаження (на 5 місць). Заслуговує на увагу зарубіжний досвід створення у приміщеннях та в зоні їх розміщення на територіях підприємств спеціальних візуальних комфортних умов та забезпечення вимог виробничої естетики, дотримання норм рівнів виробничого шуму та акустичної тиші за межами офісу.

Також дуже важливим є використання в офісних приміщеннях та кабінетах психофізіологічного розвантаження функціональної музики, яка сприяє попередженню перевтоми і підтриманню необхідного рівня розумової працездатності фахівців комп'ютерної галузі. Все це сприяє підвищенню ефективності роботи з новою комп'ютерною технікою приблизно на 10-15% у порівнянні з традиційною моделлю охорони праці фахівців з НІТ. Пропозиції та заходи щодо удосконалення охорони праці фахівців з сучасних інформаційних технологій запроваджено на підприємстві «Kozak Group», розроблено інструкцію з охорони праці при роботі за комп'ютером. Використання заходів з удосконалення охорони праці фахівців сфери ІТ-індустрії суттєво розширює інформаційну культуру працівників, формує копінг-стратегії (поведінку безпеки праці), попереджує розвиток перевтоми, знижує ризик психофізіологічних перенавантажень при роботі з новою комп'ютерною технікою.

ВИСНОВКИ

Підсумовуючи загальний зміст дослідження, можемо констатувати наступне:

1. Для оптимізації процесів виробничої діяльності підприємства зацікавлені в тому, щоб якомога більше підвищити автоматизаційні можливості моніторингу власних інтернет-продуктів. В результаті це сприятиме покращенню продуктивності роботи установи 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. 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-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. 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.

5. 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.

5. Задачі веб-моніторингу включають в себе:

- 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.

6. Розроблено та впроваджено модель системи моніторингу веб-середовища в рамках комерційного підприємства 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 моніторингу веб-середовища;

- визначино переваги та недоліки наявних СІМ;

- досліджено алгоритм створення програми для моніторингу веб-середовища;

- спроектувано модель СІМ для заданих умов;

- розроблено методичні рекомендації щодо використання засобів системного програмування для реалізації клієнт-сервісних систем під час створення програми моніторингу веб-середовища з метою забезпечення інформаційної безпеки підприємства.

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

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

4. Інтернет-ресурс. Режим доступу - http://www.itfb.com.ua/monitoring.html.

5. Інтернет-ресурс. Режим доступу - http://habrahabr.ru/company/ croc/blog/14494.

6. Інтернет-ресурс. Режим доступу - http://www.pingwinsoft.ru/pages/ resheniya /resheniya/pwsitmonitoring.

7. Інтернет-ресурс. Режим доступу - http://amigosteam.ru/blog/item/11-zabbix.

8. Інтернет-ресурс. Режим доступу - http://www.opennms.org.

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

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

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

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

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

14. Роберт Каллан. Основні концепції нейроних мереж = The Essence of Neural Networks First Edition. - 1-е. - «Вильямс», 2001. - С. 200-233.

15. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Д. Рутковская, М. Пилиньский, Л. Рутковский. - М. Горячая линия-Телеком. 2004. – С. 34-46.

16. Саати Томас Л. Принятие решений при зависимостях и обратных связях: Аналитические сети [Текст] Пер. с англ. / Науч. Ред. А. В. Андрейчиков, О. Н. Андрейчикова. – М.: Издательство ЛКИ, 2008. – С. 28-39.

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

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

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

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

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

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

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

24. 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.

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

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

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

28. 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.

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

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