

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

**І. А. Терейковський, Л. О. Терейковська,
К. О. Радченко**

ЗАХИСТ ІНФОРМАЦІЇ ВІД ВИТОКІВ ЛАБОРАТОРНИЙ ПРАКТИКУМ

*Рекомендовано Методичною радою КПІ ім. Ігоря Сікорського
як навчальний посібник для студентів,
які навчаються за спеціальністю 123 «Комп'ютерна інженерія»,
спеціалізацій «Комп'ютерні системи та компоненти»; «Системне
програмування»; «Спеціалізовані комп'ютерні системи»*

Київ
КПІ ім. Ігоря Сікорського
2018

Рецензенти: *Козловський В. В.*, д-р техн. наук, проф.
Лахно В. А., д-р техн. наук, проф.

Відповідальний редактор *Тесленко О. К.*, канд. техн. наук, доц.

*Гриф надано Методичною радою КПІ ім. Ігоря Сікорського (протокол № 9 від 24.05.2018 р.)
за поданням Вченої ради факультету прикладної математики (протокол № 9 від
23.04.2018 р.)*

Електронне мережне навчальне видання

Терейковський Ігор Анатолійович, д-р техн. наук, доц.
Терейковська Людмила Олексіївна, канд. техн. наук, доц.
Радченко Костянтин Олександрович, асист.

Захист інформації від витоків

Лабораторний практикум

Захист інформації від витоків. Лабораторний практикум [Електронний ресурс]: навч. посіб. для студ. спеціальності 123 «Комп'ютерна інженерія», спеціалізацій «Комп'ютерні системи та компоненти»; «Системне програмування»; «Спеціалізовані комп'ютерні системи» / І. А. Терейковський, Л. О. Терейковська, К. О. Радченко; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 6,01 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 81 с.

Лабораторний практикум призначений для використання студентами під керівництвом викладача та самостійно на практичних та лабораторних заняттях із захисту інформації в комп'ютерних системах. Завданням даного практикуму є набуття студентами практичних навичок використання сучасних методів управління доступом до захищених ресурсів комп'ютерної системи; основних принципів захисту інформації, порядок формування комплексу засобів захисту інформації; прийомів захисту інформації від витоків в операційних системах; розробки та застосування програмних засобів захисту інформації від витоків.

© І. А. Терейковський, Л. О. Терейковська, К. О. Радченко, 2018
© КПІ ім. Ігоря Сікорського, 2018

Зміст

ВСТУП	4
ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ЛАБОРАТОРНІ РОБОТИ.....	5
ЛАБОРАТОРНА РОБОТА №1 «ТЕХНОЛОГІЯ УСТАНОВКИ ТА ПЕРШОЧЕРГОВОГО НАЛАШТУВАННЯ ПРОГРАМНОГО КОМПЛЕКСУ SEARCHINFORM»	6
Хід виконання роботи.....	7
Питання для самоперевірки.....	34
ЛАБОРАТОРНА РОБОТА №2 «ПРИНЦИПИ ВИКОРИСТАННЯ ПРОГРАМНОГО КОМПЛЕКСУ SEARCHINFORM ДЛЯ МОНІТОРИНГУ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ».....	35
Хід виконання роботи.....	39
Питання для самоперевірки.....	78
РЕКОМЕНДОВАНА ЛІТЕРАТУРА	79
Базова література.....	79
Допоміжна література.....	80
Інформаційні ресурси.....	81

ВСТУП

Дисципліна «Захист інформації в комп'ютерних системах» є важливою складовою підготовки кваліфікованих бакалаврів за спеціальністю 123 «Комп'ютерна інженерія». Вона містить такі важливі складові, як аналіз вимог до системи захисту інформації в комп'ютерних системах; обрання засобів захисту інформації об'єктів комп'ютерних систем; розробка системи захисту інформації в комп'ютерних системах; виконання базових операцій по застосуванню засобів захисту інформації в комп'ютерних системах тощо, які дозволяють вирішити задачі визначення стійкості парольного захисту, виявлення витоків конфіденційної інформації при її передачі за допомогою: електронної пошти, служби обміну миттєвими повідомленнями (ICQ, QIP), веб-клієнтів (передача даних по протоколу HTTP в соціальні мережі, форуми, блоги), ftp-клієнтів, голосових і текстових повідомлень Skype, записі на зовнішні пристрої (Flash-носії, компакт-диски, зовнішні жорсткі диски), друку на принтері. Крім цього, існує можливість виявлення конфіденційної інформації на комп'ютерах користувачів, а також моніторингу зображень на дисплеї користувача.

Відповідно до наведених аспектів та згідно із робочою навчальною програмою дисципліни «Захист інформації в комп'ютерних системах» завданням даних методичних вказівок є набуття студентами практичних навичок створення сучасних методів управління доступом до захищених ресурсів комп'ютерної системи; особливостей інформації як об'єкту захисту нівелювання основних загроз інформації в комп'ютерних системах; основних принципів захисту інформації від витоків, порядок формування комплексу засобів захисту інформації; прийомів захисту інформації від витоків у операційних системах; способів та засобів захисту інформації від витоків технічними каналами; порядок визначення вимог щодо захисту інформації в комп'ютерній системі; розробка та застосування програмних засобів захисту інформації, набуття практичного досвіду з розробки та використання відповідних засобів захисту.

ЗАГАЛЬНА ІНФОРМАЦІЯ ПРО ЛАБОРАТОРНІ РОБОТИ

Даний лабораторний практикум охоплює наступні лабораторні роботи:

№ 1: "Технологія установки та першочергового налаштування програмного комплексу SearchInform" (обсяг: 6 академічних годин).

№ 2: "Принципи використання програмного комплексу SearchInform для моніторингу витоку конфіденційної інформації" (обсяг: 6 академічних годин).

Порядок виконання лабораторних робіт

1. Ознайомлення з метою, загальним завданням та теоретичними відомостями відповідної лабораторної роботи.
2. Розробка плану виконання роботи.
3. Виконання завдання, використовуючи вказані у завданні технології, інструментальне програмне забезпечення тощо.
4. Тестування окремих програмних модулів та програми в цілому.
5. Підготовка відповідей на питання для самоперевірки до роботи.
6. Підготовка протоколу виконання лабораторної роботи.
7. Демонстрація викладачеві результатів функціонування програми.

Вимоги до формлення лабораторних робіт

Протокол має містити наступні складові частини, які розміщують кожен з нової сторінки: титульний аркуш, загальне завдання до лабораторної роботи, діаграма структури програми із призначенням кожного модуля, екранні форми («screenshots») візуального інтерфейсу програмних модулів, відповіді на питання для самоперевірки.

ЛАБОРАТОРНА РОБОТА № 1 «ТЕХНОЛОГІЯ УСТАНОВКИ І ПЕРШОЧЕРГОВОГО НАЛАШТУВАННЯ ПРОГРАМНОГО КОМПЛЕКСУ SEARCHINFORM»

Мета лабораторної роботи засвоїти основні прийоми використання програмного комплексу SearchInform.

Теоретичні відомості. Перед виконанням лабораторної роботи слід ознайомитися з прийомами використання емулятора віртуального комп'ютера VMware Player.

Запропонована для вивчення версія програмного комплексу «Контур інформаційної безпеки *SearchInform*» призначена для виявлення витоків конфіденційної інформації при її передачі за допомогою:

- електронної пошти,
- служби обміну миттєвими повідомленнями (ICQ, QIP),
- веб-клієнтів (передача даних по протоколу HTTP в соціальні мережі, форуми, блоги),
- ftp-клієнтів,
- голосових і текстових повідомлень Skype,
- записі на зовнішні пристрої (Flash-носії, компакт-диски, зовнішні жорсткі диски),
- друку на принтері.

Крім цього, існує можливість виявлення конфіденційної інформації на комп'ютерах користувачів, а також моніторингу зображень на дисплеї користувача.

Укрупнено виявлення витоків інформації розділяється на чотири етапи:

- перехват інформації, переданої по контрольованим каналам,
- запис перехваченої інформації у сховище,
- пошук в інформаційному сховищі конфіденційних даних,
- оповіщення про знайдені конфіденційні дані.

Завдання на лабораторну роботу:

1. Встановити програмний комплекс VMware Player з образом операційної системи Windows Server і встановленою системою *SearchInform*.
2. Встановити пароль на обліковий запис адміністратора операційної системи Windows Server.
3. Використовуючи вбудовані засоби захисту *SearchInform* змінити паролі доступу до консолей.
4. Обмежити права доступу користувачів до індексів *Search Server*.
5. Управління користувачами системних служб *SearchInform*.
6. Налаштувати параметри функціонування *SearchInform AlertCenter*.
7. Налаштування системної служби *SearchInform DataCenter: agent*.
8. Налаштування параметрів функціонування *SearchInform NetworkSniffer*.

Хід виконання роботи

1. Підготовчі роботи

- Встановити програмний комплекс VMware Player.
- В папку вказану викладачем скопіювати образ комп'ютера з операційною системою Windows Server і встановленою системою SearchInform (папка VMwareSI).
- Запустити VMware Player, вікно якого показано на рис. 1.1.



Рис. 1.1. Вікно VMware Player

- Використовуючи VMware Player, відповідно до рис. 1.2 – 1.4 запустити віртуальний комп'ютер. В подальшому вся робота виконується тільки на віртуальному комп'ютері, вікно якого показано на рис. 1.5.

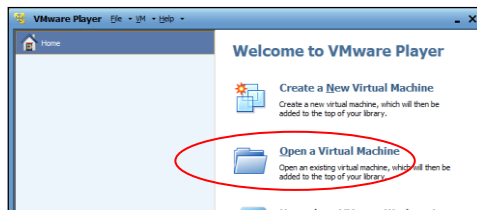


Рис. 1.2. Відкриття файлу образу

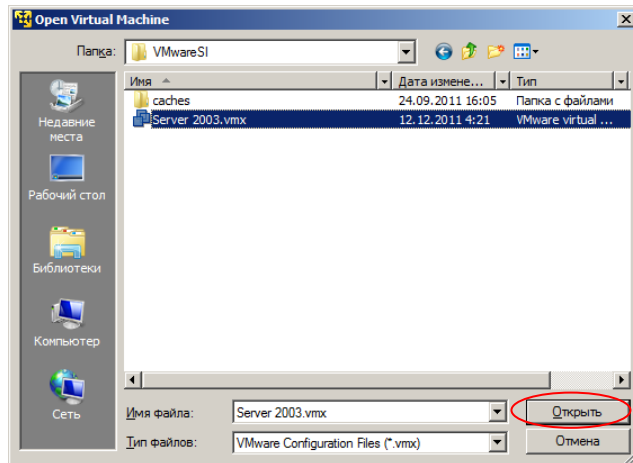


Рис. 1.3. Вибір файлу образу

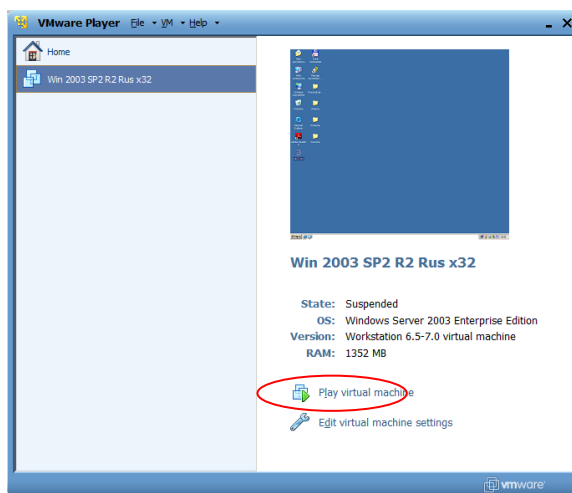


Рис. 1.4. Запуск файлу образу

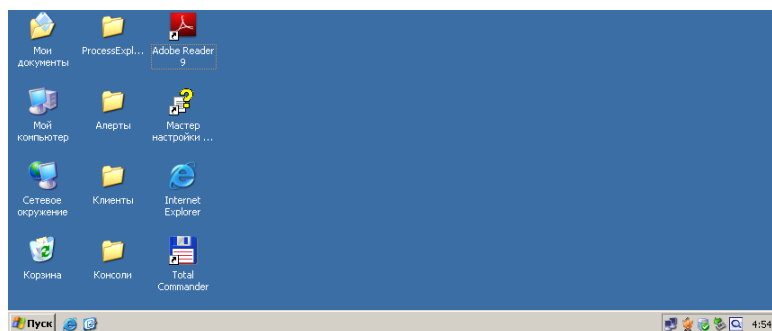


Рис. 1.5. Вікно віртуального комп'ютеру

2. Встановить пароль на обліковий запис адміністратора операційної системи Windows Server. Для цього:

- Відповідно до рис. 1.6 – 1.8 слід запустити оснащення управління комп'ютером.

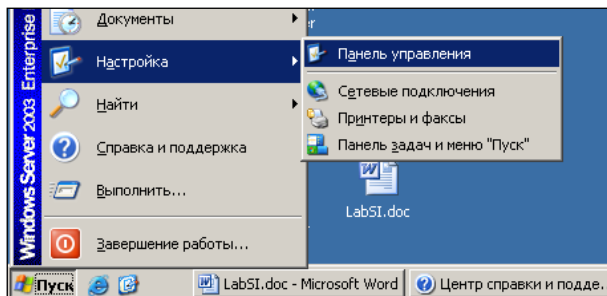


Рис. 1.6. Запуск панели управления

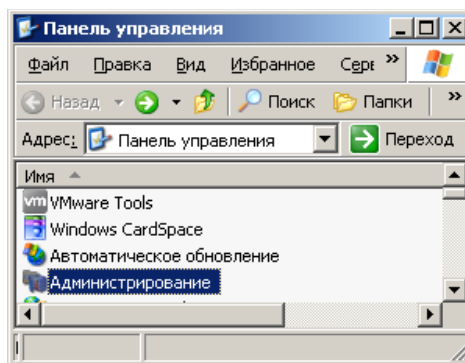


Рис. 1.7. Запуск оснащения администрирования

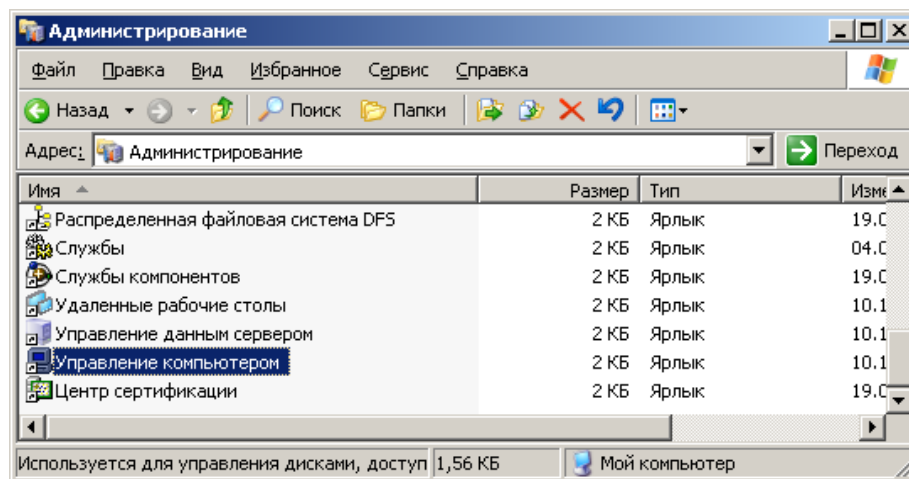


Рис. 1.8. Запуск оснащения управления комп'ютером

- Відповідно до рис. 1.9 – 1.11 входимо в режим зміни паролських даних адміністратора системи

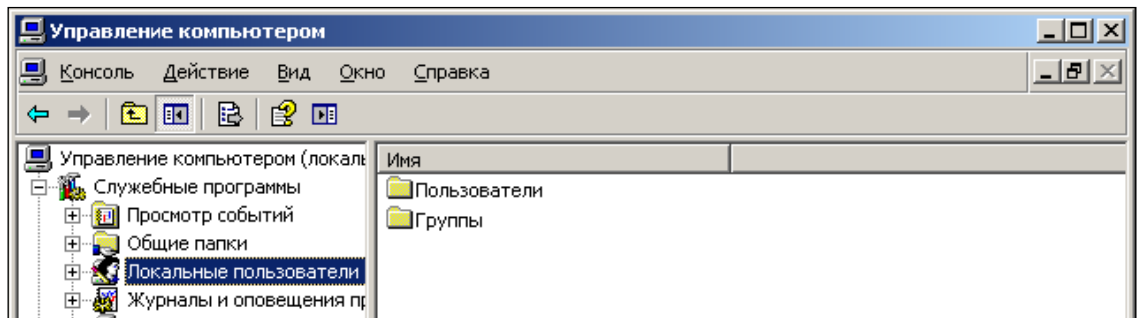


Рис. 1.9. Перехід у режим зміни параметрів локальних користувачів

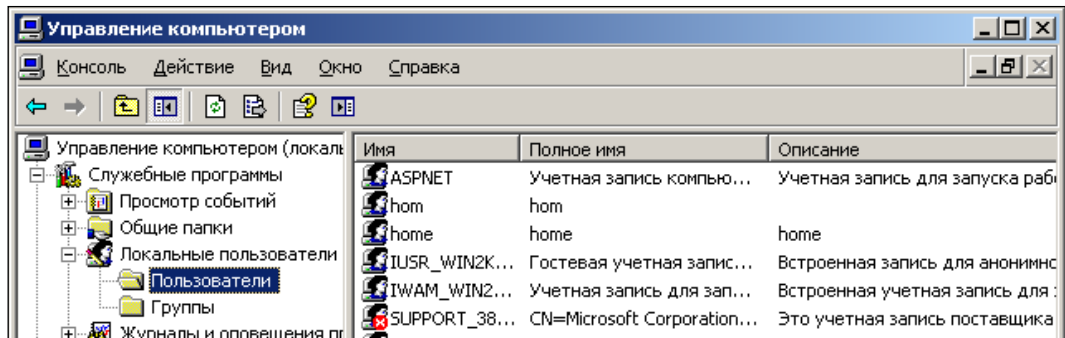


Рис. 1.10. Вікно параметрів локальних користувачів

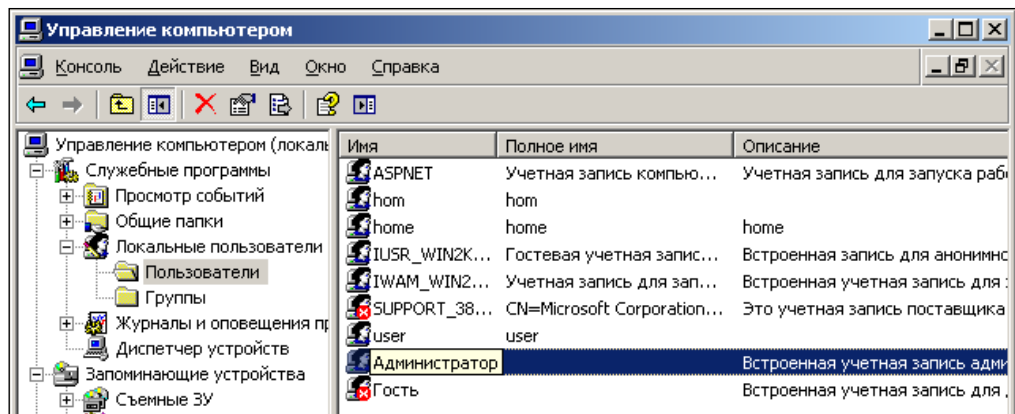


Рис. 1.11. Вхід в режим редагування параметрів адміністратора системи

- Відповідно до рис. 1.129 – 1.17 встановлюємо пароль для облікового запису користувача «Адміністратор». (Для навчальних цілей рекомендується встановлювати прості паролі).

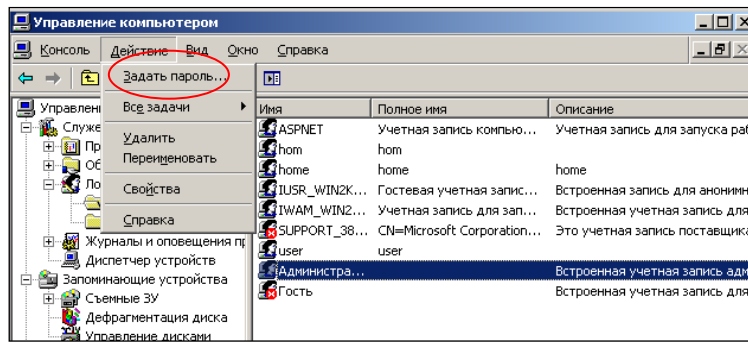


Рис. 1.12. Вхід в режим редагування паролівних даних

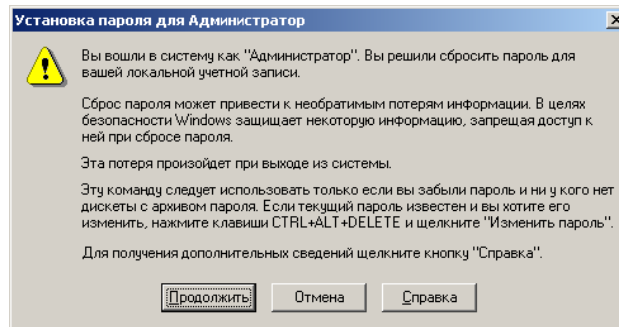


Рис. 1.13. Перший етап змінення паролівних даних

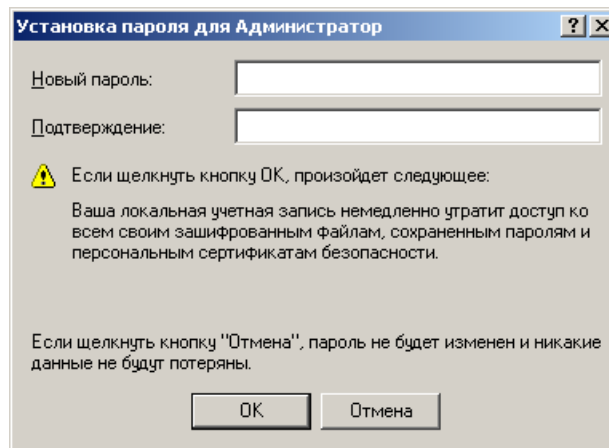


Рис. 1.14. Вікно введення паролівних даних

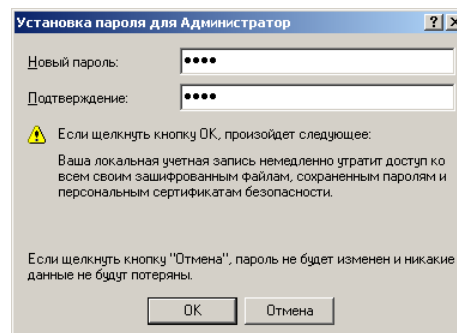


Рис. 1.15. Введення особистих паролівних даних

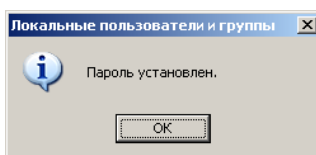


Рис. 1.16. Індикація установки пароля

- Відповідно до рис. 1.17 – 1.19 змінюємо властивості облікового запису адміністратора

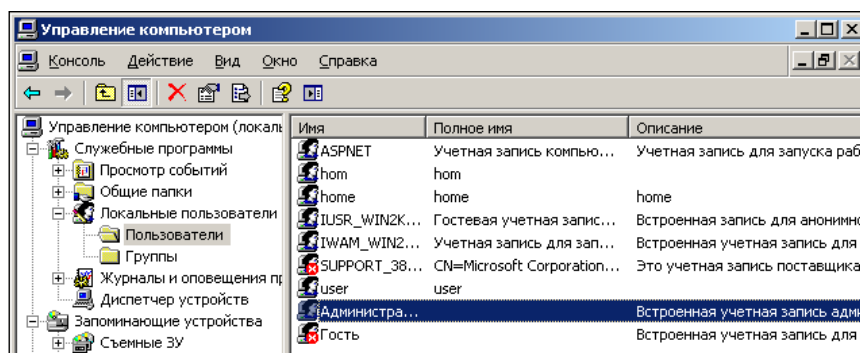


Рис. 1.17. Перехід до редагування параметрів парольних даних

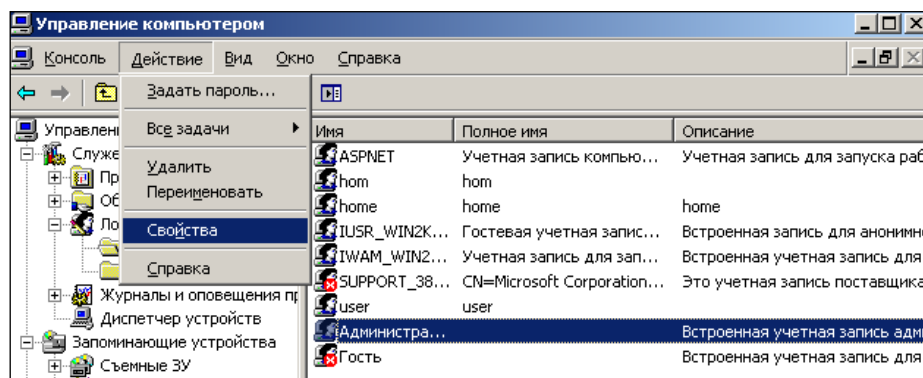


Рис. 1.18. Виклик меню змінення властивостей облікового запису

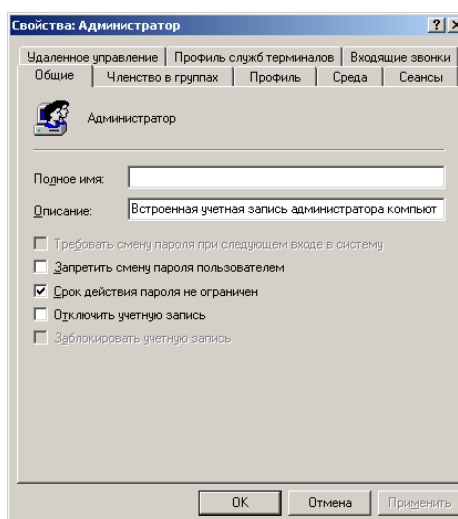


Рис. 1.19. Зміння параметрів облікового запису

3. З використанням вбудованих засобів захисту SearchInform змінити паролі доступу до консолей . (За замовчуванням пароль Admin)

Для цього:

- Відкрити розташовану на робочому столі папку «Консоли».
- За допомогою відповідного ярлика запустити консоль *Search Server*

(рис. 1.20).

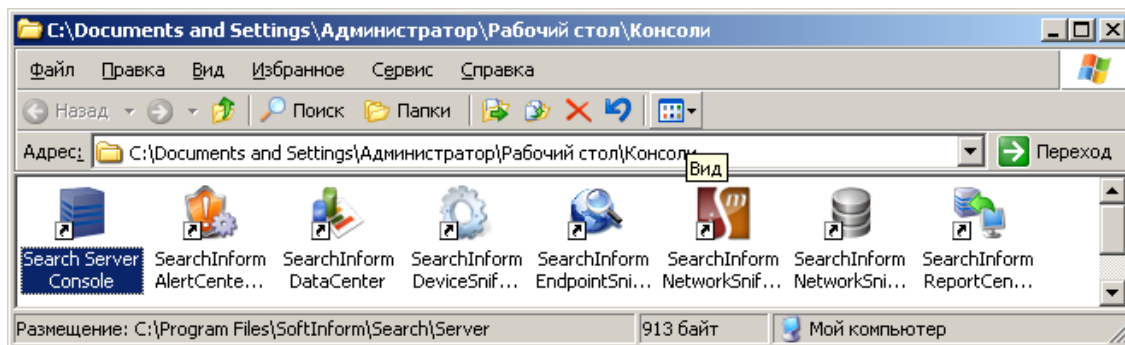


Рис. 1.20. Запуск консолі *Search Server*

- Відповідно до рис. 1.21 – 1.23 увійти в консоль *Search Server*

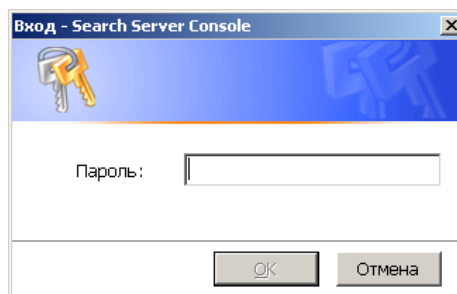


Рис. 1.21. Вікно запити пароля консолі *Search Server*

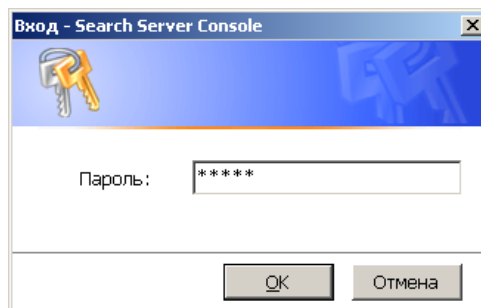


Рис. 1.22. Введення стандартного пароля Admin в консоль *Search Server*

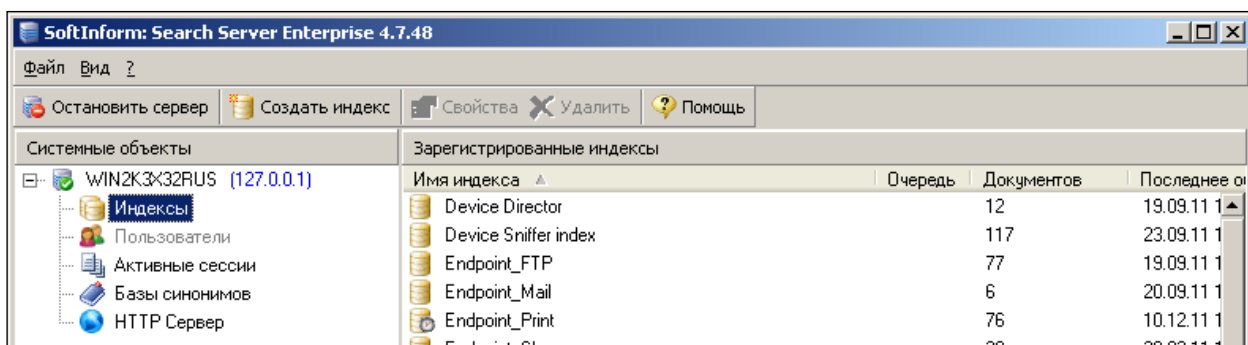


Рис. 1.23. Вікно консолі *Search Server*

- Відповідно до рис. 1.24 – 1.25 задати новий пароль консолі *Search Server*. У прикладі, показаному на рис. 1.25 використаний пароль 123456. При цьому була вибрана необов’язкова опція «Показувати пароль»

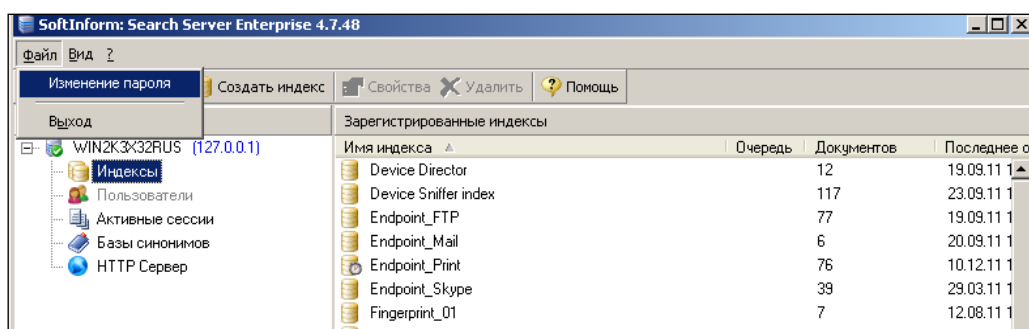


Рис. 1.24. Використання меню змінення пароля консолі *Search Server*

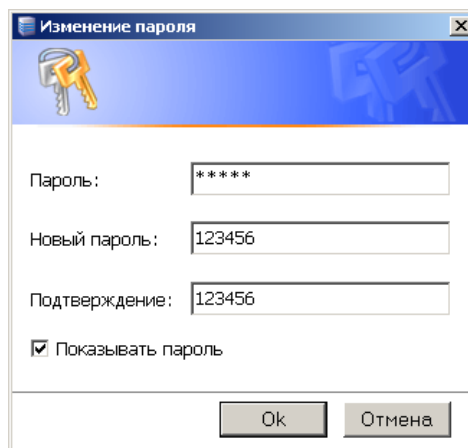


Рис. 1.25. Введення парольних даних консолі *Search Server*

- Закрити консоль *Search Server*.
- За допомогою відповідного ярлика, розміщеного у папці «Консолі» запустити консоль *SearchInform DataCenter*.

- Відповідно до рис. 1.26 – 1.27 увійти в консоль *SearchInform DataCenter*

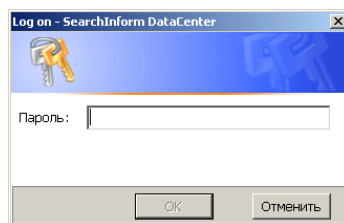


Рис. 1.26. Вікно запиту пароля консолі *SearchInform DataCenter*

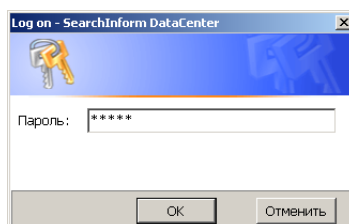


Рис. 1.27. Введення стандартного пароля Admin в консоль *SearchInform DataCenter*

- Відповідно до рис. 1.28 – 1.29 задати новий пароль консолі *SearchInform DataCenter*. У прикладі, показаному на рис. 1.21 використаний пароль 123456. При цьому була вибрана необов'язкова опція «Показати пароль».

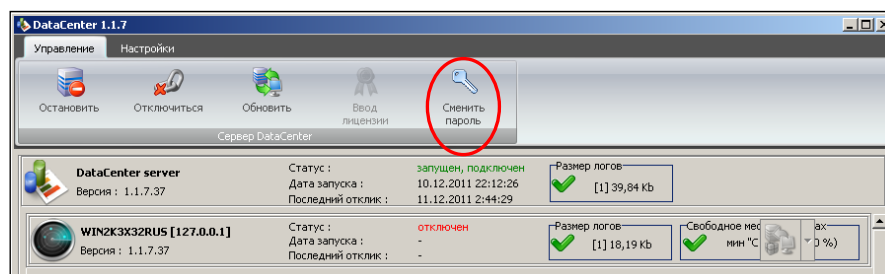


Рис. 1.28. Використання кнопки змінення пароля *SearchInform DataCenter*

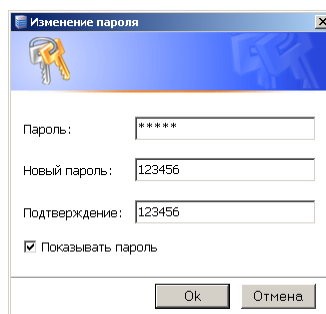


Рис. 1.29. Введення паролських даних консолі *DataCenter*

- Закрити консоль *DataCenter*.
- За допомогою відповідного ярлика, розміщеного у папці «Консолі» запуснути консоль *SearchInform EndpointSniffer*.
- За аналогією з рис. 1.26 – 1.27 увійти в консоль *SearchInform EndpointSniffer*.
- Відповідно до рис. 1.30, 1.29 задати новий пароль консолі *EndpointSniffer*.

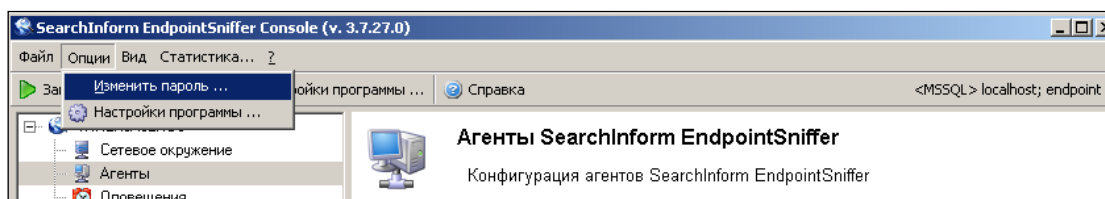


Рис. 1.30. Використання меню зміни пароля консолі *EndpointSniffer*

- Закрити консоль *EndpointSniffer*.
- За допомогою відповідного ярлика, розміщення у папці «Консолі» запуснути *SearchInform NetworkSniffer Administrator Console*.
- За аналогією з рис. 1.26 – 1.27 увійти в *NetworkSniffer Administrator Console*.
- Відповідно до рис. 1.31, 1.29 задати новий пароль *NetworkSniffer Administrator Console*.

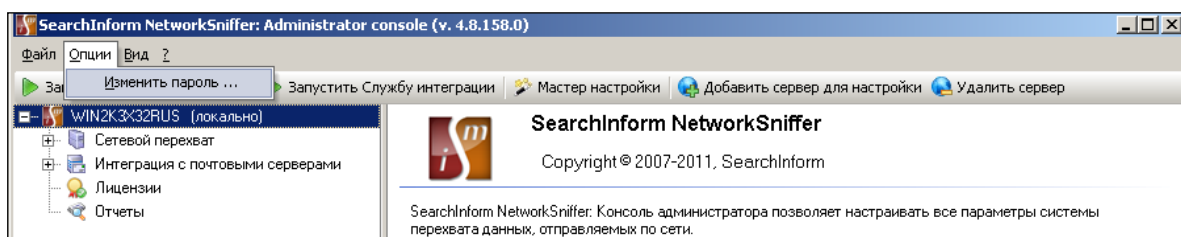


Рис. 1.31. Використання меню змінення пароля консолі *NetworkSniffer Administrator*

- Закрити консоль *NetworkSniffer Administrator*.
- За допомогою відповідного ярлика, розміщеного у папці «Консолі» запуснути *SearchInform ReportCenter Console*.

- За аналогією з рис. 1.26 – 1.27 увійти в *SearchInform ReportCenter Console*.

- Відповідно до рис. 1.32, 1.29 задати новий пароль *SearchInform ReportCenter Console*.

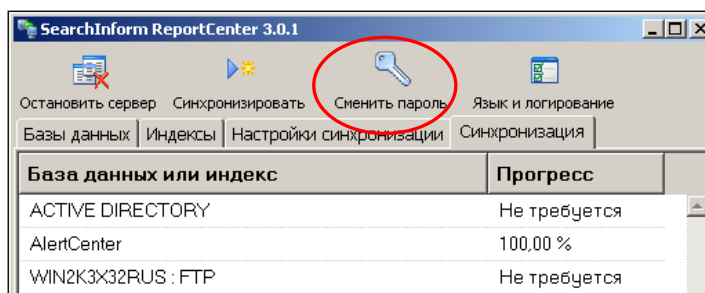


Рис. 1.32. Використання кнопки змінення пароля консолі *ReportCenter*

- Закрити консоль *ReportCenter*.

- Відкрити папку «Клиенты», яка знаходиться на робочому столі (рис. 1.33) і за допомогою ярлика «*SearchInform AlertCenter Client*» запустити відповідну службу. Вікно служби показано на рис. 1.34.

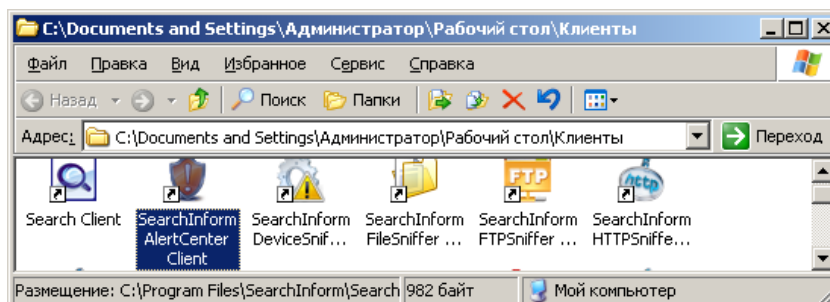


Рис. 1.33. Вікно папки «Клиенты»

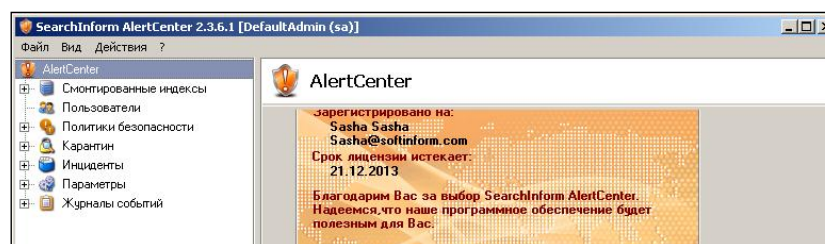


Рис. 1.34. Вікно служби *AlertCenter Client*

- Відповідно до рис. 1.35 – 1.39 Встановити пароль на використання служби «*SearchInform AlertCenter Client*».

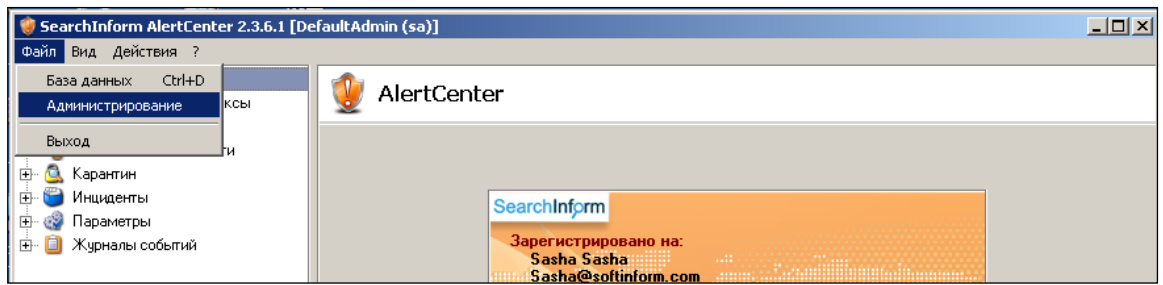


Рис. 1.35. Використання меню адміністрування служби *AlertCenter Client*

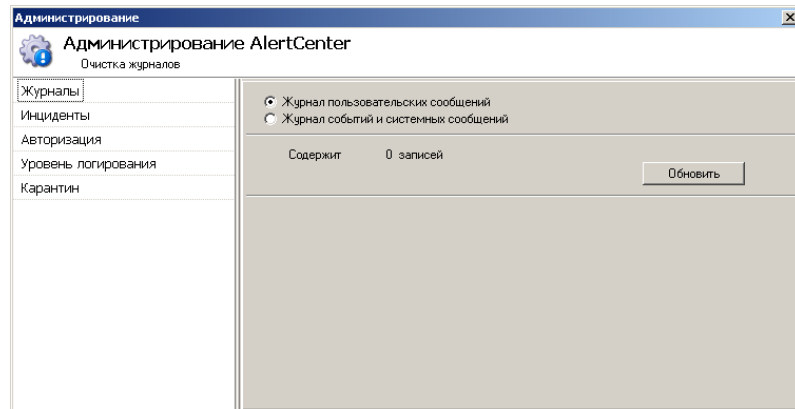


Рис. 1.36. Вікно адміністрування *AlertCenter Client*

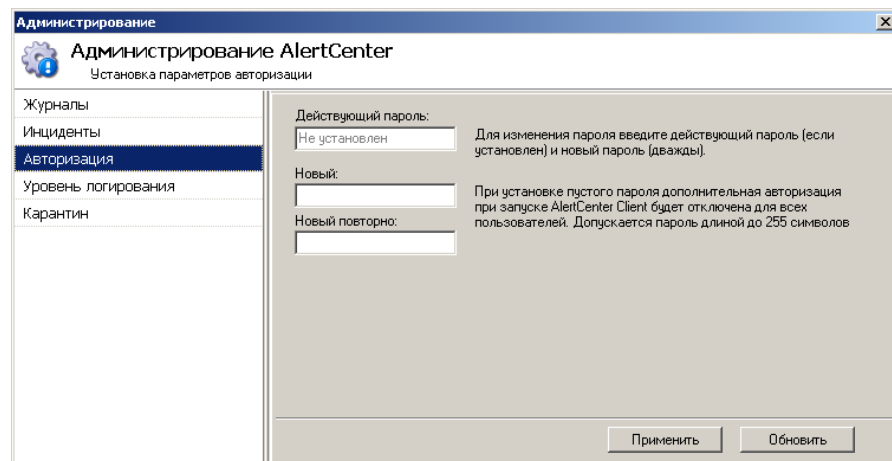


Рис. 1.37. Вибір опції авторизації *AlertCenter Client*

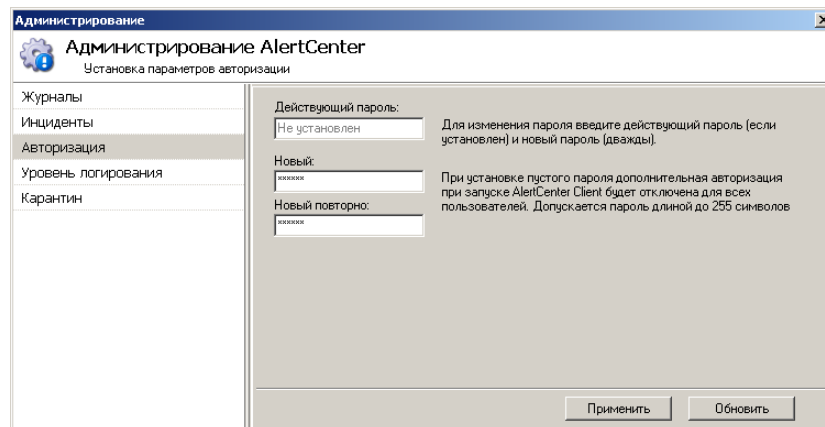


Рис. 1.38. Встановлення пароля *AlertCenter Client*

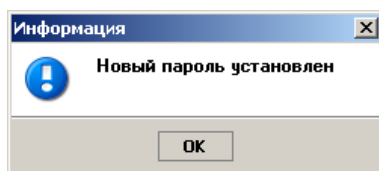


Рис. 1.39. Вікно підтвердження установки пароля *AlertCenter Client*

- Закрити вікно служби *AlertCenter Client*.

4. Обмежити права доступу користувачів до індексів *Search Server*:

- За допомогою відносного ярлика, розміщеного у папці «Консоли» запустити консоль *Search Server*. У разі необхідності ввести пароль.

- Відповідно до рис. 1.40 вибрати індекс і натиснути кнопку «Свойства».

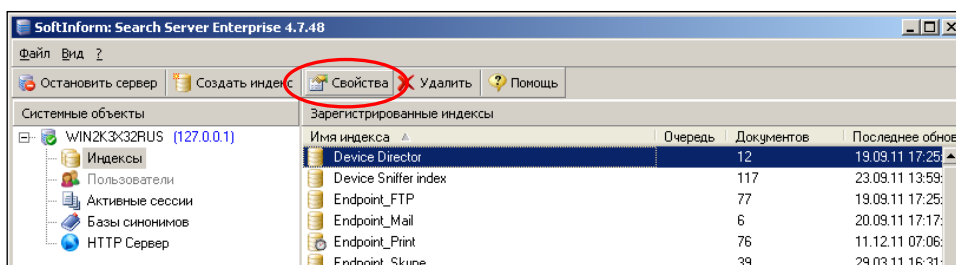


Рис. 1.40. Перехід до редагування властивостей індексу

- Відповідно до рис. 1.41 – 1.48 встановити можливість доступу до даному індексу тільки користувачам операційної системи, які відносяться до групи «Адміністраторы».

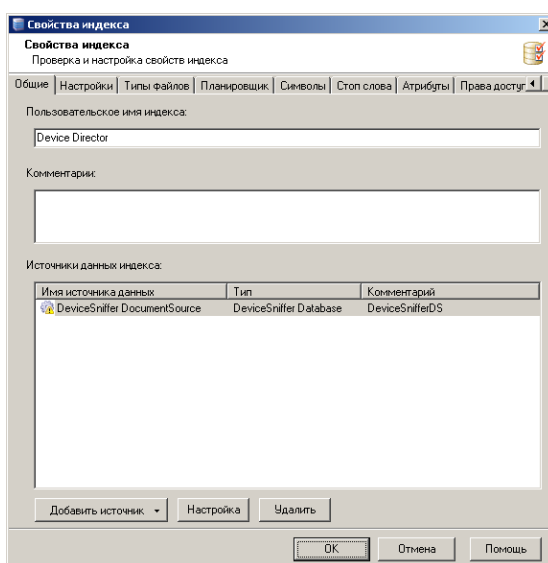


Рис. 1.41. Вікно властивостей індексу

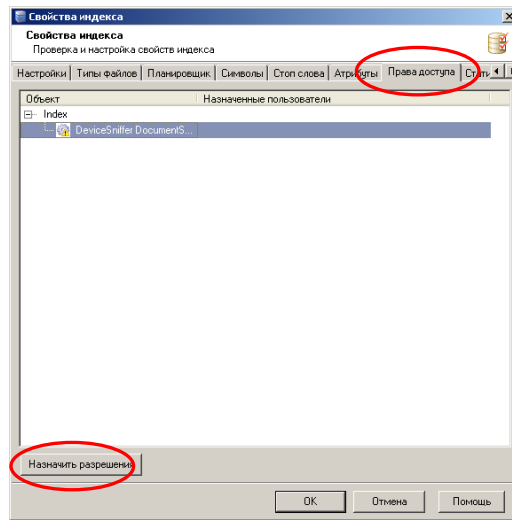


Рис. 1.42. Перехід до редагування прав доступу до індексу

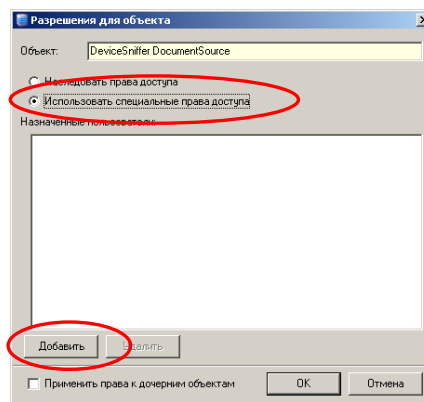


Рис. 1.43. Перехід до редагування списку користувачів індексу

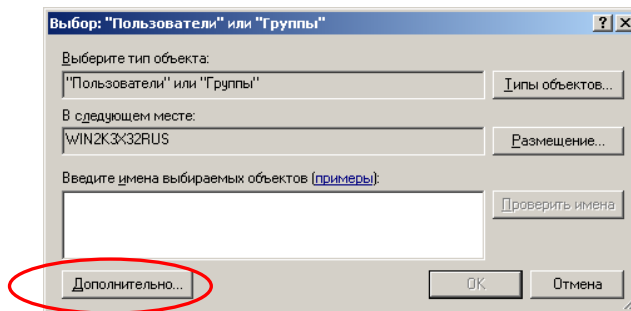


Рис. 1.44. Перший етап пошуку користувачів

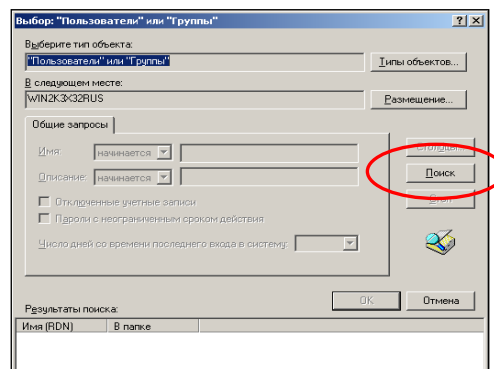


Рис. 1.45. Другий етап пошуку користувачів

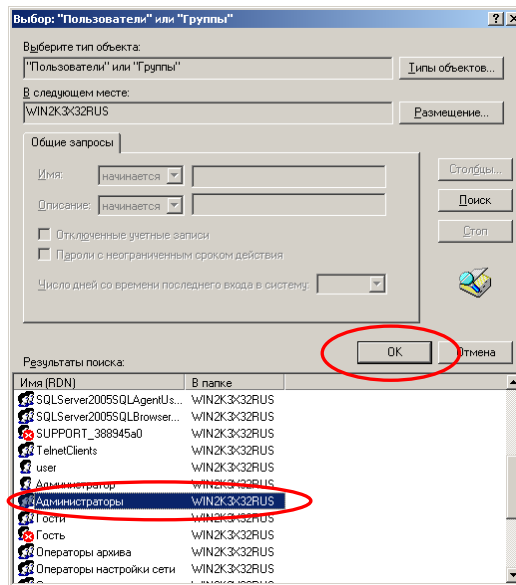


Рис. 1.46. Вибір групи «Администраторы»

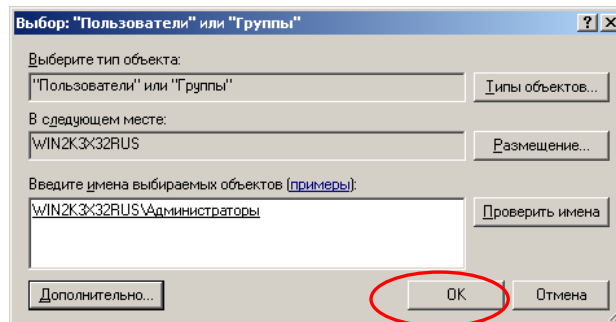


Рис. 1.47. Підтвердження вибору групи «Администраторы»

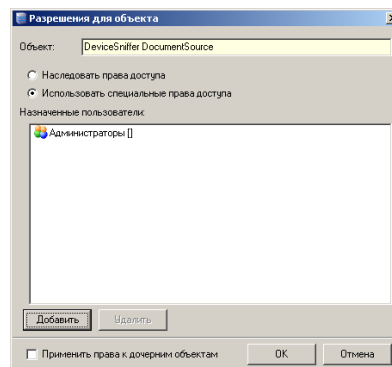


Рис. 1.48. Індикація можливості доступу до індексу для групи «Администраторы»

- Закрити консоль *Search Server*.

5. Управління користувачами системних служб *SearchInform*.

Встановити, що служба *AlertCenter* працює від імені користувача, «Администратор». Для цього:

- Відкрити вікно панелі управління ОС Windows Server (команди *Пуск→Настройка→Панель управления*);

- Відповідно до рис. 1.49 запусити вкладку *Администрирование*.

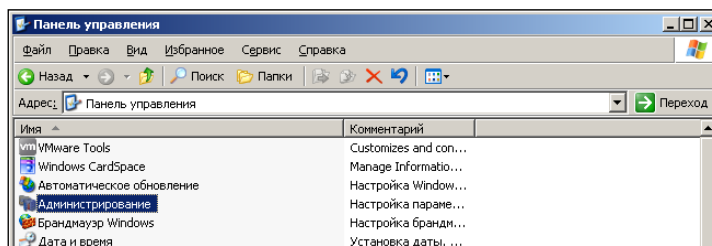


Рис. 1.49. Вибір вкладки *Администрирование*

- У новому вікні, яке показано на рис. 1.50 запусити компонент *Службы*.

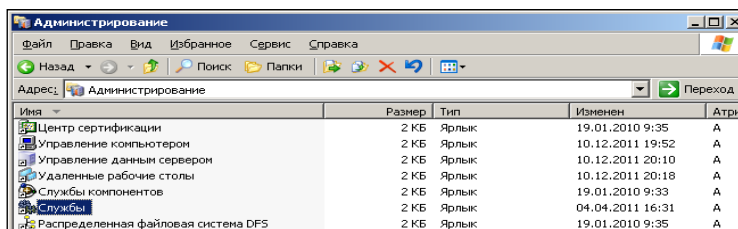


Рис. 1.50. Вибір компонента *Службы*

- Відповідно до рис. 1.51 викликати контекстне меню служби *SearchInform AlertCenter server*.

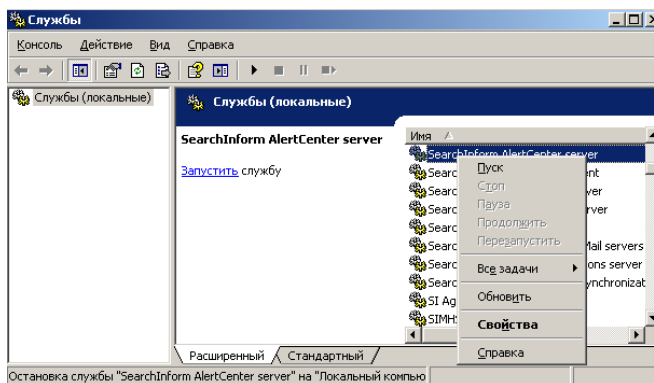


Рис. 1.51. Виклик контекстного меню служби *SearchInform AlertCenter server*

- В контекстном меню выбрать команду *Свойства*.

- У вікні, показаному на рис. 1.52 перейти на вкладку *Вход в систему* (рис 1.53).

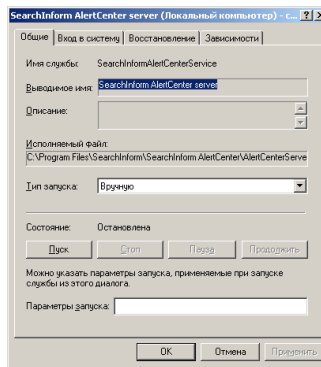


Рис. 1.52. Вікно властивостей служби вкладка *Общие*

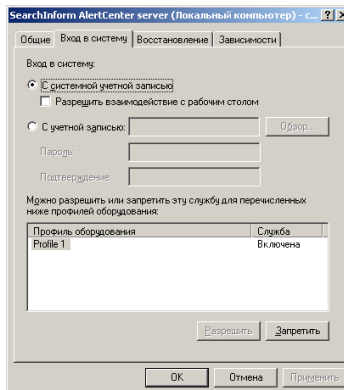


Рис. 1.53. Вікно властивостей служби вкладка *Вход в систему*

- Слiдувати iнструкцiям, якi показанi на рис. 1.54 – 1.62.

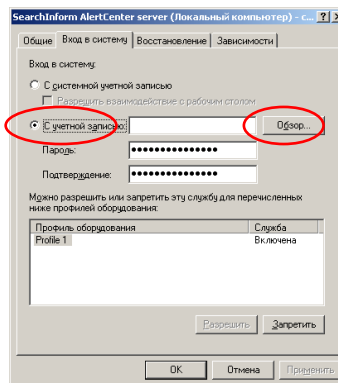


Рис. 1.54. Перший етап вибору користувача «Адміністратор»

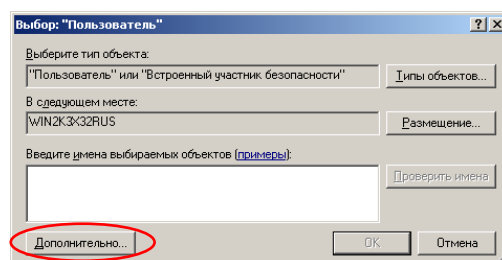


Рис. 1.55. Другий етап вибору користувача «Адміністратор»

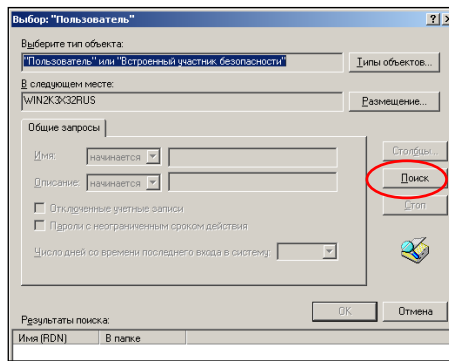


Рис. 1.56. Третий этап выбору користувача «Администратор»

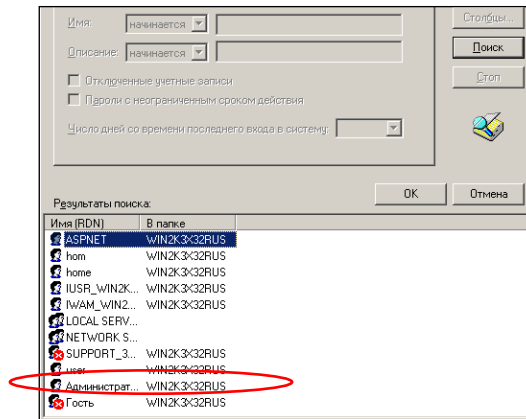


Рис. 1.57. Четвертый этап выбору користувача «Администратор»

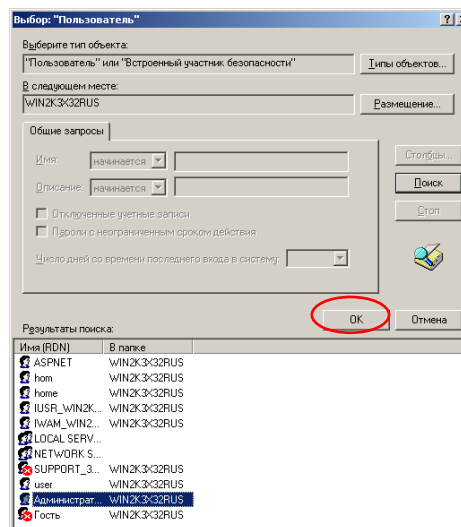


Рис. 1.58. П'ятий этап выбору користувача «Администратор»

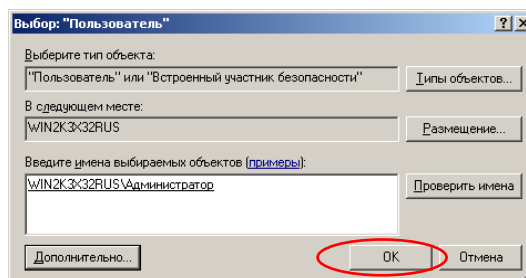


Рис. 1.59. Підтвердження выбору користувача «Администратор»

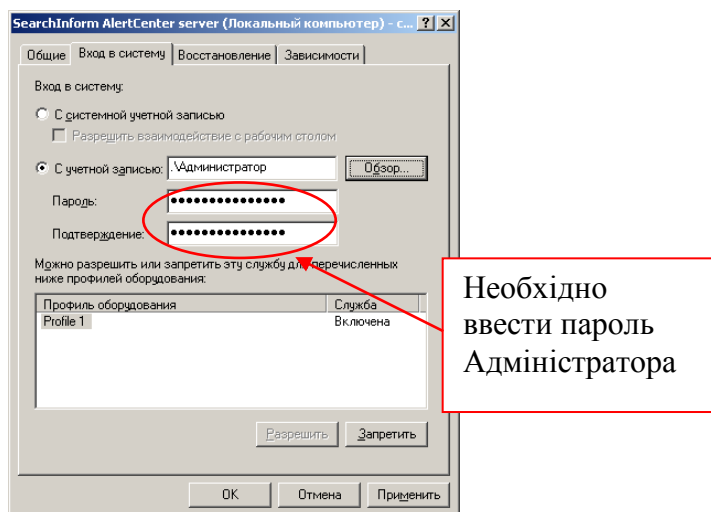


Рис. 1.60. Введення парольних даних користувача «Адміністратор»

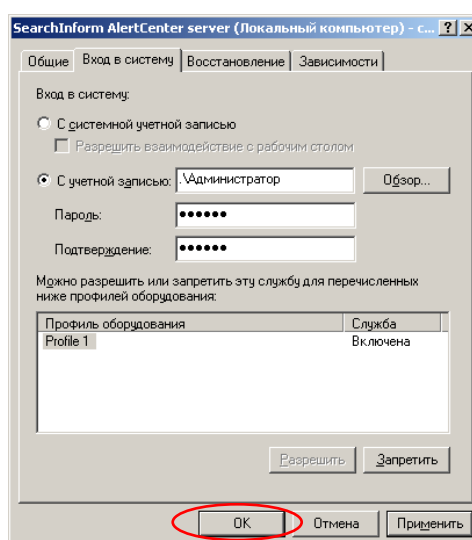


Рис. 1.61. Закінчення введення парольних даних користувача «Адміністратор»

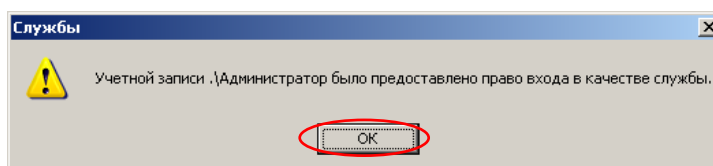


Рис. 1.62. Підтвердження входу в систему служби *SearchInform AlertCenter server* від імені користувача «Адміністратор»

- Закрити вікна *Службы* і *Администрирование*.
- При необхідності (уточнити у викладача), за аналогією з *SearchInform AlertCenter* встановити, що служби *SearchInform DataCenter: agent*, *DataCenter: server*, *DeviceSniffer Server*, *NetworkSniffer*, *SearchInform*

NetworkSniffer Mail servers integration, SearchInform Regular Expressions server, SearchInform ReportCenter: synchronization service, SI Agents Control Service, SIMHSvc, SoftInform Search Server, SQL Server (MSSQLSERVER), SQL Server VSS Writer також працюють від імені користувача «Адміністратор».

- Якщо попередній пункт не виконувався (служби не працюють в режимі «Адміністратор»), то встановить, що служба *SearchInform AlertCenter server* працює з системним обліковим записом (рис. 1.63).

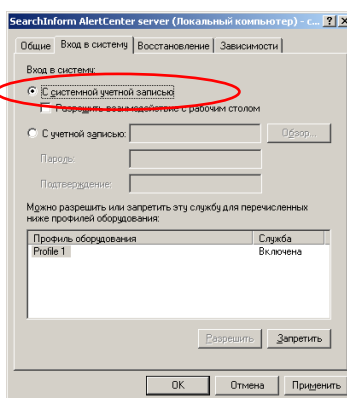


Рис. 1.63. Установка входу в систему службы *SearchInform AlertCenter server* з системою облікового запису

6. Налаштування параметрів функціонування *SearchInform AlertCenter*.

- Запустити консоль «*SearchInform AlertCenter Console*».
- Відповідно до рис. 1.64, 1.65 перевірити з'єднання з базою даних.

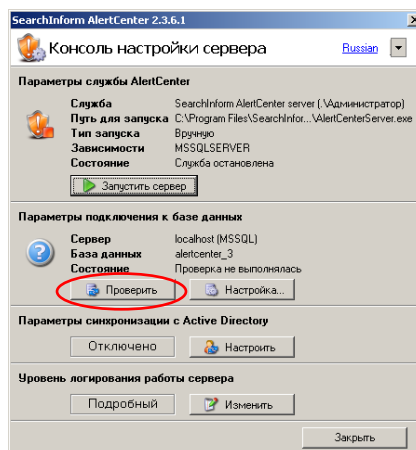


Рис. 1.64. Проверка з'єднання з базою даних

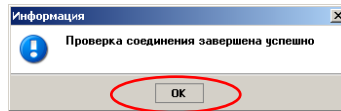


Рис. 1.65. Індикація успішного з'єднання з базою даних

- Відповідно до рис. 1.66 – 1.68 переглянути параметри з'єднання з системою управління базами даних.

- Перевірити з'єднання з базами даних, що перераховані у списку (рис. 1.68). Для цього треба вибрати із списку базу даних и натиснути кнопку «Проверить подключение».

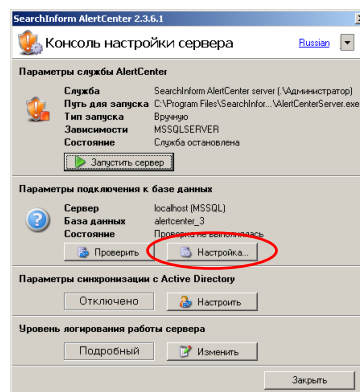


Рис. 1.66. Вхід в режим налаштування з'єднання з базою даних

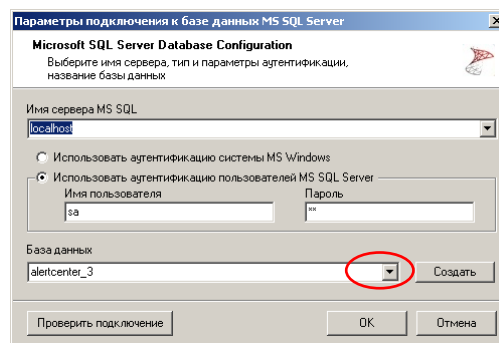


Рис. 1.67. Вікно налаштування з'єднання з базою даних

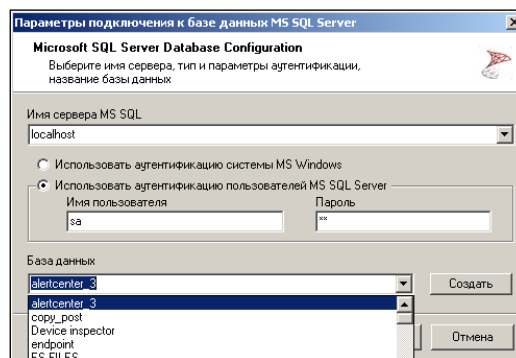


Рис. 1.68. Вибір бази даних для з'єднання

- Вибравши базу даних alertcenter_3 і натиснувши кнопку «ОК» (рис. 1.67), вийти з режиму налаштування підключення.

- Відповідно до рис. 1.69, 1.70 встановити рівень логування сервера AlertCenter.

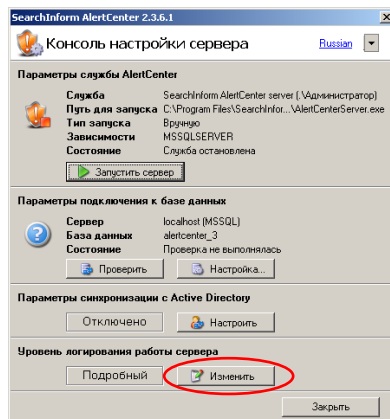


Рис. 1.69. Вхід в налаштування режиму логування

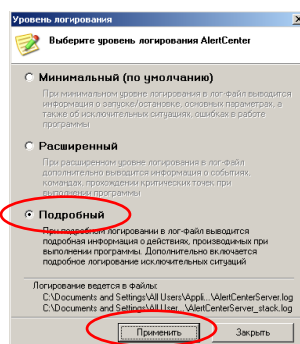


Рис. 1.70. Вибір бази даних для з'єднання

- Відповідно до рис. 1.71, 1.72 запустити сервер і закрити консоль AlertCenter.

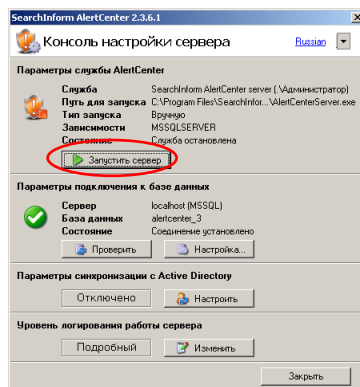


Рис. 1.71. Запуск сервера AlertCenter

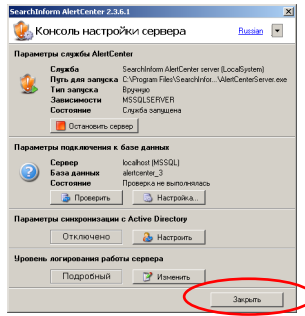


Рис. 1.72. Індикація запуску сервера *AlertCenter*

7. Налаштування системної служби *SearchInform DataCenter: agent*.

Для цього:

- Запустити оснащення *Служби* і відповідно до рис. 1.73 – 1.76 встановити автоматичний запуск служби *SearchInform DataCenter: agent* при завантаженні операційної системи.

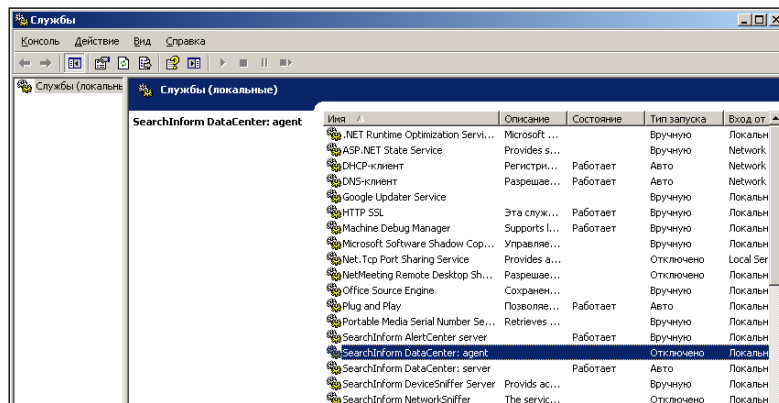


Рис. 1.73. Перший етап установки автоматичного запуску *SearchInform DataCenter: agent*

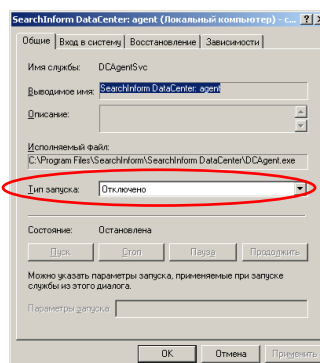


Рис. 1.74. Другий етап установки автоматичного запуску *SearchInform DataCenter: agent*

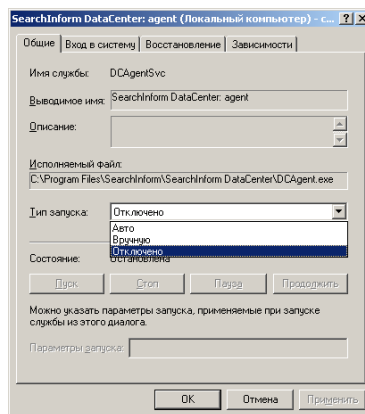


Рис. 1.75. Третій етап установки автоматичного запуску *SearchInform DataCenter : agent*

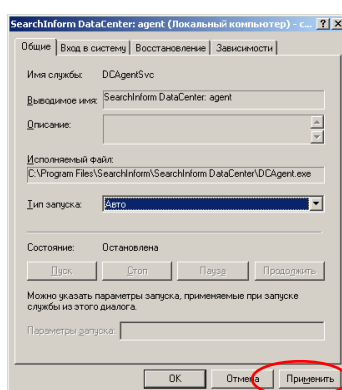


Рис. 1.76. Четвертий етап установки автоматичного запуску *SearchInform DataCenter: agent*

- Відповідно до рис. 1.77 – 1.78 примусово запуснути службу *SearchInform DataCenter: agent* і вийти з режиму управління *Службами* операційної системи.

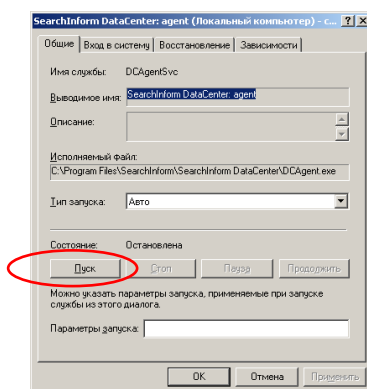


Рис. 1.77. Перший етап примусового запуску служби *SearchInform DataCenter: agent*

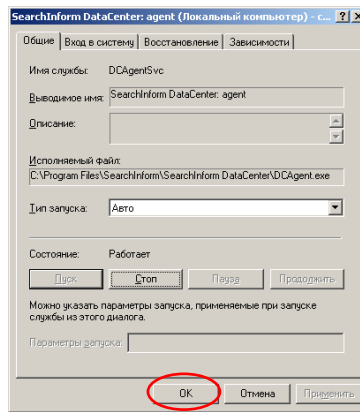


Рис. 1.78. Другий етап примусового запуску служби *SearchInform DataCenter: agent*

8. Налаштування параметрів функціонування *SearchInform NetworkSniffer*. Для цього:

- Відкрити консоль *SearchInform DataCenter*.
- Відповідно до рис. 1.79 – 1.80 переконаватися, що *SearchInform NetworkSniffer* не функціонує.

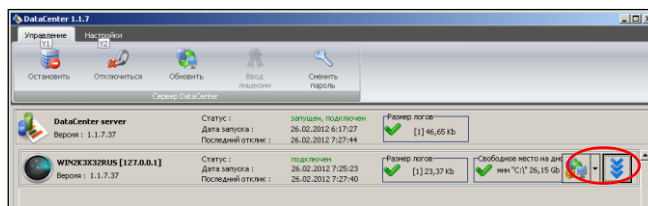


Рис. 1.79. Консоль *DataCenter*

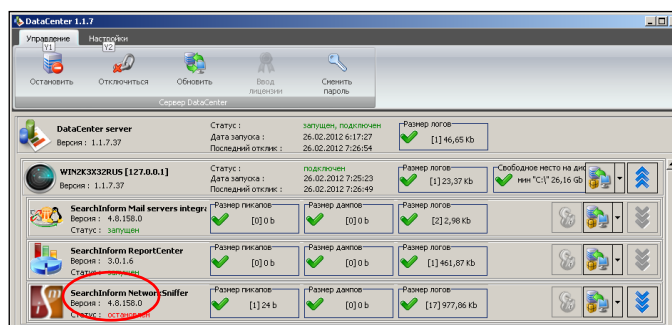


Рис. 1.80. Деталізація параметрів консолі *DataCenter*

- Увійти в режим управління **Службами** Операційної системи Відповідно до рис. 1.81 – 1.76 встановити автоматичний запуск служби *SearchInform NetworkSniffer* при завантаженні операційної системи.

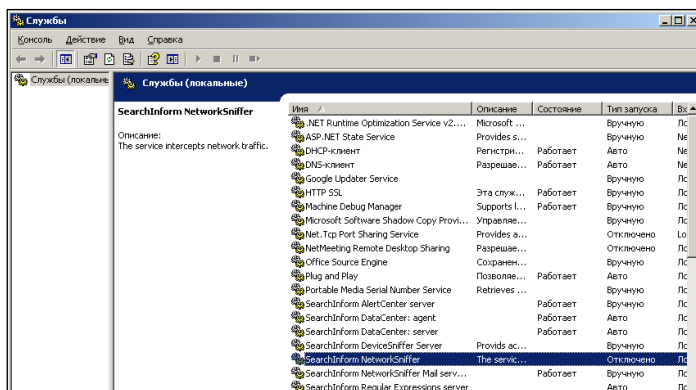


Рис. 1.81. Перший етап установки автоматичного запуску *SearchInform NetworkSniffer*

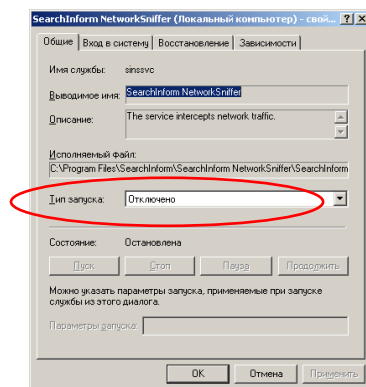


Рис. 1.82. Другий етап установки автоматичного запуску *SearchInform NetworkSniffer*

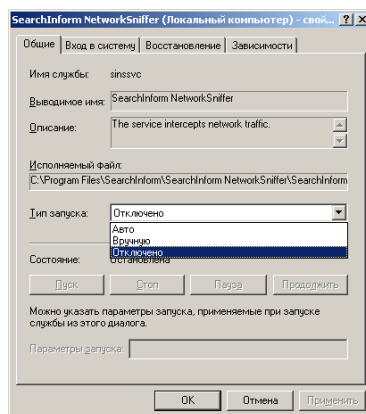


Рис. 1.83. Третій етап установки автоматичного запуску *SearchInform NetworkSniffer*

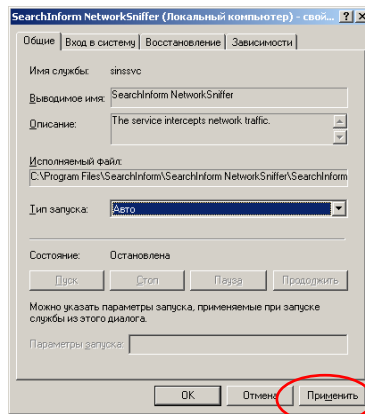


Рис. 1.84. Четвертый этап установки автоматического запуска
SearchInform NetworkSniffer

- Відповідно до рис. 1.85 – 1.86 примусово запуснути службу *SearchInform NetworkSniffer* і з режиму управління *Службами* операційної системи.

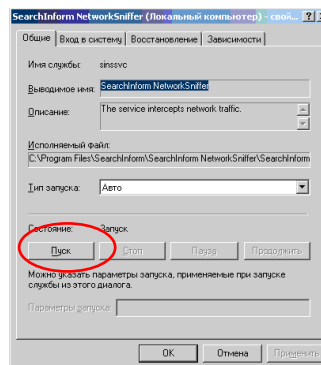


Рис. 1.85. Перший етап установки автоматического запуска службы
SearchInform NetworkSniffer

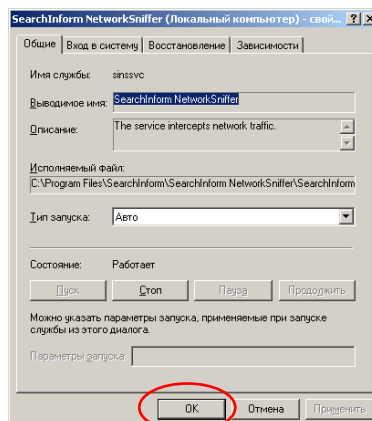


Рис. 1.86. Другой этап установки автоматического запуска службы
SearchInform NetworkSniffer

- Закрити консоль управління службами операційної системи.
- Закрити консоль **DataCenter**.
- Завершити роботу з віртуальним комп'ютером.

Питання для самоперевірки

1. Для чого потрібне перехоплення усіх документів, які покидають периметр організації, незалежно від каналів, по яким це відбувається?
2. Чи потрібен системний адміністратор у штаті служби інформаційної безпеки і чому?
3. За якими схемами можна увімкнути контур інформаційної безпеки у мережу підприємства?
4. Яка зі схем підключення найбільш оптимальна при наявності технічної можливості?
5. Як встановити пароль для користувача «Адміністратор» Windows Server?
6. Як встановити пароль на консоль Search Server?
7. Як встановити пароль на консоль DataCenter?
8. Як встановити пароль на консоль EndpointSniffer?
9. Як встановити пароль на консоль NetworkSniffer?
10. Як встановити пароль на консоль ReportCenter?
11. Як встановити пароль на службу AlertCenter?
12. Як розмежувати права доступу до індексів?

ЛАБОРАТОРНА РОБОТА №2 «ПРИНЦИПИ ВИКОРИСТАННЯ ПРОГРАМНОГО КОМПЛЕКСУ SEARCHINFORM ДЛЯ МОНІТОРИНГУ ВИТОКУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ»

Мета лабораторної роботи: засвоїти основні прийоми використання програмного комплексу *SearchInform* для перехоплення і пошуку витоків конфіденційної інформації.

Теоретичні відомості. Досліджувана версія програмного комплексу «Контур інформаційної безпеки *SearchInform*» призначена для виявлення витоків конфіденційної інформації при її передачі, зокрема для перехоплення переданих даних використовуються: *MailSniffer*, *IMSniffer*, *HTTPSniffer*, *FTPSniffer*, *SkypeSniffer*, *PrintSniffer*, сервер індексації робочих станцій, *MonitorSniffer*. Перехоплені дані записуються в базу даних *MS SQL Server* і піддаються процедурі індексації, необхідність якої пояснюється підвищенням швидкості пошуку. Власне пошук конфіденційних даних здійснюється за індексами, які представляють собою елементи, які включають в себе інформацію про розташування і зміст перехоплених документів і список всіх слів цих документів. Для індексації даних використовується компонент *DataCenter*. Оповіщення про знайдені конфіденційні дані, тобто про виявлений факт витоку, реалізується з допомогу компонента *AlertCenter*.

Відзначимо, що в багатьох організаціях, є користувачі, документи яких повинні бути виключені з перехоплення. Для виключення перехоплення слід використовувати фільтри *SearchInform EndpointSniffer Console* і *SearchInform NetworkSniffer Administrator Console*. Фільтри по користувачах особливо актуальні для сервера *NetworkSniffer*, який управляє компонентами *MailSniffer*, *IMSniffer* і *HTTPSniffer*. Так як перехоплення йде на рівні мережевих адаптерів і за замовчуванням перехоплюються документи всіх користувачів. Фільтри по користувачам не настільки важливі для компонентів *SkypeSniffer*, *PrintSniffer* і *DeviceSniffer*, тому що інформація

перехоплюється тільки агентами, встановленими на цільові робочі станції. Документи користувачів, виключених з перехоплення, не будуть розміщені в базу даних. Ще однією причиною обмеження користувачів, документи яких повинні бути виключені з перехоплення може бути обмеженість придбаної ліцензії комплексу *SearchInform*.. Наприклад, якщо ви придбали ліцензію на 50 робочих станцій, а є 60 користувачів електронної пошти, то потрібно налаштувати або обмежувальний фільтр на 10 користувачів, або дозвільний фільтр на 50 користувачів.

Існують загальні правила роботи фільтрів. Якщо опція фільтрації включена, але список фільтрів порожній, перехоплення буде здійснюватися без обмежень за адресами. Щоб пакет даних потрапив під правило ("заборонити" або "дозволити" перехоплення), досить збігу по одному атрибуту. Одночасно можна використовувати або заборонні фільтри, або дозвільні фільтри. При використанні заборонних фільтрів у базу даних будуть передаватися усі перехоплені пакети, за винятком збігів по фільтрам. При використанні дозвільних фільтрів в базу даних будуть передані всі перехоплені пакети, що збігаються з фільтрами.

В консолі *EndpointSniffer* для заборони фільтрації повинна бути включена опція "*Виключити з перехоплення трафіку*", а для роздільної фільтрації повинна бути включена опція "*Включити в перехоплення трафіку*".

Якщо потрібно зробити так, щоб документи перехоплювалися і розміщувалися в базу, але по ним не генерувалися повідомлення, слід налаштувати фільтри *SearchInform AlertCenter Client*.

Найбільш складним етапом виявлення витоку є пошук в перехоплених документах конфіденційних даних. Реалізація ефективного пошуку вимагає комплексного застосування різних прийомів і методів, які істотно залежать від змісту аналізованого документа і характеру конфіденційних даних.

З точки зору ефективного пошуку, аналізовані документи поділяються на формалізовані (структуровані) і неформалізовані (неструктуровані).

Прикладами структурованих документів є фінансові звіти, бізнес-плани, рахунки-фактури, авансові відомості. До неструктурованих документів найчастіше відносяться повідомлення соціальних мереж, форумів, ICQ, Skype. Очевидно, що виявити структурований конфіденційний документ найпростіше на підставі визначення деяких формальних атрибутів, які присутні в подібних документах. Розпізнати неструктуровану конфіденційну інформацію складніше. Для цього слід проаналізувати зміст тексту документа.

Пошук конфіденційної інформації здійснюється за допомогою клієнтів *MailSniffer*, *IMSniffer*, *HTTPSniffer*, *PrintSniffer*, *DeviceSniffer*, *SkypeSniffer*, *SoftInform Search*, а також компонента *AlertCenter*, які забезпечують:

1. Повнотекстовий пошук – пошук за ключовими словами і словосполученнями в тексті перехоплених документів. При повнотекстовому пошуку не враховується порядок слів і їх положення в документі.

2. Фразовий пошук – пошук за ключовими словами, залежно від положення одне щодо іншого. Дозволяє відкинути документи, в яких ключові слова розкидані по всьому тексту.

3. Пошук схожих – пошуковий запит являє собою цілий текст, з яким порівнюється кожен перехоплений документ. Система обчислює ступінь схожості (релевантність) для кожного перехопленого документа і якщо релевантність перевищує заданий аудитором рівень, система генерує оповіщення для аудитора безпеки. При обчисленні показника релевантності враховується безліч факторів, у тому числі відсоток загальних слів, порядок слів запиту, розмір запиту, розмір необхідного документа. Інтелектуальні можливості цього типу пошуку дозволяють відслідковувати відсилання конфіденційних документів навіть у тому випадку, якщо вони були попередньо відредаговані. В якості пошукового запиту використовуються як фрагменти документів, так і документи цілком, а результатом пошуку є документи, не тільки містять весь пошуковий запит, але і схожі на нього за змістом.

4. Пошук за технічними параметрами документа – імені користувача, який його відправив, датою перехоплення, методу передачі і т.д.

Крім цього для виявлення конфіденційної інформації, компонент *AlertCenter* має додаткові можливості:

1. Використання синонімічних рядів при повнотекстовому і фразових пошуку.

2. Розширений пошук по технічним параметрам документа.

3. Пошук нерозпізнаних документів, тобто таких з яких не вдалося витягти текст.

4. Складні запити – комбінування декількох простих запитів для тексту, атрибутів і нерозпізнаних документів.

5. Запити з регулярними виразами – пошук критичної інформації по одному або декільком шаблонами заданого формату.

6. Запити з цифровими відбитками – порівняння всіх перехоплених документів з набором контрольних документів. Цей вид пошуку передбачає визначення групи конфіденційних документів і зняття з них цифрових відбитків, за якими в подальшому і буде здійснюватися пошук. За допомогою даного методу можна швидко виявляти в інформаційних потоках документи, що містять великі фрагменти тексту з документів, що відносяться до конфіденційних. Основною перевагою методу є висока швидкість роботи, а до недоліків можна віднести його неефективність при внесенні в документ значущих змін і необхідність оперативного створення цифрових відбитків усіх нових документів для можливості їх пошуку.

При цьому, компонент *AlertCenter* дозволяє:

- Налаштовувати і зберігати пошукові запити, які використовуються для визначення документів, які містять конфіденційну інформацію.

- Налаштовувати розклад, за яким відбувається пошук конфіденційних документів.

Примітка: детальна інформація про налаштування пошуку міститься в керівництві аудитора безпеки системи *SearchInform*, а також у довідці клієнтів *MailSniffer*, *IMSniffer*, *HTTPSniffer*, *PrintSniffer*, *DeviceSniffer*, *SkypeSniffer*, *SoftInform Search*, компонента *AlertCenter*, а також консолів *EndpointSniffer*, *DeviceSniffer*, *NetworkSniffer Administrator*.

Завдання на лабораторну роботу:

Для виявлення витоків конфіденційної інформації в програмному комплексі *SearchInform* спочатку слід налаштувати:

1. Список користувачів, дані яких перехоплюватимуться системою.
2. Режим індексації перехоплених документів і режим використання індексів.
3. Список користувачів, за перехопленими даними в яких будуть генеруватися повідомлення.
4. Параметри аналізу індексів пошуковими клієнтами і компонентом *AlertCenter*.

Хід виконання роботи

1. Підготовчі роботи

Відповідно до методичних вказівок лабораторної роботи №1 запустити віртуальний комп'ютер з встановленим програмним комплексом *SearchInform*. Надалі вся робота виконується тільки на цьому віртуальному комп'ютері.

2. Визначення переліку користувачів, дані яких перехоплюватимуться системою

– За допомогою ярлика *SearchInform AlertCenter Console*, відповідно до рис. 2.1, 2.2 запустити сервер *AlertCenter* і закрити вікно консолі.

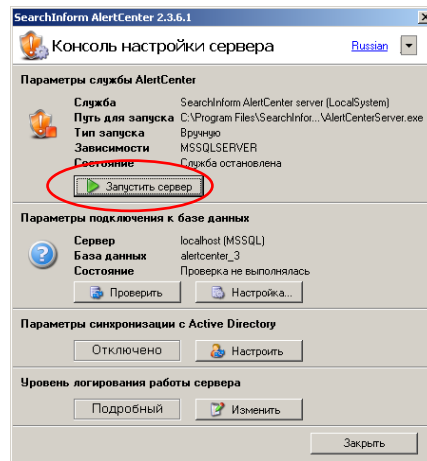


Рис. 2.1. Запуск сервера *AlertCenter*

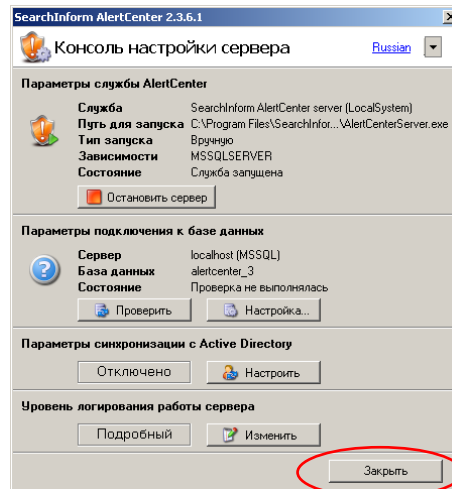


Рис. 2.2. Консоль функціонування сервера *AlertCenter*

– За допомогою відповідного ярлика запустити *SearchInform NetworkSniffer Administrator Console*, вікно якого показано на рис. 2.3. Відзначимо, що в процесі запуску може знадобитися введення парольних даних, встановлених в попередній лабораторній роботі.

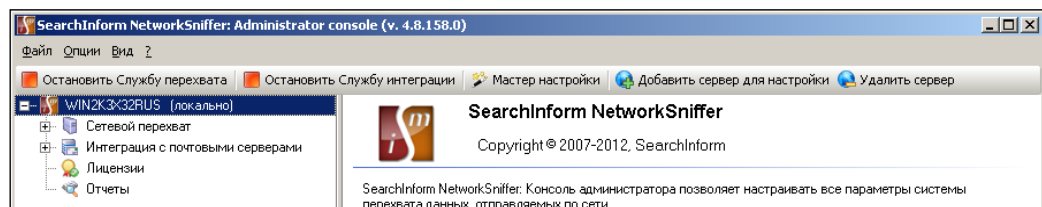


Рис. 2.3. Вікно *SearchInform NetworkSniffer Administrator Console*

– Відповідно до рис. 2.4 – 2.7 проведемо редагування фільтра перехоплення інформації. Редагування полягає у видаленні з фільтра

користувача demhenko для всіх контрольованих протоколів. Після редагування будуть перехоплюватися дані всіх користувачів для всіх контрольованих протоколів.

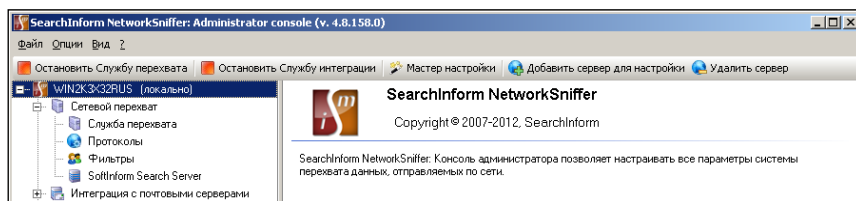


Рис. 2.4. Відкриття гілки «Сетевой перехват»

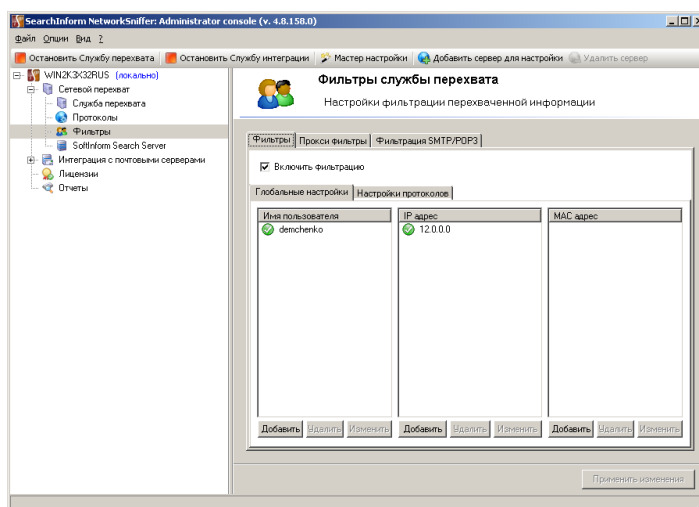


Рис. 2.5. Перехід в режим редагування фільтрів для всіх контрольованих протоколів

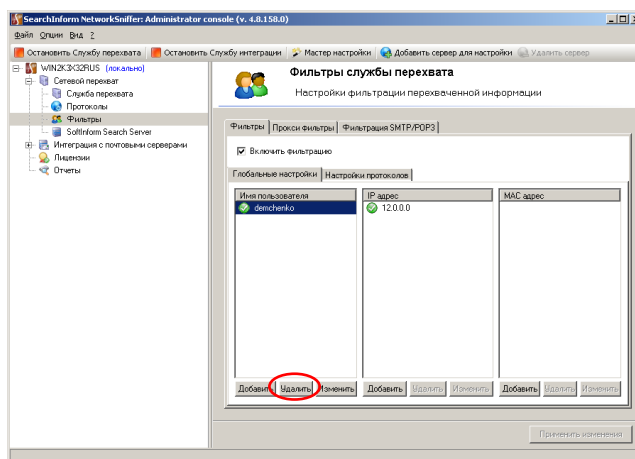


Рис. 2.6. Вибір опції видалення фільтра користувача для всіх контрольованих протоколів

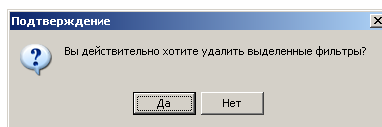


Рис. 2.7. Підтвердження видалення фільтра

– Відповідно до рис. 2.8 – 2.13 додати фільтр, який дозволяє перехоплення даних по всім користувачам для всіх контрольованих протоколів.

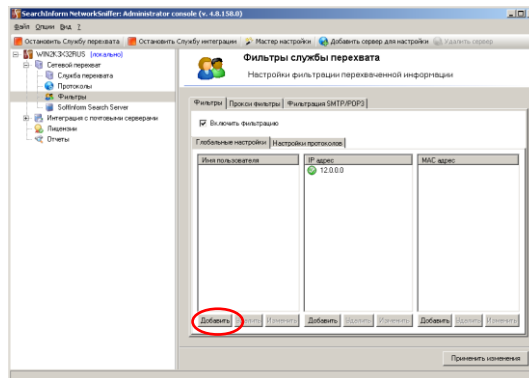


Рис. 2.8. Вхід в режим додавання фільтра для всіх контрольованих протоколів

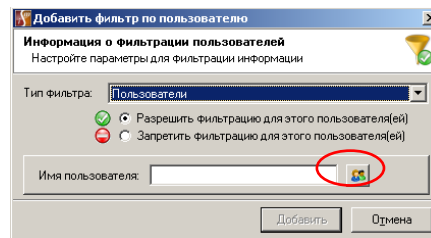


Рис. 2.9. Вхід в режим вибору користувачів для дозволяє фільтру

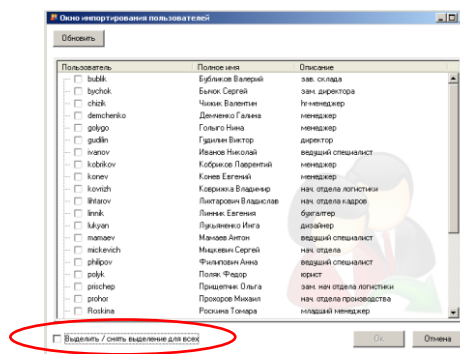


Рис. 2.10. Вікно вибору користувачів для фільтра

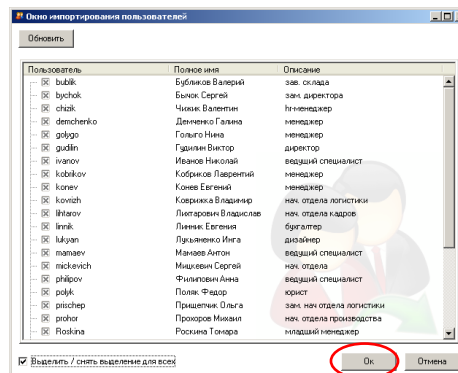


Рис. 2.11. Підтвердження вибору користувачів для фільтрації

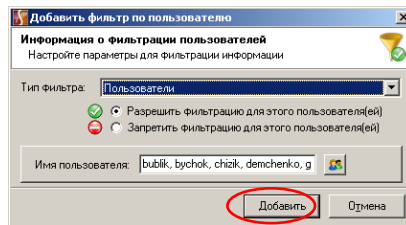


Рис. 2.12. Підтвердження налаштування фільтра

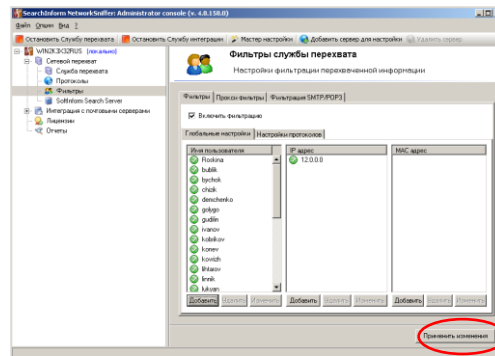


Рис. 2.13. Індикація дозволяючих фільтрів по користувачам для всіх контрольованих протоколів

– Відповідно до рис. 2.14 – 2.15 видалити фільтр, який дозволяє перехоплення даних користувача kopev для всіх контрольованих протоколів.

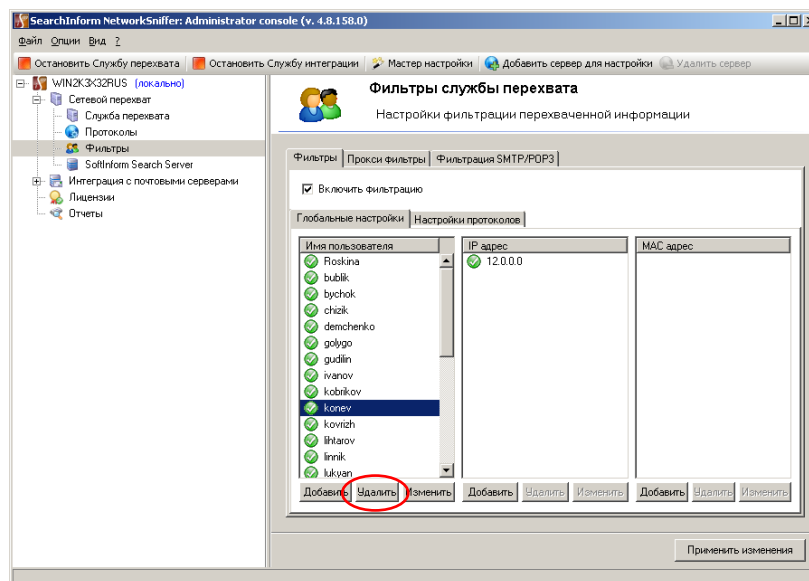


Рис. 2.14. Видалення дозвоільного фільтра для пошуку користувача kopev для всіх контрольованих протоколів

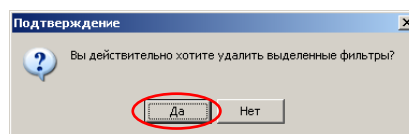


Рис. 2.15. Підтвердження видалення фільтра

– Відповідно до рис. 2.16 – 2.22 налаштувати фільтрацію даних, що перехоплюються по мережевий масці і MAC-адресам для всіх контрольованих протоколів. Відзначимо, що для входу в режим налаштування фільтрації по мережевий масці необхідно натиснути кнопку «Додати» в розділі «IP-адреса», а для налаштування фільтрації за MAC-адресами – в розділі «MAC-адреса».

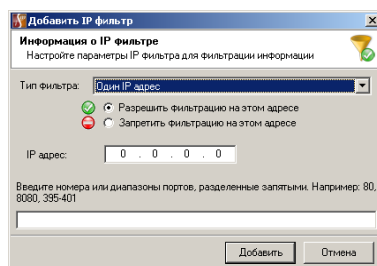


Рис. 2.16. Перший етап додавання роздільованої фільтрації за параметрами мережі

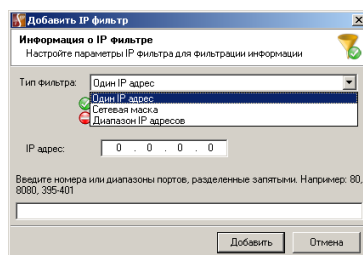


Рис. 2.17. Вибір опції «Сетевая маска»

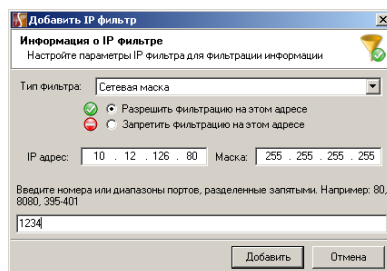


Рис. 2.18. Задання мережевої маски для прослуховування портів

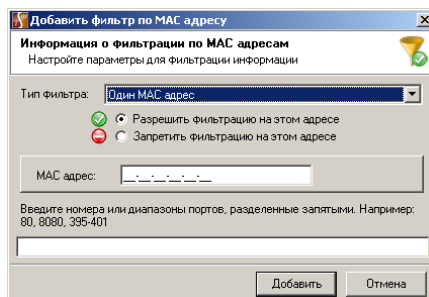


Рис. 2.19. Перший етап додавання роздільної фільтрації за MAC-адресами

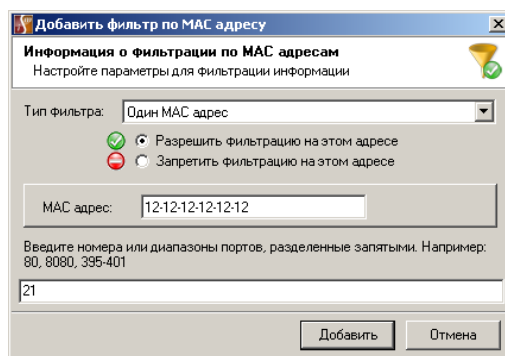


Рис. 2.20. Задання MAC-адреси і портів для прослуховування

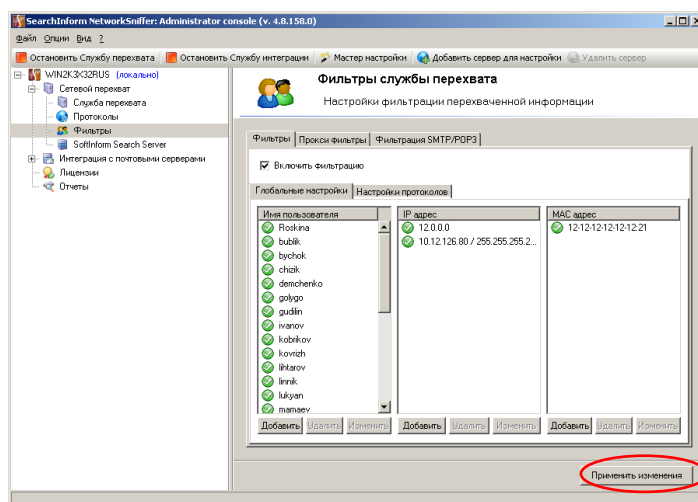


Рис. 2.21. Підтвердження додавання фільтрів за IP-адресами і MAC-адресами для всіх контрольованих протоколів

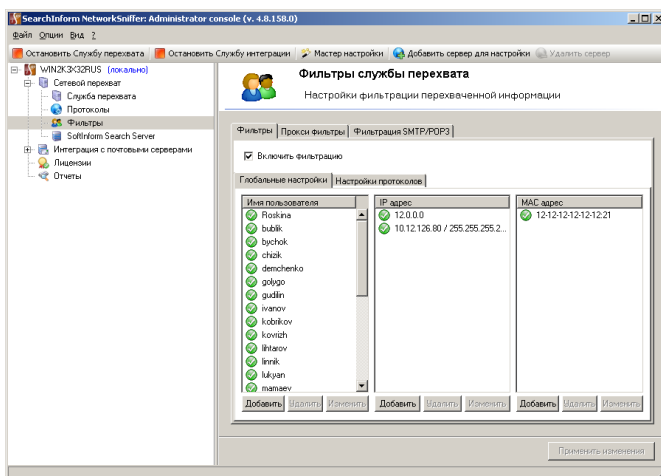


Рис. 2.22. Індикація фільтрів для всіх контрольованих протоколів

– Відповідно до рис. 2.23 – 2.28 налаштувати фільтр заборони перехоплення даних по протоколу HTTP для користувача Roskina.

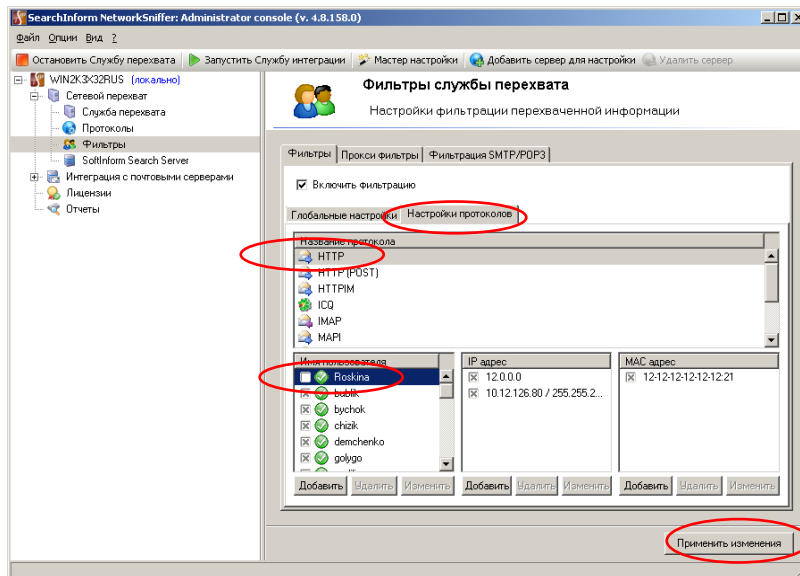


Рис. 2.23. Скасування дозвільного фільтру по протоколу HTTP для користувача Roskina

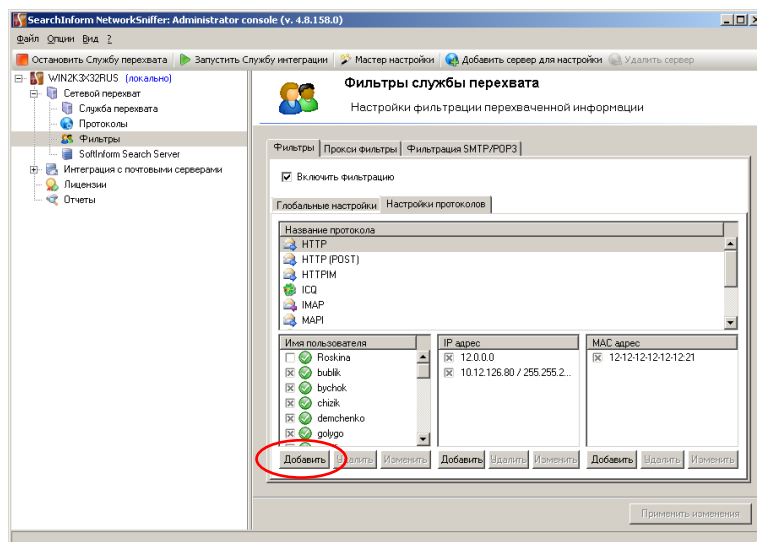


Рис. 2.24. Вхід в режим додавання нового фільтра користувачів по протоколу HTTP

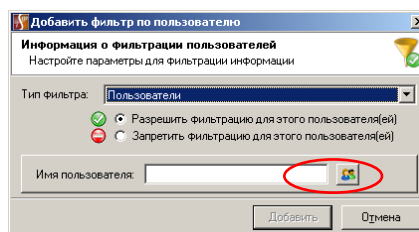


Рис. 2.25. Вхід в режим вибору користувачів

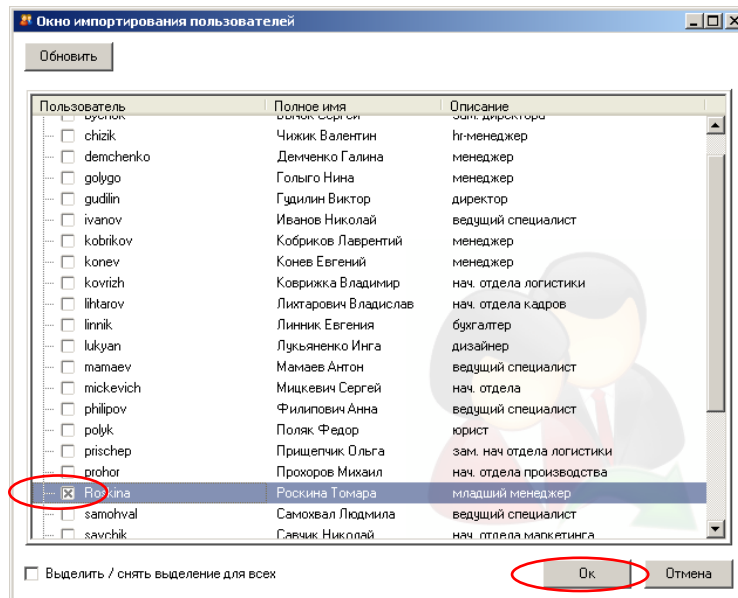


Рис. 2.26. Вибір користувача Roskina

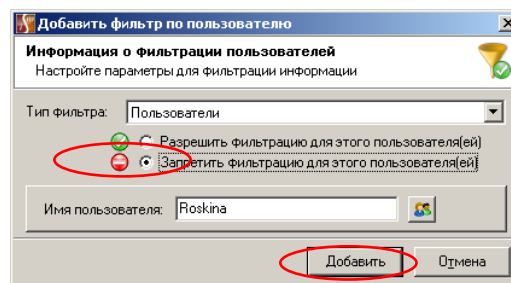


Рис. 2.27. Вибір фільтра заборони

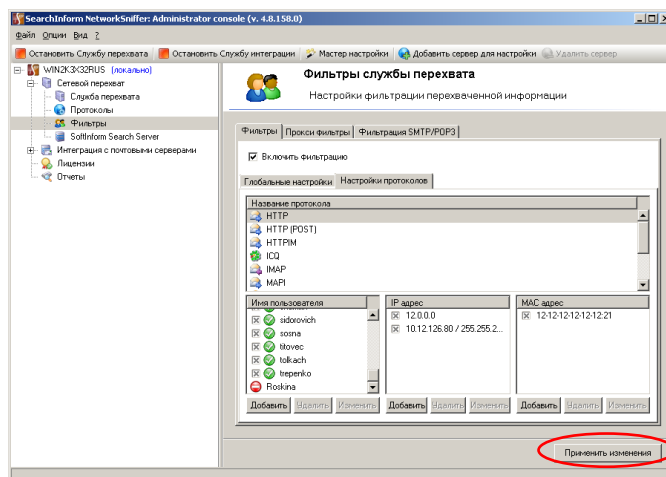


Рис. 2.28 Підтвердження додавання нового фільтра заборони

– Відповідно до рис. 2.29 – 2.33 налаштувати проксі-фільтр.

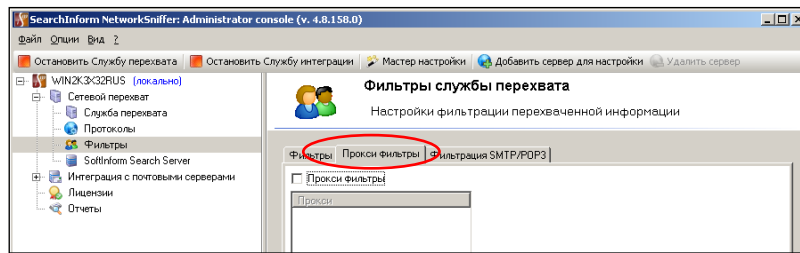


Рис. 2.29. Перехід до налаштувань фільтрації по проксі-серверів

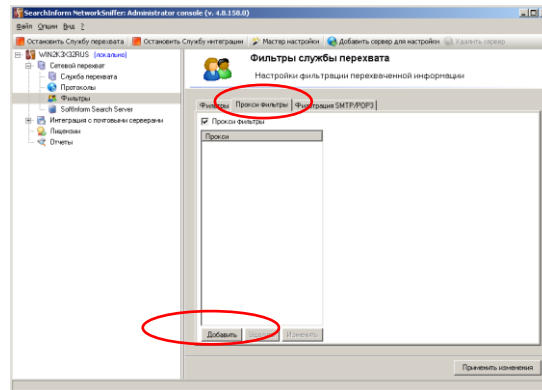


Рис. 2.30. Перший етап додавання проксі фільтра

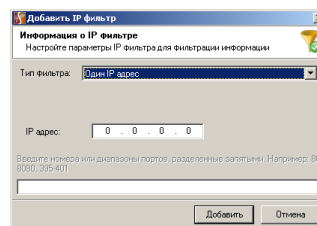


Рис. 2.31. Вікно вводу параметрів проксі-сервера

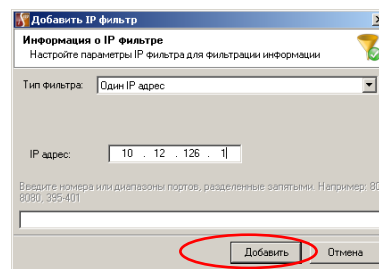


Рис. 2.32. Додавання параметрів проксі-сервера

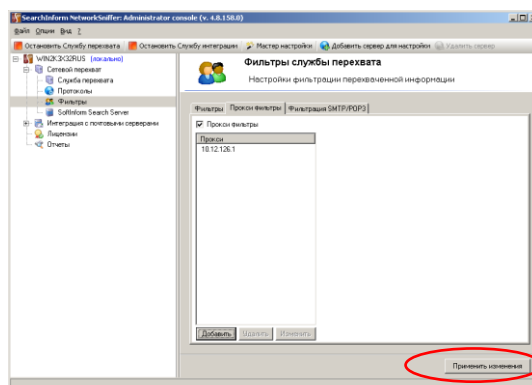


Рис. 2.33. Підтвердження параметрів проксі-сервера

– Відповідно до рис. 2.34 – 2.36 видалити проксі-фільтр.

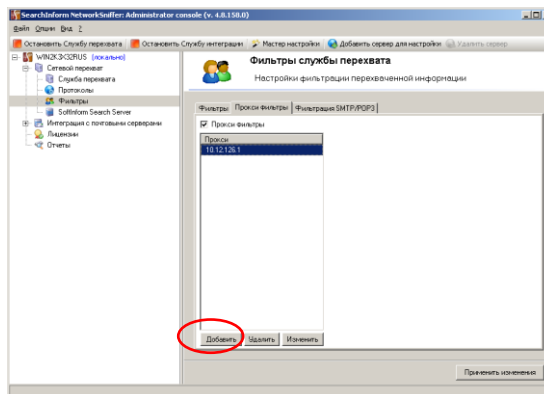


Рис. 2.34. Вибір проксі-фільтра для видалення

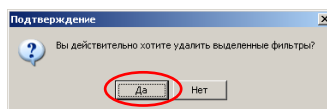


Рис. 2.35. Підтвердження видалення фільтра

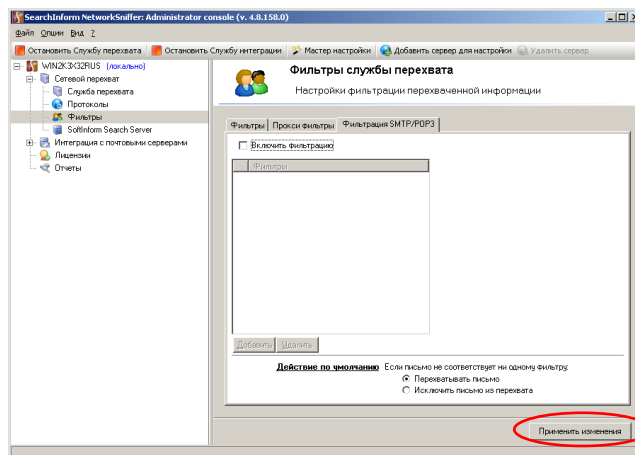


Рис. 2.36. Підтвердження налаштувань з видалення фільтра

– Відповідно до рис. 2.37 – 2.40 створити фільтр на поштові адреси для повідомлень більше 10000 байт.

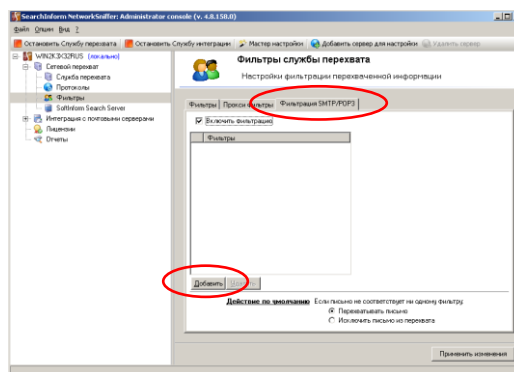


Рис. 2.37. Вхід в режим додавання фільтра на поштові адреси

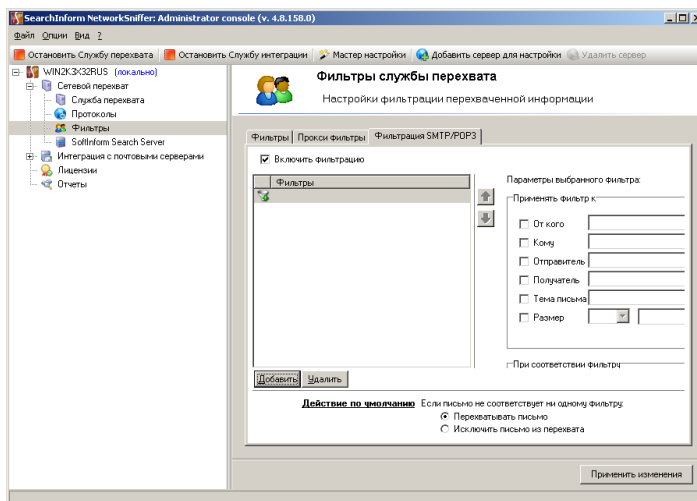


Рис. 2.38. Вікно налаштування параметрів на поштові адреси

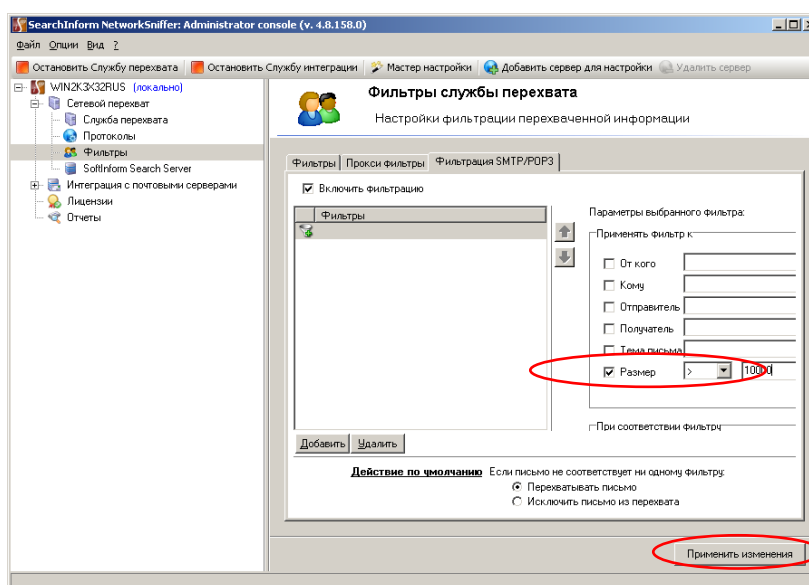


Рис. 2.39. Установка размера повідомлення

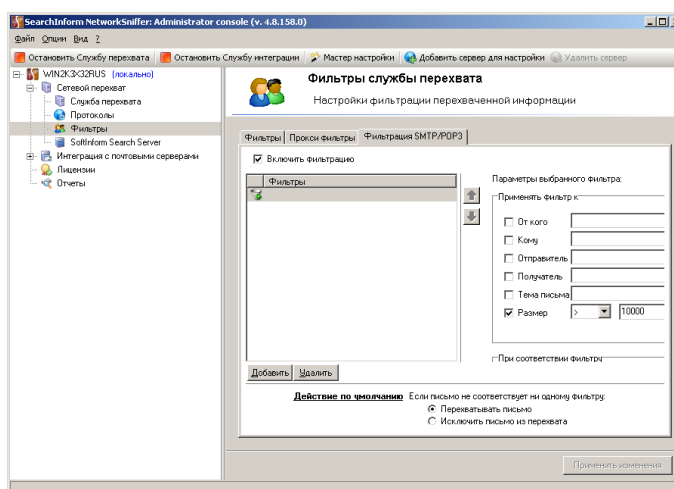


Рис. 2.40. Індикація встановленого фільтра на поштові адреси

– Відповідно до рис. 2.41 – 2.47 вказати відповідність користувача 123 поштової адресі 123@ukr.net.

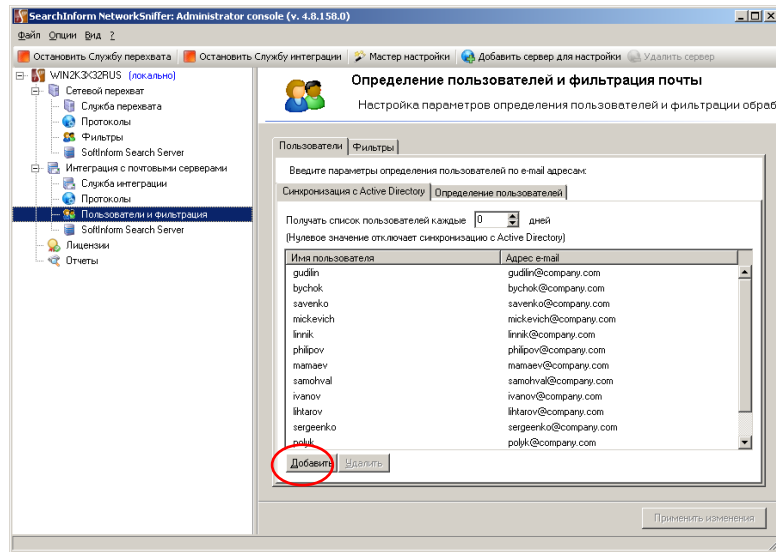


Рис. 2.41. Додавання адреси

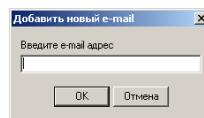


Рис. 2.42. Введення адреси

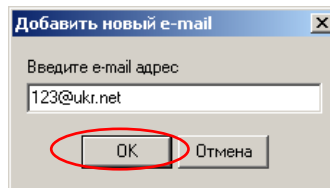


Рис. 2.43. Підтвердження введенної адреси

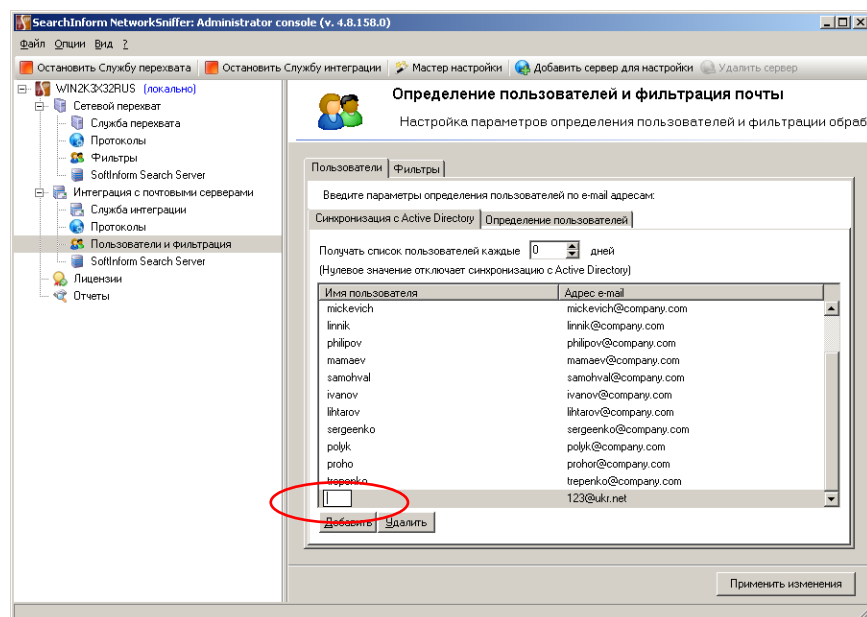


Рис. 2.44. Поле введення ім'я користувача

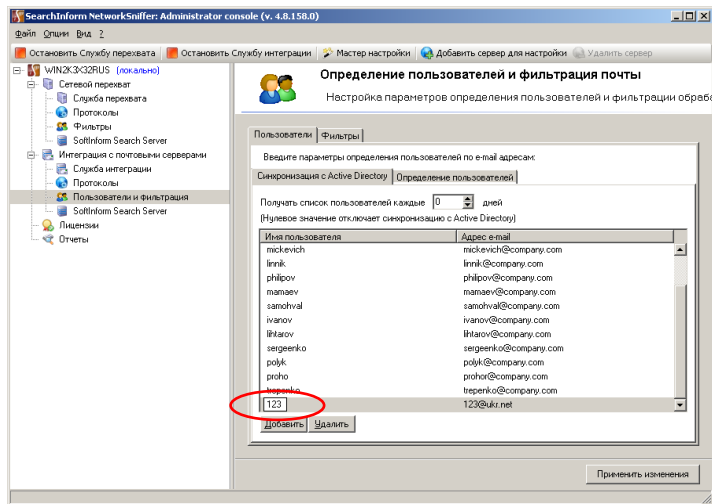


Рис. 2.45. Введення імені користувача

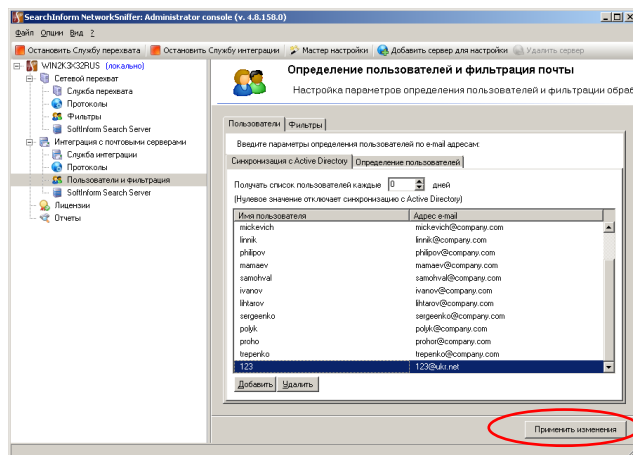


Рис. 2.46. Підтвердження відповідності адреси користувачу

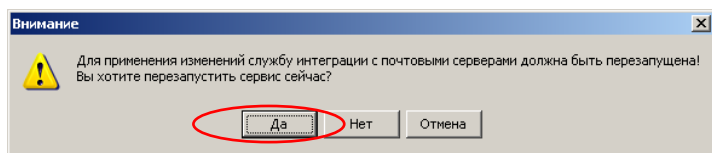


Рис. 2.47. Підтвердження перезапуску служби інтеграції з поштовими серверами

– Відповідно до рис. 2.48 – 2.51 створити список визначення масок поштових адрес користувачів.

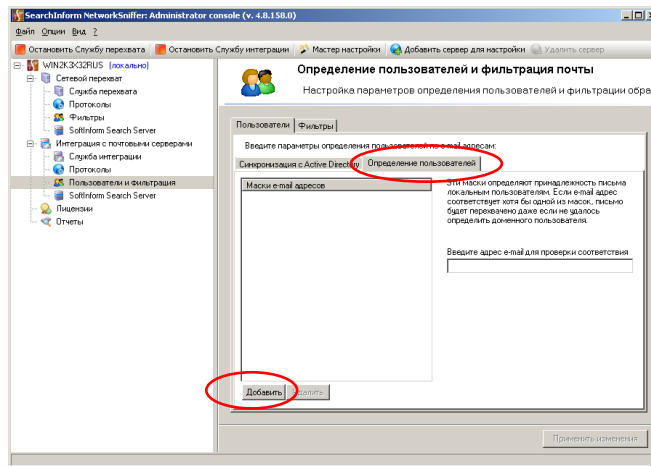


Рис. 2.48. Додавання маски

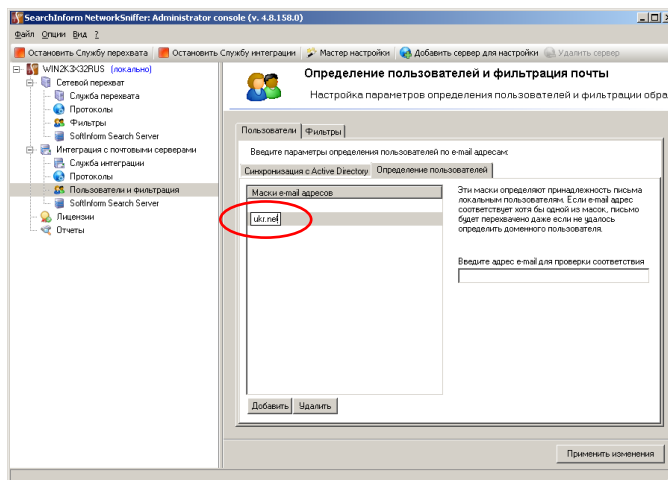


Рис. 2.49. Введення маски *@ukr.net

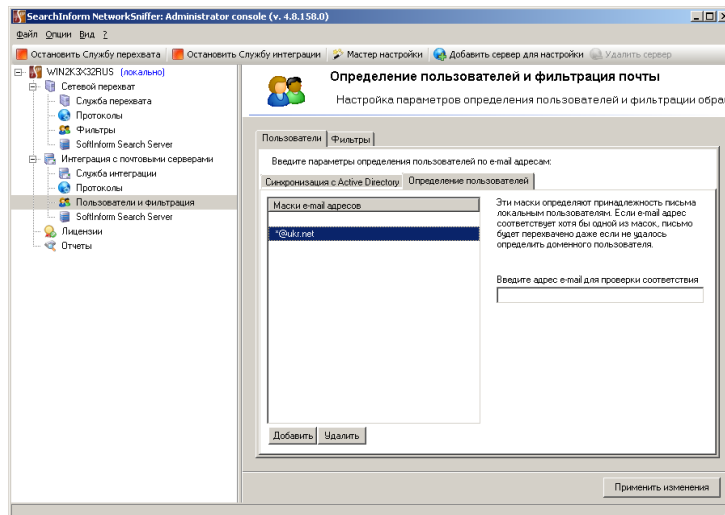


Рис. 2.50. Індикація введеної маски

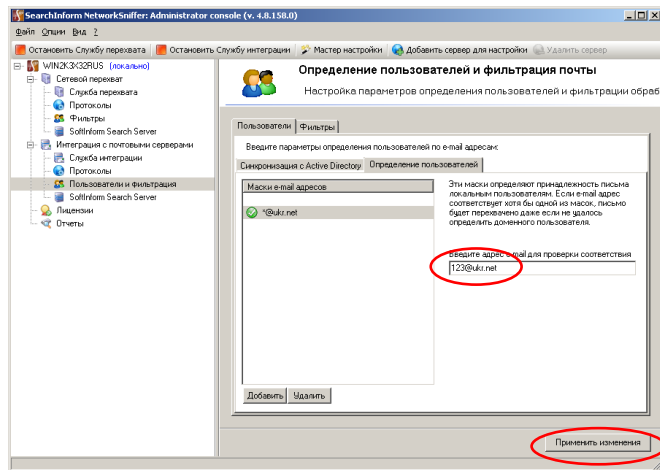


Рис. 2.51. Перевірка введеної маски

– Відповідно до рис. 2.52 – 2.55 створити фільтр поштою користувачам, визначивши пошук наявності в темі листа слова «корупція».

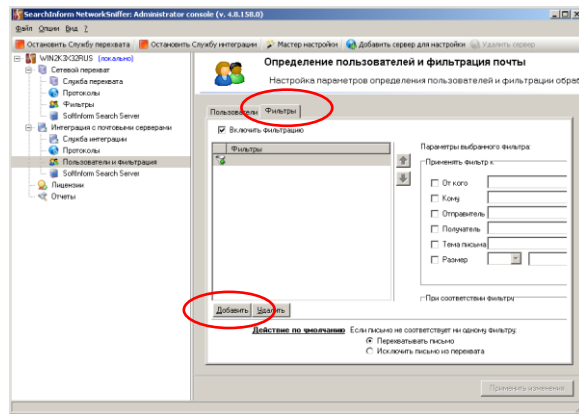


Рис. 2.52. Перехід для створення фільтра

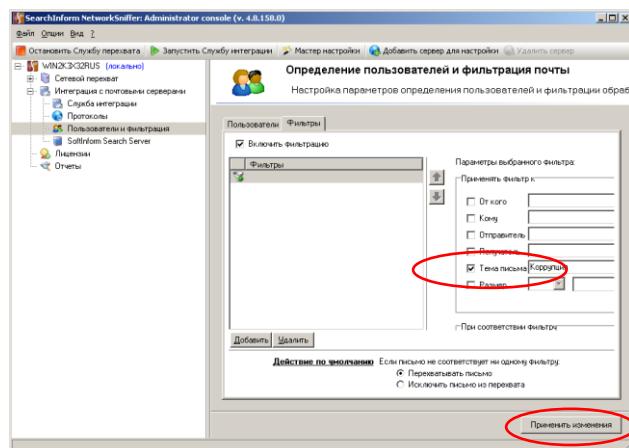


Рис. 2.53. Визначення параметрів фільтра

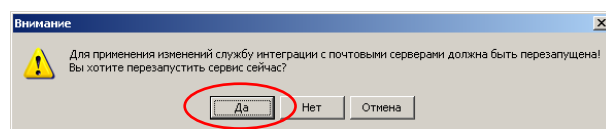


Рис. 2.54. Підтвердження перезапуску служби інтеграції

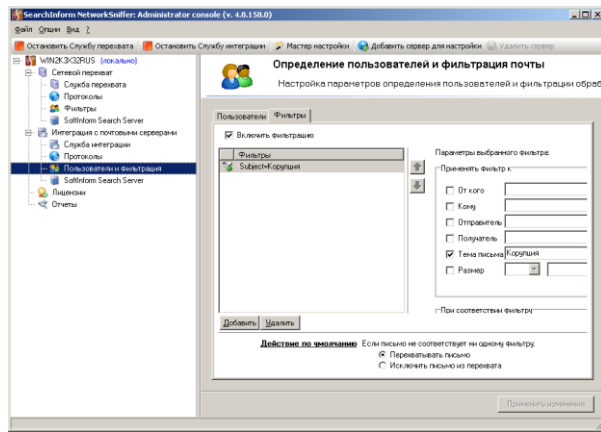


Рис. 2.55. Індикація успішного створення фільтра

- Закрити вікно консолі *NetworkSniffer Administrator*.
- Відкрити вікно консолі *SearchInform EndpointSniffer*.

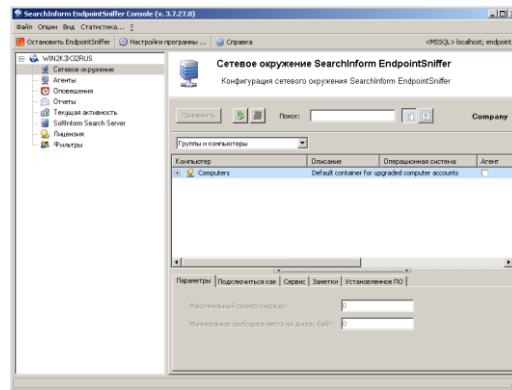


Рис. 2.56. Вікно *SearchInform EndpointSniffer Console*

- Відповідно до рис. 2.57 – 2.62 видалити з фільтрації по всіх протоколах дані користувача «Адмін».

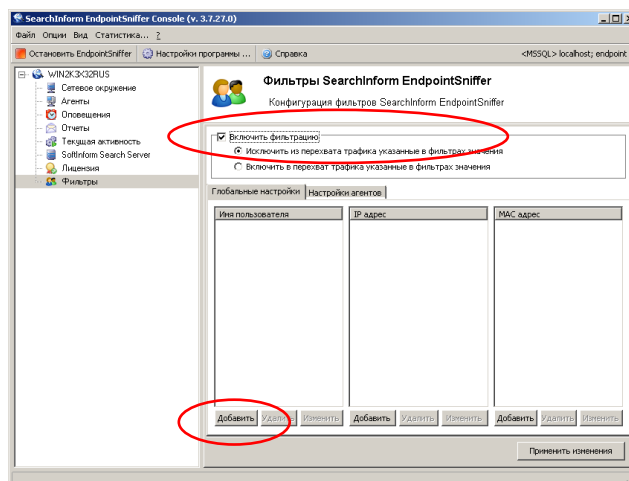


Рис. 2.57. Додавання фільтра по всіх протоколах

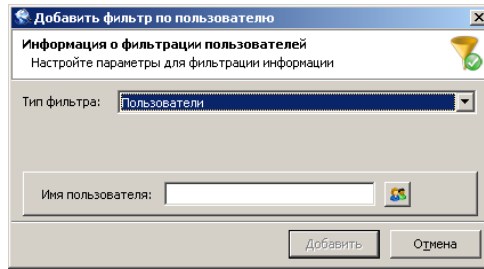


Рис. 2.58. Вікно введення імені користувача

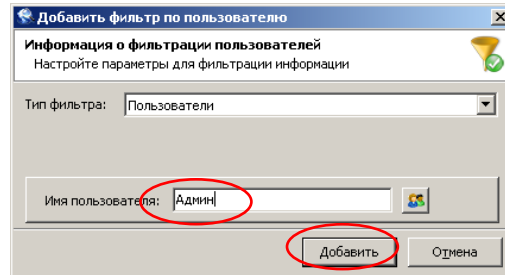


Рис. 2.59. Введення імені користувача

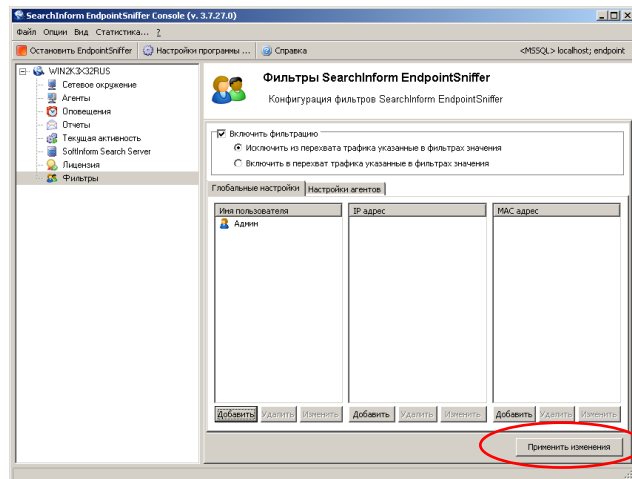


Рис. 2.60. Підтвердження додавання фільтра по всіх протоколах

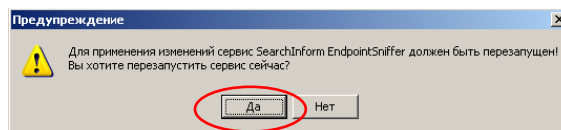


Рис. 2.61. Підтвердження перезапуску сервера

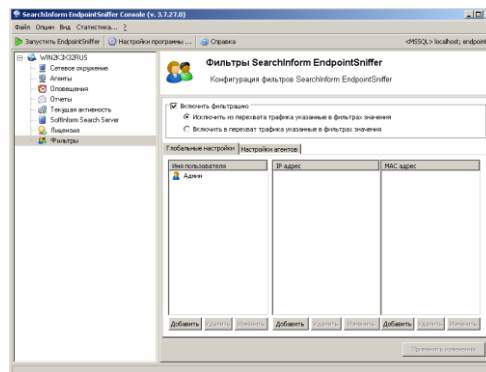


Рис. 2.62. Індикація створеного фільтра по всіх протоколах

– Відповідно до рис. 2.63 – 2.66 видалити з фільтрації монітор користувача «user».

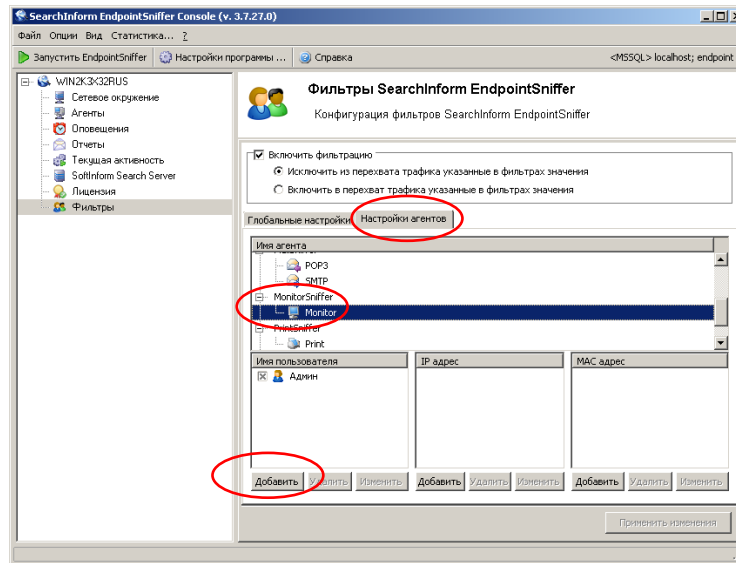


Рис. 2.63. Вибір *MonitorSniffer* і додавання нового користувача

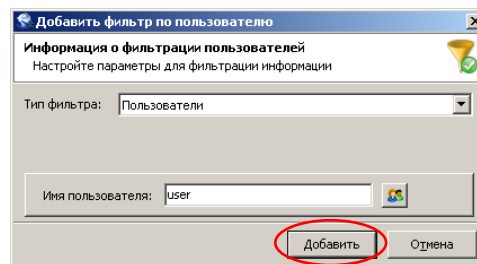


Рис. 2.64. Введення імені користувача

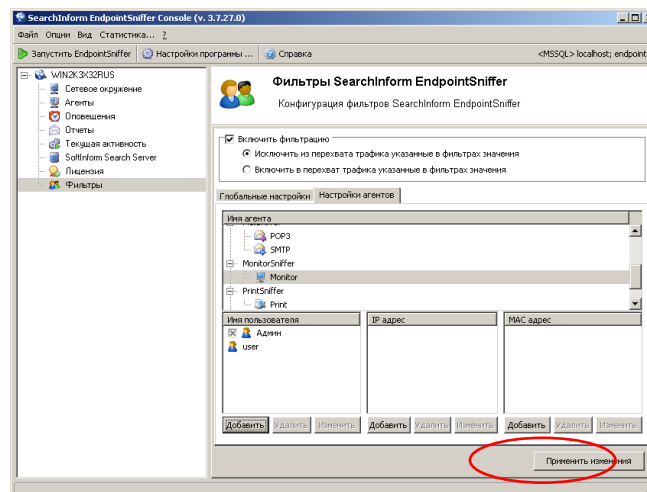


Рис. 2.65. Підтвердження змін

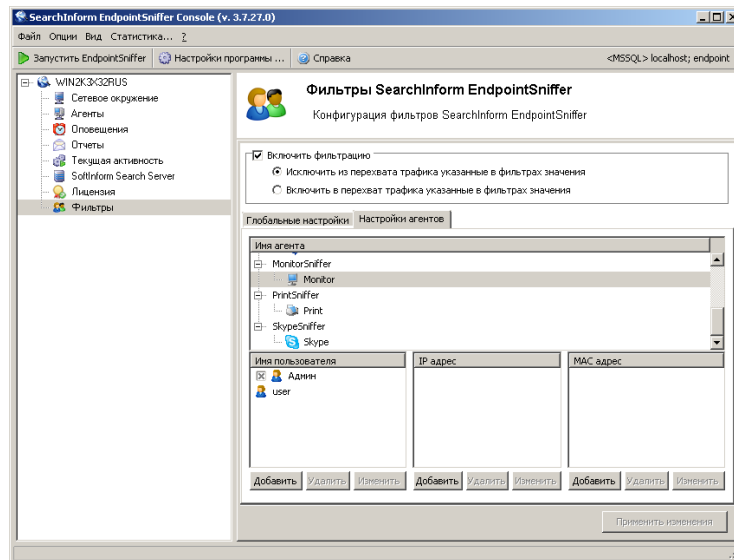


Рис. 2.66. Индикация створених фільтрів

- Закрити вікно консолі *SearchInform EndpointSniffer*.
- Відкрити вікно консолі *NetworkSniffer Administrator*.

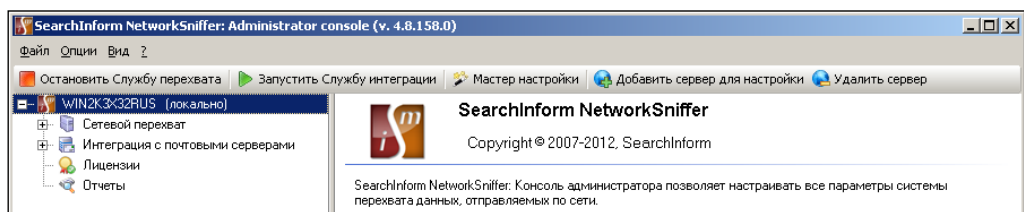


Рис. 2.67. Вікно консолі *NetworkSniffer Administrator*

- Відповідно до рис. 2.68 – 2.73 налаштувати розклад поновлення індексів `Network_POST`. Передбачаємо оновлення індексів через кожні 5 ХВИЛИН.

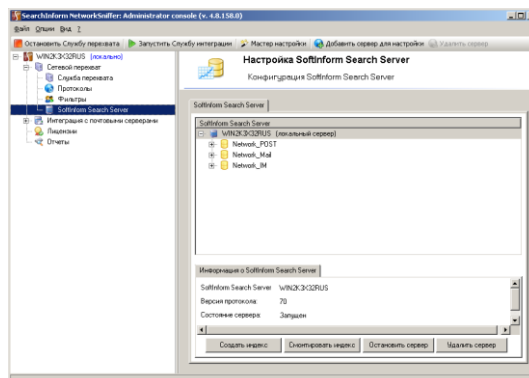


Рис. 2.68. Вікно редагування параметрів індексів

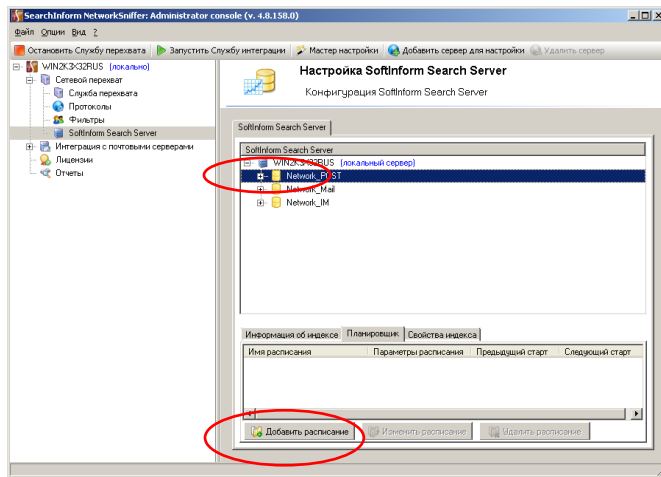


Рис. 2.69. Додавання розкладу для індексу Network_POST

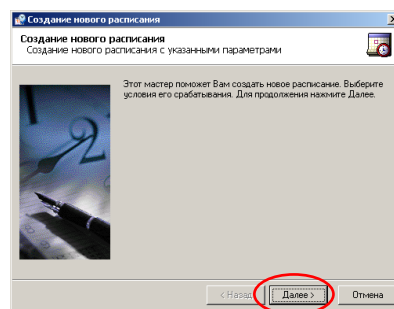


Рис. 2.70. Перший етап створення розкладу

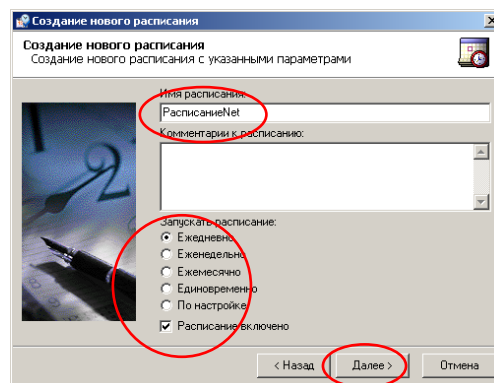


Рис. 2.71. Другий етап створення розкладу

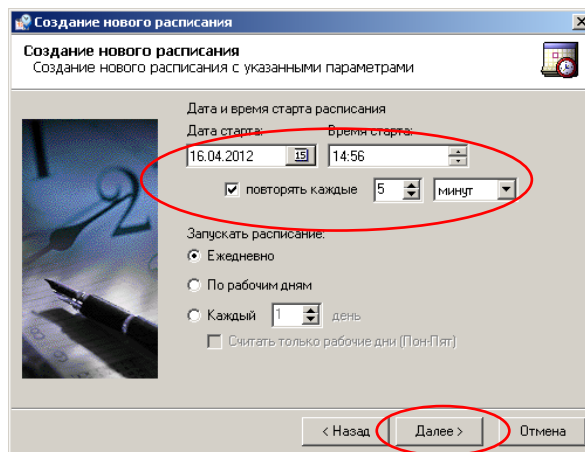


Рис. 2.72. Третій етап створення розкладу

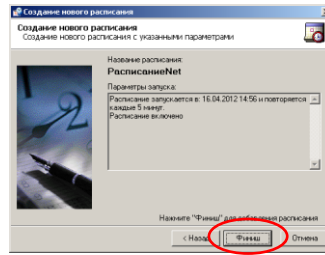


Рис. 2.73. Заключный этап створення розкладу

– Відповідно до рис. 2.74 – 2.77 налаштувати розклад поновлення індексів Network_Mail. Передбачаємо оновлення індексів через кожні 10 ХВИЛИН.

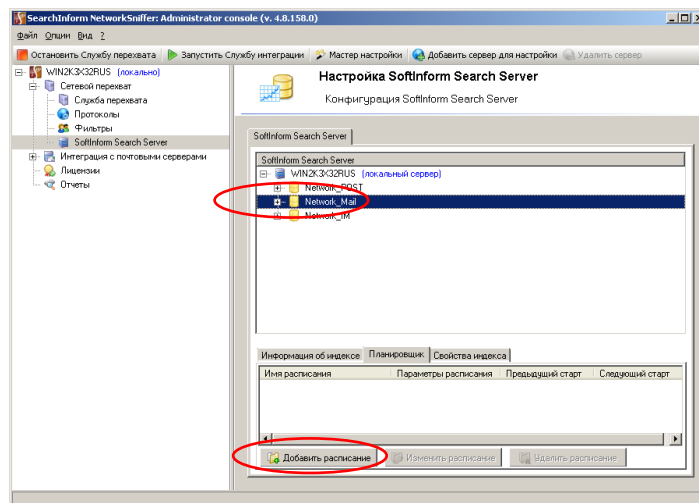


Рис. 2.74. Додавання розкладу для індексу Network_Mail

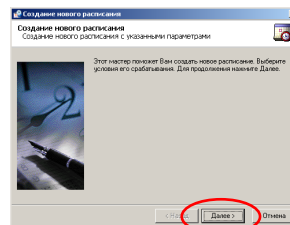


Рис. 2.75. Перший етап створення розкладу

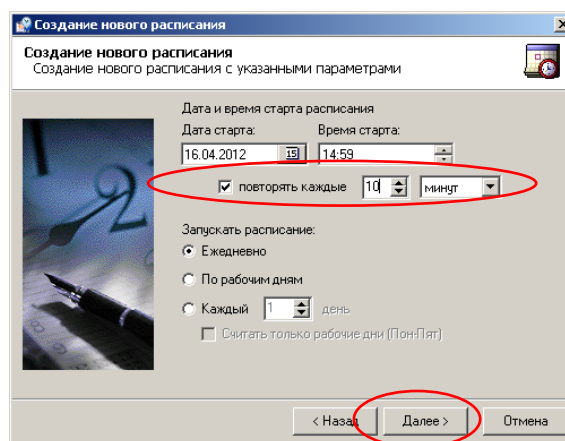


Рис. 2.76. Другий етап створення розкладу

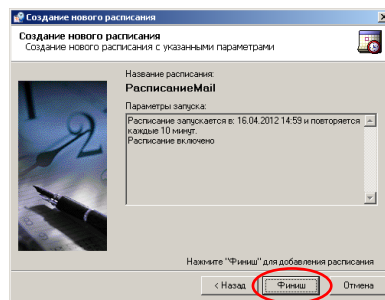


Рис. 2.77. Третий этап створення розкладу

– Відповідно до рис. 2.78 – 2.81 налаштувати розклад поновлення індексів Network_IM. Передбачаємо оновлення індексів через кожні 3 хвилини.

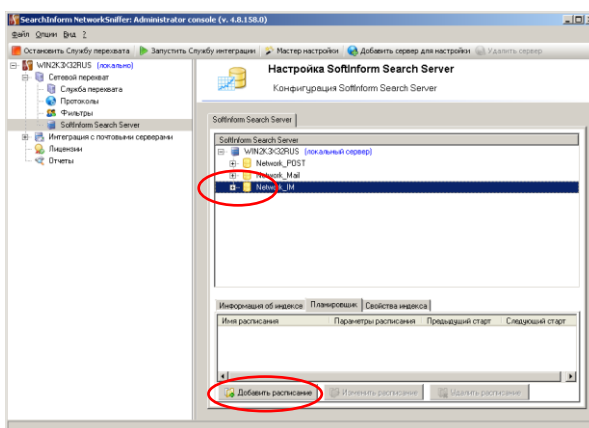


Рис. 2.78. Додавання розкладу для індексу Network_IM

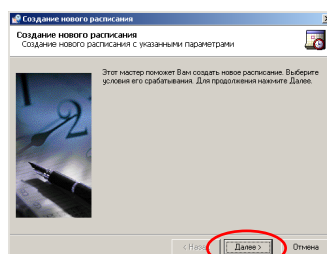


Рис. 2.79. Перший етап створення розкладу

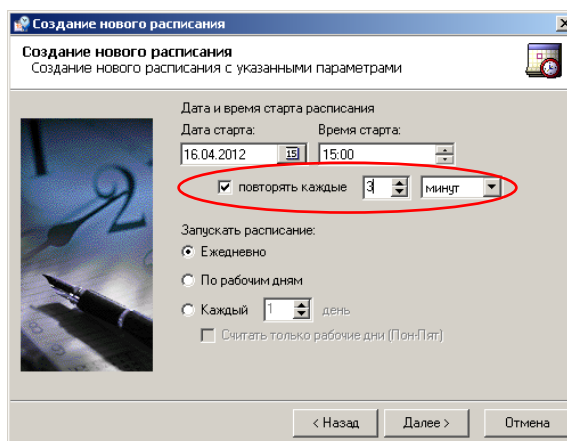


Рис. 2.80. Другий етап створення розкладу

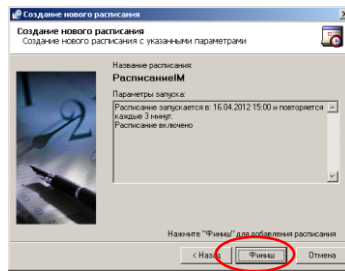


Рис. 2.81. Третій етап створення розкладу

- Закрити вікно *NetworkSniffer Administrator Console*.
- Відкрити вікно *AlertCenter Client*. Відповідно до рис. 2.82 відкрити гілку «Політика безпеки».

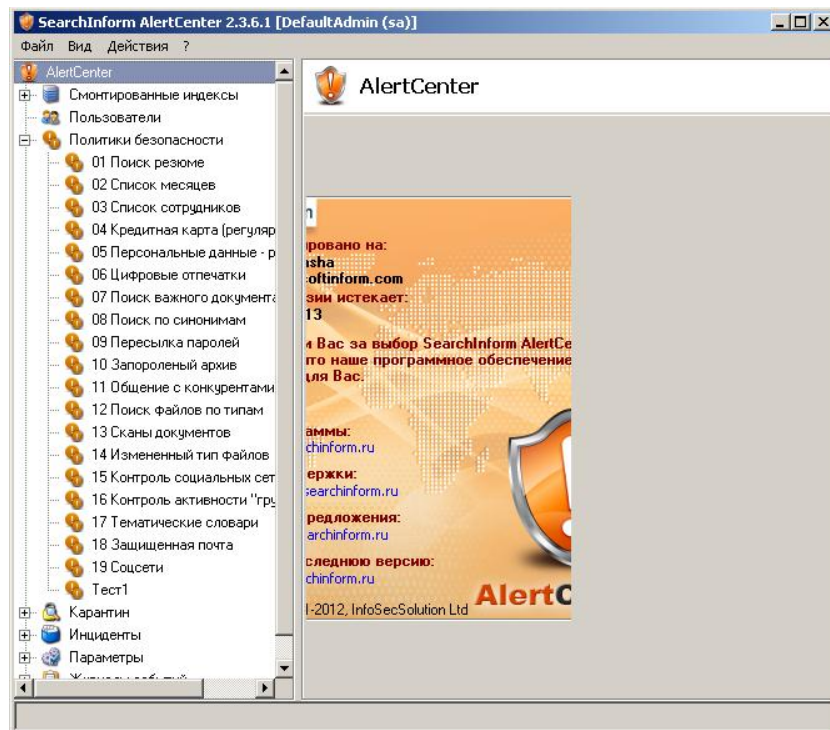


Рис. 2.82. Гілка «Політика безпеки»

- Відповідно до рис. 2.83 – 2.88 змінити параметри політики безпеки «Список місяців». Передбачити перевірку індексів кожні 10 хвилин.

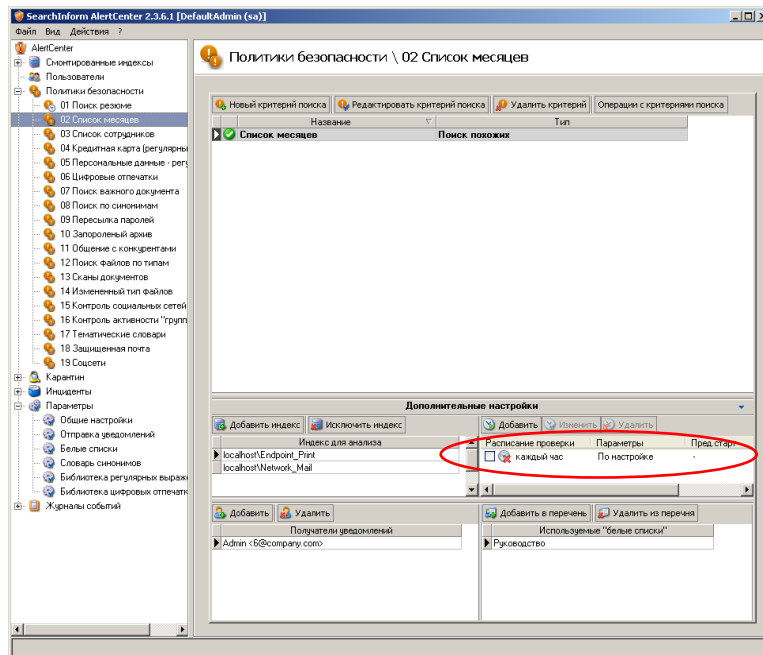


Рис. 2.83. Вибір налаштувань «Розклад перевірок» для політики «Список місяців»

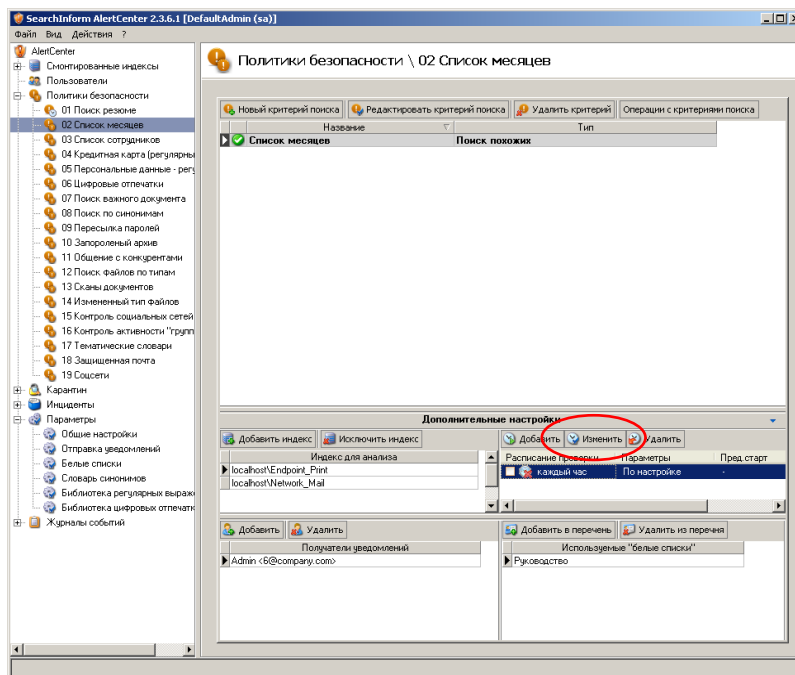


Рис. 2.84. Вхід в режим зміни налаштувань розкладу

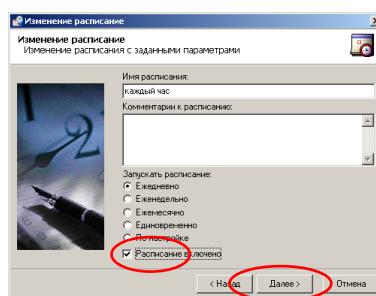


Рис. 2.85. Перший етап зміни розкладу

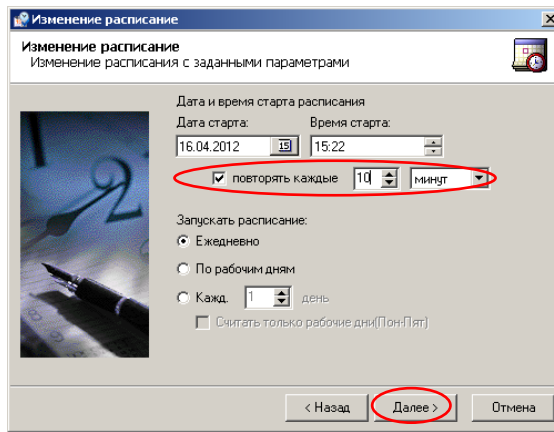


Рис. 2.86. Другой этап зміни розкладу

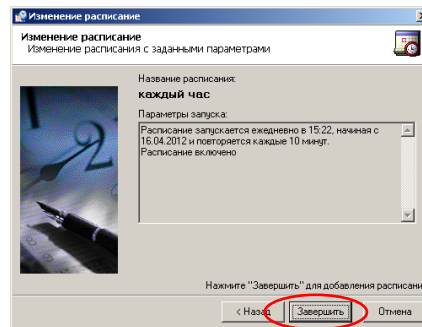


Рис. 2.87. Третій етап зміни розкладу

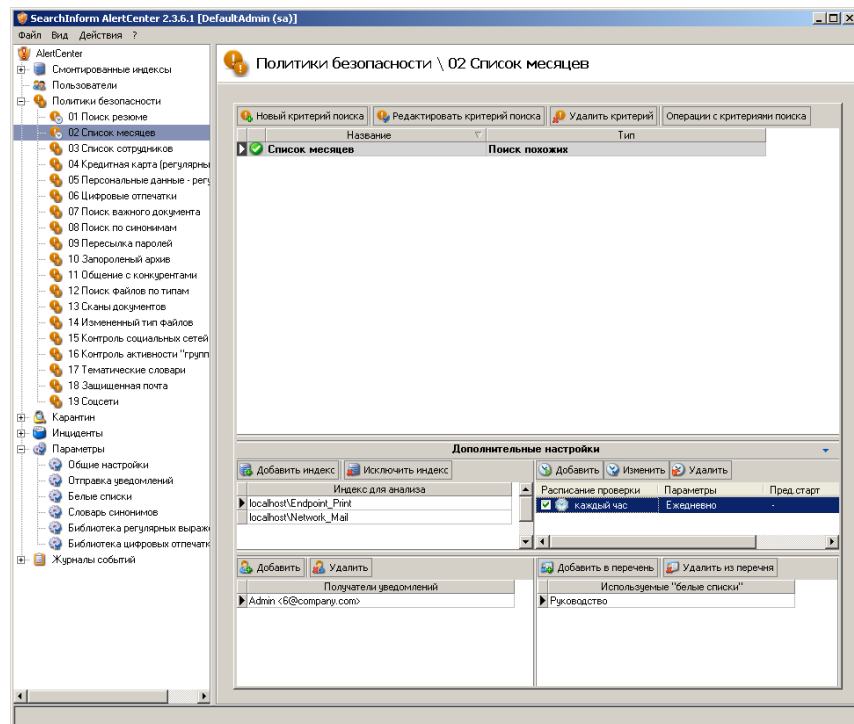


Рис. 2.88. Індикація зміни розкладу

– Відповідно до рис. 2.89 – 2.94 створити новий розклад політики «Список співробітників». Назва розкладу «Навчальний розклад». Інтервал перевірки індексів 7 хвилин.

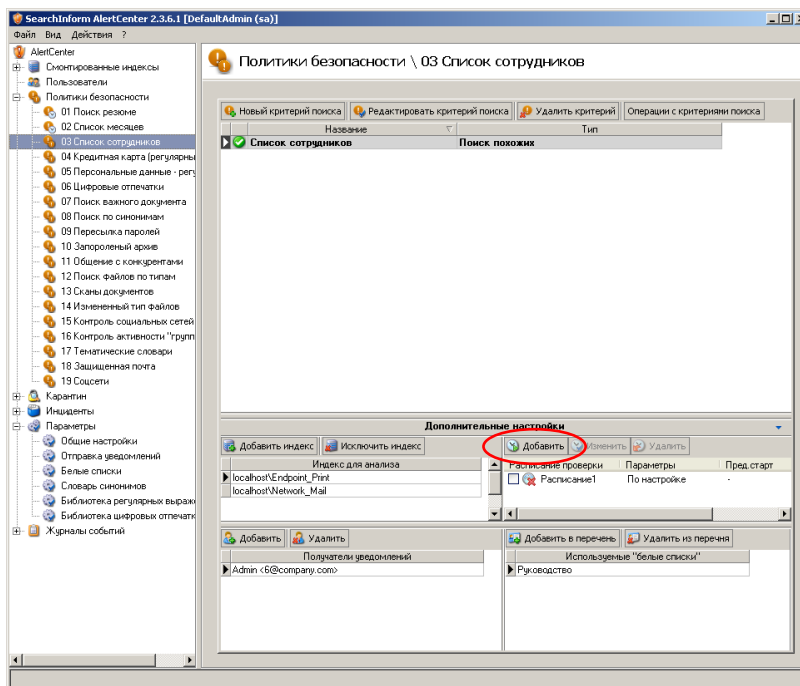


Рис. 2.89. Вибір політики «Список співробітників» і додавання нового розкладу

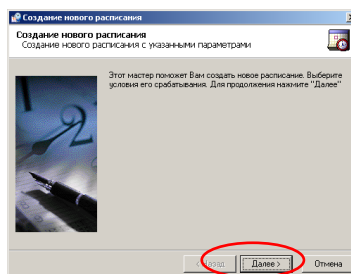


Рис. 2.90. Перший етап зміни розкладу

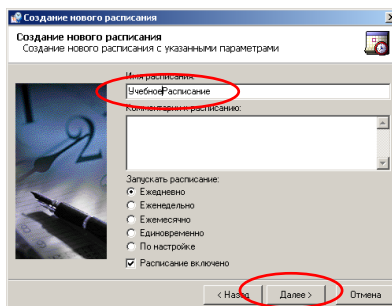


Рис. 2.91. Введення імені розкладу - «Навчальний розклад»

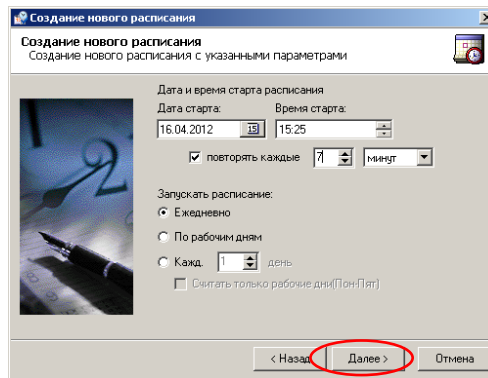


Рис. 2.92. Введення інтервалу перевірки - 7 хвилин

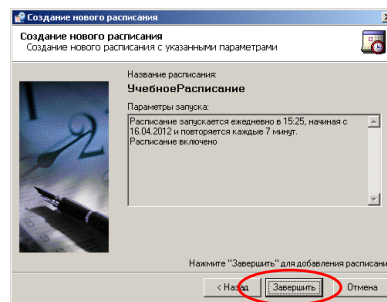


Рис. 2.93. Заключний етап формування розкладу

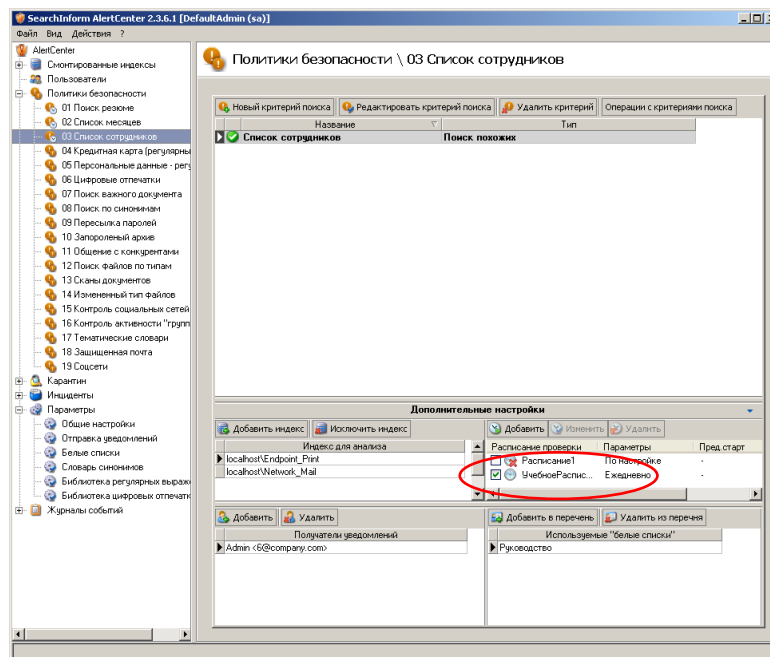


Рис. 2.94. Индикация нового раскладу

– Відповідно до рис. 2.95 – 2.97 відредагувати білий список «Лояльних співробітників». Додати в нього користувача «Vassiliy».

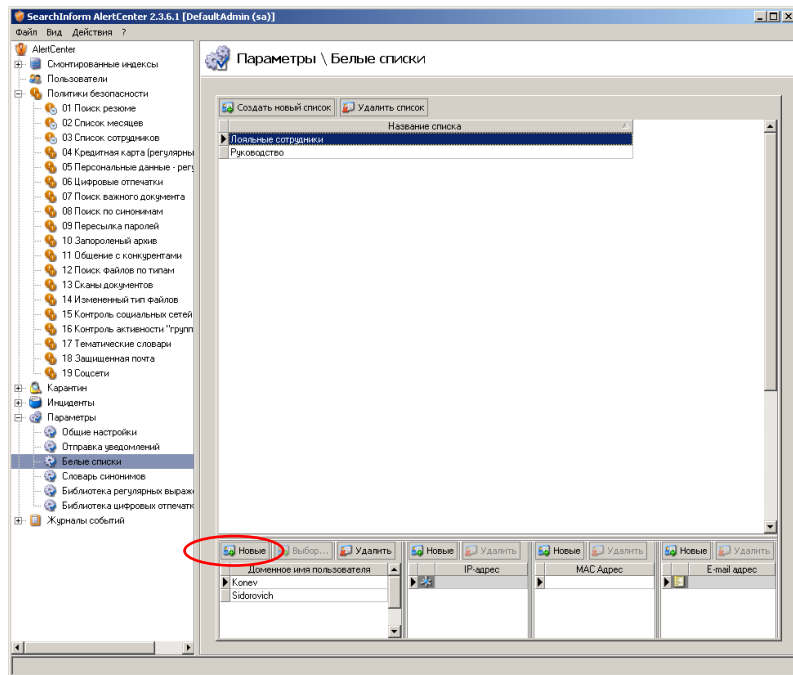


Рис. 2.95. Вхід в режим додавання нового користувача

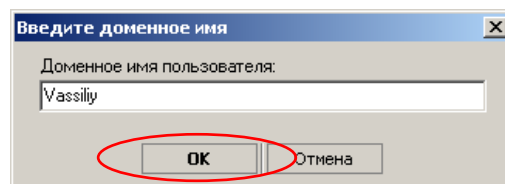


Рис. 2.96. Введення імені користувача

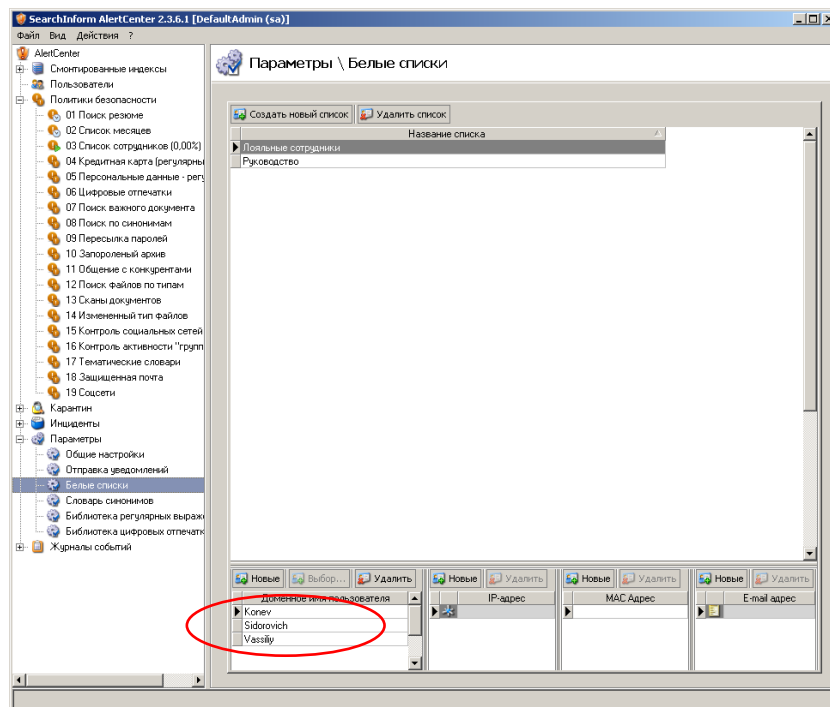


Рис. 2.97. Індикація користувачів в білому списку «Лояльні співробітники»

– Відповідно до рис. 2.98 – 2.102 створити білий список «Мій список».
Додати в нього користувача «Адміністратор».

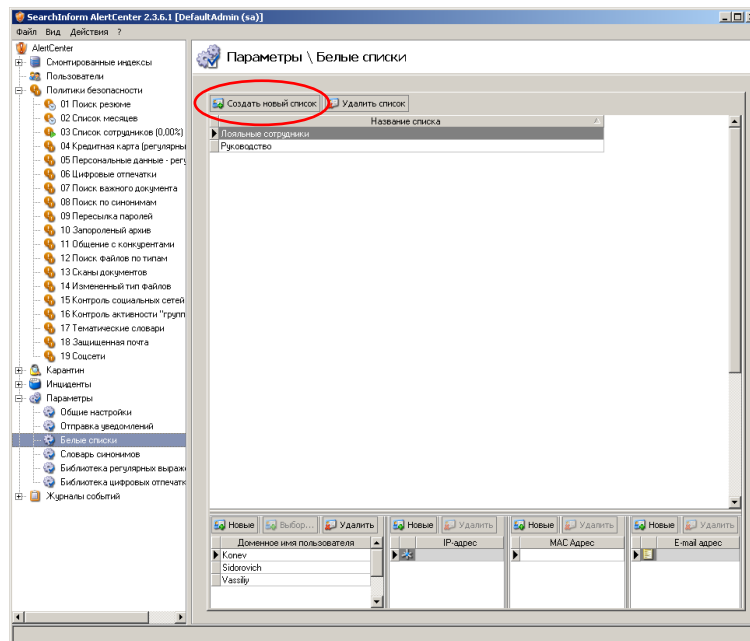


Рис. 2.98. Перший етап створення нового білого списку

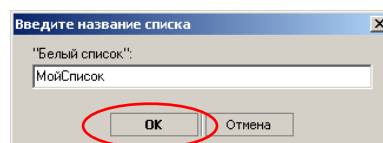


Рис. 2.99. Введення імені списку

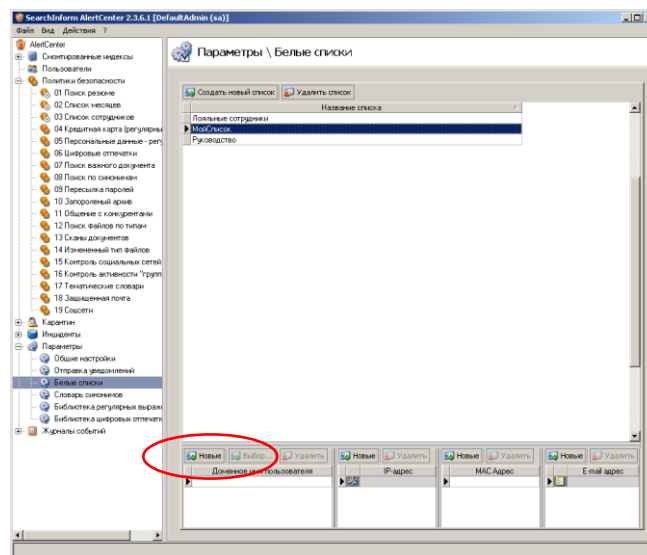


Рис. 2.100. Перший етап додавання нового користувача в список

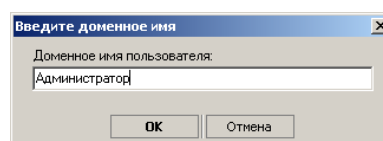


Рис. 2.101. Введення імені нового користувача

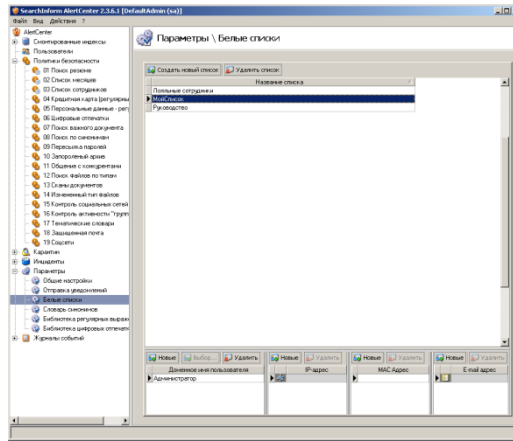


Рис. 2.102. Індикація параметрів створеного списку «Мій список»

– Відповідно до рис. 2.103 переглянути виявлені порушення (інциденти)

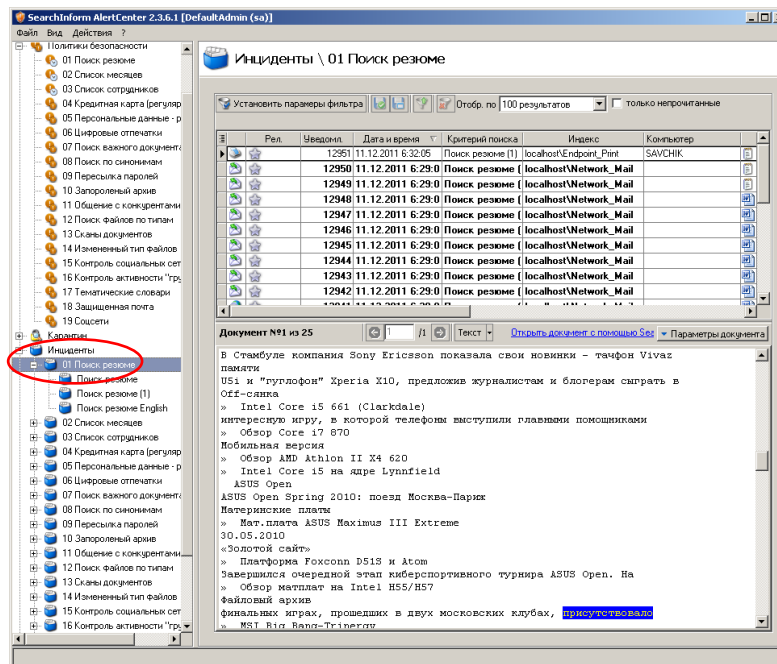


Рис. 2.103. Перегляд виявлених порушень політики «Пошук резюме»

– Відповідно до рис. 2.104 – 2.106 створити нову політику безпеки з назвою «Тест1».

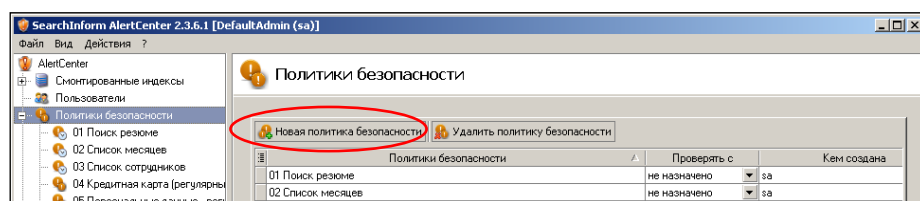


Рис. 2.104. Вхід в режим створення нової політики

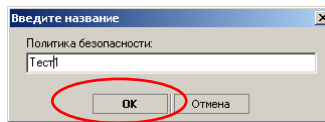


Рис. 2.105. Введення імені політики

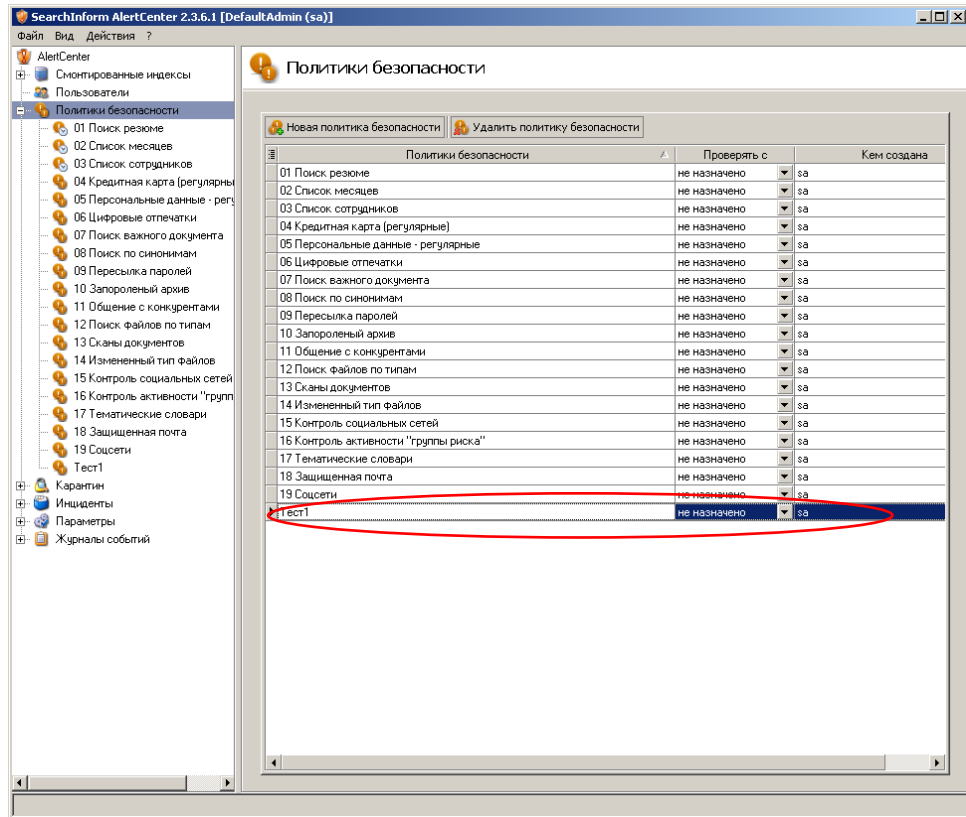


Рис. 2.106. Індикація створеної політики

– Відповідно до рис. 2.107 – 2.109 додати в політику «Тест1» фразовий пошук і пошук по атрибутам перехоплених даних.

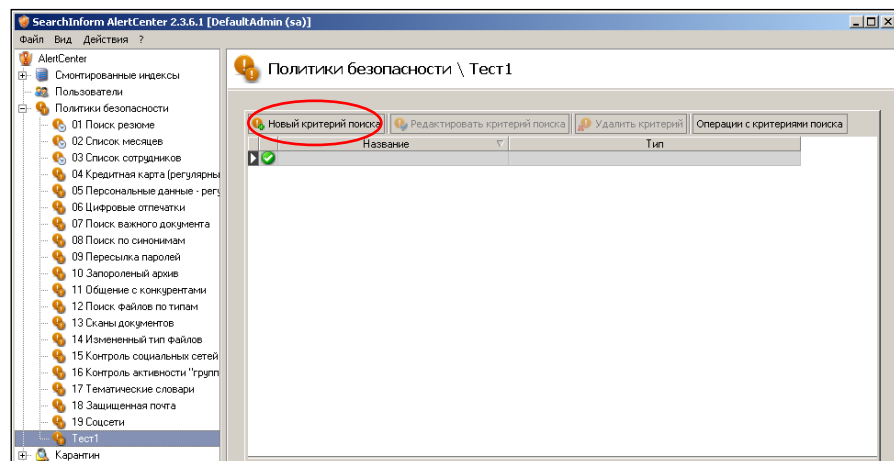


Рис. 2.107. Вхід в режим створення критеріїв пошуку

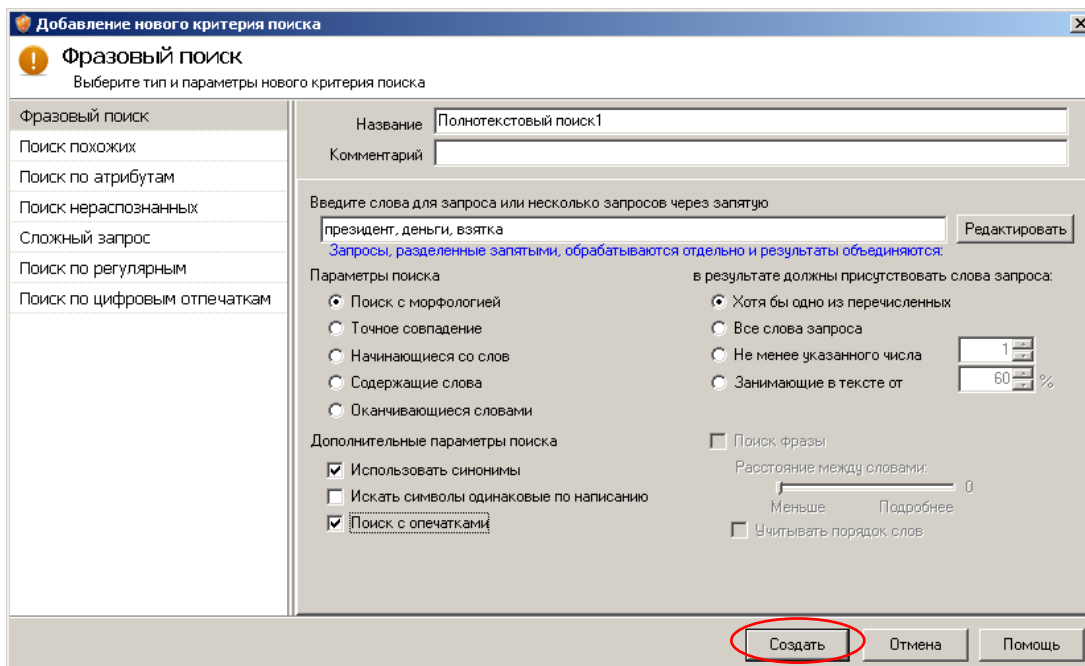


Рис. 2.108. Введення параметрів фразового пошуку

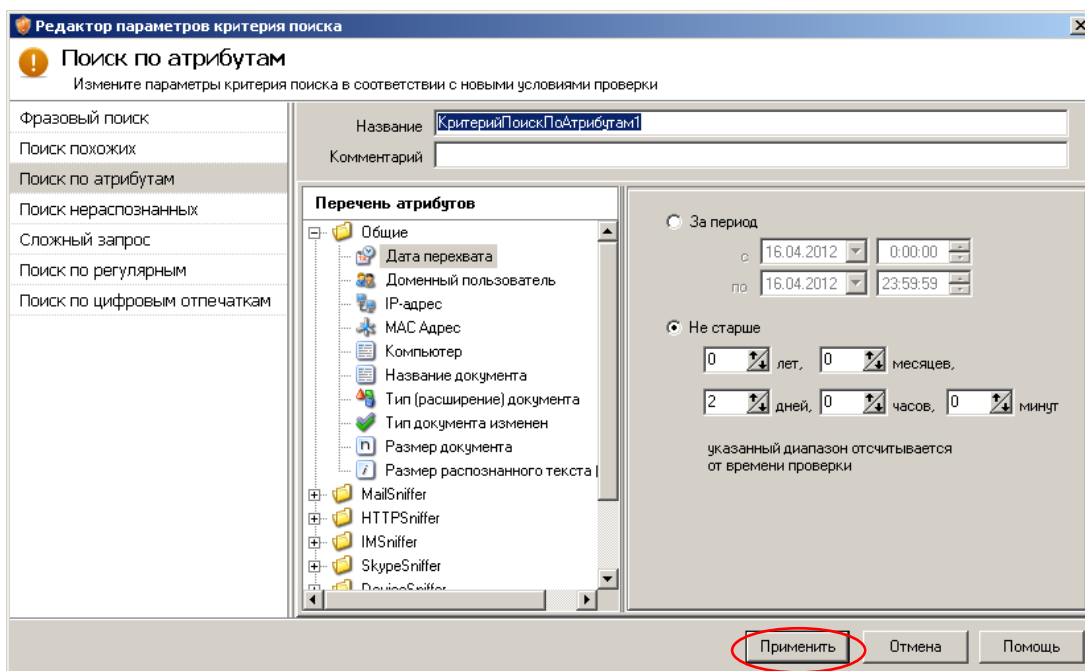


Рис. 2.109. Введення параметрів пошуку по атрибутам

– Відповідно до рис. 2.110 – 2.122 додати в політику «Тест1» список перевіряються індексів, розклад перевірки індексів, список одержувачів повідомлень про порушення і білий список користувачів.

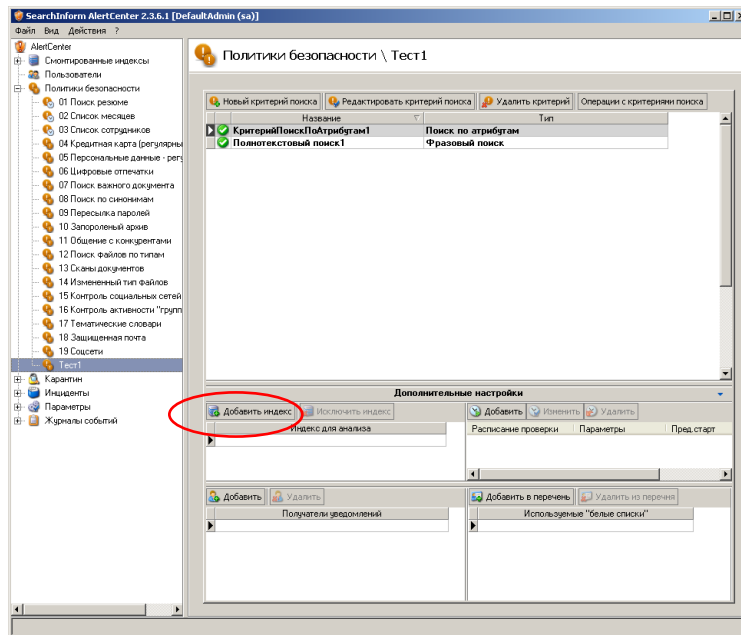


Рис. 2.110. Вхід в режим додавання індексів

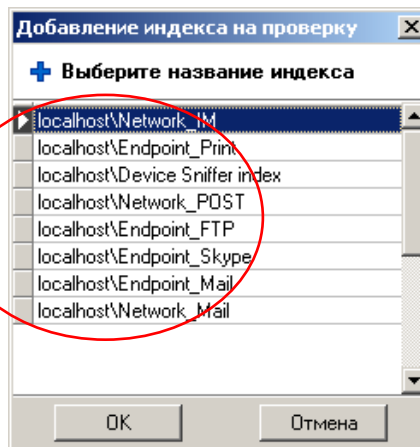


Рис. 2.111. Вікно додавання імен індексів

(Для вибору декількох індексів слід затиснути клавішу «Ctrl»)

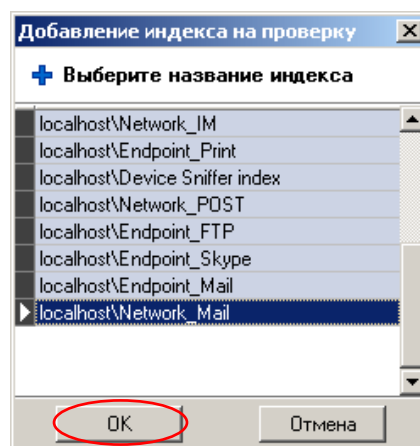


Рис. 2.112. Вікно обраних індексів

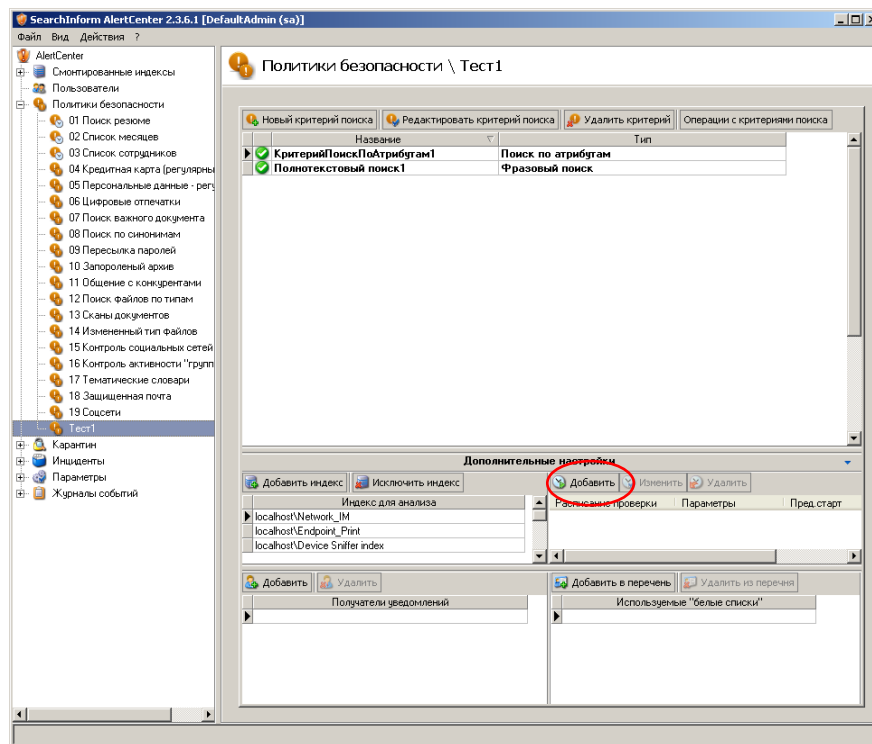


Рис. 2.113. Кнопка додавання нового розкладу перевірок індексів

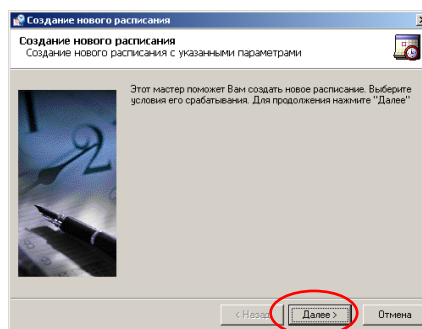


Рис. 2.114. Перший етап формування розкладу перевірок індексів

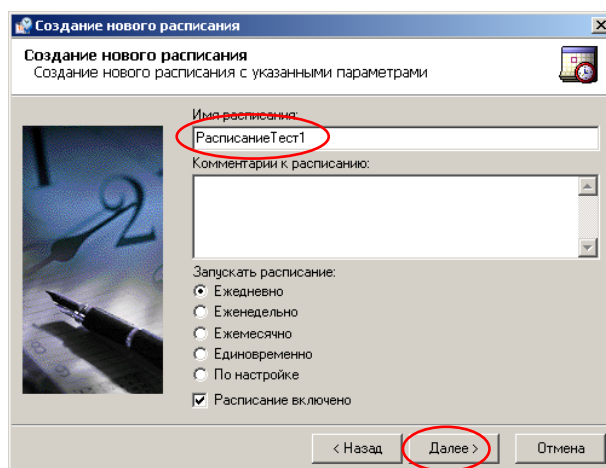


Рис. 2.115. Другий етап формування розкладу перевірок індексів
(Назва розкладу – «РасписаниеТест1»)

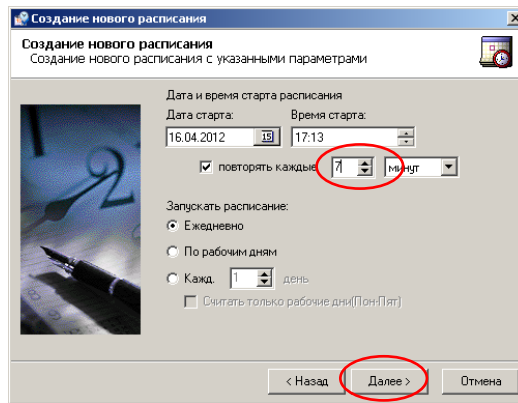


Рис. 2.116. Третий этап формування розкладу перевірок індексів (Інтервал перевірки – 7 хвилин)

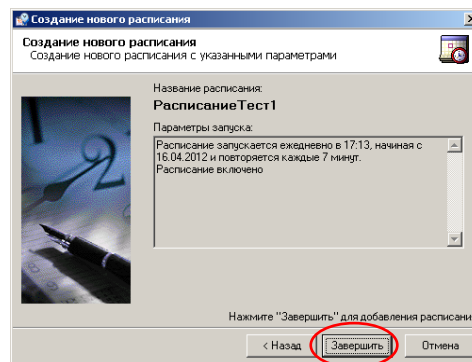


Рис. 2.117. Заключний етап формування розкладу перевірок індексів

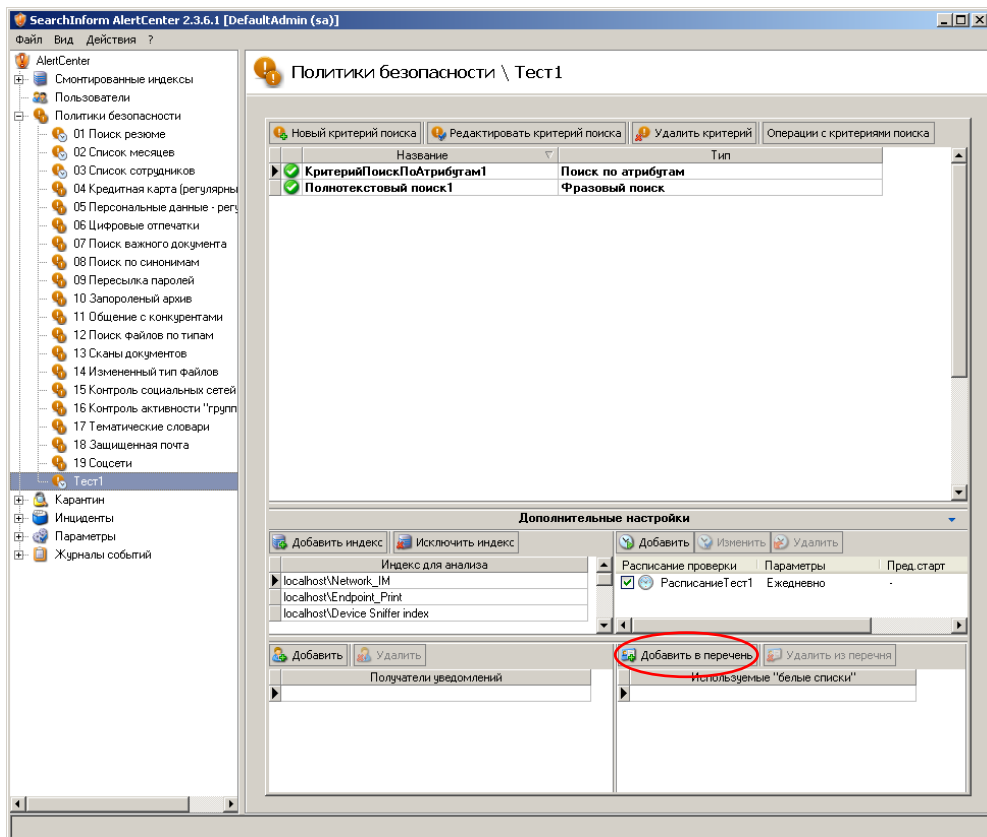


Рис. 2.118. Перший етап додавання білого списку в політику «Тест1»

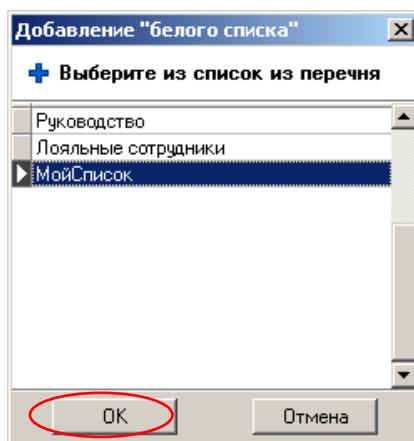


Рис. 2.119. Другий етап додавання білого списку «Мій список» в політику «Тест1»

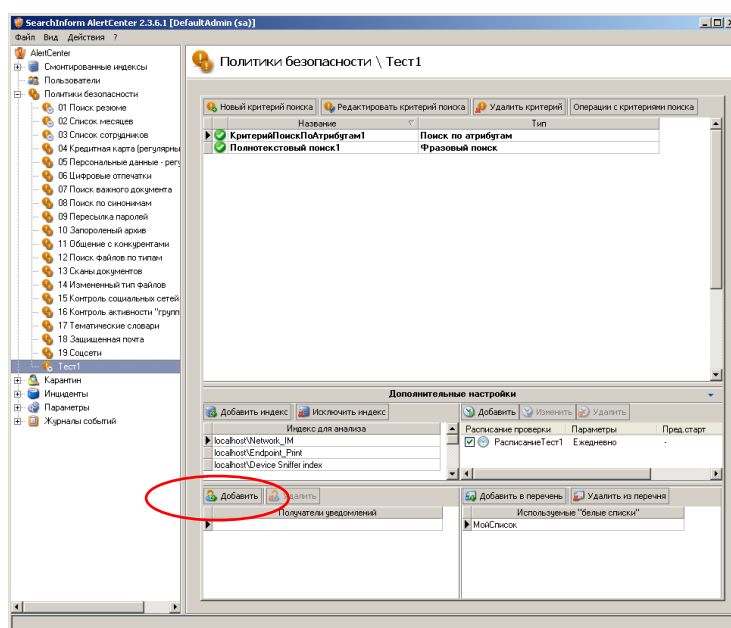


Рис. 2.120. Перший етап формування списку одержувачів повідомлень про порушення політики безпеки «Тест1»

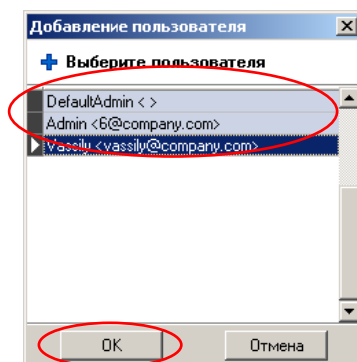


Рис. 2.121. Вибір імен одержувачів

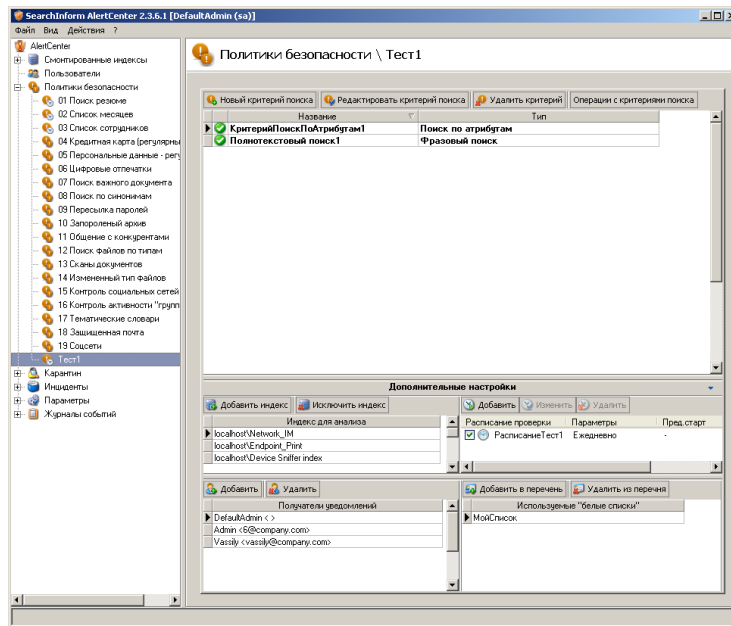


Рис. 2.122. Відображення параметрів політики безпеки «Тест1»

– Відповідно до рис. 2.123 – 2.124 перевірити порушення політики безпеки «Тест1». Перевірку провести через 7 хвилин після закінчення формування політики.

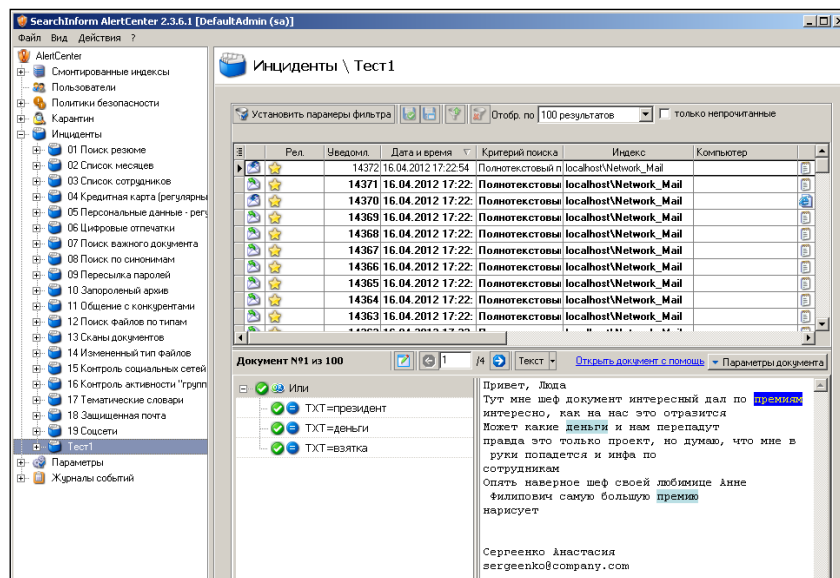


Рис. 2.123. Перевірка першого порушення

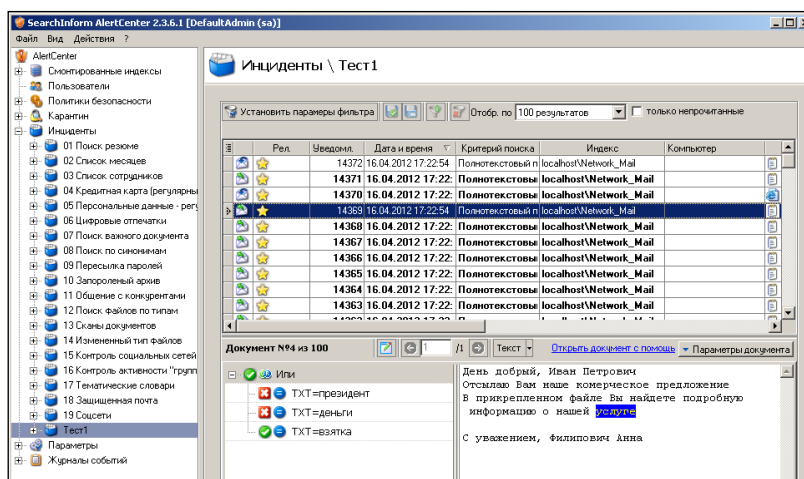


Рис. 2.124. Перевірка четвертого порушення

– Відповідно до рис. 2.125 відключити реалізацію політики «Тест1».

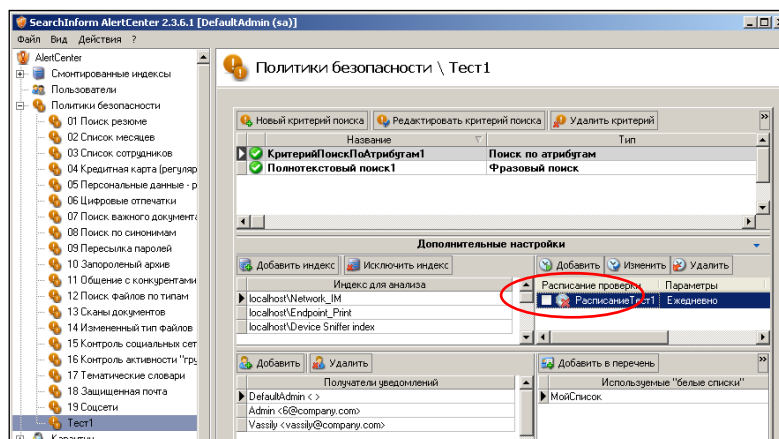


Рис. 2.125. Відключення реалізації політики «Тест1»

- Закрити вікно *AlertCenter Client*.
- Завершити роботу з віртуальним комп'ютером.

Завдання для самостійної роботи

- Сформуванати параметри власної політики безпеки, які повинні включати в себе: розклад перевірки, список індексів для перевірки, перелік білих списків, кілька найпростіших критеріїв пошуку конфіденційної інформації.
- Узгодити параметри політики безпеки з викладачем.
- Реалізувати політику безпеки.
- Переглянути перелік виявлених порушень.

Питання для самоперевірки

1. Навіщо потрібна фільтрація проксі-серверів?
2. Навіщо потрібна фільтрація з поштових серверів?
3. Чим відрізняється створення індексу від монтування індексу?
4. Які види пошуку рекомендуються для структурованих документів?
5. Які види пошуку рекомендуються для неструктурованих документів?
6. Що таке фільтр обмежень по перехопленню?
7. Що таке «білий список»?
8. Як використовується «дозвільний білий список»?
9. Як використовується «заборонний білий список»?
10. Чим відрізняється глобальний фільтр від фільтра за протоколами?
11. Навіщо підключати *AlertCenter* до індексів?
12. Який повинен бути інтервал оновлення індексів?

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

Базова література

1. Безруков Н. Н. Компьютерная вирусология / Н. Н. Безруков. – К. : Инкомбук, 1990. – 450 с.
2. Богуш В.М. Моніторинг систем інформаційної безпеки: навч. посібник [для студ. вищ. навч. закл.] / В.М. Богуш, А. М. Кудін. – К. : ДУІКТ, 2006. – 414 с.
3. Зима В. М. Безопасность глобальных сетевых технологий / В. М. Зима, А. А. Молдовян, Н. А. Молдовян. – СПб. : БХВ-Петербург, 2000. – 450 с.
4. Лукацкий А.В. Обнаружение атак. – СПб.:БХВ-Петербург,2010. – 624 с.
5. Касперски К. Техника и философия хакерских атак / К. Касперски. – М. : Солон, 2010. – 256 с.
6. Колисниченко Д.Н. Rootkits под Windows / Д. Н. Колисниченко. – СПб. : Наука и техника, 2011. – 320 с.
7. Коробейников А.Г. Математические основы криптографии. СПб, 2004 – 106с.
8. Менаске Д. Производительность Web-служб. Анализ, оценка и планирование / Менаске Д., Виргилио А. ; пер. с англ. – СПб. : ДиаСофтЮп", 2012. – 480 с.
9. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсєєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2013. – 476 с.
10. Таненбаум Э. Компьютерные сети / Таненбаум Э. ; пер. с англ. А. Леонтьева. – СПб.: Питер, 2002. – 848 с.
11. Таненбаум Э. Современные операционные системы. 2-е изд. / Таненбаум Э. ; пер. с англ. – СПб. : Питер, 2002. – 1036 с.

12. Терейковський І. Нейронні мережі в засобах захисту комп'ютерної інформації / І. Терейковський. – К. : ПоліграфКонсалтинг. – 2007. – 209 с.

13. Ульман Л. Руководство по изучению языка MySQL / Ульман Л.; Пер. с англ. Слинкина А.А - М.: ДМК Пресс; СПб.: Питер, 2004. – 352 с.

14. Уэнстром М. Организация защиты сетей Cisco / Уэнстром М. ; пер. с англ. – М. : Вильяме, 2012. – 768 с.

15. Щеглов А. Ю. Защита компьютерной информации от несанкционированного доступа / А. Ю. Щеглов. – СПб. : Наука и техника, 2012. – 384 с.

Допоміжна література

16. Науково-технічний журнал "Захист інформації".

17. Науково-технічний журнал "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні".

18. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

19. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

20. НД ТЗІ 1.4-001-2000 Типове положення про службу захисту інформації в автоматизованій системі.

21. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.

22. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

23. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.

24. НД ТЗІ 2.1-001-2001 Створення комплексів технічного захисту інформації. Атестація комплексів. Основні положення.

25. НД ТЗІ 3.7-001-99 Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

26. НД ТЗІ 2.5-008-2002 Вимоги із захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах класу 2.

Інформаційні ресурси

27. Електронний кампус НТУУ «КПІ». Матеріали з дисципліни «Методи та засоби захисту інформації в комп'ютерних системах». – Режим доступу : <http://login.kpi.ua>.

28. Веб-портал Державної служби технічного захисту інформації України». – Режим доступу : www.dstszi.gov.ua

29. Веб-портал компанії «DrWeb». – Режим доступу : www.drweb.ru

30. Веб-портал компанії «Безпека». – Режим доступу : www.bezpeka.biz

31. Веб-портал компанії «Searchinform». – Режим доступу : www.searchinform.ru

32. Веб-портал системи виявлення вразливостей Snort. – Режим доступу : www.snort.com