ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

ТЕХНОЛОГІЯ БЕЗПЕКИ ВІРТУАЛЬНОГО СЕРЕДОВИЩА КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

Виконав студент 5 курсу, групи БСДМ- 61
спеціальності 125 Кібербезпека
освітньо-професійної програми
«Інформаційна
та кібернетична безпека»
(шифр і назва спеціальності)
Пархомець Д.С.
(прізвище та ініціали)
Керівник Гайдур Г.І.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н.С.
(прізвище та ініціали)

КИЇВ – 2022

РЕФЕРАТ

Текстова частина магістерської роботи: 60 сторінок, 30 рисунків, 1 таблиця, 8 джерел.

Об'єкт дослідження – процес забезпечення кібербезпеки віртуального середовища корпоративної інформаційної системи.

Предмет дослідження – технологія забезпечення кібербезпеки віртуального середовища корпоративної інформаційної системи.

Мета роботи – розробити варіант технології застосування методів та засобів забезпечення кібербезпеки віртуального середовища корпоративної інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

В роботі приведено основні відомості щодо впровадження віртуального середовища КІС.

Проаналізовано різні види загроз та протидія їм.

Досліджено методи та засоби кібербезпеки віртуального середовища КІС.

Досліджено технологію забезпечення кібербезпеки віртуального середовища КІС на базі рішення SVM Kaspersky Security.

На основі досліджень проведених в роботі розроблено рекомендації щодо застосування методів та засобів кібербезпеки віртуального середовища КІС в корпоративній інформаційній системі.

Галузь використання – кібербезпека корпоративних інформаційних систем.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, ЗАГРОЗИ, КІБЕРБЕЗПЕКА, ВІРТУАЛЬНЕ СЕРЕДОВИЩЕ, ВІРТУАЛЬНІ МАШИНИ, АНТИВІРУС, ЛЕГКИЙ АГЕНТ, МЕТОДИ ТА ЗАСОБИ

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АС – автоматизовна система

ІТ – інформаційні технології

КІС – корпоративна інформаційна система

ОС – операційна система

ПЗ – програмне забезпечення

VM - віртуальна машина

SVM - виділений пристрій безпеки

NAB - компонент перевірки комунікацій між віртуальними машинами

ВСТУП

Актуальність дослідження. Сучасні корпоративні інформаційні системи– це сукупність інформаційних технологій, що ґрунтується на щоденному використанні комп'ютерної техніки, мереж зв'язку, мобільних засобів спілкування та інших технічних засобів. Перехід до використання хмарних технологій змушує керівників компаній переходити на нові ІТ-технології. Саме такими технологіями є віртуалізація, яка дозволяє більш ефективно та економічно використовувати інфраструктуру компанії.

Кібератаки стали звичним явищем у всьому світі, які становлять реальну та серйозну загрозу для компаній. Кількість атак та їх складність, масштабність і летальність постійно збільшується.. Велика кількість загроз створена, націлені, на те, щод нанести збитки компаніям з різною метою. Це призводить до того що компанії стикають з економічними наслідками втраченої інформації та довіри клієнтів.

Традиційні механізми захисту не можуть протистояти силі сучасних кіберзагроз. Але використання віртуального середовище вимагає пошук інших шляхів для забезпечення кібербезпеки. Багато організацій не мають достатнього рівня обізнаності щодо впровадження таких методів та засобів, щоб захистити себе від внутрішніх і зовнішніх кіберзагроз. Саме тому впровадження кібербезпеки віртуального середовища корпоративної інформаційної системи для забезпечення стабільності бізнесу компаній, збереження клієнтів та постійного розвитку є актуальним на сьогоднішній день.

Об'єкт дослідження – процес забезпечення кібербезпеки віртуального середовища корпоративної інформаційної системи.

Предмет дослідження – технологія забезпечення кібербезпеки віртуального середовища корпоративної інформаційної системи.

Мета роботи – розробити варіант технології застосування методів та засобів забезпечення кібербезпеки віртуального середовища корпоративної інформаційної системи.

Завдання магістерської роботи:

дослідити існуючі загрози процесам функціонування корпоративних інформаційних систем;

проаналізувати застосування технологій побудови віртуального середовища в корпоративній інформаційній системі;

визначити основні загрози віртуальному середовищу в корпоративній інформаційній системі;

проаналізувати існуючі методи та засоби віртуального середовища в корпоративній інформаційній системі;

дослідити технологію застосування, налаштування програмного рішення для забезпечення кібербезпеки SVM Kaspersky Security на базі легкого агента;

розробити рекомендації фахівціям кібербезпеки при впровадженні віртуального середовища в корпоративній інформаційній системі.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, проведення експерименту.

Практичне значення одержаних результатів: рекомендації щодо застосування віртуального середовища та забезпечити кібербезпеку корпоративних інформаційних систем.

Апробація результатів: результати дослідження допопвідалось на науково-практичній конференції «Актуальні проблеми кібербезпеки».

1 АНАЛІЗ ВИКОРИСТАННЯ ВІРТУАЛЬНОГО СЕРЕДОВИЩА В КОРПОРАТИВНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1. Аналіз кібербезпеки використання віртуального середовища в корпоративних інформаційних системах

Сьогодні багато компаній використовують технології віртуалізації. Але в за перевагами віртуалізації багато компаній не звертають увагу на кібербезпеку. Саме таке завжди спостерігається коли починають масово вводити нові технології. І тільки після того, як відбудуться декілька серйозних інцидентів, компанії розуміють, що кібербезпека віртуальної інфраструктури не менш важлива, ніж фізичної, і при цьому вона вимагає великих зусиль і вкладень.

Технології віртуалізація вимагають від компаній серйозної корекції базових підходів до забезпечення кібербезпеки, а також вмінь від фахівців застосувати якісно інші технології.

Більшість компаній-респондентів застосовують віртуалізацію: зберігають і обробляють у віртуальній інфраструктурі (BI) різні типи даних, розміщують бізнес-критичні додатки [2].

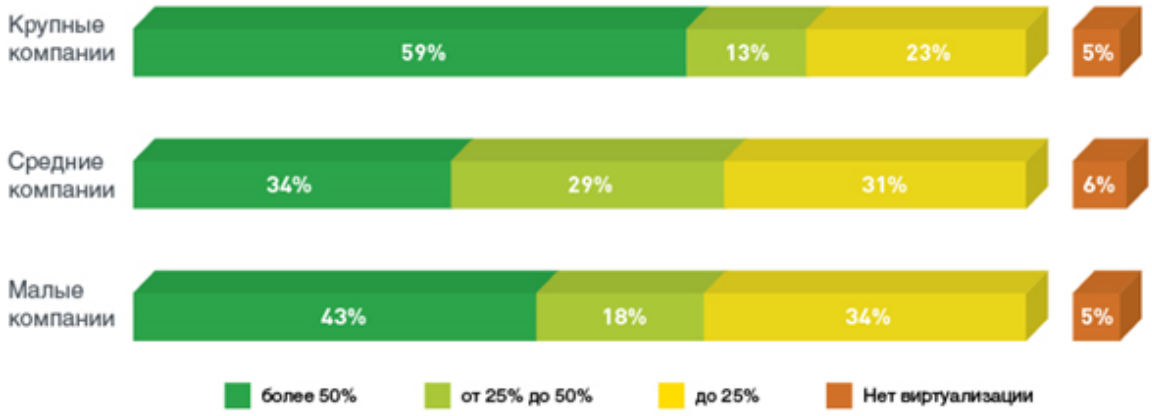


Рис.1.1. Доля віртуального середовища серверної інфрастуктури [2]

В різних компаніях відзначають, що в віртуальних інфраструктурах зберігають і обробляють загальнодоступну інформацію (76%), конфіденційні дані (70%) і відомості, що становлять державну таємницю (3%). При цьому майже у половини компаній в віртуальному середовищі одночасно зберігаються і обробляються різні типи даних [2].

Рис. 1.2. Тип інформації, яка зберігається у віртуальній інфраструктурі [2]

У багатьох дослідженнях, експерти зазначають наступний факт, який досить насторожує: менше половини опитаних компаній приймають різні політики безпеки для фізичних і віртуальних середовищ. І це при тому, що за останні кілька років дуже багато замовників перевели системи віртуалізації з тестових полігонів в продуктивне використання. В результаті, системи віртуалізації стали цікаві для потенційних хакерів і зловмисників. Більш того, вже давно випущені інструменти пошуку вразливостей віртуалізації, завдяки яким пошук дірок в системах віртуалізації став доступним для кіберзлочинців середньої кваліфікації.

1.2. Аналіз кіберзагроз у віртуальній інфраструктурі корпоративниої інформаційної системи

Визначмо найбільш вагомі загрози віртуальному середовищу корпоративної інформаційної системи від відомих вендорів.

На думку фахівців Cisco, головна кібербезпека віртуального середовища пов'язана з великою кількістю консолідації різнорідних обчислювальних ресурсів і даних в єдиній фізичної системі. До тих пір, поки різні віртуальні системи ізольовані одна від одної - ситуація стабільна. Але як тільки така ізоляція порушується, з'являються загрози, які специфічні для віртуальних середовищ. Як приклад можна представити зловмисника, який атакувавши одну віртуальну машину, може викликати нестачу ресурсів для інших віртуальних машин, які поділяють загальну обчислювальне і мережеве середовище. Інша, доволі велика загроза віртуальних середовищ викликана їх динамічної природою. Віртуальні машини можна переміщати між різними фізичними серверами і навіть між різними інфраструктурними майданчиками організації, таким чином, традиційні політики, які прив'язуються до фізичних пристроїв і портів, вже не працюють для віртуального світу [3-6].

На думку фахівців Fortinet робота з ключовими клієнтами в Україні, вказує на інші проблеми. Віртуальне середовище може спільно використовувати однакове мережеве обладнання, і деякі загрози кібербезпеки є наслідком цього. Якщо всі віртуальні середовища знаходяться в одній мережі, то можна обійти політику безпеки на брандмауері, який безпосередньо підключений до мережевої карти. Тому необхідно відстежувати правильні налаштування програмного забезпечення, яке управляє віртуальними середовищами. Крім того, жорсткі диски можна спільно використовувати декількома віртуальними середовищами, тому є ймовірність того, що віртуальне середовище може отримати доступ до файлів інших систем[3,4].

Значна кількість загроз в віртуальних середовищах виникають в наслідок помилок конфігурації. Саме про такі загрози повідомляють фахівці компанії «БМС

Консалтинг». Велика кількість помилок виникають тому, що доволі часто відсутній поділ повноважень між мережевими і системними адміністраторами, а це різні технологічні сектори, кожному з яких притаманні свої тонкощі. У віртуальних середовищах мережева інфраструктура та системне адміністрування об'єднані в рамках єдиного рішення. В результаті дуже часто виникають ситуації, як наприклад, «зайвий» DHCP-сервер у тій частині мережі, що повністю зупиняє всі комунікації в мережі [3-6].

Крім того ж, спрощення процесу виділення обчислювальних ресурсів і впровадження мобільності корпоративних інформаційних систем і додатків призводить до втрати контролю над даними що зберігаються в віртуальному середовищі. Адже віртуальні машини створюються, клонуються, переміщаються і зникають з неймовірною швидкістю і легкістю за необхідністю в в віртуальному середовищі. Ті компанії, які не турбуються про кібербезпеку при проектуванні віртуальної інфраструктури і ретельним плануванням доступу, стикаються з ситуацією, коли виток даних і несанкціонований доступ до систем стає складно не тільки запобігти, але й виявити.

Фахівці мережевих рішень компанії Інком, називають такі загрози в сфері кібербезпеки:

- неможливість контролювати інформаційний обмін між різними серверами в межах однієї віртуальної машини;
- неможливість контроль додатків, що відносяться до різних зон безпеки на рівні віртуальних машин;
- запобігання несанкціонованого розміщення системними адміністраторами різного роду додатків в одній зоні кібербезпеки;
- вредоносноий код для віртуальних середовищ.

При використанні віртуальної інфраструктури організації стикаються з проблемами забезпечення відмовостійкості і ефективності віртуальних машин, зазначають фахівці Symantec. Останнім часом все частіше з'являються віруси, які

створені саме для віртуальної інфраструктури. Крім цього існують ризики, пов'язані з тим, що вся інфраструктура управляється з однієї точки, і в разі некоректного розмежування прав можна швидко знищити всю віртуальну інфраструктуру компанії.

Про те, що є віруси, які спрямовані саме проти віртуальних середовищ, і їх число швидко зростає повідомляють фахівці корпоративних продуктів «Лабораторії Касперського».

Як показало недавнє дослідження «Лабораторії Касперського», присвячене впровадженню віртуалізації і забезпечення IT-безпеки віртуальних середовищ в Україні, понад 50% респондентів вважають, що ризики IT-безпеки для віртуального середовища нижче, ніж для фізичної. Однак таке уявлення про загрози IT-безпеки для віртуальних середовищ є невиправдано оптимістичним і в корені неправильним. Незважаючи на те, що специфічних загроз, актуальних тільки для віртуальних середовищ, трохи, вcs віруси, створені для «фізичних» серверів, представляють таку ж небезпеку і для віртуальних машин. Це і шкідливі вкладення в повідомленнях електронної пошти, drive-by завантаження, троянські програми-боти, цілеспрямований фішинг і т. д [3-6].

Таким чином по мірі зростання популярності віртуалізації розширюється і список загроз в цій області. Чинники, що викликають найбільші побоювання у корпоративного сектора, представлені на рис.1.3.

Рис.1.3. Топ-5 для загроз віртуальному середовищу

1.3. Визначення невірних підходів при впровадженні віртуальної інфраструктури

Існують хибні думки серед власників і керівників бізнесу, що забезпечення кібербезпеки хмарних сервісів - це або апріорі не потрібна річ, так як хмари безпечні (1), або це завдання хмарного провайдера. Тобто, заплатив за VPS - значить все має бути налагоджене, безпечне і працювати без проблем (2). Загально відомі інструменти безпеки не можуть забезпечити необхідний рівень захисту віртуального середовища (3) - керівники бізнесу при такому підході відмовляються від хмарних технологій в силу недовіри або нерозуміння різниці між традиційними і спеціалізованими засобами захисту (про них нижче). Четверта категорія громадян вважає, що так, захистити свою хмарну інфраструктуру треба б, але ж є стандартні антивіруси (4).

Всі ці чотири підходи невірні - вони можуть нанести збитки.

Приблизно половина великих компаній не використовує ніякого захисту для віртуальних машин, а друга половина вважає, що достатньо будь-якого стандартного антивіруса. Всі ці компанії витрачають велику кількість грошей на відновлення системи після інцидентів: на розслідування, на відновлення системи, на компенсацію витрат. Вони не задумуються, якими будуть їхні витрати в разі, якщо вони себе скомпрометують? Які будуть прямі втрати на відновлення, заміну обладнання, софт . Які будуть непрямі втрати – репутація, тощо. Це веде за собою розслідування інцидентів, часткову заміна інфраструктури, тому що вона вже себе скомпрометувала, це діалоги з урядом, це діалоги зі страховими компаніями, діалоги з замовниками, яким доводиться платити компенсації.

Проведемо аналіз чому саме ці підходи на працюють.

Підхід 1: Хмари безпечні, їх не треба захищати. Близько 240 тисяч одиниць шкідливого ПО, що з'являються щодня, відмінно «живуть» усередині хмар: від простого коду, який написав школяр і виклав в інтернет (а значить він потенційно може пошкодити дані) до складних цілеспрямованих атак, що розробляються

спеціально під конкретні організації, кейси і ситуації, які дуже добре вміють не тільки ламати і красти дані, але і «ховати» себе. Віртуальна інфраструктура цікава і хакерам: її набагато простіше зламати і отримати доступ відразу до всіх ваших віртуальних машин і даних, ніж намагатися зламати кожен фізичний сервер окремо. Плюс варто враховувати, що всередині віртуальної інфраструктури шкідливий код поширюється з величезною швидкістю - десятки тисяч машин можна заразити за десяток хвилин, а це рівнозначно епідемії. Шкідливі програми і дії вимагачів, які сприяють витоку даних компанії, становлять близько 27% від загального числа хмарних «небезпек». Самі ж вразливі місця в хмарі: незахищені інтерфейси і несанкціонований доступ - близько 80% в сумі (за даними дослідження Cloud Security Report 2019 за підтримки Check Point Software Technologies Ltd. - провідним постачальником рішень кібербезпеки для урядів і корпоративних підприємств по всьому світу) [1-4].

Рис. 1.4. Вразливість хмарного середовища

Підхід 2: Захист хмарної інфраструктури - це завдання провайдера VPS. Це частково вірно, адже постачальник віртуальних серверів піклується про стабільність

роботи своїх систем, про достатньо високий рівень захисту основних компонентів хмари: сервери, накопичувачі, мережі, віртуалізація (регулюється угодою про рівень послуг, SLA). Але він не повинен піклуватися про запобігання внутрішніх і зовнішніх загроз, які можуть виникнути в хмарної інфраструктурі клієнта [1-4]..

Підхід 3: Ніякі інструменти безпеки не можуть забезпечити необхідний захист віртуальних середовищ. Ні в якому разі. Існують спеціалізовані хмарні захисні рішення, які ми дослідимо в своїй роботі.

Підхід 4: Використання стандартного антивірусу (традиційний захист). Тут важливо знати, що традиційні інструменти безпеки, які всі звикли використовувати на локальних комп'ютерах, просто не призначені для розподілених віртуальних середовищ (вони не «бачать», як відбувається спілкування між віртуальними машинами) не захищають внутрішню віртуальну інфраструктуру від спроби внутрішнього злому. Простіше кажучи, звичайні антивіруси майже не працюють в хмарі. При цьому, встановлені на кожну WM, вони споживають величезну кількість ресурсів всієї віртуальної екосистеми при перевірках на віруси і оновлення, навантажуючи мережу і гальмуючи роботу компанії, але видаючи в результаті майже нульовий ККД по своїй основній роботі.

Тож дослідимо які ж загрози можуть виникнути у компаній при роботі з віртуальним середовищем і як їм протидіяти.

Віддалені мережеві атаки

Це різного роду інформаційний руйнівний вплив на розподілену обчислювальну систему, що здійснюється програмно по каналах зв'язку для досягнення різних цілей. Найпоширеніші з них:

DDoS-атака (Distributed Denial of Service). Масована відправка інформаційних запитів на сервер з метою витратити на атакуємій системі ресурси або пропускну здатність, щоб вивести з ладу цільову систему, завдавши тим самим шкоду компанії. Використовується конкурентами як замовна послуга, вимагачами, політичними активістами і урядами для отримання політичних дивідендів. Здійснюються такі атаки

за допомогою ботнету - мережі комп'ютерів з встановленими на них ботами (ПО, яке може містити віруси, програми для віддаленого управління комп'ютером і інструменти для приховування від ОС), які використовуються хакерами віддалено для поширення спаму і програм-вимагачів. Ping Flooding - для виклику перевантаження лінії.

Ping of Death - для виклику зависання, перезавантаження і краху системи.

Атаки на рівні додатків - для отримання доступу до комп'ютера, яке дозволяє запуск додатків для певної (привілейованої системної) облікового запису.

Фрагментація даних - для аварійного завершення системи через переповнення програмних буферів.

Авторутери - для автоматизації хакинг-процесу через сканування величезної кількості систем за короткий час за допомогою установки rootkit.

Sniffing - для прослуховування каналу.

Нав'язування пакетів - для перемикання на свій комп'ютер з'єднання, встановленого між іншими комп'ютерами.

Перехоплення пакетів на маршрутизаторі - для отримання паролів користувачів і інформації з електронної пошти.

IP Spoofing - для того, щоб хакер всередині мережі або за її межами зміг видавати себе за комп'ютер, якому можна довіряти. Здійснюється через підміну IP-адреси.

Брутфорс-атаки (brute force) - для підбору пароля шляхом перебору комбінацій. Використовують уразливості в RDP і SSH.

Smurf - для зниження пропускної здатності каналу зв'язку і / або до повної ізоляції атакується мережі.

DNS spoofing - для пошкодження цілісності даних в системі DNS через «отруєння» кешу DNS.

Підміна довіреного хоста - для можливості вести сеанс роботи з сервером від імені довіреної хоста.

TCP SYN Flood - для переповнення пам'яті сервера.

Man-in-the-middle - для крадіжки інформації, спотворення переданих даних, DoS-атак, хакинга поточного сеансу зв'язку з метою отримання доступу до приватних мережевих ресурсів, аналізу трафіку з метою отримання інформації про мережу та її користувачів.

Мережева розвідка - для вивчення інформації про мережу та додатках, що виконуються на хостах, перед атакою.

Port redirection - тип атаки, який використовує зламаний хост для передачі трафіку через міжмережевий екран. Наприклад, якщо міжмережевий екран підключений до трьох хостів (на зовнішній стороні, на внутрішній і в сегменті загальнодоступних сервісів), то зовнішній хост отримує можливість зв'язуватися з внутрішнім хостом шляхом перепризначення портів на хості загальнодоступних сервісів.

Trust exploitation - атаки, які відбуваються, коли хто-небудь користується перевагою довірчих відносин в межах мережі. Наприклад, злом однієї системи в межах корпоративної мережі (HTTP, DNS, SMTP-сервери) може привести до злому інших систем.

Соціальная інженерія

Фішинг - для отримання конфіденційної інформації (паролі, номери банківських карт та ін.) Через розсилку від імені відомих організацій, банків.

Сніфінг пакетів (Packet sniffers) - для отримання доступу до критично важливої інформації, в тому числі паролів. Має через те, що користувачі часто багаторазово використовують своє ім'я та пароль для отримання доступу до різних програм і систем. Таким способом хакер може отримати доступ до облікового запису системного користувача і створити через неї новий обліковий запис, щоб мати доступ до мережі і її ресурсів в будь-який час.

Претекстінг - сценарна атака з використанням голосових засобів зв'язку, мета якої - змусити жертву вчинити дію.

Троянський кінь - техніка, заснована на емоціях жертви: страху, цікавості. Шкідливе ПО зазвичай знаходиться у вкладенні електронного листа.

Квід про кво (послуга за послугу) - звернення зловмисника через корпоративний телефон або електронну пошту під виглядом співробітника техпідтримки, який повідомляє про проблеми на комп'ютері жертви і пропонує їх вирішити. Мета - встановити ПО і виконати шкідливі команди на цьому комп'ютері.

Дорожнє яблуко - підкидання заражених фізичних носіїв інформації в корпоративні місця загального користування (флешка в туалеті, диск в ліфті), забезпечених написами, що викликають цікавість.

Збір інформації з соціальних мереж.

Експлойти

Будь-які протиправні і несанкціоновані атаки, що мають на меті або отримання даних, або порушення функціонування системи, або захоплення контролю над системою називаються експлойта. Викликаються вони помилками в процесі розробки ПЗ, в результаті яких в системі захисту програм з'являються уразливості, успішно використовуються кіберзлочинцями для отримання необмеженого доступу до самої програми, а через неї - до всього комп'ютера і далі - до мережі машин.

Компрометація облікових записів

Злом сторонньою особою облікового запису співробітника компанії з метою отримання доступу до інформації, що захищається: від перехоплення інформації (в тому числі звуковий) і ключів шкідливим ПЗ до проникнення до фізичного зберігання носія інформації.

Компрометація репозиторіїв

Зараження серверів-сховищ файлів-установників ПО, оновлень і бібліотек.

Внутрішні ризики компанії

Сюди відноситься витоку інформації з вини самих співробітників компанії. Це може бути проста халатність чи навмисні шкідливі дії: від цілеспрямованого саботування адміністративних політик безпеки до продажу конфіденційної

інформації на сторону. Сюди ж можна віднести несанкціонований доступ, небезпечні інтерфейси, неправильну конфігурацію хмарних платформ і установку / використання несанкціонованих додатків.

Висновки до 1 розділу

В даному розділі було проведено аналіз використання віртуального середовища в корпоративних інформаційних системах. В результаті чого було виявлено зацікавленість компаній до такої технології. І в свою чергу, впровадження нових технологій вимагають забезпечення кібербезпеки КІС з використанням нових технологій, щодо налаштування, конфігурації, зберігання даних в таких середовищах. Про що свідчить необізнаність керівництва компанії щодо збереження бізнес-процесів при використанні віртуального середовища. І як наслідок, це може призвести до загроз в КІС і компрометації компанії. Тому надалі доцільно дослідити методи та засоби для забезпечення кібербезпеки сучасними КІС, які планують використовувати віртуальні середовища для роботи їх КІС.

2 МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ВІРТУАЛЬНОГО СЕРЕДОВИЩА КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

2.1. Вимоги до антивірусного захисту віртуальних машин

Технологія віртуалізації з кожним роком набирає обертів. Останнім часом велике поширення набула технологія віртуальних робочих столів (VDI): відмова від високопродуктивних робочих комп'ютерів на користь «тонких клієнтів» - малопотужних міні-комп'ютерів - підключення до серверів віртуалізації, які надають користувачеві повноцінне робоче середовище. Антивірусний захист повинен застосовуватися на будь-яких комп'ютерах, в тому числі і віртуальних. Однак, при наявності віртуальної інфраструктури, завдання якої - скорочення витрат і оптимізація використання апаратного забезпечення, неправильно використовувати класичні антивірусні продукти, які працюють ізольовано на кожному віртуальному комп'ютері [3].

Для вирішення цієї проблеми антивірусні виробники пропонують спеціалізовані рішення щодо захисту віртуальних машин, основна відмінність яких - виділення окремої віртуальної машини, яка виконує завдання сканування. Такий підхід дозволяє скоротити навантаження на віртуальні машини і оптимізувати використання апаратного забезпечення.

Один із спеціалізованих рішень для антивірусного захисту в віртуалізації - рішення «Kaspersky Security для віртуальних середовищ 3.0 Легкий агент». Попередня версія (2.x) продукту «Kaspersky Security для віртуальних середовищ» була виконана з використанням технології VMware vShield і функціонувала тільки в середовищі віртуалізації VMware vSphere [3].

Даний підхід мав кілька суттєвих недоліків - підтримка тільки одного середовища віртуалізації, відсутність ряду важливих механізмів перевірок через обмеження vShield.

Для зняття технічних обмежень в «Лабораторії Касперського» випустили нову версію продукту (3.0), в якій реалізовано «Легкий агент» - клієнтська частина, яка встановлюється на віртуальні комп'ютери. Всі антивірусні перевірки, як і в старій версії, проводяться на окремій віртуальній машині (таку віртуальну машину називають «virtual appliance»)/ [3].

В даній версії змінився механізм передачі даних для перевірки. Якщо раніше інформація передавалася через «посередника» vShield і його агента, то тепер всі дані йдуть від власного агента «Kaspersky Security для віртуальних середовищ».

Такийй підхід дозволяє реалізувати підтримку всіх популярних технологій віртуалізації і здійснювати повноцінну антивірусну перевірку і додаткові функції по захисту.

Системні вимоги Kaspersky Security для віртуальних середовищ 3.0 «Kaspersky Security для віртуальних середовищ», як і в попередній версії, вимагають наявність встановленого на одному з серверів в локальній мережі програмного забезпечення «Kaspersky Security Center» версії «10 Maintenance Release 1».

Це програмне забезпечення використовується для управління всіма функціями щодо захисту і моніторингу роботи захисних компонентів. Варто відзначити, що встановити даний продукт можна як на фізичний комп'ютер, так і на віртуальну машину.

2.2 Архітектура антивірусного забезпечення віртуального середовища

Важливо знати, що будь-який традиційний антивірус не буде надійним в при спробі забезпечити віртуальне середовище. Необхідно використовувати рішення, спеціально розроблене для віртуальних і хмарних середовищ, причому установка його так само має свої правила в даному випадку. Сьогодні існує два способи забезпечення хмарної безпеки за допомогою спеціалізованих багатокомпонентних антивірусів,

розроблених за новітніми технологіями: безагентний захист і захист легкого агента [3].

2.2.1. Архітектура безагентного захисту

Безагентний захист. Розроблено в компанії «VMware» і можлива тільки на її рішеннях. На фізичному сервері з віртуальними машинами розгортаються дві додаткові віртуальні машини: Сервер Захисту (SVM) і Сервер Мережевий Захисту (Network Attack Blocker, NAB). Всередину кожного з них не ставиться нічого. В SVM - виділений пристрій безпеки - встановлюється тільки антивірусне ядро. У машині NAB - компонент відповідає тільки за перевірку комунікацій між віртуальними машинами і тим, що відбувається в екосистемі (і за комунікацію з технологією NSX). Перевіркою всього трафіку, що приходить на фізичний сервер, займається SVM. Вона становить пул вердиктів, який доступний всім віртуальним машинам захисту через загальний кеш вердиктів. До цього пулу кожна віртуальна машина захисту звертається в першу чергу, замість сканування всієї системи - цей принцип дозволяє знижувати витрати ресурсів і прискорювати роботу екосистеми [3].

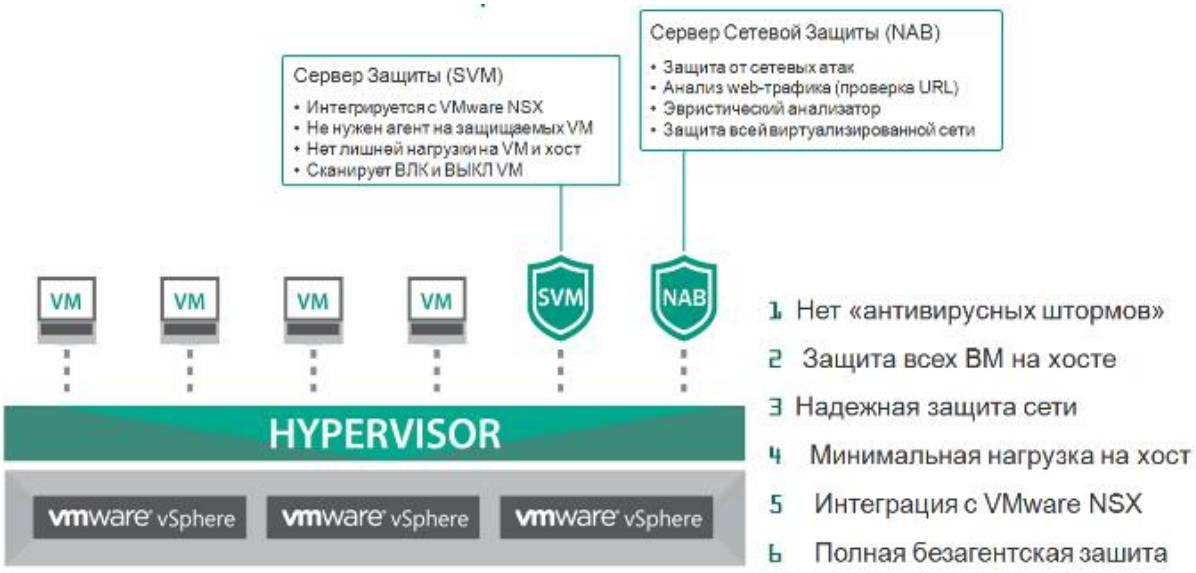


Рис. 2.1. Безагентний захист

2.2.2. Захист з легким агентом

Захист з легким агентом розроблено в компанії Kaspersky і не має обмежень «VMware». Як і в безагентному захисті на SVM встановлюється антивірусний движок, але на відміну від неї існує ще легкий агент, що встановлюється всередину кожної WM. Агент не виконує перевірок, а займається лише моніторингом за всім, що відбувається всередині рідної WM на основі технології самонавчаючихся мереж. Ця технологія запам'ятовує правильну послідовність роботи додатків; стикаючись з тим, що послідовність дій додатки всередині WM відбувається неправильно, вона їх блокує [3].

Рис. 2.3. Легкий агент

2.3. Функціональні можливості Kaspersky Security

Функціональние можливості Kaspersky Security для віртуальних середовищ 3.0 «Kaspersky Security для віртуальних середовищ» пропонує не тільки функції класичного антивіруса. До складу функціональних компонентів продукту також входить ряд інших захисних механізмів:

Контроль запуску програм - цей механізм відстежує спроби запуску програм у віртуальній машині і дозволяє дозволяти або забороняти запуск за встановленими правилами.

Контроль активності програм - класичні механізми системи запобігання вторгнень рівня вузла («Host-based Intrusion Prevention System»). Агент «Kaspersky Security для віртуальних середовищ» реєструє всі дії, що здійснюються процесами в операційній системі і може дозволяти або забороняти певну діяльність програми на підставі групи, до якої даний компонент відніс цю програму. Правила для груп додатків регламентують доступ процесів до даних користувача (папка «Мої документи», файли cookie, дані про активність користувача, файли, папки і ключі реєстру, що містять дані популярних додатків) і ресурсів операційної системи.

Моніторинг вразливостей - ще один механізм системи запобігання вторгнень. Даний компонент в реальному часі здійснює контроль запущених і запускаються на наявність вразливостей.

Контроль пристроїв - розмежування доступу до носіїв даних (жорсткі диски, флеш-накопичувачі, знімні носії і т.д.), пристроїв передачі інформації (модемів), принтерів і інтерфейсами, до яких можуть бути підключені пристрої (наприклад, USB, Bluetooth, інфрачервоний порт).

Веб-Контроль - обмеження доступу користувачів до веб-ресурсів.

Мережевий екран - класичний персональний мережевий екран, що дозволяє фільтрувати мережеву активність захищається віртуальної машини. Дозволяє

налаштувати правила доступу як на рівні мережевих параметрів з'єднань, так і на рівні окремих додатків.

Захист від мережевих атак - моніторинг вхідного мережевого трафіку для виявлення активності, характерної для мережевих атак. При виявленні такої активності, здійснюється блокування джерела підозрілого трафіку.

Антивірусні можливості «Kaspersky Security для віртуальних середовищ» представлені таким набором компонентів:

Файловий Антивірус - резидентна перевірка всіх відкритих, збережених і запущених файлів.

Поштовий Антивірус - перевірка вхідних і вихідних повідомлень електронної пошти на наявність в них вірусної загрози.

Веб-Антивірус - виявлення вірусних загроз в веб-трафіку і захист від підозрілих веб-ресурсів та веб-ресурсів, що підроблюють популярні сайти («фішинг»).

ІМ-Антивірус - перевірка трафіку інтернет-месенджерів, програм, призначених для обміну повідомленнями та файлами між користувачами мережі Інтернет.

3. ТЕХНОЛОГІЯ НАЛАШТУВАННЯ ЛЕГКОГО АГЕНТА KASPERSKY-SECURITY ДЛЯ ВІРТУАЛЬНОГО СЕРЕДОВИЩА

Легкий агент 5.0 є складовою комплексного рішення Kaspersky Security для віртуальних і хмарних середовищ і поєднує в собі практично всі плюси повноцінного засобу захисту кінцевих робочих станцій і серверів. Таке рішення споживає менше ресурсів віртуальної інфраструктури, , він підтримує всі популярні платформи віртуалізації, працює з усіма гостьовими операційними системами, має гнучку систему розподілу ліцензій і багато іншого [3-8].

3.1. Технології оптимізації роботи легкого агента

Легкий агент підтримує передові технології повноцінних антивірусних рішень, реалізованих також в Kaspersky Endpoint Security (KES):

- система запобігання вторгнень;
- персональний міжмережевий екран;
- система моніторингу додатків;
- контроль web-трафіку;
- контроль пристроїв;
- контроль системи;
- автоматичне блокування експлойтів;
- самоконтроль і самозахист.

Основною метою такого рішення є зниження навантаження на кожну захищається віртуальну машину. Тому на SVM розгортаються такі компоненти:

Повноцінний антивірусний движок для перевірки файлів

Повноцінний набір антивірусних баз

Інструмент «Загальний кеш вердиктів» (Shared Cache) для оптимізації перевірок на одному хості

Модуль управління завданнями сканування

Механізм розподілу ліцензій

Балансувальник задач

Для підвищення відмовостійкості за для, повноцінного функціонування всього рішення, необхідно встановити спеціальний компонент - Сервер інтеграції [3-8].

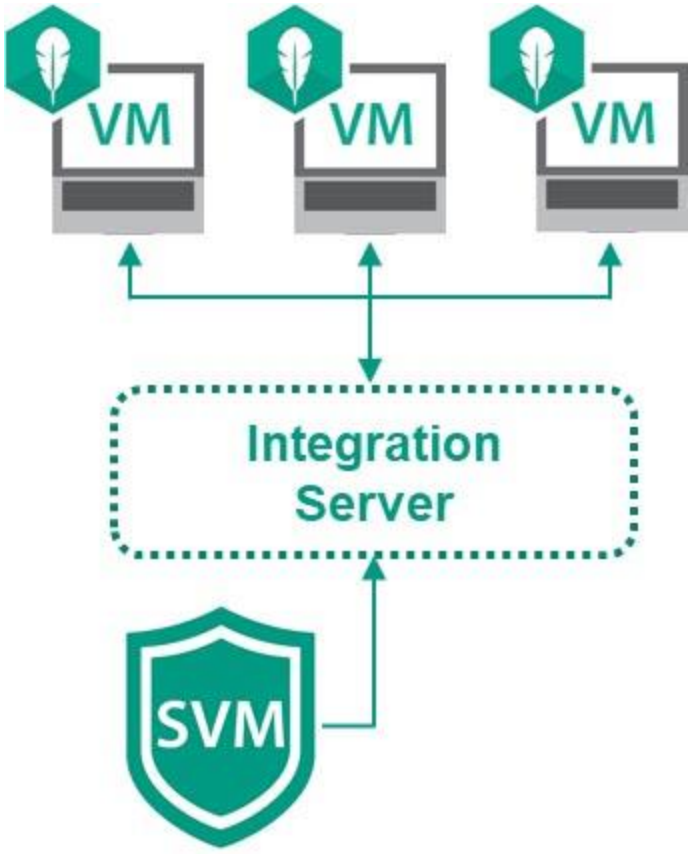


Рис.3.1 Компонент Сервер інтеграції Kaspersky Security для віртуальних середовищ /легкий агент

Сервер інтеграції збирає інформацію про всі SVM і актуальні налаштування, обмінюючись з ними даними кожні 5 хвилин. Зібрані відомості передаються на встановлені агенти з метою оптимізації вибору підключення до однієї з SVM (в тому числі з метою балансування навантаження), розгорнутих в мережі, для антивірусної

перевірки. Однією з особливих технологіях, реалізованих в описуваномув даному продукті – це інструментарій загального і локального кешей вердиктів [3].

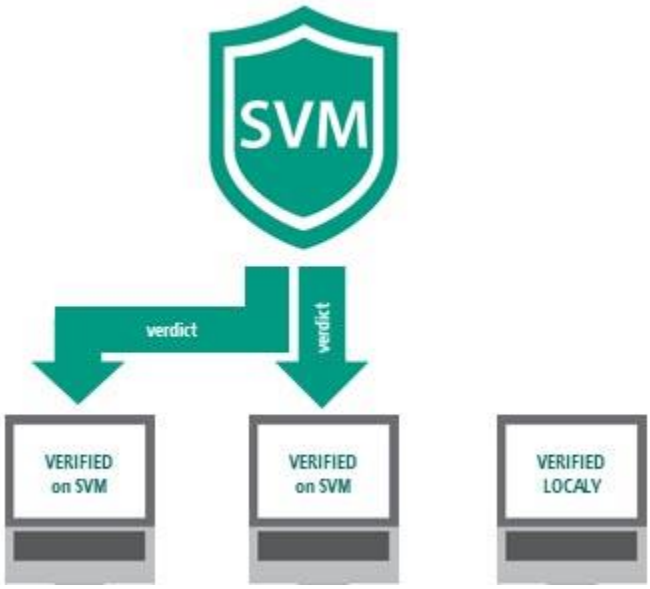


Рис.3.2 Принцип роботи кеш вердиктів

У момент звернення до файлу на віртуальній машині агент, як і в разі класичного антивіруса, автоматично перевіряє цей файл, щоб переконатися в його безпеці. Потім результат перевірки зберігається в загальній централізованій базі вердиктів SVM (Shared Cache), кожен запис якій ідентифікує унікальний зразок файлу. Якщо цей же файл відкривається на інший віртуальній машині, розташованій на тому ж хості, агент автоматично визначає, що подальша перевірка не потрібна. Файл перевіряється повторно тільки в тому випадку, якщо в нього були внесені зміни або перевірка запущена вручну. Крім того, в пам'яті кожної віртуальної машини розміщується додатково локальний кеш, який скорочує використання мережі. Файл при перевірці звіряється спочатку з ним і, якщо знаходиться вірний вердикт, то інформація з загального кеша не вимагається.

Інша технологія, яка використовується в даному рішенні - черга відкладеної перевірки.

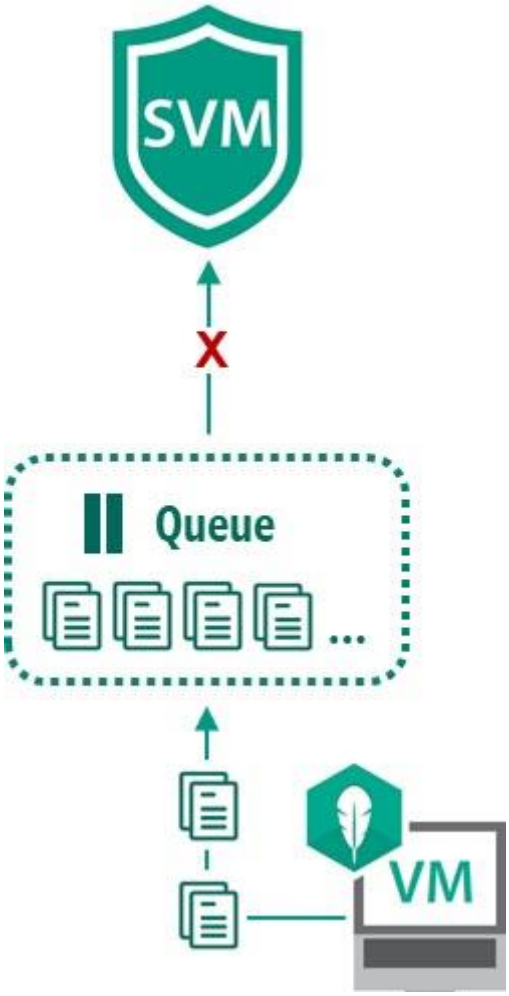


Рис.3.3. Черга відкладеної перевірки.

Таким чином, ресурсно витратну процедуру з антивірусної перевірки виконує SVM, тим самим знижуючи навантаження на кожну з користувацьких віртуальних машин. Встановлений агент відправляє файли для аналізу на SVM, яка, в разі недоступності по тій або іншій причині, формує чергу відкладеної перевірки. У підсумку всі файли незалежно від ситуації піддаються антивірусному аналізу. Розглянемо реалізацію механізмів відмово стійкості [3].

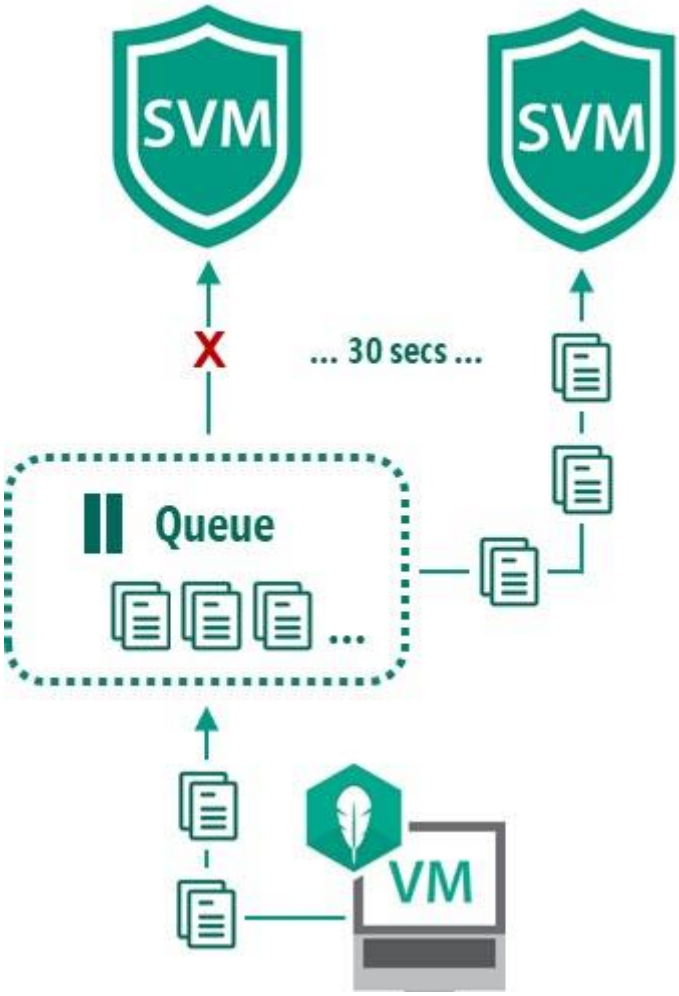


Рис.3.4. Реалізація відмовостійкості для віртуальних середовищ | легкий агент

Зазначимо, що у віртуальній інфраструктурі компанії може бути розгорнуто скільки завгодно багато SVM. Для антивірусної перевірки файлів насамперед встановлений агент ініціює підключення до зазначеного за замовчуванням при установці SVM. Однак якщо вона виявляється недоступною, агент намагається знайти і підключитися до іншої такої в мережі, при цьому час «вимушеного простою» не перевищує 30 секунд.

Розглянемо основні переваги використання легкого агента для віртуального середовища корпоративної інформаційної системи. Дані порівняння представлено у таблиці 3.1.

Таблиця 3.1.

Переваги використання легкого агента для віртуального середовища

	Kaspersky Security для віртуальних середовищ Захист без агента	Kaspersky Security для віртуальних середовищ Легкий агент
Серверная віртуалізация	Інтеграція тільки з VMware vSphere і NSX Постійний захист віртуальних машин Немає зайвого навантаження на ресурси Блокування атак здійснюється на мережевому рівні	Підтримка всіх популярних гіпервізорів Збереження ресурсної ефективності Контроль віртуальних машин зсередини Застосування максимальної чкількості технологій захисту
Віртуалізація робочих місць	Необхідно встановлювати KES	Підтримка всіх сучасних VDI-платформ Контроль пристроїв, пошти і web-трафіку Контроль активності програм, що запускаються Засіб виявлення вторгнень Автоматичний захист від експлойтів Збереження продуктивності для VDI
Хмара	Більше підходить для базового захисту в хмарі	Для багаторівневого захисту в хмарі

	Повна інтеграція з VMware vSphere Підтримка технології VMware NSX Немає зайвого навантаження на ресурси Додатковий захист забезпечується на рівні мережі	Підтримка гібридних інфраструктур Висока доступність і надійність Робота в складних мережевих топологіях Розроблено технології захисту

3.2. Налаштування віртуального середовища з використанням легкого агента

Розглянемо основні системні вимоги для налаштування роботи легкого агента віртуального середовища KIC.

Легкій агент працює з усіма популярними на ринку платформами віртуалізації:

Microsoft Windows Server 2016 Hyper-V (в режимі повної установки або в режимі Server Core) з усіма доступними оновленнями.

Microsoft Windows Server 2012 R2 Hyper-V (в режимі повної установки або в режимі Server Core) з усіма доступними оновленнями.

Citrix XenServer 7. Citrix XenServer 7.1 LTSR.

VMware ESXi 6.7 з останніми оновленнями.

VMware ESXi 6.5 з останніми оновленнями.

VMware ESXi 6.0 с останніми оновленнями.

VMware ESXi 5.5 с останніми оновленнями.

KVM (Kernel-based Virtual Machine) на базі однієї з наступних операційних систем:

Ubuntu Server 16.04 LTS;

Ubuntu Server 14.04 LTS;

Red Hat Enterprise Linux Server 7 виправлення 4. CentOS 7.4;

Proxmox 5.0. (На базі KVM);

Proxmox 5.1. (На базі KVM).

Підтримується установка і робота програми на Гіпервізор Microsoft Windows Server (Hyper-V), які входять до складу кластера гіпервізора під керуванням служби Windows Failover Clustering. На вузлах кластера повинна бути включена технологія Cluster Shared Volumes.

Для функціонування SVM потрібно виділити наступну мінімальну кількість системних ресурсів: двоядерний віртуальний процесор; обсяг вільного місця на диску - 30 ГБ; обсяг оперативної пам'яті - 2 ГБ; віртуалізувати мережевий інтерфейс з пропускною здатністю 100 Мбіт / сек. Сам агент може бути встановлений на досить широку лінійку гостьових операційних систем [3]:

Сам агент може бути встановлений на досить широку лінійку гостьових операційних систем:

Windows 7 Professional / Enterprise Service Pack 1 (32 і 64-розрядна).

Windows 8.1 Update 1 Professional / Enterprise (32 і 64-розрядна).

Windows 10 Pro / Enterprise / Enterprise LTSB / RS1 / RS2 / RS3 / RS4 (32 і 64-розрядна).

Windows Server 2008 R2 Service Pack 1 всі редакції (в повному режіме) (64-розрядна).

Windows Server 2012 всі редакції (в повному режимі) (64-розрядна).

Windows Server 2012 R2 всі редакції (в повному режимі) (64-розрядна).

Windows Server 2016 всі редакції (в повному режимі) (64-розрядна).

Debian GNU / Linux 8.9 (32 і 64-розрядна).

Debian GNU / Linux 9.1 (64-розрядна).

Ubuntu Server 16.04 LTS (64-розрядна).

Ubuntu Server 18.04 LTS (64-розрядна).

CentOS 6.9 (64-розрядна).

CentOS 7.4 (64-розрядна).

Red Hat Enterprise Linux Server 6.9 (64-розрядна).

Red Hat Enterprise Linux Server 7.4 (64-розрядна).

SUSE Linux Enterprise Server 12 Service Pack 1 (64-розрядна).

Для установки і функціонування агента на гостьових системах віртуальна машина повинна відповідати таким мінімальним характеристикам:

віртуальний процесор з частотою 1,5 ГГц;

обсяг вільного місця на диску - 2 ГБ;

обсяг оперативної пам'яті - 2 ГБ;

віртуалізувати мережевий інтерфейс з пропускною здатністю 100 Мбіт / сек.

Для роботи з продуктом, як і з переважною більшістю рішень «Лабораторії Касперського», обов'язковою є установка консолі управління - Kaspersky Security Center (KSC).

Для її роботи необхідно виділити машину з наступними ресурсами:

Процесор з частотою 1.4 ГГц;

обсяг оперативної пам'яті - 4 Гб;

обсяг вільного місця на диску - 100 Гб.

KSC може бути встановлений як на фізичний, так і на віртуальний (підтримуються всі популярні платформи віртуалізації) сервер під керуванням гіпервізора:

VMware vSphere 5.5

VMware vSphere 6

Vmware Workstation 12.x Pro

Microsoft Hyper-V Server 2008

Microsoft Hyper-V Server 2008 R2

Microsoft Hyper-V Server 2008 R2 SP1 і вище

Microsoft Hyper-V Server 2012

Microsoft Hyper-V Server 2012 R2

Microsoft Virtual PC 2007 (6.0.156.0)

Citrix XenServer 6.2

Citrix XenServer 6.5

Citrix XenServer 7

Parallels Desktop 11 і вище

Oracle VM VirtualBox 4.0. 4-70112 (підтримуються тільки гостьові операційні системи Windows)

Для розгортання KSC необхідно інсталювати операційну систему сімейства Windows (підтримуються як серверні, так і десктопні) і СУБД одного з двох виробників на вибір (MS SQL Server або MySQL).

Перейдемо до налаштування консолі управління Kaspersky Security Center

Будь-який корпоративний антивірусний продукт «Лабораторії Касперського» найзручніше розгортати через єдиний Центр управління безпекою (Kaspersky Security Center - KSC), який поставляється безкоштовно в комплекті з будь-яким enterprise-рішенням вендора.

Однак у випадку з Kaspersky Security для віртуальних середовищ/ Легкий агент це не рекомендація, але обов'язкова умова, оскільки всі серверні компоненти, необхідні для його функціонування, встановлюються за допомогою KSC, який складається з двох базових компонентів:

Сервер адміністрування - центральний компонент, відповідальний за управління пристроями організації та зберігання даних в СУБД.

Консоль адміністрування - основний інструмент адміністратора. Консоль адміністрування поставляється разом з Сервером адміністрування, але може бути також встановлений окремо на один або кілька пристроїв адміністратора.

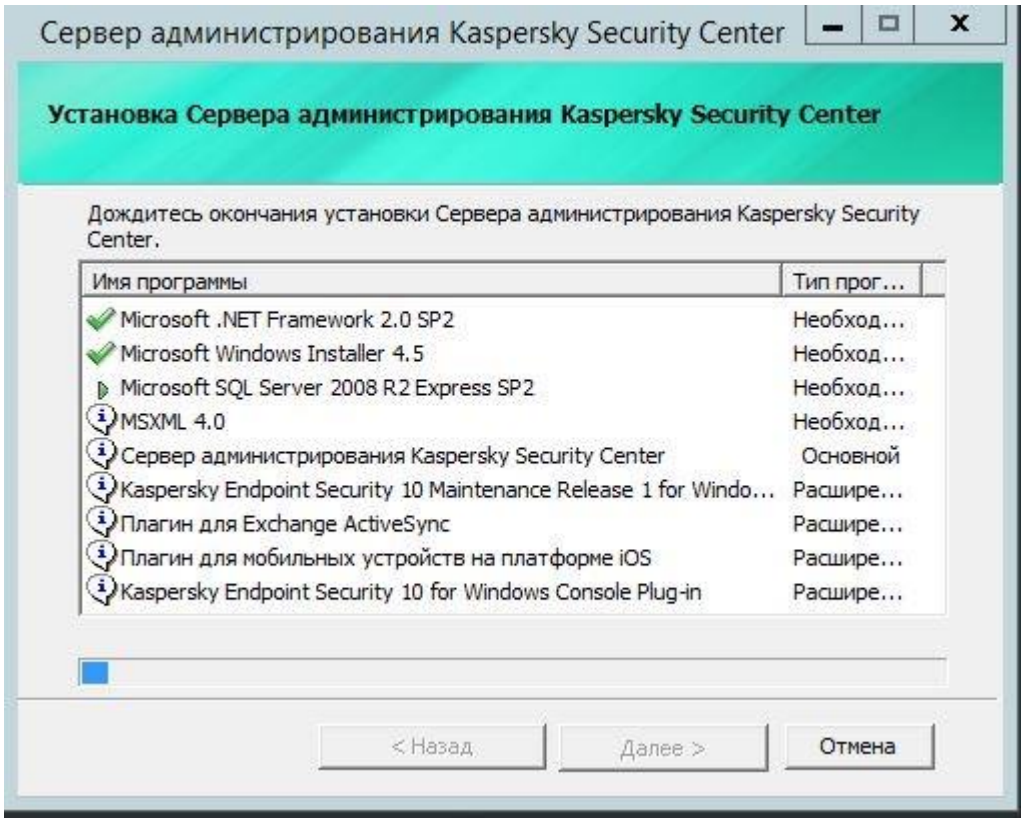


Рис.3.5 Установка Kaspersky Security Center

Незалежно від того, використовуються в компанії фізичні, віртуальні або хмарні ресурси, що розширена архітектура Kaspersky Security Center включає плагіни для управління захисними рішеннями для всіх платформ з єдиної консолі.

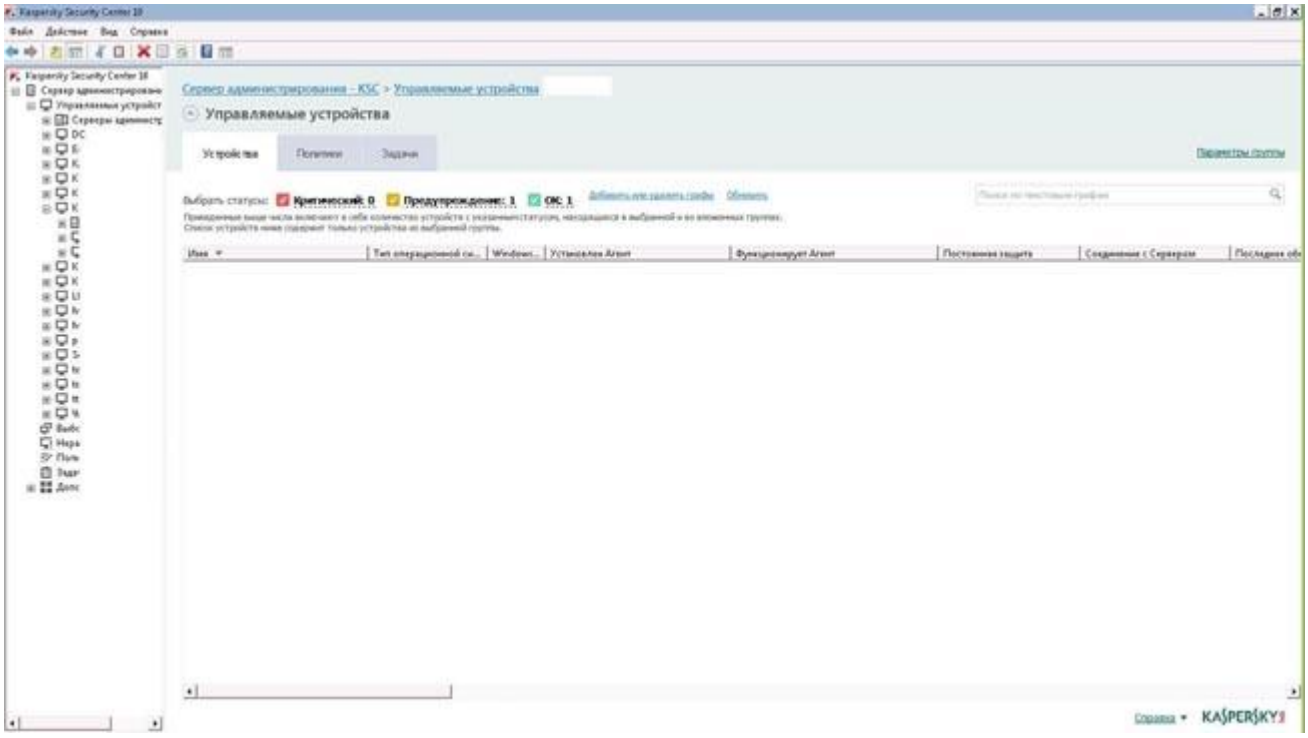


Рис.3.6. Конфігурація керованих пристроїв в Kaspersky Security Center

Встановлення та налаштування Сервера інтеграції Приступаючи до безпосереднього розгортання Kaspersky Security для віртуальних середовищ/Легкий агент, для початку встановимо Сервер інтеграції. В якості найбільш оптимального способу розгортання вендор рекомендує інсталювати спеціальний exe-файл, який додає і запускає відповідну службу в операційній системі на вже розгорнутому KSC. Після успішного завершення процесу в інтерфейс KSC додаються нові розділи меню, а в список сервісів Windows - нова служба. Початкове налаштування параметрів Сервера інтеграції також не займає багато часу, все стандартно: імена, адреси, порти.

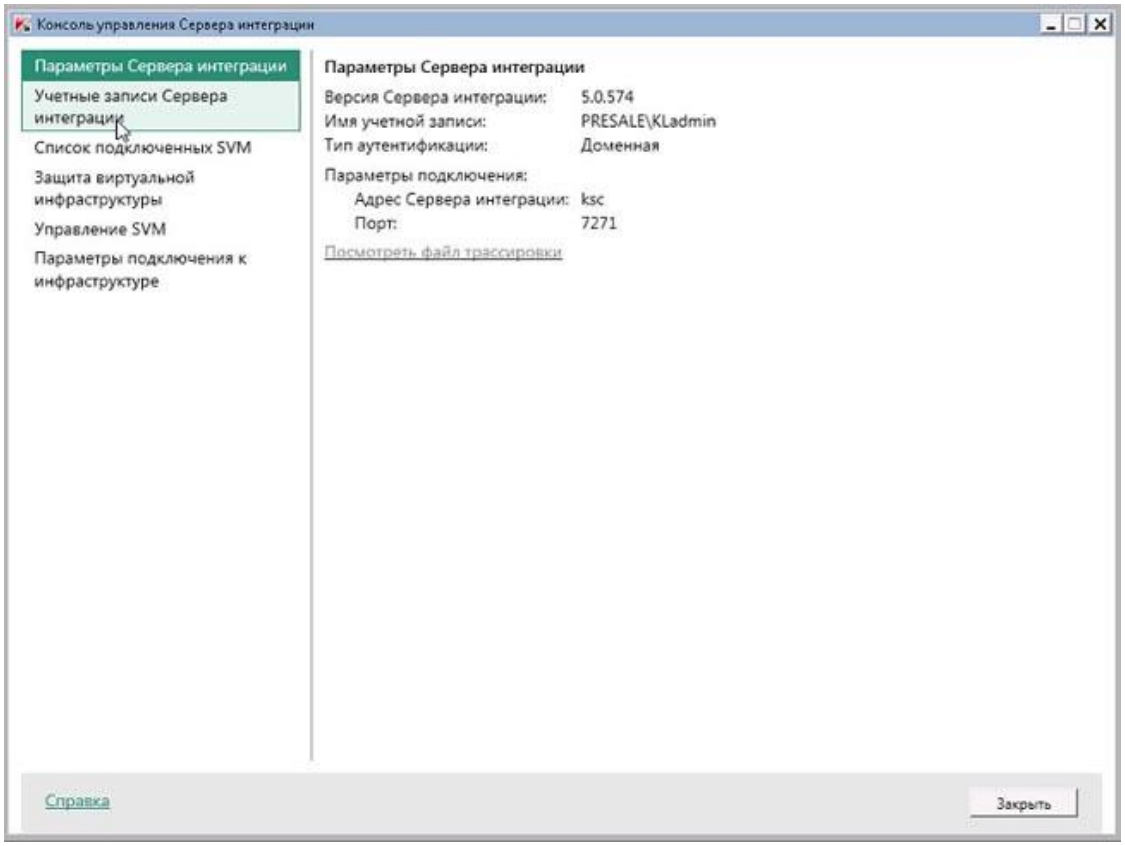


Рис3.7. Налаштування параметрів Сервера інтеграції Kaspersky Security для віртуальних середовищ / легкий агент

Для управління сервером інтеграції використовується службовий обліковий запис admin, При необхідності можна поміняти пароль або налаштувати інші дані для підключення.

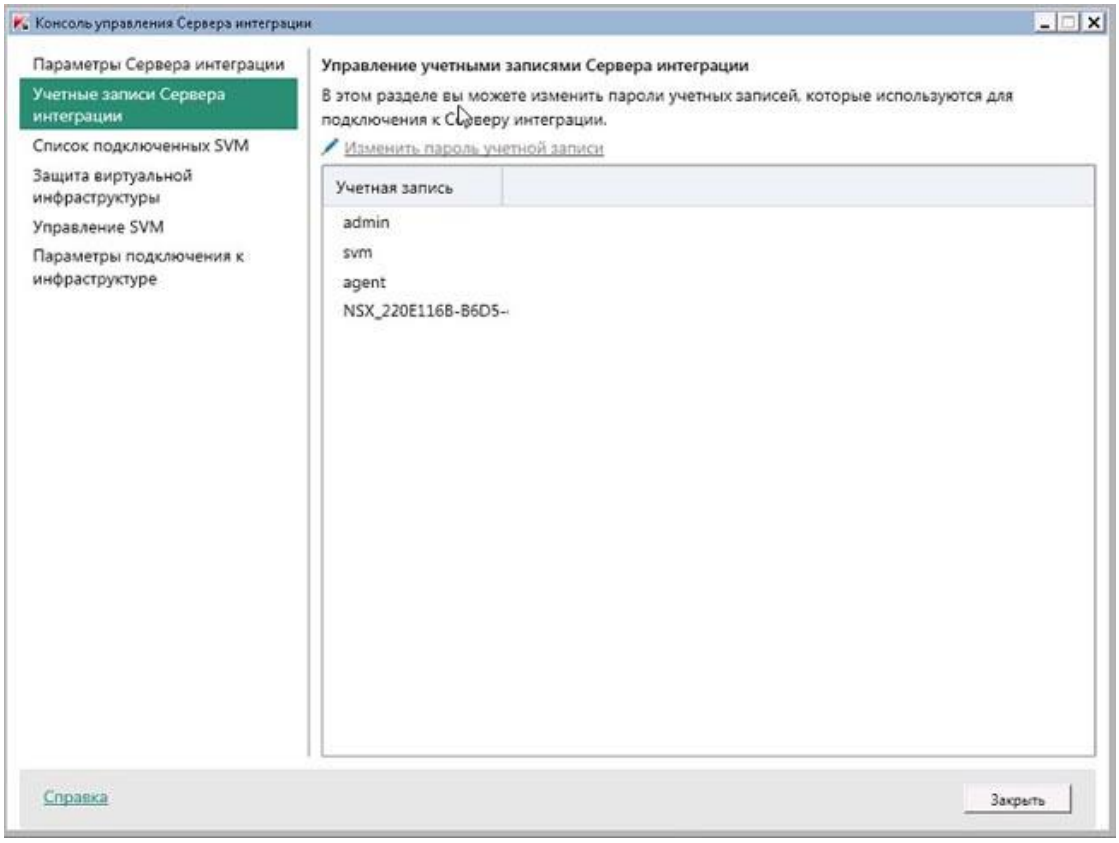


Рис.3.8. Налаштування облікових записів Сервера інтеграції Kaspersky Security для віртуальних середовищ / легкий агент

Про успішну установку Сервера інтеграції свідчать поява в розділі Додатково встановлені плагіни управління:

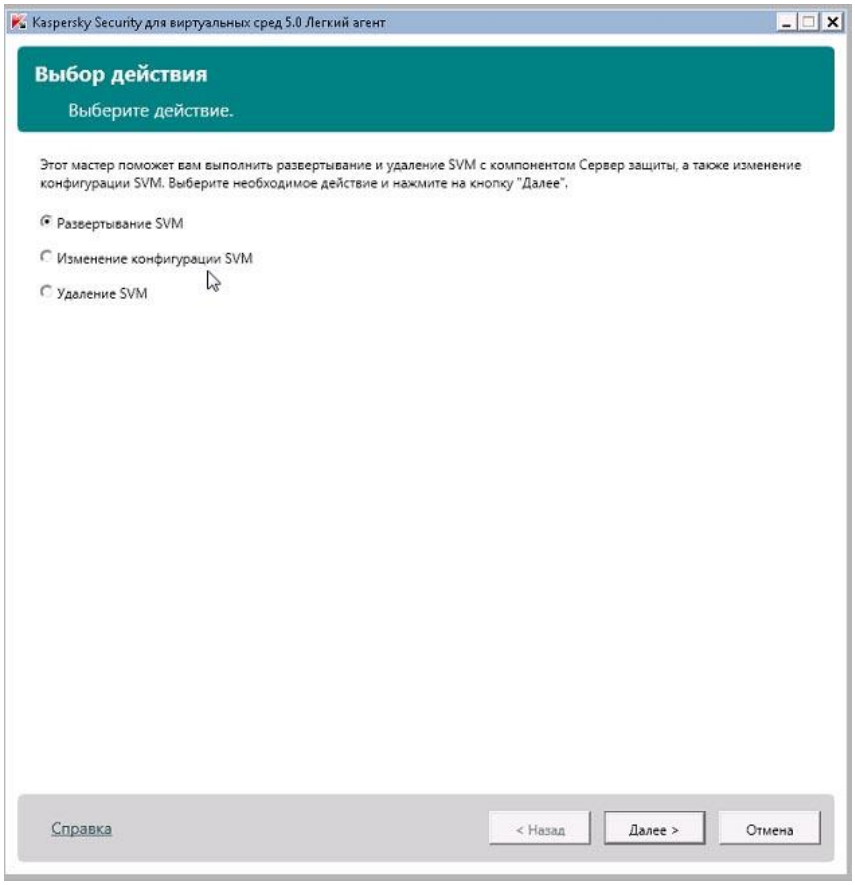
Kaspersky Security для віртуальних середовищ 5.0 Легкий агент - Сервер захисту.

Kaspersky Security для віртуальних середовищ 5.0 Легкий агент для Linux.

Kaspersky Security для віртуальних середовищ 5.0 Легкий агент для Windows.

Установка і налаштування віртуальної машини безпеки. Ядром системи антивірусного захисту при функціонуванні Kaspersky Security для віртуальних середовищ / Легкий агент є спеціальна віртуальна машина безпеки (SVM). Для інсталяції нової SVM необхідно активувати відповідний пункт меню і слідувати

вказівкам майстра. Попередньо необхідно завантажити з сайту вендора образ, відповідний виробнику розгорнутого середовища віртуалізації в компанії.



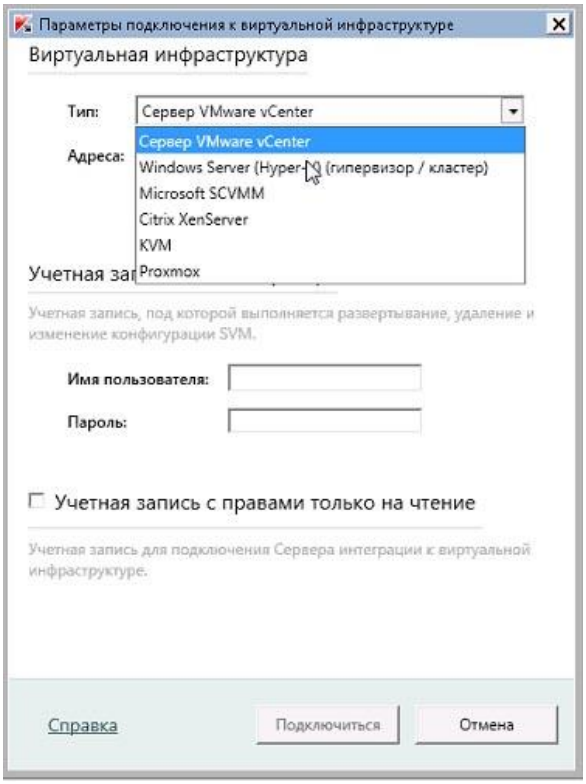
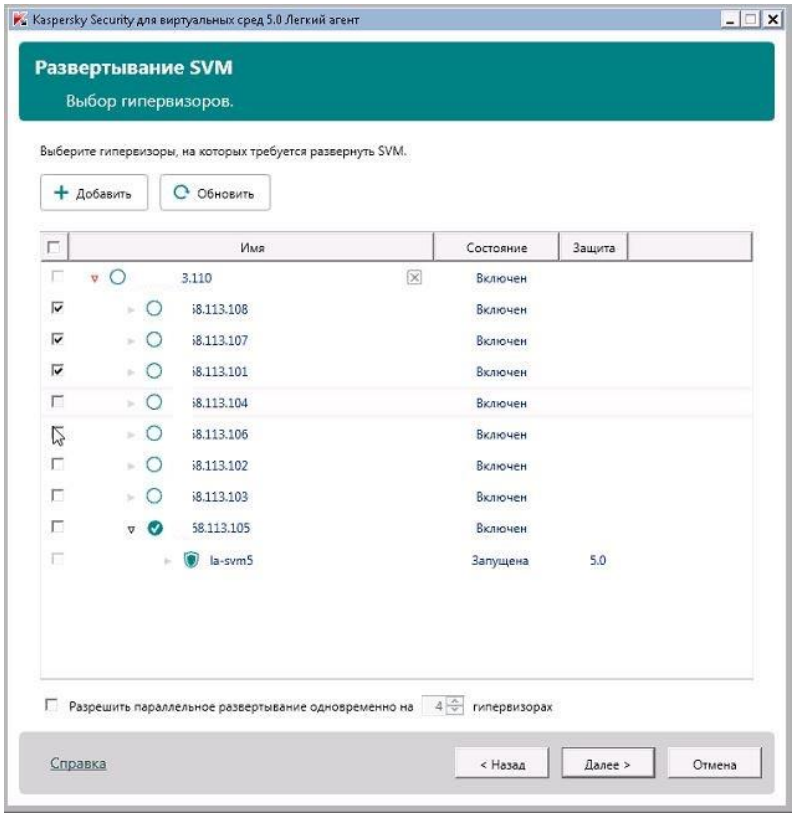


Рис.3.9. Майстер установки SVM Kaspersky Security для віртуальних середовищ / легкий агент

Завершуючи процес установки SVM, вибираємо цільової ESX-хост і налаштовуємо параметри мережі.



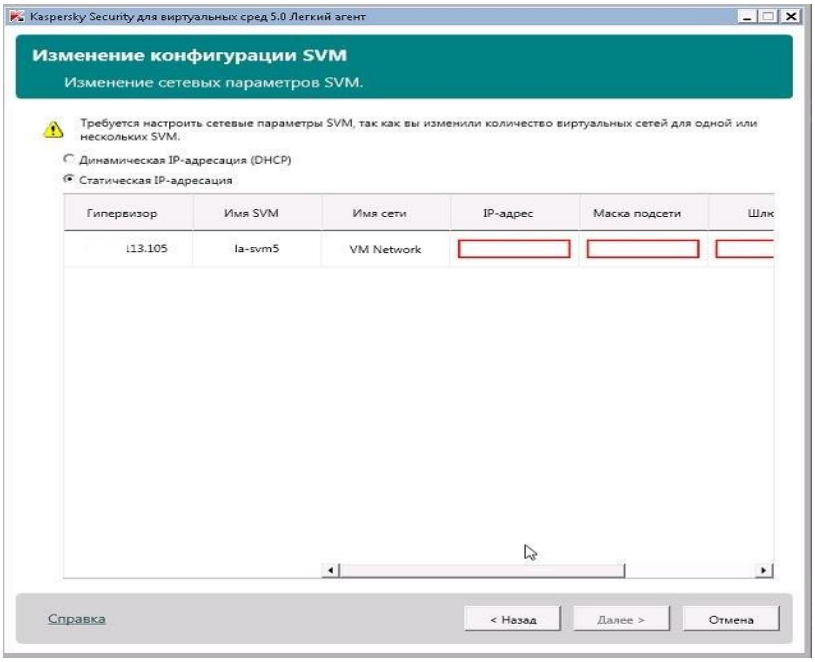


Рис3.10. Конфігурація SVM Kaspersky Security для віртуальних середовищ / Легкий агент

Після закінчення роботи майстра в основний консолі управління KSC з'явиться новий щойно створений сервер захисту SVM.

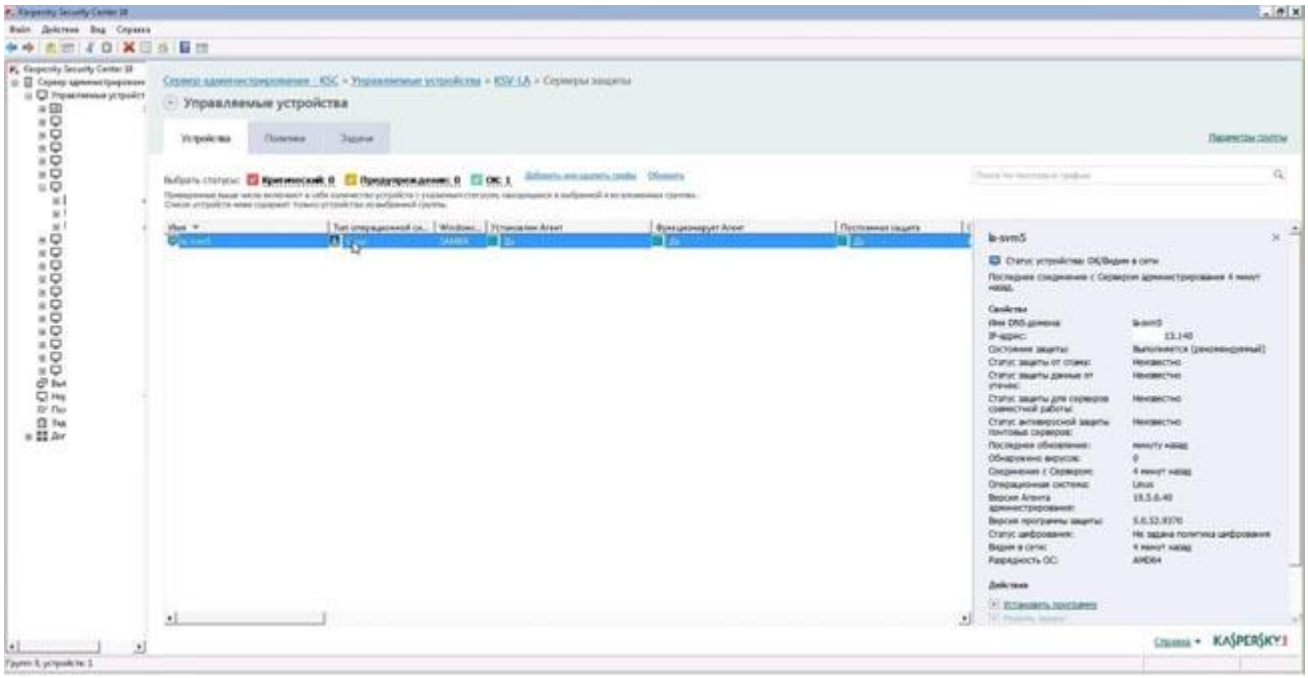


Рис.3.11 Управління SVM в KSC Kaspersky Security для віртуальних середовищ / Легкий агент

По завершенні процесу розгортання SVM було розглянуто інтерфейс гипервізора. Міні-дослідження показало, що він побудований на базі Red Hat Enterprise Linux, складно придумати реальний сценарій, при якому потрібен був би прямий консольний доступ до нього.

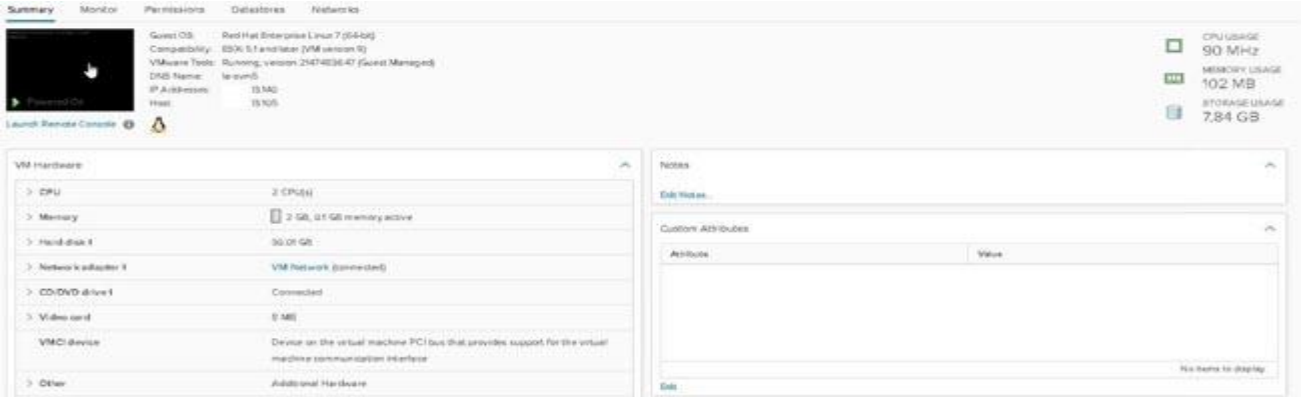


Рис.3.12. Віртуальна машина SVM в інтерфейсі гипервизора Kaspersky Security для віртуальних середовищ / Легкий агент

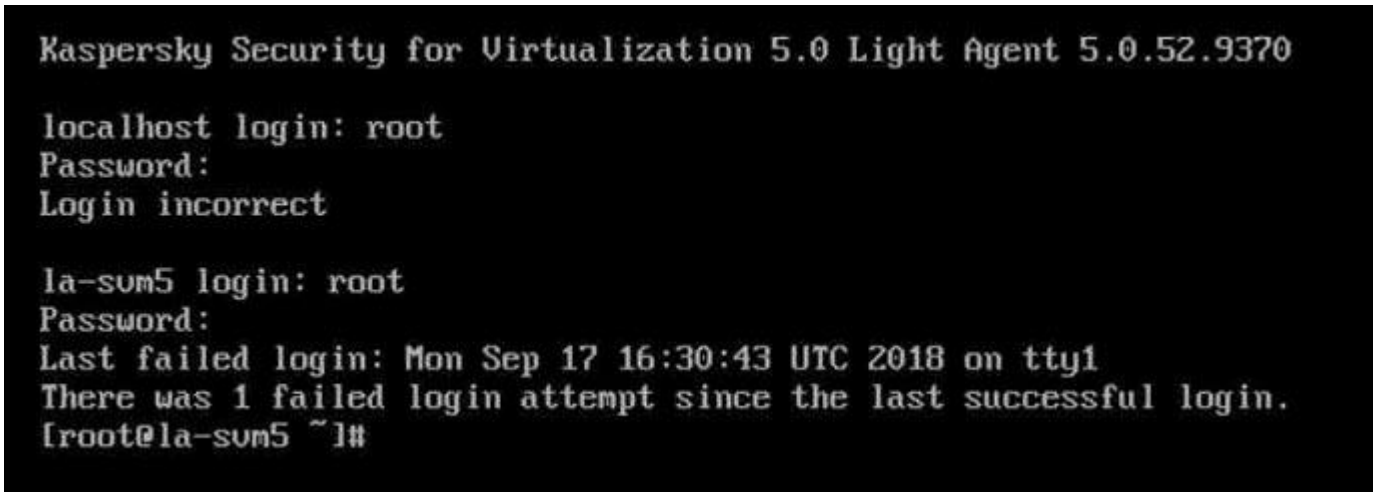


Рис.3.13. Віртуальна машина SVM в інтерфейсі гипервизора Kaspersky Security для віртуальних середовищ / Легкий агент

Повертаємося до більш звичного для користувача інтерфейсу. Надалі необхідно закінчити процедуру організації мережевої зв'язності шляхом настройки підключення SVM до Сервера інтеграції через створення нової політики у відповідному оснащенні KSC.

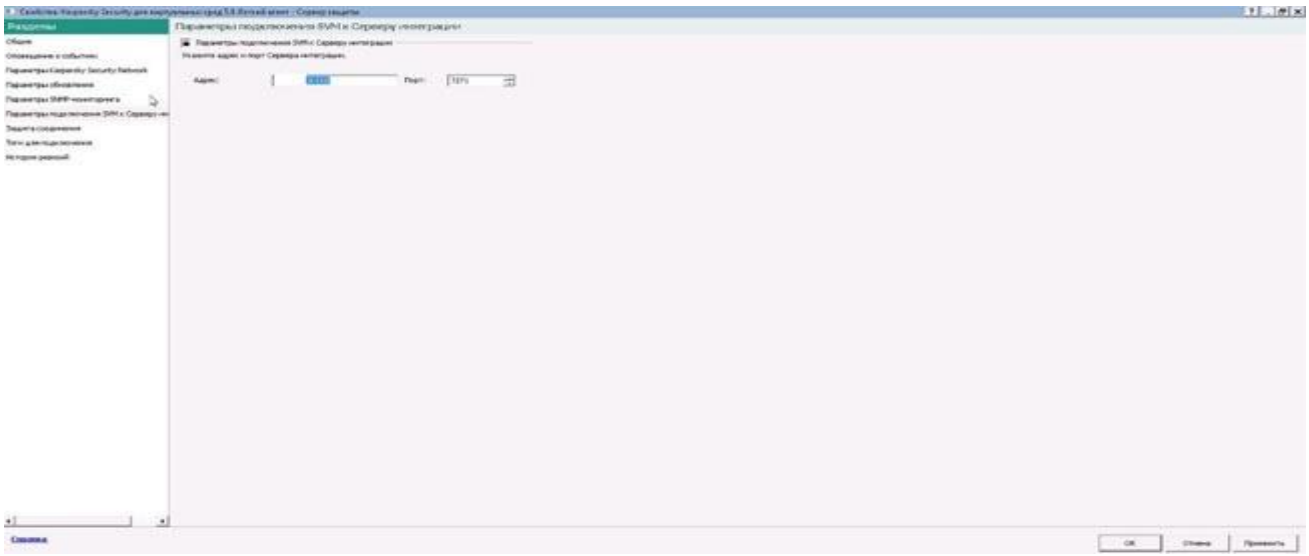


Рис.3.14. Налагодження підключення SVM до Сервера інтеграції в KSC Kaspersky Security для віртуальних середовищ / Легкий агент

На цьому первинна конфігурація SVM завершена. Далі необхідно створити першочергові завдання: активувати ліцензію і запустити оновлення антивірусних баз і можна переходити до встановлення агентів на призначені для користувача віртуальні машини.

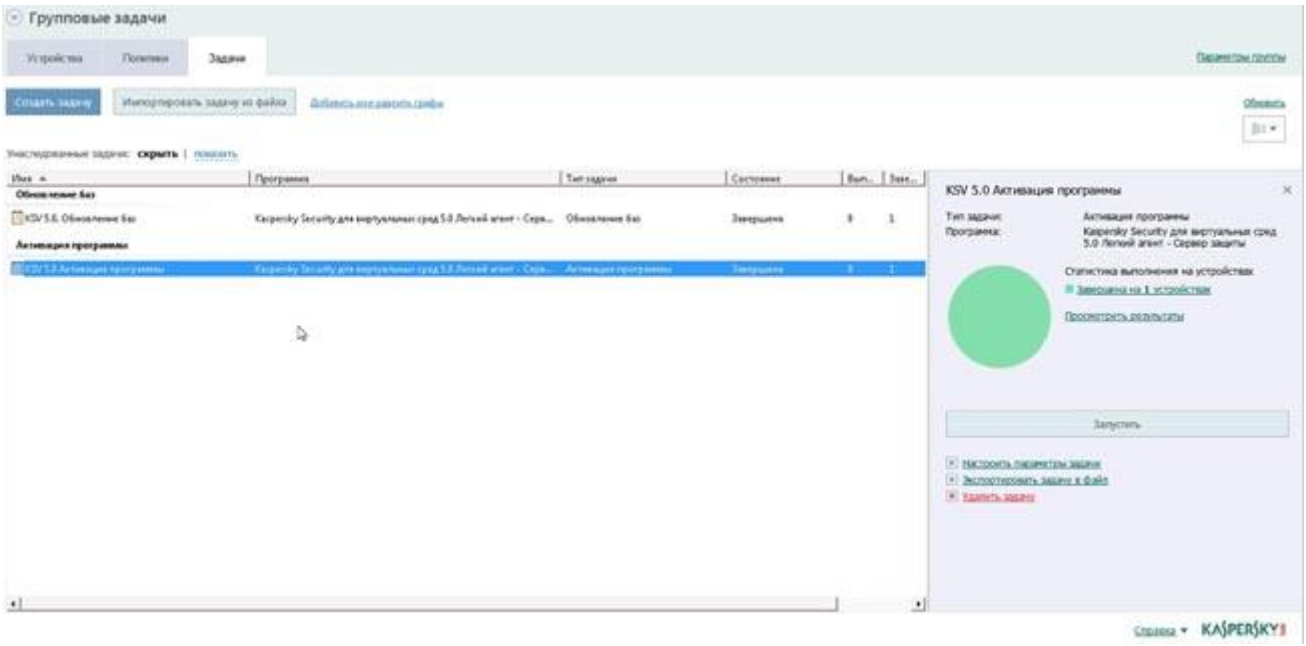


Рис.3.15. Створення завдань для SVM Kaspersky Security для віртуальних середовищ / Легкий агент

Виконуємо звичну для постійних користувачів роцедуру створення інсталяційного пакету, вибираємо образ агента для відповідної гостьової операційної системи, перелік підтримки яких, досить значний. Для цілей тестування упинились на версії для Windows.

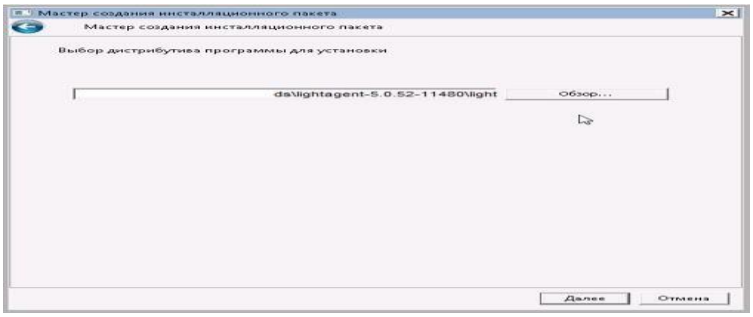


Рис.3.16 Створення інсталяційного пакета агентів Kaspersky Security для віртуальних середовищ | легкий агент

Дуже важливо на цьому етапі налаштувати параметри інсталяційного пакета. Це необхідно, щоб уникнути конфліктів і для підвищення надійності роботи агентів на критичних серверах рекомендується обмежитися файловим антивірусом і мережевим екраном, розставивши галочки відповідним чином.

Для цього необхідно вибратио режим «все включено», щоб максимально повно оцінити можливості продукту.

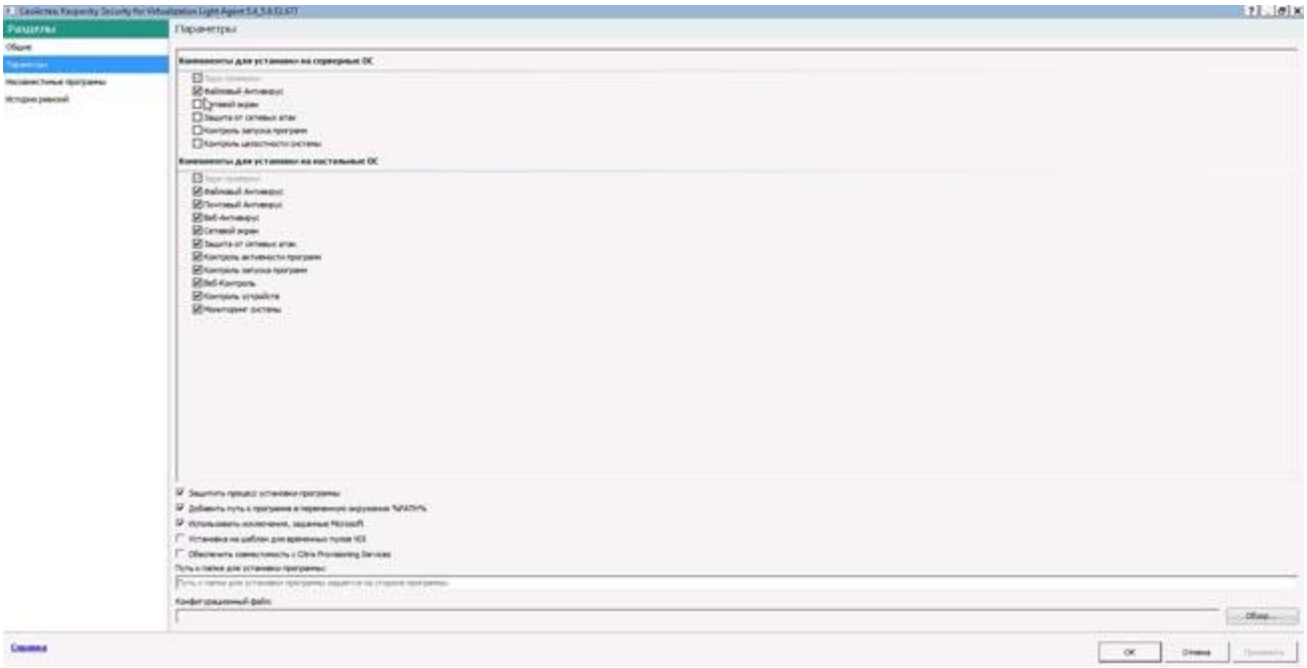


Рис.3.17. Налаштування інсталяційного пакета Kaspersky Security для віртуальних середовищ / Легкий агент

Зконфігурований пакет для установки агента, розгортається на всіх цільових віртуальних машинах в мережі. Важливою особливістю є те, що процес пошуку таких машин і саму установку можна максимально автоматизувати. Наприклад, можна створити таке правило, після відпрацювання якого всі знайдені віртуальні машини з певним типом і атрибутами автоматично потраплятимуть в категорію «Легкі агенти» з подальшою їх автоматичною установкою.

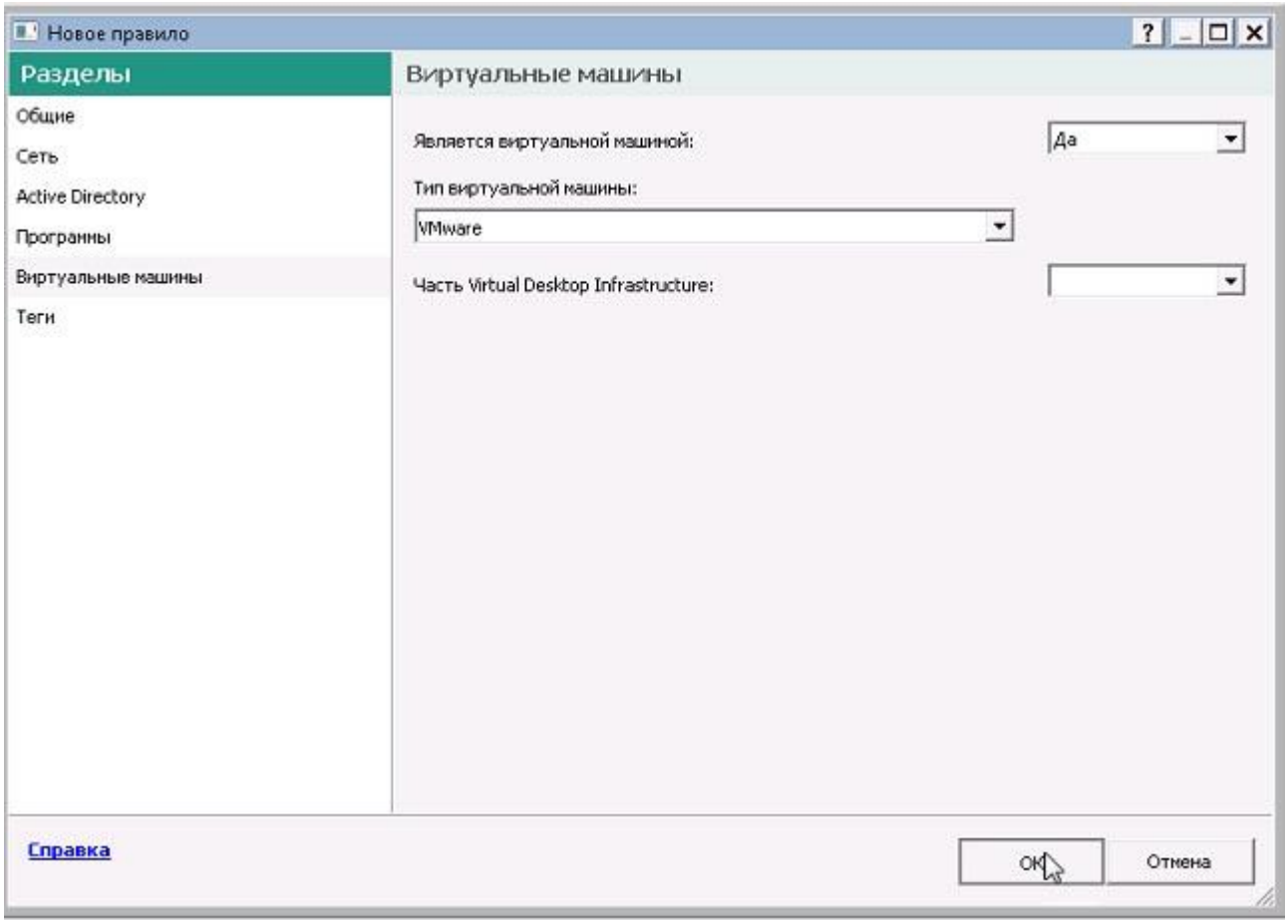


Рис.3.18. Налаштування правила переміщення віртуальних машин для установки агентів Kaspersky Security для віртуальних середовищ / Легкий агент

Після успішної установки агентів на захищені віртуальні машини в консолі управління стає доступний статус по ним.

Крім оперативно технічного зведення по захищеним машинам, в цьому розділі ми не знайшли нічого складного. Навіть дані по необробленим об'єктам та інших загроз можливо отримати лише у вигляді журналу подій, більш детальний розбір здійснюється безпосередньо або в окремому меню KSC (для віддалених заражених файлів - розділ «Сховище»), або в інтерфейсі самого агента.

Режими функціонування налаштовуються в оснащенні «Політика» і багато в чому повторюють аналогічні для антивіруса KES.

Відмітною пунктом є параметри підключення до SVM, які налаштовуються в залежності від обраного способу інтеграції.

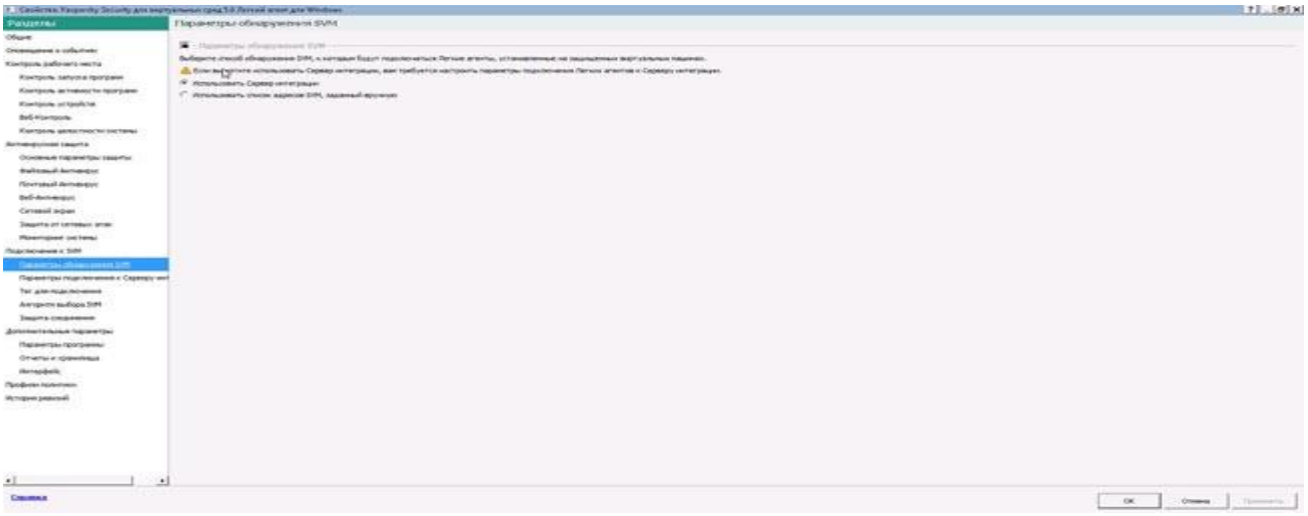


Рис.3.20. Налаштування політик агентів Kaspersky Security для віртуальних середовищ / Легкий агент

Для цілей тестування нами був встановлений агент на захищає віртуальну машину під керуванням Windows 7 SP1. Зовні інтерфейс продукту багато в чому схожий на KES, що цілком логічно.

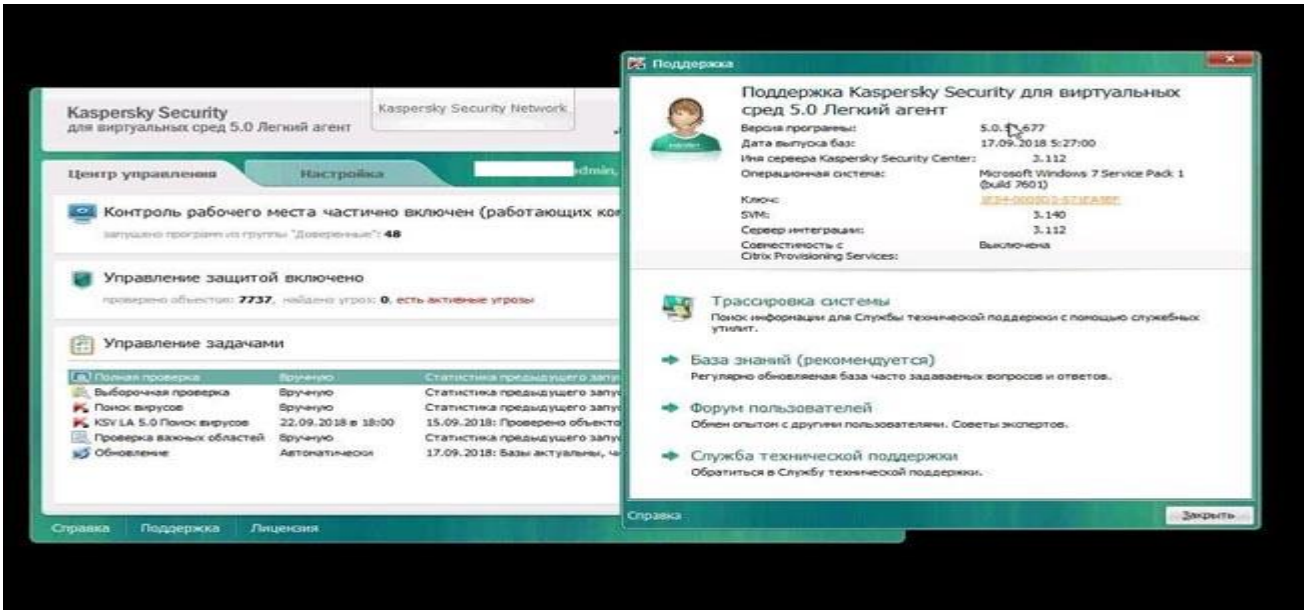


Рис.3.21. Зведення про стан агенту на захищеній робочій станції Kaspersky Security для віртуальних середовищ /Легкий агент

Оскільки раніше в інтерфейсі KSC ми налаштували відповідну політику, зміна переважної більшості параметрів для звичайного користувача недоступно.

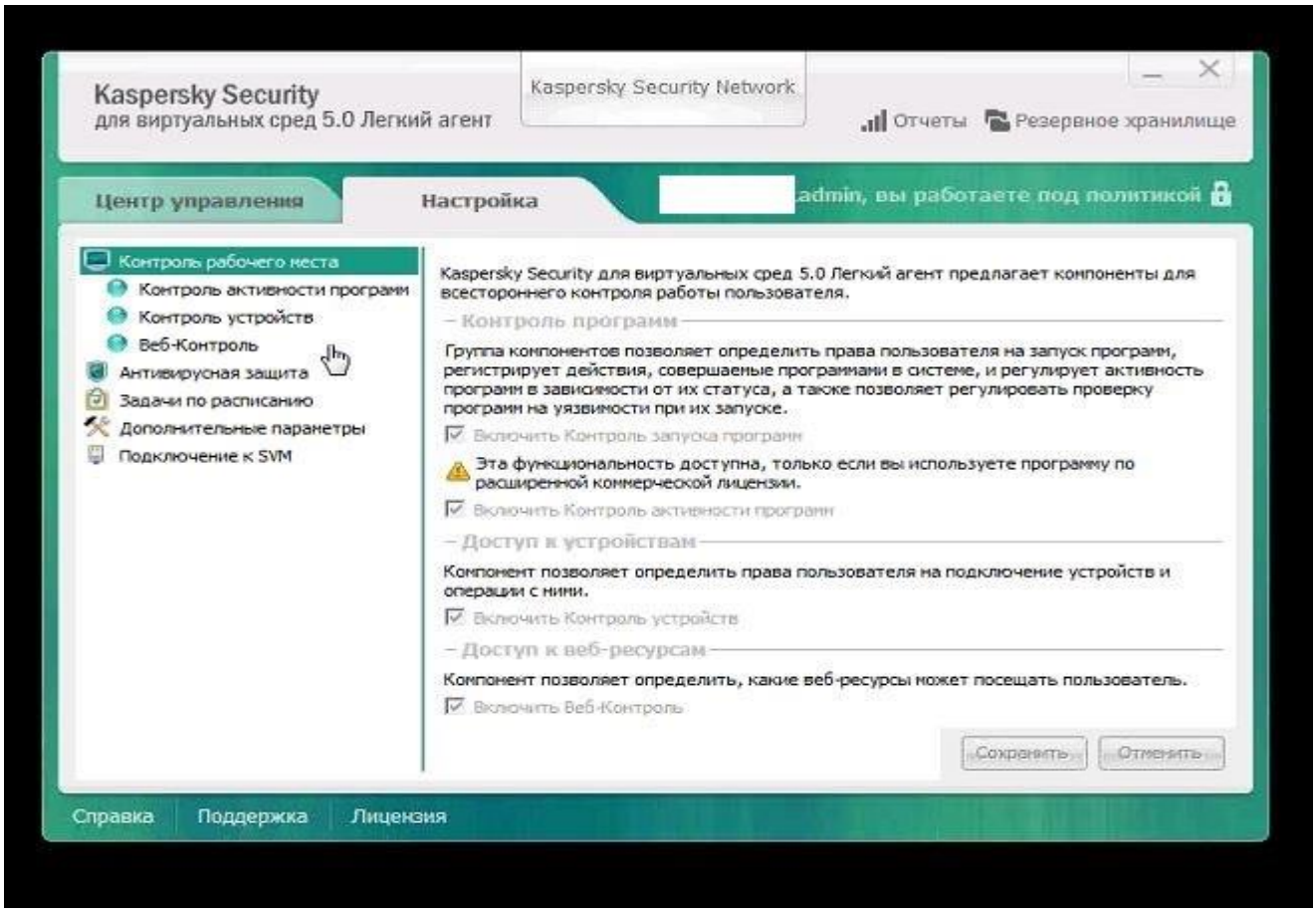


Рис.3.22. Налаштування параметрів агенту на захищені робочої станції Kaspersky Security для віртуальних середовищ / Легкий агент

Як ми вже відзначали, детальна інформація щодо виявлених заражень крім спеціального розділу в KSC відображається тут же, в інтерфейсі агента на захищеній машині. А, наприклад, необроблені об'єкти подивитися можна виключно локально.

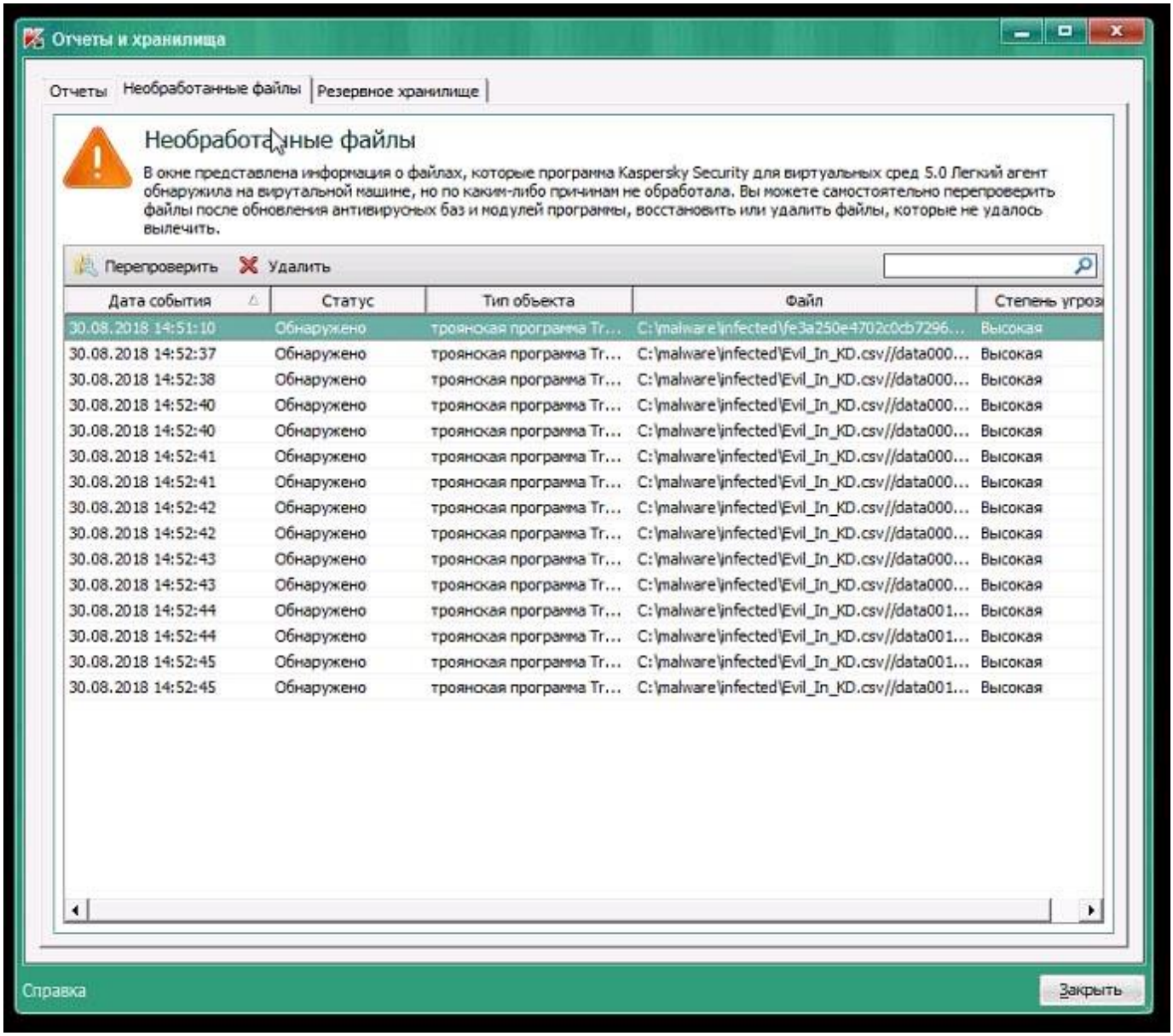


Рис.3.23. Дані по заражень в інтерфейсі агента на захищається робочої станції Kaspersky Security для віртуальних середовищ | легкий агент

Розглянемо особливості ліцензування та сертифікати. Kaspersky Security для віртуальних середовищ / Легкий агент в рамках єдиної ліцензії входить до складу комплексного рішення Kaspersky Security для віртуальних і хмарних середовищ (Kaspersky Hybrid Cloud Security - KHCS).

Крім нього KHCS включає в себе також:

Kaspersky Security для віртуальних середовищ / Захист без агента

Kaspersky Endpoint Security для Linux

Kaspersky Security для Windows

Server Kaspersky Security для віртуальних і хмарних середовищ для AWS

Kaspersky Security для віртуальних і хмарних середовищ для Microsoft Azure

Такий підхід дозволяє управляти захистом гібридної інфраструктури на базі уніфікованої точки контролю з єдиної консолі: всі корпоративні пристрої, включаючи робочі місця і сервери в офісах, центрах обробки даних і хмарі. Сам процес управління ліцензіями організований в поставляється в комплекті єдиного корпоративного центрі управління встановленими продуктами «Лабораторії Касперського» - Kaspersky Security Center - і буде звичним для постійних користувачів антивірусних продуктів вендора.

Таким чином в даній роботі було розроблено рекомендації з інсталяції і тестування на практиці нової версії Kaspersky Security віртуальних середовищ / Легкий агент 5.0.

Головною перевагою даного продукту можна відзначити близький до ідеального баланс функціональності і ресурсних вимог. На відміну від традиційних важких рішень, що вимагають установки повноцінного endpoint на кожну віртуальну машину, весь антивірусний движок тут розгортається лише на виділеній SVM, а на гостьові системи інсталюється практично непомітне програмне забезпечення - легкий агент, назва якого виправдовує себе повною мірою.

Хоча технологічно файлова перевірка винесена на рівень окремо виділеної SVM, для користувача захищеної віртуальної машини вона абсолютно прозора і виконується як ніби локально. У той же час крім сканування на віруси в продукті доступний весь набір захисних технологій «Лабораторії Касперського», який використовується в повних версіях EPP, таких, наприклад, як десктопний антивірус Kaspersky Endpoint Security: сигнатурний і евристичний аналіз для захисту від складних резидентних шкідливих програм, контроль програм , пристроїв і веб,

персональний міжмережевий екран, система запобігання вторгнень і захисту від мережевих атак, моніторинг системи та інші.

3.3. Розробка рекомендацій фахівцям кібербезпеки щодо використання віртуального середовища

В результаті проведеного дослідження є можливість скласти рекомендації, які дозволять фахівцям з кібербезпеки розгортати, налаштовувати та адмініструвати віртуальне середовище корпоративної інформаційної інфраструктури.

Тому рекомендується вживати певних заходів безпеки. По-перше, необхідно встановити обмеження між хостом і гостями віртуального середовища, з метою уникнення згодом прямого доступу до хоста. Тому що це може дозволити зловмиснику скомпрометувати всі системи «одним пострілом». По-друге, фізичний доступ на хост, де працює кілька віртуальних середовищ повинен бути обмежений. Заборона зовнішніх пристроїв, підключених до нього (USB, CD та інші), також є запобіжним засобом.

Захист операційних систем, служб і додатків, розгорнутих на віртуальних машинах, слід забезпечувати настільки ж ретельно, як якщо б вони були розгорнуті на фізичному обладнанні. Однак в погано контрольованому середовищі віртуалізації зловмисникові буде простіше спровокувати відмову в обслуговуванні або викрасти файли з дисками віртуальних машин. У цьому випадку йому навіть не доведеться виносити жорсткі диски з серверної.

Своєчасно перевіряти і встановлювати оновлення безпеки.

Використовуйте виділені мережеві адаптери для управління сервером. Ізолюйте його від інших підмереж.

Забезпечте безпеку сховищ, в яких розміщуються файли віртуальних машин.

Налаштувати антивірусне програмне забезпечення.

Не запускати додатки в керуючій операційній системі - всі програми повинні виконуватися в віртуальних машинах.

Не надавати адміністраторам віртуальних машин права на управління хост-сервером.

Забезпечити захист свої віртуальних машини, це підвищить загальний рівень безпеки системи.

Використовуйте шифрування BitLocker для захисту ресурсів.

Захищайте ресурси хост-сервера від віртуальних машин шляхом виділення відповідних пулів ресурсів для віртуальних машин.

Розмежовуйте права доступу в середовищі гіпервізора.

Отже, забезпечення безпеки платформи віртуалізації - це комплекс технічних і організаційних заходів. При цьому адміністративний аспект часто не беруть до уваги. Необхідно щоб кількість адміністраторів команди супроводу було обмежено, вони повинні бути добре підготовлені, а процесно-регламентну складову необхідно добре пропрацювати.

ВИСНОВКИ

Використання інформаційних систем (ІС) і інформаційних технологій (ІТ) в умовах інтенсивного розвитку цифрової економіки є одним із найбільш важливих елементів ефективної роботи будь-якої компанії. Тому для підвищення використання сучасних інформаційних технології для ведення бізнес-процесів компанії в магістерській роботі отримано наступні результати:

проведено аналіз використання віртуального середовища в корпоративних інформаційних системах. В результаті чого було виявлено зацікавленість компаній до такої технології. І в свою чергу, впровадження нових технологій вимагають забезпечення кібербезпеки КІС з використанням нових методів та засобів, щодо налаштування, конфігурації, зберігання даних в таких середовищах. Отримано дані, які свідчать про необізнаність керівництва компанії щодо збереження бізнес-процесів при використанні віртуального середовища. І як наслідок, це може призвести до загроз в КІС і компрометації компанії.

досліджено методи та засоби забезпечення кібербезпеки віртуального середовища корпоративної інформаційної системи, на основі визначення вимог до антивірусного захисту віртуальних машин.

досліджено архітектуру побудови середовища корпоративної інформаційної системи, на основі щодо організації антивірусного захисту. В результаті якого було досліджено SVM Kaspersky Security на базі легкого агента.

розроблено рекомендації щодо впровадження, налаштування SVM Kaspersky Security на базі легкого агента для забезпечення кібербезпеки корпоративних інформаційних системи, які використовують віртуальне середовище.

ПЕРЕЛІК ПОСИЛАНЬ

1. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/С.В. Кавун, В.В. Носов, О.В. Мажай. –Харків: Вид. ХНЕУ, 2008. – 352 с.

2. Теория информационной безопасности и методология защиты информации: учебное пособие. /И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина -Казань: Изд-во Казан. гос. техн. ун-та, 2008. – 358 с.

3. Кібербезпека Касперський [Електронний ресурс]. - Режим доступу: https://www.anti-malware.ru/reviews/Kaspersky_Security_for_virtualization_3_0.

4. Уразливості віртуальних машин [Електронний ресурс]. - Режим доступу: https://book.cyberyozh.com/ru/uyazvimosti-virtualnyih-mashin-kak-hakeryi-vyihodyat-za-predelyi-virtualnoj-sredyi/ .

5. Сороковская А. А. Информационная безопасность предприятия : новые угрозы и перспективы [Электронный ресурс]. – Режим доступа : http://nbuv.gov.ua/portal/Soc_Gum/Vchnu_ekon/2010_2_2/032-035.pdf.

6. Безпека віртуального середовища [Електронний ресурс]. - Режим доступу: https://channel4it.com/publications/Bezopasnost-v-virtualnyh-sredah-1183.html

7. «Защита виртуальной инфраструктуры» [Електронний ресурс]. - Режим доступу: https://www.galex.ru/about/news/news_vendors.php?ELEMENT_ID=38318&redir=Y

8. Віртуальна машина [Електронний ресурс]. - Режим доступу: https://book.cyberyozh.com/ru/virtualnaya-mashina-i-virtualnaya-operatsionnaya-sistema/

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ
(ПРЕЗЕНТАЦІЯ)