РЕФЕРАТ

Об'єкт дослідження – процес забезпечення захисту кінцевих точок корпоративної інформаційної системи.

Предмет дослідження – технологія захисту кінцевих точок корпоративної інформаційної системи.

Мета роботи – розробити варіант технології захисту кінцевих точок корпоративної інформаційної системи.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння, моделювання топології системи захисту кінцевих точок корпоративної інформаційної системи

В роботі зроблено аналіз проблеми кібербезпеки корпоративної інформаційної системи та визначено мета та завдання захисту кінцевих точок корпоративної інформаційної системи. Проведено аналіз існуючих технологій захисту кінцевих точок корпоративної інформаційної системи.

Досліджено методи та засоби захисту кінцевих точок на прикладі. Визначено призначення, основні функції та склад програмного комплексу McAfeeEndpointSecurity. Визначено призначення, основні функції та принципи роботи модуля "Попередження загроз". Визначено призначення, основні функції та принципи роботи модуля "Міжмережевий екран". Визначено призначення, основні функції та принципи роботи модуля "Контроль Інтернету". Визначено призначення, основні функції та принципи роботи модуля "Адаптивний захист від загроз".

На основі досліджень проведених в роботі розроблено варіанту топології системи захисту кінцевих точок корпоративної інформаційної системи із застосування рішення McAfeeEndpointSecurity.

Галузь використання – кібербезпека.

КОРПОРАТИВНА ІНФОРМАЦІЙНА СИСТЕМА, КІБЕРБЕЗПЕКА, ЗАХИСТ КІНЦЕВИХ ТОЧОК, ТЕХНОЛОГІЯ ЗАХИСТУ КІНЦЕВИХ ТОЧОК, МЕТОДИ ТА ЗАСОБИ ЗАХИСТУ КІНЦЕВИХ ТОЧОК, МІЖМЕРЕЖЕВИЙ ЕКРАН, ПОПЕРЕДЖЕННЯ ЗАГРОЗ, КОНТРОЛЬ ІНТЕРНЕТУ, АДАПТИВНИЙ ЗАХИСТ ВІД ЗАГРОЗ.

1 АНАЛІЗ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

1.1. Призначення, структура, функції та умови функціонування корпоративної інформаційної системи.

В останні роки в Україні досить стрімко на великих підприємствах почались впроваджуватися корпоративні інформаційні системи (КІС), що базуються на клієнт-серверній архітектурі. В даний час на ринку програмних продуктів України пропонується більше десятка зарубіжних і декілька вітчизняних зразків корпоративних систем.

Керівництво будь-якої швидкозростаючої компанії рано чи пізно стикається з проблемою систематизації інформації та автоматизації процесів, що беруть участь в обробці цієї інформації.

Якщо на початковому етапі розвитку компанії можлива ситуація, коли співробітники використовують стандартні офісні програми, то з часом зростання обсягів інформації ставить перед компанією завдання створення сучасної корпоративної інформаційної системи.

Корпоративні інформаційні системи (КІС) - це інтегровані системи управління територіально розподіленої корпорацією, засновані на поглибленому аналізі даних, широке використання систем інформаційної підтримки прийняття рішень, електронних документообіг і діловодстві. КІС покликані об'єднати стратегію управління підприємством і передові інформаційні технології.

Корпоративна інформаційна система - це сукупність технічних і програмних засобів підприємства, що реалізують ідеї і методи автоматизації.

Комплексна автоматизація бізнес процесів підприємства на базі сучасної апаратної та програмної підтримки може називатися по-різному. В даний час поряд з назвою Корпоративні інформаційні системи (КІС) вживаються, наприклад, такі назви:

1. Автоматизовані системи управління (АСУ);
2. Інтегровані системи управління (ІСУ);
3. Інтегровані інформаційні системи (ІВС);
4. Інформаційні системи управління підприємством (ІСУП).

Головне завдання КІС - ефективне управління всіма ресурсами підприємства (матеріально-технічними, фінансовими, технологічними і інтелектуальними) для отримання максимального прибутку і задоволення матеріальних і професійних потреб усіх співробітників підприємства.

КІС за своїм складом - це сукупність різних програмно-апаратних платформ, універсальних і спеціалізованих додатків різних розробників, інтегрованих в єдину інформаційно-однорідну систему, яка найкращим чином вирішує в деякому роді унікальну задачу кожного конкретного підприємства. Тобто, КІС - людино-машинна система і інструмент підтримки інтелектуальної діяльності людини, яка під його впливом повинна:

Накопичувати певний досвід і формалізовані знання;

Постійно вдосконалюватися і розвиватися;

Швидко адаптуватися до мінливих умов зовнішнього середовища і нових потреб підприємства.

Комплексна автоматизація підприємства має на увазі переклад в площину комп'ютерних технологій всіх основних ділових процесів організації. І використання спеціальних програмних засобів, що забезпечують інформаційну підтримку бізнес-процесів, як основи КІС представляється найбільш виправданим і ефективним. Сучасні системи управління бізнес-процесами дозволяють інтегрувати навколо себе різне програмне забезпечення, формуючи єдину інформаційну систему. Тим самим вирішуються проблеми координації діяльності співробітників і підрозділів, забезпечення їх необхідною інформацією і контролю виконавської дисципліни, а керівництво отримує своєчасний доступ до достовірними даними про хід виробничого процесу і має кошти для оперативного прийняття і втілення в життя своїх рішень. І, що найголовніше,

Під корпоративною інформаційною системою будемо розуміти інформаційну систему організації, що відповідає наступним мінімальним переліком вимог:

1. Функціональна повнота системи
2. Надійна система захисту інформації
3. Наявність інструментальних засобів адаптації та супроводу системи
4. Реалізація віддаленого доступу і роботи в розподілених мережах
5. Забезпечення обміну даними між розробленими інформаційними системами та ін. Програмними продуктами, що функціонують в організації.
6. Можливість консолідації інформації
7. Наявність спеціальних засобів аналізу стану системи в процесі експлуатації

Функціональна повнота системи

- виконання міжнародних стандартів управлінського обліку MRP II, ERP, CSRP
- автоматизація в рамках системи вирішення завдань планування, бюджетування, прогнозування, оперативного (управлінського) обліку, бухгалтерського обліку, статистичного обліку та фінансового-економічного аналізу
- формування і ведення обліку одночасно по російським і міжнародним стандартам
- кількість одноразово врахованих параметрів діяльності організації від 200 до 1000, кількість формованих таблиць баз даних - від 800 до 3000.

Система захисту інформації

- парольний система розмежування доступу до даних і реалізованим функцій управління
- багаторівнева система захисту даних (засоби авторизації вводиться і корректируемой інформації, реєстрація часу введення і модифікації даних)

Інструментальні засоби адаптації та супроводу системи

- зміна структури і функцій бізнес-процесів

- зміна інформаційного простору
- зміна інтерфейсів введення, перегляду і коригування інформації
- зміна організаційного і функціонального наповнення робочого місця користувача
- генератор довільних звітів
- генератор складних господарських операцій
- генератор стандартних форм

Можливість консолідації інформації

- на рівні організації - об'єднання інформації філій, холдингів, дочірніх компаній і т.д.
- на рівні окремих завдань - планування, обліку, контролю і т.д.
- на рівні тимчасових періодів - для виконання аналізу фінансово-економічних показників за період, що перевищує звітний

Спеціальні засоби аналізу стану системи в процесі експлуатації

- аналіз архітектури баз даних
- аналіз алгоритмів
- аналіз статистики кількості обробленої інформації
- журнал виконаних операцій
- список працюючих станцій серверів
- аналіз внутрісистемної пошти

Найбільш розвинені корпоративні ІС (КІС) призначені для автоматизації всіх функцій управління корпорацією: від науково-технічної та маркетингової підготовки її діяльності до реалізації її продукції і послуг. В даний час КІС мають в основному економічну і виробничу спрямованість.

Сучасні КІС мають такі основні характеристики.

Масштабність. ІС повинна мати в своєму підпорядкуванні :сервери, операційні системи, сис-теми комунікації, системи управління базами даних, та потребує значних зусиль спеціалістів з проектування і упровадження таких систем.

Робота в неоднорідному обчислювальному середовищі - це можливість роботи в мережах, до яких входять комп'ютери, що працюють під управлінням різних операційних систем. При цьому має бути забезпечена взаємодія всіх операційних систем, які використовуються. Розподілені обчислення. Це один із видів роботи в клієнт-сер-верній архітектурі, коли дані чи запити, які надходять з клієнтських машин розподіляються поміж кількома серверами, що збільшує пропускну здатність для користувача і дає можливість багатозадачної роботи. Це сприяє макси-мальному використанню обчислювальних ресурсів, зниженню витрат і підвищенню ефективності системи. Забезпечення розподіленої роботи — це обов'язкова вимога до інформаційних систем корпоративного рівня.

КІС надають користувачеві можливість вирішення таких глобальних задач:

• зробити прозорим для керівництва корпорацією використання вкладених у бізнес капіталів;

• надати повну інформацію для економічної доцільності стратегічного планування;

• професійно керувати витратами, наочно і своєчасно показувати, за рахунок чого можна мінімізувати витрати;

• реалізувати оперативне управління підприємством згідно вибраних ключових показників (собівартість продукції, структура витрат, рівень прибутковості тощо);

• забезпечити гарантовану прибутковість підприємства за рахунок оптимізації і прискорення ряду процесів (строків виконання нових замовлень, перерозподілу ресурсів і т. д.).

КІС повинна забезпечити інформаційну прозорість підприємства, формувати єдиний інформаційний простір який об'єднує інформаційні потоки, що йдуть від виробництва, з даними фінансово-господарських служб і видавати необхідні результативні рішення для всіх рівнів управління підприємством.

Сучасні КІС мають такі основні характеристики:

масштабованість. Це одна з важливих характеристик КІС, оскільки вони повинні створюватись на масштабованій програмно-апаратній платформі (сервери, операційні системи, системи комунікації, СУБД). Оскільки варіантів конфігурації базового устаткування і програмного забезпечення може бути багато, то КІС має бути багатоплатформовою.

багатоплатформність. В КІС виникає потреба втому, щоб прикладна програма працювала на кількох апаратних і програмних платформах. При цьому мають бути забезпечені однакові інтерфейси та логіка роботи. Реалізувати прикладну програму одночасно в кількох середовищах нелегко. В зв'язку з цим з'явились інтегровані програмні середовища розробки, які значно полегшують перенесення прикладних програм з одного середовища в інше. До них зокрема належать: Windows OpenSystem (WOSA), Win32, загальне відкрите програмне середовище UNIX COSE AppWareFoundation тощо;

- розподілені обчислення. Це один із видів роботи в клієнт-серверній архітектурі, коли дані чи запити, які надходять з робочих станцій, розподіляються між кількома серверами, що забезпечує можливість багатозадачної роботи та оптимізацію використання обчислювальних ресурсів.

Забезпечення розподіленої роботи і віддаленого доступу до документів - це обов'язкова вимога до інформаційних систем корпоративного рівня. Останнім часом невід'ємною складовою частиною цієї вимоги стала підтримка роботи в мережевій архітектурі.

Цілісність КІС забезпечується чотирма чинниками:

концептуальна узгодженість бізнес-процесів, для автоматизації яких створюється ІС, що зберігається впродовж усього життєвого циклу;

технологічна цілісність, яка проявляється в застосуванні погодженого набору інформаційних технологій для управління інформаційними ресурсами;

відповідність функціональності робочих місць співробітників їхнім посадовим обов’язкам;

єдиний регламент обслуговування та експлуатації всіх компонентів ІС, який розробляється при її створенні.

Поєднання цих властивостей принципово відрізняє КІС від суми компонентів з тим же набором функцій і дозволяє справлятись з комплексом проблем, які складно вирішувати у разі безсистемної інформатизації бізнесу.

Корпоративні інформаційні системи, призначені для автоматизації різних видів господарського обліку та управління підприємством можна умовно поділити на три класи: локальні системи, середні інтегровані системи, великі інтегровані системи.

Корпоративні ІС призначені для автоматизації всіх функцій управління фірмою або корпорацією, що має територіальну роз'єднаність між підрозділами, філіями, відділеннями, офісами.

Також вона охоплює всі бізнес- функції і всі управлінські процеси корпорації. В умовах великих підприємств і корпорацій вона може бути більш ефективна, оскільки забезпечує взаємодію масових і добре організованих процесів швидкодіючими засобами сучасних інформаційних і телекомунікаційних технологій високого науково-технічного рівня.

1.2. Аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи.

Безліч сучасних рішень щодо захисту кінцевих станцій не спираються на старі парадигми, сформовані виробниками класичних антивірусів, але при цьому мають відмінні результати, що доводять, що навіть в такій консервативній галузі є багато місця для експериментів і нестандартних ідей. Примітно, що багато класичні рішення змогли успішно адаптуватися до нових реалій і очолити списки сучасних систем по захисту кінцевих станцій. Які ж основні тенденції в розвитку технологій захисту кінцевих станцій? Кінцеві станції завжди були якщо не головним, то одним з основних джерел загроз інформаційній безпеці. При цьому саме поняття кінцевої станції

істотно розширилося за останні кілька років, особливо з розвитком мобільних платформ. Тепер в область визначення «кінцевої станції» входять не тільки персональні комп'ютери користувачів і корпоративні сервера, але і мобільні пристрої (смартфони, планшети, ноутбуки) і пристрої IoT (InternetofThings). З цієї ж причини значно збільшилася кількість векторів атак, як на корпоративні мережі, так і на простих (т. Н. Домашніх) користувачів. Стрімкий розвиток концепції BYOD (BringYourOwnDevice) в середині 2000-х років внесло свої корективи в розмивання периметра організацій і збільшення векторів атак. Якщо раніше смартфони, домашні комп'ютери і ноутбуки користувачів не представляли великого комерційного інтересу для зловмисників, то з перенесенням на них частини корпоративних функцій вони стали вельми бажаними цілями для атак. Лавиноподібне збільшення спрямованих атак в 2010-х роках, відмінною рисою яких є експлуатація вразливостей нульового дня, унеможливило для використання класичний підхід до захисту кінцевих станцій, пов'язаний виключно з сигнатурним і статичним аналізом запускаються файлів. Останнім часом йде збільшення спрямованих атак на кінцеві станції, що реалізуються за допомогою т. Зв. filelessmalware, що зберігаються виключно в оперативній пам'яті і не залишають записи про свою активності в файлової системі. В цьому випадку з архітектури атаки повністю зникає головний об'єкт перевірки класичного антівіруса- сам заражений файл. Піонерами в захисті кінцевих станцій, безумовно, були антивіруси, історія яких починається з середини 80-х років минулого століття. Основою будь-якого антивіруса завжди був сигнатурний аналіз - технологія, що дозволяє по деякому принципом обчислювати контрольну суму зараженого файлу і записувати її в централізовану сигнатурну базу.При подальшій перевірці кожного проходить файлу його контрольна сума порівнюється з усіма записами в сигнатурної базі і при збігу файл позначається як заражений. Очевидним недоліком такого методу є те, що з його допомогою можна виявити лише ту загрозу, інформація про яку вже є в базі - нові уразливості і методи їх експлуатації

випадають з поля зору сигнатурного аналізу. Наступним логічним кроком у розвитку антивірусних систем став статичний (або, як його частіше називають, евристичний) аналіз. Суть статичного методу полягає в тому, що на базі певного набору патернів і статичних ознак (властивостей) евристичний механізм намагається передбачити поведінку аналізованого файлу до того, як той зможе завдати шкоди системі. Незважаючи на те, що статичний аналіз в цілому збільшив відсоток виявлень шкідливих файлів (в тому числі відсутніх в сигнатурної базі), він також має низку недоліків. Основний з них - це обмеженість методу при ідентифікації атак, в яких, наприклад, експлуатуються невідомі уразливості в системному або прикладному програмному забезпеченні. В цьому випадку статичні властивості та інструкції, які використовуються зараженим файлом, з точки зору евристичного ядра можуть нічим не відрізнятися від інструкцій в легітимних файлах. Не завжди основним вектором атаки є заражені виконувані файли. Дуже часто атаки на кінцеві станції йдуть через експлуатацію вразливостей в системному і прикладному програмному забезпеченні. Починаючи від атак на вразливості браузерів, коли користувач завантажує заражену веб-сторінку, і закінчуючи доставкою шкідливої корисного навантаження на кінцеву станцію через уразливості мережевих протоколів і операційних систем. В цьому випадку недостатньо просто перехоплювати і аналізувати заражений файл - необхідно забезпечувати захист мережевих з'єднань, аналізуючи мережевий трафік, що приходить і виходить з кінцевої станції. В рамках такого підходу до функціональності класичного антивіруса додаються технології мережевого захисту, такі як міжмережевий екран, система запобігання вторгнень і система контролю підключаються до кінцевої станції пристроїв. Саме з цього моменту формується новий тип продуктів - платформа захисту кінцевих станцій, або EndpointProtectionPlatform (EPP). EndpointProtectionPlatform - це система комплексного захисту кінцевої станції, що включає в себе як класичну функціональність антивірусного захисту, так і розширені технології безпеки -

персональні міжмережеві екрани, системи запобігання вторгнень, системи контролю портів і пристроїв, що підключаються, системи шифрування дисків та ін.З певного моменту більшість EPP-рішень перестали задовольняти сучасним вимогам до безпеки кінцевих станцій. В першу чергу це було пов'язано з ростом спрямованих атак, які в основному використовують уразливості нульового дня і відрізняються масовістю завдяки використанню ботнетів і внутрішньої архітектури горизонтального поширення. Також необхідно відзначити окремий клас загроз - кріптолокеров (або шифрувальників), які в принципі, з точки зору системного програмного забезпечення, не роблять нічого протиправного. Відмінною рисою всіх цих атак є те, що вони не використовують відомі підходи і проломи, а експлуатують ще невідомі уразливості і способи свого поширення. Безумовно, EPP-рішення були змушені еволюціонувати, щоб відповідати сучасним викликам в сфері захисту кінцевих станцій. Підсумком такого еволюційного розвитку стала поява нових систем, об'єднаних під загальною назвою - NGEPP. NGEPP (NextGenerationEndpointProtectionPlatform) - це системи захисту кінцевих станцій, які крім базової функціональності класичного антивіруса, захисту мережі та контролю портів володіють розширеними функціями для боротьби з сучасними загрозами. Додатковими системами, що розширюють можливості класичних EPP-систем, можуть бути: Системи емуляції проходять файлів в пісочниці (sandboxing) для боротьби з погрозами нульового дня. Системи Anti-Bot для боротьби з ботнетами, засновані на аналізі патернів трафіку і визначення в них бот-активності. EDR-системи (EndpointDetectandResponse) - системи реактивної захисту кінцевих станцій, що відповідають за розслідування інцидентів шкідливої активності і подальшого відновлення системи. Більш докладно про ці системи можна дізнатися з нашого недавнього Огляду ринку EndpointDetectionandResponse (EDR). Системи контролю додатків, які відповідають за блокування недовірених додатків (у тому числі на основі поведінкової аналітики), не дозволяючи останнім впливати на основні

процеси та критичні дані. Системи захисту пам'яті, проактивно блокують підозрілу активність при зверненні додатків до оперативної пам'яті. Системи захисту даних, що включають в себе системи резервного копіювання, системи шифрування даних, системи запобігання витокам і системи боротьби з фішингом.

1.3. Мета та завдання захисту кінцевих точок корпоративної інформаційної системи.

Однією з різновидів Корпоративних Інформаційних Систем є рішення класу ERP (EnterpriseResourcePlanningSystem) .

Сучасні ERP-системи призначені для побудови єдиного інформаційного простору підприємства і ефективного управління всіма ресурсами компанії, пов'язаними з виробництвом, продажами та обліком замовлень.

Рішення класу ERP (EnterpriseResourcePlanningSystem) забезпечують повну функціональність для управління всією адміністративною і операційною діяльністю компанії, об'єднуючи у єдиний ланцюжок фінансовий облік, процеси збуту, виробництва, управління матеріальними потоками, планування і взаємодії з постачальниками і партнерами.

В якості платформи для побудови ERP-проектів Група Смарт Технології використовує систему SAP, яка є визнаним лідером в класі програмного забезпечення для управління бізнесом.

Впровадження ERP-системи дозволить вашій компанії підвищити ефективність діяльності і зміцнити конкурентоспроможність, а також ви зможете:

приймати виважені управлінські рішення, грунтуючись на точних і актуальних даних

планувати і моделювати різні варіанти розвитку вашої компанії

швидко і ефективно вирішувати оперативні питання управління фінансовими потоками

аналізувати витрати і контролювати відхилення

контролювати реальні витрати, доходи і прибуток

Першим і основним елементом інформаційної системи управління підприємством є система управління бізнес процесами підприємства – це система класу ERP (EnterpriseResourcesPlanning – Ціанування ресурсів підприємства). Основним призначенням ERP систем є автоматизація процесів планування, обліку і управління за основними напрямками діяльності підприємства і тому ERP-системи – системи планування ресурсів підприємства), в загальних рисах можна розглядати як інтегровану сукупність наступних основних підсистем:

управління фінансами;

управління матеріальними потоками;

управління виробництвом;

управління проектами;

управління сервісним обслуговуванням;

управління якістю;

управління персоналом.

Новий якісний етап у розвитку систем управління підприємствами виражає концепцією ERP II (2001 р.). Під системами такого класу розуміють бізнес – стратегію і набір додатків, орієнтованих на особливості конкретної галузі і підвищують цінність компанії для клієнтів і власників за рахунок підтримки і оптимізації оперативних і фінансових процесів спільної роботи підрозділів усередині підприємства або декількох підприємств. Спільна робота підприємства та його партнерів реалізується за рахунок переходу від закритої архітектури традиційних ERP – систем до відкритої компонентної Web – архітектурі. В якості підсистем використовуються CRM (

CustomerRelationshipManagement – управління відносинами з клієнтами) і SCM (SupplyChainManagement – управління ланцюгами поставок).

Системи класу ERP називають також корпоративними інформаційними системами (КІС), так як вони охоплюють автоматизацією практично всі сфери діяльності підприємства (корпорації).

Другим елементом є системи автоматизації проектно конструкторської діяльності та технологічної підготовки виробництва (САПР / АСТПП – CAD / CAM / CAE / PDM), що забезпечують зниження часу виробничого циклу і підвищення якості продукції.

Третій елемент – системи управління технологічним процесом виробництва. Сполучне програмне забезпечення забезпечує взаємодію всіх раніше описаних рішень в рамках єдиної інформаційно – аналітичної системи управління підприємством.

Сполучне програмне забезпечення забезпечує взаємодію всіх вище описаних елементів

Системами автоматизації підприємства, які найбільш користуються попитом є ERP-системи.

Рис. 1. 1. Функціональний склад ERP

Завдання інформаційних систем

Корпоративні системи дозволяють вирішити такі завдання:

гарантувати необхідну якість управління підприємством;

підвищити оперативність та ефективність взаємодії між підрозділами;

забезпечити керованість якістю продукції, що випускається;

збільшити економічну ефективність діяльності підприємства;

створити систему статистичного обліку на підприємстві;

здійснювати прогноз розвитку підприємства;

створити систему стратегічного і оперативного планування, систему прогнозування.

Системи обробки даних призначені для обліку та оперативного регулювання господарських операцій, підготовки стандартних документів для зовнішнього середовища. Горизонт оперативного управління господарськими процесами, становить від одного до кілька днів і реалізує реєстрацію і обробку подій, наприклад оформлення і моніторинг виконання

замовлень, прихід і витрата матеріальних цінностей на складі, ведення табеля обліку робочого часу і т.д. Ці завдання мають ітеративний, регулярний характер, виконуються безпосередніми виконавцями господарських процесів і пов'язані з оформленням і пересиланням документів відповідно до чітко визначеними алгоритмами. Результати виконання господарських операцій через екранні форми вводяться в базу даних. Інформаційні системи управління орієнтовані на тактичний рівень управління: середньострокове планування, аналіз і організацію робіт протягом декількох тижнів, наприклад аналіз і планування поставок, збуту, складання виробничих програм. Для даного класу задач характерні регламентованість формування результуючих документів і чітко визначений алгоритм розв'язання завдань, наприклад звід замовлень для формування виробничої програми і визначення потреби в комплектуючих деталях і матеріалах на основі специфікації виробів. Рішення подібних завдань призначено для керівників різних служб підприємств. Завдання вирішуються на основі накопиченої бази оперативних даних.

Системи підтримки прийняття рішень використовуються в основному на верхньому рівні управління має стратегічну довгострокову знання протягом року або декількох років. До таких завдань належать формування стратегічних цілей, планування, залучення ресурсів, джерел фінансування, вибір місця розміщення підприємств і т.д. Рідше завдання класу СППР зважуються на тактичному рівні. Завдання СППР мають, як правило, нерегулярний характер.

Для задач СППР властиві недостатність наявної інформації, її суперечливість і нечіткість, перевага якісних оцінок цілей і обмежень, слабке формулювання алгоритмів рішення. Як інструменти узагальнення найчастіше використовуються засоби складання аналітичних звітів довільної форми, методи статистичного аналізу, експертних оцінок і систем, математичного та імітаційного моделювання. При цьому застосовуються бази знань про правила та моделях прийняття рішень.

Інформаційна система, яка включає в себе всі три типи перерахованих інформаційних систем, називається стратегічною інформаційною системою.

1.4. Аналіз існуючих технологій захисту кінцевих точок корпоративної інформаційної системи

Корпоративні інформаційні системи (КІС) грають дуже велику роль в наш час. КІС - основна рушійна сила НТР (науково-технічна революція) і розвитку світової сучасної економіки. Завдяки численним дослідам доведено, що правильно підібрана і впроваджена КІС покращує, причому істотно, керованість підприємства, підвищує ефективність роботи підприємства. У зв'язку з цим виникає питання: яку КІС краще всього вибрати для автоматизації діяльності підприємства? Вибір КІС є складним процесом для впровадження через декількох критеріїв:

високa вартість продукту;

велика різноманітність КІС;

тривалість підготовки по впроваджуваного продукту фахівцями, зазвичай від півроку до року;

тривалість самого впровадження, зазвичай від кількох місяців до кількох років.

Будь-яка з сучасних корпоративних інформаційних систем - це інструмент збільшення ефективності, якості управління, прийняття рішень на основі автоматизованої обробки інформації. При грамотному впровадженні КІС забезпечує втілення програм і стратегічних ініціатив підприємства в дійсність. Також інвестування в КІС має окупитися через вдосконалення управлінськихпроцесів, скорочення витрат, підвищення ефективності виробництва.

У виборі КІС має бути зацікавлене керівництво підприємства. Впровадження КІС змінює розподіл ролей і робочий процес на підприємстві. впровадження КІС змінює характер службових обов'язків.

В даний час існує близько 100 ППП управління промисловими і торговими підприємствами. Всього існує 500 фірм, які займаються створенням ПО для корпоративних клієнтів.

Найбільш відомими програмними продуктами управління підприємствами в країнах СНД є: Галактика, БОС-Корпорація, 1С, БЕСТ-ПРО, Еверест; Компас. Нижче розглянемо деякі з ППП.

Галактика. Корпорація Галактика працює на ринку економічного програмного забезпечення більше 13 років. ПО Галактика призначений для великих і середніх підприємств. Корпорація пропонує галузеві рішення і концентрує свої зусилля на їх просуванні в наступних галузях: нафтогазової; зв'язку та телекомунікацій; харчовий; вугільної; лісової; деревообробної; целюлозно-паперової; металургії; торгівлі; енергетиці та атомній промисловості

Галактика ERP - автоматизована система управління, що дозволяє в єдиному інформаційному просторі оперативно вирішувати головні управлінські завдання, а також забезпечувати персонал підприємства різного рівня управління необхідною і достовірною інформацією для прийняття управлінських рішень.

Система комплексної автоматизації управління підприємством «Галактика» - повнофункціональним рішенням, в якому реалізований весь спектр управлінських задач: планування всіх видів ресурсів, оперативне управління діяльністю підприємства, наскрізний оперативний і бухгалтерський облік, фінансовий і економічний аналіз

БОС-Корпорація. Призначена для управління фінансово-господарською діяльністю середніх та великих виробничих, державних і торгових підприємств і організацій. У ній автоматизовані різноманітні види обліку (бухгалтерський, оперативний і виробничий), фінансове і виробниче планування, управління персоналом

В функціональний склад БОС-Корпорація входять наступні модулі: Головна книга, Операції на розрахункових рахунках, Операції з готівковими

коштами, Журнал господарських операцій та розрахунків, Фінансовий контролінг, Управління закупівлями, Управління запасами, Управління продажами, Основні засоби, Штатний розклад, Кадри, Зарплата.

БЕСТ. ПО БЕСТ-ПРО позиціонується для застосування на середніх і великих підприємствах. є версія для промислових підприємств і для оптової торгівлі, готується окрема розробка для супермаркетів.

До складу БЕСТ-ПРО входять підсистеми управління запасами, закупівлями і продажами, контролю договірнихзобов'язань, фінансів, взаєморозрахунків з постачальниками і покупцями. Крім того, є блоки обліку кадрів, зарплати, основних фондів, бухгалтерського та податкового обліку. Система має відкриту архітектуру, структура БД входить в комплект поставки. Користувачі і / або партнери можуть робити власні доробки системи (нові модулі, звіти, функції)

1С. ПО фірми 1С позиціонується компанією в 2-х напрямках. По-перше, як універсальний засіб створення прикладних рішень для автоматизації економічної діяльності (платформа 1С: Підприємство) в цьому випадку система використовується для оптової та роздрібної торгівлі, для змішаних форм підприємств, для обліку послуг і т. д. По-друге, як готові рішення, що поставляються 1С.

У систему програм «1С: Підприємство 8» входить платформа та прикладні рішення, які розроблені на її основі, які призначені для автоматизації роботи організацій.

1С Підприємство 8 - це система програм, яка була розроблена для автоматизації обліку підприємств. При розробці враховувалися побажання користувачів. Завдяки великій кількості впроваджень існує можливість постійного вдосконалення продуктів. Програми відповідають законодавству і визнані стандартом обліку в нашій країні.

Як відомо, для вибору програми потрібно звернути увагу на рівень автоматизації. існують рішення для невеликих компаній і для великих корпорацій.

ERP-система - це інтегрована система на базі IT, яка призначена для управління внутрішніми і зовнішніми ресурсами підприємства. такими ресурсами можуть бути фізичні активи, фінансові, людські та матеріально-технічні ресурси.

Мета ERP-системи - це взаємодія потоків інформації між усіма господарськими підрозділами всередині підприємства, а також інформаційна підтримка зв'язків з іншими підприємствами. ERP-система формує єдиний інформаційний простір підприємства і будується на централізовану базу даних. За допомогою ERP-системи можна використовувати одну інтегровану програму замість деякого числа розрізнених програм. Така система може управляти бухгалтерським обліком, запасами, логістикою і доставкою, дистрибуцією, виставленням рахунків-фактур.

ERP-система являє собою віртуальну проекцію компанії.

За допомогою таких програм можна проводити проектні роботи з доопрацювання та тестування програми, а також з навчання персоналу. Перш за все, комплексну автоматизацію потрібно починати з ділянок обліку, які необхідно автоматизувати в першу чергу. Потрібно визначити, чи підійде обрана програма для повної автоматизації, чи допоможе вона вирішити поточні завдання або ж навпаки - ускладнить роботу. після цього, можна приймати рішення про вибір ПП.

При покупці такої системи, потрібно звертати увагу на можливості настройки конфігурації до специфіки ведення обліку на даному підприємстві. Фірмою «1С» розроблені галузеві програми, які допомагають вирішувати вузькоспеціальні завдання обліку. також існує можливість платформи, яка дозволяє створювати необхідні організації індивідуальні рішення.

1С Підприємство 8 - це система прикладних рішень, які побудовані на єдиній технологічній платформі за єдиними принципами. Керівник підприємства має можливість вибрати рішення, яке буде відповідати актуальним потребам, яке в майбутньому буде розвиватися в міру росту підприємства і у міру розширення завдань автоматизації. завдання обліку і управління відрізняються в залежності від необхідного рівня автоматизації, роду діяльності підприємства, від його галузі, розміру, структури підприємства, специфіки продукції, послуг, що надаються. Програми, яка б була призначена для масового використання і задовольняла б при цьому потребам більшості підприємств не існує. Керівнику необхідно рішення, яке б відповідало специфіці саме його підприємства. І великим плюсом при виборі рішення є застосування певного масового перевіреного продукту. Поєднання всіх перерахованих потреб забезпечує система програм "1С: Підприємство».

1С Підприємство 8 - це універсальна програма масового призначення, яка призначена для автоматизації бухгалтерського і податкового обліків і включає підготовку регламентованої звітності в організаціях, які здійснюють будь-які види комерційної діяльність. Для розрахунку собівартості паливної

складової якраз необхідна така програма, так як ТЕС здійснює комерційну діяльність - виробництво, надання послуг, торгівлю.

В 1С Підприємство 8 реалізовані відповідно до чинного законодавства Республіки Казахстан бухгалтерський і податковий обліки.

Головною складовою управління є управлінський облік і він необхідний для управління підприємством. Автоматизація управлінського обліку вже здійснюється на платформі 1С Підприємства. серед явних плюсів 1С можна відзначити наступні:

- низька вартість експлуатації і низька вартість впровадження;
- можливість розробки власних бухгалтерських, облікових завдань на платформі 1С;
- максимально оперативна і якісна підтримка рішень з боку Компанії 1С.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ КІНЦЕВИХ ТОЧОК НА ПРИКЛАДІ MCAFEE ENDPOINT SECURITY

2.1. Призначення, основні функції та склад програмного комплексу McAfeeEndpointSecurity

У сучасних компаніях питаннями безпеки може займатися один або кілька відділів. В організаціях корпоративного типу за безпеку нерідко відповідають відразу кілька відділів: IT-адміністратори, відділ операцій щодо забезпечення безпеки та ін. При виборі платформи для захисту кінцевих точок ваші головні вимоги до її функцій і результатами роботи природним чином залежать від вашої посади в компанії, відрізняючись від пріоритетів інших відділів компанії.

Використовуване вами рішення для захисту кінцевих точок має відповідати вашим найголовнішим пріоритетам. Незалежно від ваших функціональних обов'язків в компанії, рішення McAfeeEndpointSecurity відповідає вашим конкретним насущним завданням, починаючи від запобігання і пошуку загроз до індивідуальної настройки засобів захисту. Завдяки McAfeeEndpointSecurity ви зможете забезпечити своїм користувачам безперебійну роботу систем, знайти більше можливостей для автоматизації операцій і спростити складні робочі процеси.

McAfeeEndpointSecurity дає клієнтам можливість реагувати на загрози і управляти життєвим циклом захисту від загроз за допомогою засобів попереджувальної захисту і відновлення систем. повернення систем в працездатний стан здійснюється за допомогою функції автоматичного відкоту, що дозволяє підвищити продуктивність праці користувачів і адміністраторів. завдяки автоматичного відкоту їм не доведеться витрачати робочий час на очікування внесення виправлень, на роботу по відновленню

систем або на переустановку образів на заражених системах.Між кінцевими точками і інтегрованим рішенням McAfee MVISION EDR відбувається обмін даними про глобальні загрози та інформацією про локальні події, отримуючи в реального часу. Це дозволяє збирати відомості про події загроз, виявляти і запобігати загрозі, що намагаються уникнути виявлення, і зіставляти їх з матрицею MITRE ATT & CK для проведення подальших розслідувань. Для спрощення процесів управління використовується консоль централізованого управління, що дозволяє вибрати один з трьох видів розгортання: локальне, у вигляді SaaS або у віртуальному середовищі.

Для збору інформації про загрози на різних рівнях взаємодії в McAfeeEndpointSecurity використовується один-єдиний програмний агент, що дозволяє усунути надмірність, притаманну середах, в яких використовується велика кількість різних спеціалізованих продуктів. Результатом став комплексний підхід до забезпечення безпеки, що усуває необхідність в ручному зіставленні загроз і дозволяє автоматично доводити до відомості фахівців з реагування на інциденти інформацію, що вимагає подальшого розслідування. Завдяки функції StoryGraph дані про події загроз представляються в простому і наочному форматі, який візуалізує інформацію про погрози і дає адміністраторам можливість без праці аналізувати їх і шукати джерела шкідливих об'єктів.

Для захисту від нових складних загроз організаціям допоможуть також додаткові засоби захисту від складних загроз, пропоновані в рамках інтегрованої платформи McAfeeEndpointSecurity, такі як DynamicApplicationContainment (DAC - динамічне стримування додатків) .1 Так, наприклад, DAC аналізує потенційно небезпечне ПО і інші нові шкідливі програми і ізолює їх з метою запобігання заражень. Захист від складних загроз забезпечує також технологія RealProtect, що дозволяє виявляти шкідливе ПЗ «нульового дня» і оптимізувати процеси виявлення загроз шляхом класифікації поведінки шкідливих програм за допомогою

методів машинного навчання. Йдеться про класифікацію поведінки без використання сигнатур, яка виконується в хмарі і відрізняється низьким ресурсопотреблением на клієнтському комп'ютері, причому виявлення загроз відбувається в режимі майже реального часу. Одержану аналітичну інформацію можна використовувати для створення ознак атаки і ознак злому. З конкретних областей застосування аналітичної інформації можна назвати виявлення загроз в міжвузловими трафіку, виявлення «нульових пацієнтів», атрибуцію загроз, проведення компьютернотехніческіх експертиз і усунення вразливостей. Крім того, з часом швидкість аналізу, проведеного за допомогою RealProtect, збільшується, тому що механізм класифікації поведінки автоматично вдосконалюється, а набір правил, дозволяють виявляти схожі атаки шляхом аналізу коду (як статичного, так і під час виконання), поповнюється. Нарешті, коли реальність загрози підтверджується, клієнт відновлює кінцеву точку, відкочуючись її до останньої робочої конфігурації. Це дозволяє без зволікання запобігти зараженню кінцевої точки і заощадити час адміністраторів ІБ.

Чим краще інформація про погрози, тим краще результати. Обмінюючись (в режимі реального часу) отриманої в ході спостережень інформацією з великою кількістю підключених до нього технологій для захисту кінцевих точок, McAfeeEndpointSecurity забезпечує взаємодію цих технологій і прискорює процес виявлення випадків підозрілої поведінки, забезпечує більш ефективну координацію різних засобів захисту і підвищує рівень захищеності від цілеспрямованих атак і загроз "нульового дня». Збір таких даних, як хеш файлу, URL-адресу джерела, події AMSI і PowerShell, і передача їх не тільки в інші засоби захисту, але і на клієнтський інтерфейс і інтерфейс управління, 4 McAfeeEndpointSecurity допомагає користувачам визначати характер атак і постачати адміністраторів практично застосовної інформацією про загрози для проведення комп'ютерно-технічної експертизи.

Эффективность интеллектуальных средств защиты может быть сведена на нет низкой скоростью сканирования, долгим процессом установки или сложностью в управлении. Для экономии рабочего времени пользователей в McAfeeEndpointSecurity используется общий уровень обслуживания и наш новый модуль защиты от вредоносного ПО, помогающий сократить объем ресурсов иэнергопотребления, необходимый для работы систем пользователей. Сканирование конечных точек не влияет на производительность труда пользователей, поскольку выполняется только в режиме простоя устройства и автоматически возобновляется после его перезагрузки или выключения. Адаптивный характер процесса сканирования помогает также снизить нагрузку на ЦП: поняв, какие процессы и источники являются надежными, модуль сканирования ограничивается только теми процессами, которые кажутся подозрительными или имеют неизвестные источники. BMcAfeeEndpointSecurity имеется встроенный брандмауэр, с помощью McAfeeGTI обеспечивающий защиту конечных точек от бот-сетей, распределенных атак типа «отказ вобслуживании» (DDoS), сложных постоянных угроз (APT) и опасных веб-соединений.

Из-за стремительного роста числа защитных продуктов с частично совпадающими функциями и отдельными консолями управления многим организациям оказывается непросто составить точную картину потенциальных атак. В случае McAfeeEndpointSecurity надежность защиты в долгосрочной перспективе обеспечивается благодаря открытой и расширяемой платформе, служащей фундаментом для централизации управления как уже имеющимися, так и будущими решениями для защиты конечных точек. Для обеспечения взаимодействия с уже приобретенными организацией техническими решениями на данной платформе используется уровень обмена данными DataExchangeLayer. Его интегрированная архитектура легко объединяется с другими продуктами McAfee, что сокращает число оставшихся брешей в защите, несовместимых технологий и избыточность. Снижение эксплуатационных расходов и

упрощение процессов управления стимулирует рост производительности. Для еще большего упрощения работы можно использовать программное обеспечение McAfeeePolicyOrchestrator® (McAfee ePO™), позволяющее осуществлять мониторинг происходящего, развертывание средств защиты и управление конечными точками из единой консоли. Наличие настраиваемых представлений и эффективных рабочих процессов на понятном языке позволяет быстро оценивать уровень защищенности, выявлять зараженные устройства и снижать риски путем помещения систем в карантин, прекращения вредоносных процессов или блокирования попыток эксфильтрации данных. Кроме того, решение позволяет централизованно управлять всеми конечными точками, другими технологиями McAfee и более чем 130защитными решениями сторонних поставщиков.

Функція RealProtect

Модуль классификации поведения с помощью методов машинного обучения позволяет обнаруживать угрозы «нулевого дня» в режиме почти реального времени и получать информацию об угрозах для принятия конкретных мер реагирования.

Автоматически совершенствует механизм классификации поведенческих признаков, позволяющий определять угрозы по поведению и добавлять правила для выявления похожих атак в будущем.

Функція Защита конечных точек от целенаправленных атак

Позволяет сократить разрыв между обнаружением угрозы и ее сдерживанием с нескольких дней до нескольких миллисекунд.

Собирая информацию об угрозах из разных источников, McAfeeThreatIntelligenceExchange дает компонентам системы безопасности возможность мгновенно обмениваться информацией о новых и сложных многоэтапных атаках.

Регистрация событий с помощью AMSI и PowerShell позволяет обнаруживать и отражать бесфайловые атаки и атаки, проводимые с использованием сценариев.

Функція Интеллектуальное, адаптивное сканирование

Повышает уровень производительности и быстродействия благодаря отказу от сканирования надежных процессов и приоритизации подозрительных процессов и приложений.

Адаптивные функции поведенческого сканирования позволяют осуществлять мониторинг происходящего, выявлять угрозы и при обнаружении подозрительной активности передавать эту информацию на следующий уровень.

Функція Устранение угроз путем отката

Автоматически отменяет изменения, внесенные вредоносными программами, и возвращает системы в их последнее работоспособное состояние, поддерживая тем самым производительность труда пользователей.

Функція Упреждающая веб-защита

Обеспечивает безопасный просмотр веб-сайтов благодаря функциям веб-защиты и фильтрации веб-трафика на конечных точках.

Функція Динамическое сдерживание приложений

Обеспечивает защиту от программ-вымогателей и потенциально опасных программ, а также помогает выявлять «нулевых пациентов».

Функція Блокирование агрессивных сетевых атак

На основе оценок репутации, получаемых с помощью McAfee GTI, встроенный брандмауэр обеспечивает защиту конечных точек от бот-сетей, DDoS-атак, сложных постоянных угроз и подозрительных веб-подключений.

Во время запуска системы брандмауэр пропускает только исходящий трафик, обеспечивая тем самым защиту конечных точек, находящихся за пределами корпоративной сети.

Функція StoryGraph

Дает администраторам возможность быстро определить местонахождение, причину и продолжительность заражения, чтобы проанализировать угрозу и быстрее принять меры реагирования.

Функція Централизованное управление (платформа McAfee ePO) с несколькими вариантами развертывания

Эта по-настоящему централизованная платформа управления позволяет обеспечить более полный сбор информации о происходящем, упростить операции, повысить производительность труда ИТ-подразделений, объединить процессы ИБ и снизить затраты.

Функція Открытая, расширяемая платформа для защиты конечных точек

Интегрированная архитектура дает средствам защиты конечных точек возможность взаимодействовать друг с другом и обмениваться информацией с целью обеспечения более надежной защиты.

Способствует снижению эксплуатационных расходов за счет устранения избыточности и оптимизации процессов.

Легко интегрируется с другими продуктами McAfee и продуктами сторонних поставщиков, сокращая бреши в защите.

McAfeeEndpointSecurity дает сегодняшним специалистам по ИБ все необходимое для того, чтобы лишить злоумышленников преимущества первого удара: набор интеллектуальных, взаимодействующих друг с другом

средств защиты и платформу для упрощения сложных сред. Высокие показатели надежности, быстродействия и эффективности обнаружения угроз, подтвержденные результатами независимых тестов, позволяют организациям защитить своих пользователей, повысить производительность труда и обрести уверенность в собственной защищенности. Компания McAfee, лидер на рынке безопасности конечных точек, предлагает полный спектр решений для обеспечения эшелонированной обороны, сочетающих в себе надежные средства защиты и эффективную систему управления. Сокращение времени для принятия мер защиты, повышенный уровень быстродействия и эффективное управлениепозволяют специалистам по безопасности выявлять больше угроз, делая это быстрее и с меньшими затратами ресурсов.

Всредах с актуальными версиями программного обеспечения McAfeeePO, McAfeeVirusScanEnterprise и McAfeeAgent автоматизированный перенос имеющихся политик в McAfeeEndpointSecurity с помощью нашей утилиты занимает не более 20 минут.

Кроме того, McAfeeEndpointSecurity даст вам следующие преимущества:

сканирование не снижает производительность труда пользователей;

наличие более точных данных для проведения компьютерно-технической экспертизы, представляемых в наглядном формате StoryGraph, позволяет быстро разобраться в ситуации и упрощает задачу проведения расследований с целью ужесточения ваших политик безопасности;

функция отката автоматически отменяет внесенные вредоносными программами изменения и поддерживает системы в работоспособном состоянии;

меньшее количество используемых агентов и отказ от сканирований позволяет сократить объем вводимых вручную данных;

взаимодействие средств защиты позволяет эффективнее бороться со сложными угрозами;

к вашим услугам платформа нового поколения, легко интегрируемая с другими нашими решениями для защиты от сложных угроз и решениями (EndpointDetectionandResponse— обнаружение угроз и реагирование на инциденты на конечных точках).

2.2. Призначення, основні функції та принципи роботи модуля “Попередження загроз”.

McAfeeEndpointSecurity – это расширяемое комплексное решение для обеспечения безопасности, которое защищает серверы, компьютерные системы, ноутбуки и планшеты от известных и неизвестных угроз. Эти угрозы включают в себя вредоносные программы, подозрительные соединения, небезопасные веб-сайты и загруженные файлы.

EndpointSecurity обеспечивает работу нескольких технологий для обеспечения безопасности, которые обмениваются данными в режиме реального времени, чтобы анализировать угрозы и защищать от них.

Принцип работы модуля предотвращение угроз

Модуль предотвращение угроз состоит из двух компонентов: расширения, установленного на сервере McAfeeePO, и ПО для защиты (включая ядро сканера и файлы содержимого), установленного в клиентской системе. Кроме того, в клиентской системе установлен модуль EndpointSecurity: общие параметры, который включает в себя Клиент EndpointSecurity. С помощью McAfeeAgent клиентское программное обеспечение связывается с McAfeeePO для настройки и отправки отчетов, с McAfee® GlobalThreatIntelligence™ (McAfee GTI) для получения

информации о репутации, а также с McAfeeLabs для обновления файла содержимого и ядра.

EndpointSecurity состоит из следующих модулей безопасности.

предотвращение угроз – не позволяет угрозам проникнуть в систему, автоматически проверяет файлы при доступе и выполняет целевые проверки на наличие вредоносных программ в клиентских системах.

Принцип работы EndpointSecurity

EndpointSecurity перехватывает угрозы, следит за общим состоянием системы и составляет отчеты по обнаружениям и состоянию. Для выполнения этих задач клиентское программное обеспечение устанавливается в каждую систему. Вы или системный администратор можете установить один или несколько модулей EndpointSecurity, настроить функции и управлять обнаружениями. Обычно клиентское программное обеспечение работает в фоновом режиме и не требует никаких действий со стороны пользователя.

Пример рабочего процесса – защита доступа

Модуль предотвращение угроз следует этой базовой процедуре при защите файлов, разделов реестра, значений реестра, процессов и служб.

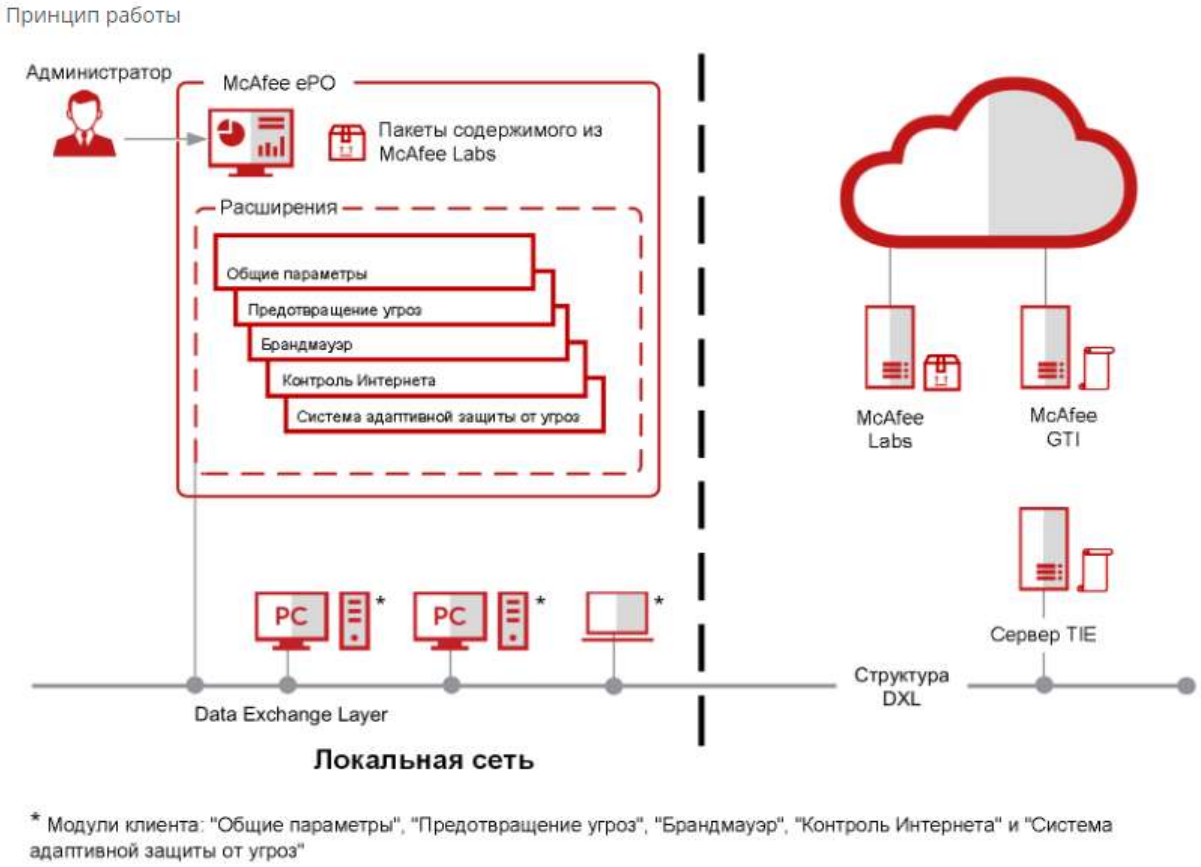
1. Администратор настраивает правила защиты в политике модуля Защита доступа в McAfeeePO и применяет ее в клиентской системе.

2. Администратор загружает последние версии файлов содержимого в McAfeeLabs.

3. Пользователь загружает безопасную (не вредоносную) программу, MyProgram.exe, в Интернете и запускает ее. MyProgram.exe запускается сама и запускает дочерний процесс под названием AnnoyMe.exe. AnnoyMe.exe совершает попытку внести изменения в операционную систему, чтобы

убедиться в том, что AnnoyMe.exe всегда загружается при запуске. Модуль предотвращение угроз обрабатывает запрос и сопоставляет действие с существующим правилом защиты, определенным McAfee или пользователем. Модуль предотвращение угроз не дает AnnoyMe.exe внести изменения в операционную систему.

4. Модуль Модуль предотвращение угроз регистрирует сведения, а затем создает событие и отправляет его в McAfeeePO.



Регулярное обновление EndpointSecurity позволяет защитить компьютеры пользователей от самых новых угроз.

Клиентское программное обеспечение соединяется с локальным или удаленным сервером McAfeeePO либо напрямую с сайтом в Интернете,

чтобы выполнить обновление. EndpointSecurity проверяет наличие следующих обновлений.

Обновление файлов содержимого, используемых для обнаружения угроз. Файлы содержимого содержат описание угроз, например вирусов и шпионских программ. С обнаружением новых угроз эти описания обновляются.

Обновления компонентов программного обеспечения, например разного рода исправления.

предотвращение угроз в McAfee® EndpointSecurity блокирует проникновение угроз в системы, автоматически проверяет файлы при доступе и выполняет целевой поиск вредоносных программ в клиентских системах.

предотвращение угроз в EndpointSecurity обнаруживает угрозы на основе файлов содержимого безопасности. Обновления содержимого безопасности загружаются автоматически, чтобы обеспечивать защиту от конкретных уязвимостей и блокировать возникающие угрозы.

Модуль предотвращение угроз защищает вашу среду от указанных ниже проблем.

Вирусы, черви и троянские кони

Нарушения защиты точек доступа (нежелательные изменения файлов, общих ресурсов, разделов реестра, параметров реестра). Этот модуль также предотвращает или ограничивает подозрительное поведение процессов и служб.

Средства использования уязвимостей, связанные с переполнением буфера

Недопустимое использование API – злонамеренные вызовы API, выполняемые неизвестными или пораженными приложениями

Вторжения в сеть, например атаки, нацеленные на снижение пропускной способности, и сетевые атаки типа "отказ в обслуживании"

Потенциально нежелательные коды и программы

Угрозы, связанные с уязвимостями

Средства использования уязвимостей нулевого дня

Угрозы в сценариях, созданных не на основе браузера, например PowerShell, JavaScript и VBScript

Развернуть модуль предотвращение угроз в клиентских системах и управлять им можно с помощью McAfeeePO.

Основные функции модуля предотвращение угроз

Основные функции модуля предотвращение угроз направлены на защиту вашей среды от угроз, обнаружение в ней вредоносных программ, а также исправление ошибок путем очистки или восстановления зараженных файлов.

Описанные ниже функции модуля предотвращение угроз обеспечат защиту ваших систем от вторжений до того, как они получат доступ к вашей среде.

Защита доступа– защита от внесения нежелательных изменений в клиентские системы путем ограничения доступа к определенным файлам, общим ресурсам, разделам реестра, параметрам реестра, а также предотвращение или ограничение угрожающего поведения процессов и служб.

Предотвращение действий средств использования уязвимостей – модуль предотвращение угроз использует сигнатуры в обновлениях содержимого для защиты от указанных ниже уязвимостей.

Защита от переполнения буфера – останавливает выполнение произвольного кода при переполнении буфера в результате атаки.

Недопустимое использование API – защита от злонамеренных вызовов API, выполняемых неизвестными или вредоносными приложениями в системе.

Предотвращение вторжений в сеть (сетевая IPS) – защита от атак, нацеленных на снижение пропускной способности, и сетевых атак типа "отказ в обслуживании", которые снижают работоспособность сети.

Расширенные правила – предоставляются дополнительные параметры и увеличивается гибкость по сравнению с пользовательскими правилами модуля "Защита доступа". Однако чтобы создать расширенные правила, нужно понимать собственный синтаксис McAfee.

Интерфейс командной строки – полную проверку, быструю проверку, выборочные проверки и обновление содержимого безопасности можно выполнять из командной строки или в рамках развертывания пакетного файла.

Обнаружение

Описанные ниже функции модуля предотвращение угроз позволят обнаруживать угрозы при их возникновении в среде.

Проверка при доступе – проверка на наличие угроз при чтении файлов с диска или их записи на диск. Проверка интегрируется с интерфейсом AntimalwareScanInterface (AMSI), чтобы обеспечить

улучшенную проверку наличия угроз в сценариях, не связанных с браузером.

Проверка по требованию – запуск или планирование предопределенных проверок, включая проверку наличия записей в реестре для шпионских программ, которые не были очищены ранее. Проверки выполняются только при бездействии системы. Чтобы оптимизировать производительность проверки, следует ограничить загрузку ЦП.

Потенциально нежелательные программы – обнаружение потенциально нежелательных программ (например, шпионских программ и программ для показа рекламы), а также предотвращение их запуска в вашей среде.

Карантин – помещение в карантин зараженных элементов, попытка их очистки или восстановления либо их автоматическое удаление.

Панели мониторинга и мониторы – отображение статистики модуля предотвращение угроз, включая продолжительность проверки, состояние обновления содержимого, а также приложения с наибольшим количеством уязвимостей. (Управляемые системы)

Запросы и отчеты – получение подробных сведений о модуле предотвращение угроз, включая количество угроз, выполнение проверки, ответы на обнаруженные угрозы, события сокращения количества ложных положительных результатов, а также уровень чувствительности McAfee GTI. (Управляемые системы)

Защита от вредоносных программ с ранним запуском – поддерживает функцию ELAM, доступную в Windows 8 и более поздних выпусках. ELAM собирает список драйверов устройств, загруженных во время цикла запуска, и проверяет их после запуска служб поиска.

Исправление

Описанные ниже функции модуля модуля предотвращение угроз позволяют устранять проблемы безопасности, обрабатывать обнаруженные угроз, улучшить производительность и усилить защиту.

- Действия – выполнение определенных действий в случае обнаружения угроз.
- Предупреждения – уведомление в случае обнаружения угроз, а также ограничение трафика с помощью фильтров.
- Файлы Extra.DAT – защита от новых угроз (например, масштабной вирусной эпидемии). (McAfeeePOOn-Premises)
- Запланированные проверки – запуск проверок в периоды низких нагрузок позволяет повысить производительность системы и проверок.
- Репозитории содержимого – снижение сетевого трафика через Интернет или внутреннюю сеть предприятия за счет перемещения репозитория файлов содержимого ближе к клиентским системам. (Управляемые системы)
- Файлы журнала (Клиент EndpointSecurity) – предоставление истории обнаруженных элементов, которую можно использовать для определения необходимости изменить настройки, чтобы усилить защиту или повысить производительность системы.
- Панели мониторинга и мониторы – отслеживание операций и использование этой информации для настройки параметров модуля предотвращение угроз. (Управляемые системы)
-

Модуль предотвращение угроз состоит из двух компонентов: расширения, установленного на сервере McAfeeePO, и ПО для защиты (включая ядро сканера и файлы содержимого), установленного в

клиентской системе. Кроме того, в клиентской системе установлен модуль EndpointSecurity: общие параметры, который включает в себя Клиент EndpointSecurity. С помощью McAfeeAgent клиентское программное обеспечение связывается с McAfeeePO для настройки и отправки отчетов, с McAfee® GlobalThreatIntelligence™ (McAfee GTI) для получения информации о репутации, а также с McAfeeLabs для обновления файла содержимого и ядра.

Проверка компьютера на наличие вредоносных программ

Проверка компьютера на наличие вредоносных программ с помощью выбора параметров в Клиент EndpointSecurity или WindowsExplorer.

Типы проверок

EndpointSecurity имеет два типа проверок: проверки при обращении и по требованию.

• Проверка при доступе – администратор настраивает запуск проверок при доступе на управляемых компьютерах. На самостоятельно управляемых компьютерах параметры проверки при доступе настраиваются на странице Настройки. При каждом обращении к файлам, папкам и программам сканер проверки при доступе перехватывает операцию и проверяет объект в соответствии с критериями, определенными в настройках.

• Проверка по требованию

Вручную

Администратор (а в случае системы с самостоятельным управлением – пользователь) настраивает предопределенные или выбор

◦ Предопределенную проверку по требованию можно в любой момент запустить из Клиент EndpointSecurity, нажав и указав тип проверки: Быстрая

проверка запускает быструю проверку наиболее уязвимых для заражения областей системы.

Полная проверка выполняет полную проверку всех областей системы. (Рекомендуется в случае подозрения, что компьютер заражен.)

◦ Щелкните правой кнопкой мыши файл или папку и выберите во всплывающем меню Проверить на наличие угроз, чтобы проверить отдельный файл или папку в любое время через WindowsExplorer.

◦ Настройте выборочную проверку по требованию и запустите ее от имени администратора из Клиент EndpointSecurity:

◦ Выберите Настройки → Общие параметры → Задачи.

◦ Выберите задачу для выполнения.

◦ Нажмите Выполнить сейчас.

Запланированные

Администратор (или пользователь, или самостоятельно управляемая система) настраивает и планирует запуск проверок при обращении на компьютерах.

Перед началом проверки по требованию EndpointSecurity отображает сообщение в нижней части экрана. Пользователь может сразу же начать проверку либо отложить ее, если это разрешено. Настройка и планирование предопределенных проверок по требованию типа Быстрая проверка и Полная проверка:

1. Настройки → Проверка по требованию → вкладка Полная проверка или вкладка Быстрая проверка – настройка проверок по требованию.

2. Настройки → Common → Задачи – позволяет планировать проверки по требованию.

Запуск полной проверки или быстрой проверки

Используйте Клиент EndpointSecurity, чтобы вручную запустить быструю проверку или полную проверку на компьютере.

Подготовка

Необходимо установить модуль предотвращение угроз.

Поведение при полной проверке и быстрой проверке зависит от заданных параметров. При наличии учетных данных администратора можно изменить или запланировать эти проверки в параметрах Проверки по требованию.

В зависимости от настройки параметров вы можете управлять обнаружением угроз из Клиент EndpointSecurity.

Политики позволяют настроить, применить и задействовать параметры для управляемых систем своей среды. Политики представляют собой наборы параметров, которые можно создавать, настраивать, сохранять и принудительно применять. Большинство параметров политик соответствуют параметрам, настраиваемым в Клиент EndpointSecurity. Другие параметры политик – это основной интерфейс для настройки программного обеспечения. Ваш управляемый продукт добавляет следующие категории в каталог политик. В каждой категории доступны свои параметры.

2.3. Призначення, основні функції та принципи роботи модуля “Міжмережевий екран”.

Брандмауэрзащищает информацию и предотвращает взлом систем, сетевых ресурсов и приложений.

брандмауэрработает как фильтр между компьютером и сетью или Интернетом. Брандмауэр проверяет весь входящий и исходящий трафик на пакетном уровне. При изучении каждого поступающего или отправляемого

пакета брандмауэр обращается к своему списку правил, который представляет собой набор критериев со связанными действиями. Если пакет соответствует всем критериям правила, брандмауэр действует согласно этому правилу, блокируя или разрешая пакет через брандмауэр.

Брандмауэрполностью интегрируется сMcAfeeeРОи использует структуру этого приложения для распространения и принудительного применения политик. Этот подход позволяет использовать единую систему управления для масштабного развертывания до 100 000 систем на разных языках в рамках всего предприятия.

Принцип работы правил брандмауэра

Правила программыбрандмауэропределяют, каким образом должен обрабатываться сетевой трафик. Каждое правило включает набор условий, которым должен соответствовать трафик, а также действие для разрешения или блокировки трафика.

Когда программа брандмауэр обнаруживает трафик, отвечающий условиям правила, она выполняет соответствующее действие.

Область применения правил может быть широкой (например, весь IP-трафик) или узкой (например, определенное приложение или служба), также имеется возможность задавать параметры. Для упрощения управления можно группировать правила в соответствии с функциями, службами или приложениями. Как и отдельные правила, группы правил можно задавать в соответствии с сетью, типом передачи, приложением, планированием и местоположением.

Программабрандмауэриспользует приоритет применения правил:

Брандмауэрприменяет правило, находящееся вверху списка правил брандмауэра.

Еслитрафик отвечает условиям этого правила, программа брандмауэр разрешает или блокирует этот трафик. Программа не пытается применить другие правила из списка.

Если трафик не отвечает условиям первого правила, программа брандмауэр обращается к следующему правилу в списке и действует таким образом до тех пор, пока не найдет правило, которому соответствует трафик.

Если трафик не соответствует ни одному из правил, брандмауэр автоматически блокирует его.

Если включен адаптивный режим, для трафика создается разрешающее правило. Иногда перехваченный трафик соответствует нескольким правилам в списке. В этом случае принцип приоритета подразумевает, что программабрандмауэрприменяет только первое правило, которому соответствует трафик.

Рекомендации

В соответствии с политикой правил брандмауэра конкретные правила следует размещать в начале списка, а общие – в конце. Такой порядок позволяет программе брандмауэр надлежащим образом выполнять фильтрацию трафика.

Например, чтобы разрешить все HTTP-запросы, кроме запросов, поступающих с определенного адреса (например, IP-адреса 10.10.10.1), нужно создать два следующих правила:

Блокирующее правило— блокировка трафика HTTP с IP-адреса 10.10.10.1. Это конкретное правило.

Разрешающее правило— разрешение всего трафика через службу HTTP. Это общее правило.

В списке правил брандмауэра блокирующее правило следует поместить выше разрешающего. Когда брандмауэр перехватит HTTP-запрос с адреса 10.10.10.1, первым соответствующим правилом, которое он найдет, будет правило, подразумевающее блокировку этого трафика с помощью брандмауэра.

Если общее разрешающее правило находится выше конкретного блокирующего, то программа брандмауэр сопоставит запрос с разрешающим правилом до того, как найдет блокирующее. В этом случае трафик будет разрешен, несмотря на намерение блокировать HTTP-запрос, поступающий с данного адреса.

Защита с помощью брандмауэр работает на нескольких уровнях сетевой архитектуры, причем на каждом из них для ограничения сетевого трафика используются разные критерии. Данная сетевая архитектура построена на базе комплекта протоколов TCP/IP (TransmissionControlProtocol/InternetProtocol).

В протоколе канального уровня дается описание метода управления доступом к устройству (MAC), а также ряда вспомогательных средств обнаружения ошибок. К этому уровню относятся локальная сеть Ethernet (802.3), беспроводная сеть Wi-Fi (802.11x) и виртуальная локальная сеть (виртуальная частная сеть). Для проводной, беспроводной и виртуальной связи действуют разные правила и группы брандмауэра.

Протоколы сетевого уровня определяют схемы адресации, маршрутизации и управления сетью, действующие в рамках всей сети. Этот уровень также поддерживает произвольные протоколы, не связанные с IP, однако не способен определять для них параметры сетевого или транспортного уровня. В лучшем случае этот уровень позволяет администратору блокировать или разрешать эти протоколы сетевого уровня. Номера для протоколов, не связанных с IP, определяются номерами Ethernet,

которые указаны в реестре IANA (InternetAssignedNumbersAuthority). брандмауэр обеспечивает полную поддержку протоколов IPv4 и IPv6 в Windows XP, WindowsVista, WindowsServer 2008, Windows 7, Windows 8 и Windows 10.

2.4. Призначення, основні функції та принципи роботи модуля “Контроль Інтернету”

Обзор EndpointSecurity

McAfeeEndpointSecurity обеспечивает защиту серверов, компьютерных систем, ноутбуков и планшетов от известных и неизвестных угроз. Эти угрозы включают в себя вредоносные программы, подозрительные соединения, небезопасные веб-сайты и загруженные файлы.

EndpointSecurity обеспечивает работу нескольких технологий для обеспечения безопасности, которые обмениваются данными в режиме реального времени, чтобы анализировать угрозы и защищать от них. EndpointSecurity состоит из следующих модулей безопасности.

предотвращение угроз – не позволяет угрозам проникнуть в систему, автоматически проверяет файлы при доступе и выполняет целевые проверки на наличие вредоносных программ в клиентских системах.

брандмауэр – отслеживает обмен данными между компьютером и ресурсами в сети и в Интернете. Перехватывает подозрительные сообщения.

контроль Интернета – отслеживает поиск и просмотр страниц в Интернете в клиентских системах и блокирует вебсайты и загрузки на основе рейтинга и содержимого безопасности.

Адаптивная защита от угроз – анализирует содержимое в корпоративной среде пользователя и определяет, какие действия выполнять, используя данные о репутации файлов, правила и пороговые значения репутации.

В модуле Общие параметры можно настроить общие функции, например защиту интерфейса и регистрацию событий в журнале. Этот модуль устанавливается автоматически при установке любого другого модуля. Все модули интегрируются в единый интерфейс EndpointSecurity в клиентской системе. Каждый модуль работает в комплексе с другими и автономно, чтобы обеспечить несколько уровней защиты.

Принцип работы Endpoint

SecurityEndpointSecurity перехватывает угрозы, следит за общей работоспособностью системы и составляет отчеты по обнаружениям и состоянию. Для выполнения этих задач клиентское программное обеспечение устанавливается в каждую систему.

Как правило, пользователь устанавливает один или несколько модулей EndpointSecurity в клиентские системы, управляет обнаружениями и настраивает параметры, которые определяют принцип работы функций продукта

. McAfeeePO

Развернуть модули McAfee® ePolicyOrchestrator® (McAfee® ePO™) в клиентских системах и управлять ими можно с помощью EndpointSecurity.

Каждый модуль включает в себя расширение и пакет ПО, которые устанавливаются на сервер McAfeeePO. Затем McAfeeePO развертывает ПО в клиентских системах. (McAfeeePOOn-Premises) Клиентское программное обеспечение обменивается данными с McAfee® Agent с помощью McAfeeePO, чтобы получать обновления продукта, отчеты и конфигурацию политик, а также чтобы принудительно применять эти политики.

Модули клиента

Клиентское программное обеспечение защищает системы благодаря регулярным обновлениям, непрерывному отслеживанию и подробной отчетности.

Это ПО отправляет данные об обнаружениях на компьютерах пользователей на сервер McAfeeePO. Эти данные используются при составлении отчетов об обнаружениях и проблемах безопасности на вашем компьютере.

Сервер TIE и Data Exchange Layer

ПрииспользованиимодуляАдаптивнаязащитаотугрозплатформа Endpoint Security интегрируетсяс McAfee® Threat Intelligence Exchange (TIE) и McAfee® Data Exchange Layer (DXL). Эти дополнительные продукты позволяют пользователям локально управлять репутацией файлов и мгновенно предоставлять общий доступ к информации по всей среде.

McAfee GTI

Модули предотвращение угроз, брандмауэр, контроль Интернета и Адаптивная защита от угроз отправляют запрос McAfee®

GlobalThreatIntelligence™ (McAfee GTI), чтобы получить информацию о репутации и определить, как следует обрабатывать файлы в клиентской системе.

McAfeeLabs

Клиентское программное обеспечение обменивается данными с McAfeeLabs, чтобы получать файлы содержимого и обновления ядра. McAfeeLabs регулярно выпускает обновленные пакеты содержимого.

Обзор модуля контроль Интернета

контроль Интернета в McAfee® EndpointSecurity отслеживает поиск в Интернете и просмотр веб-страниц на клиентских компьютерах. Модуль защищает от угроз на веб-страницах и в загрузках файлов. Команда McAfee анализирует все веб-сайты и на основании результатов проверки присваивает им цветовые рейтинги безопасности. Цвет отражает уровень безопасности веб-сайта. контроль Интернета использует эти результаты проверки для определения угроз в Интернете. ПО, установленное в клиентской системе, предоставляет дополнительные функции, которые отображаются в окне браузера и в результатах поиска для уведомления пользователей. Развернуть модуль контроль Интернета в клиентских системах и управлять им можно с помощью McAfeeePO. Параметры позволяют контролировать доступ к сайтам в соответствии с их рейтингом безопасности, типом содержимого, а также URL-адресом и доменным именем.

Основные функции модуля контроль Интернета

Основные функции модуля контроль Интернета направлены на защиту ваших систем от веб-угроз, обнаружение угроз и исправление ошибок, связанных с загрузкой файлов

Защита

Описанные ниже функции модуля контроль Интернета помогут вам защитить системы от вредоносных веб-сайтов и загрузок.

Список блокировок и разрешений – предотвращает посещение пользователями определенных URL-адресов или доменов либо всегда разрешает доступ к сайтам, важным для вашего бизнеса.

Блокировка веб-категорий и действий на основе рейтинга – рейтинги безопасности и веб-категории, определенные McAfee, используются для контроля доступа пользователей к сайтам, страницам и загрузкам.

Безопасный поиск – автоматическая блокировка опасных сайтов из результатов поиска на основании их рейтинга безопасности.

Самозащита – запрещает пользователям отключать подключаемый модуль контроль Интернета, а также удалять или изменять файлы, разделы реестра, значения реестра, службы и процессы модуля контроль Интернета.

Обнаружение

Описанные ниже функции модуля контроль Интернета помогут вам обнаруживать вредоносные веб-сайты.

Кнопка контроль Интернета в окне браузера – в подключаемом модуле контроль Интернета отображается кнопка, указывающая рейтинг безопасности сайта. Нажмите эту кнопку, чтобы получить больше информации о сайте.

Значок контроль Интернета на страницах результатов поиска – отображается возле каждого сайта из списка. Цвет значка указывает на рейтинг безопасности сайта. Наведите курсор на этот значок, чтобы получить больше информации о сайте.

Отчеты сайта – в них содержатся подробные сведения о том, каким образом был вычислен рейтинг безопасности на основе типов обнаруженных

угроз, результатов проверок и других данных. • Панели управления и мониторы – отображают статистику операций модуля контроль Интернета, включая посещения и загрузки с сайтов по рейтингу, тип содержимого, а также список блокировок и разрешений.

Запросы и отчеты – предоставление подробной информации о событиях в браузере модуля контроль Интернета с возможностью ее сохранения в отчетах.

Исправление

Описанные ниже функции модуля контроль Интернета позволяют выполнять отслеживание и настройку.

Взаимная блокировка с другими продуктами McAfee – автоматически отключает модуль контроль Интернета, если он обнаруживает устройство интернет-шлюза или если установлено McAfee® ClientProxy, а также в режиме перенаправления.

Проверка загружаемых файлов – модуль контроль Интернета отправляет файлы в модуль предотвращение угроз для проверки. В случае обнаружения угрозы модуль предотвращение угроз отвечает настроенным действием (например, очисткой) и уведомляет пользователя.

Панели управления и мониторы – отслеживают операции, чтобы понять, какие действия в Интернете вы выполняете, и затем используют эту информацию для настройки параметров модуля контроль Интернета.

Исключения – предотвращают назначение рейтинга для определенных IP-адресов и их блокировку модулем контроль Интернета.

Принцип работы модуля контроль Интернета

Модуль контроль Интернета запрашивает у McAfee GTI информацию о репутации, чтобы определить, какие действия следует предпринимать при навигации по URL-адресам.

1. Администратор настраивает параметры модуля контроль Интернета в McAfeeePO и принудительно применяет политику в клиентской системе.

2. Пользователь заходит на веб-сайт или получает доступ к его ресурсам.

3. Модуль контроль Интернета запрашивает репутацию URL-адреса у McAfee GTI.

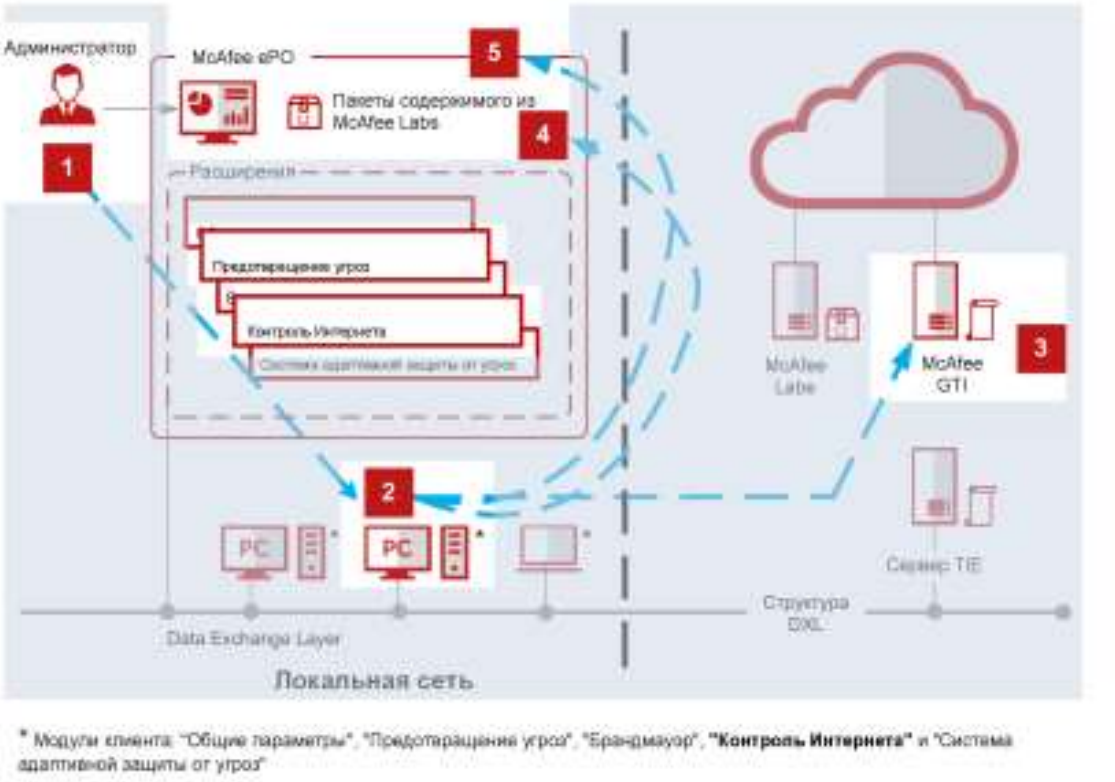
Если репутация URL-адреса зеленого цвета, модуль контроль Интернета разрешает перейти по этому URL-адресу и отображает страницу. В противном случае модуль контроль Интернета переходит на страницу блокировки или предупреждения, в зависимости от настроек.

Если репутация URL-адреса не имеет рейтинга, но соответствует категории в McAfee GTI, модуль контроль Интернета разрешает или блокирует переход по URL-адресу в зависимости от настроек Действия на основе содержимого.

4. Если это запрос на загрузку файлов, а файл не имеет репутации вредоносного, то модуль контроль Интернета разрешает загрузку, даже если URL-адрес имеет репутацию вредоносного. Если репутация файла неизвестна, контроль Интернета отправляет файл в модуль предотвращение угроз, чтобы проверить его сканером по требованию. Модуль предотвращение угроз сравнивает файл с файлом содержимого AMCore. Если его содержимое соответствует сигнатуре или хэшу, загрузка файла блокируется. В другом случае файл загружается.

5. Модуль Модуль контроль Интернета регистрирует сведения, а затем создает событие и отправляет его в McAfeeePO.

Принцип работы



* Модули клиента: "Общие параметры", "Предотвращение угроз", "Брандмауэр", **"Контроль Интернета"** и "Система адаптивной защиты от угроз"

Модуль контроль Интернета и McAfeeClientProxy

Когда модуль контроль Интернета отключен из-за наличия ClientProxy, который выполняет перенаправление:

модуль контроль Интернета игнорирует действия, связанные с рейтингом и принудительным применением;

элементы управления браузером модуля контроль Интернета отключаются.

На странице Состояние Клиент EndpointSecurity для модуля контроль Интернета отображается состояние Отключен.

На странице Параметры Клиент EndpointSecurity указано, что модуль контроль Интернета отключен, поскольку обнаружен ClientProxy.

Обзор функций

Поддерживаемые и неподдерживаемые браузеры

Модуль контроль Интернета поддерживает MicrosoftEdge, GoogleChrome, MozillaFirefox и MicrosoftInternetExplorer.

Примечание: Подключаемый модуль контроль Интернета имеет доступ ко всем данным в браузере, включая потенциально конфиденциальную информацию, например пароли или данные кредитных карт. Однако контроль Интернета не хранит эти данные. контроль Интернета поддерживает указанные ниже браузеры и версии.

Edge – текущая версия

Примечание: контроль Интернета поддерживает браузер Edge только в системах Windows с обновлением Windows 10 CreatorsUpdate (15063) и более поздних версий.

Chrome – текущая версия. Chrome не поддерживает функцию Всплывающая подсказка.

Firefox – текущая версия, включая многопроцессорную архитектуру (E10S)

Firefox ESR (ExtendedSupportRelease) – текущая и предыдущая версии InternetExplorer 11 Поскольку новые версии браузеров Microsoft, Google и Mozilla выходят часто, контроль Интернета может некорректно работать с обновленной версией. Обновления для модуля контроль Интернета выходят по возможности сразу после изменения версий браузеров Edge, Chrome или Firefox. Актуальную информацию о браузерах, которые поддерживает модуль контроль Интернета, см. в статье базы знаний KB82761.

Примечание: В системах с самостоятельным управлением по умолчанию разрешены все браузеры (как поддерживаемые, так и неподдерживаемые).

При вводе ключевых слов в популярных поисковых системах, например Google, Yahoo, Bing или Ask, рядом с веб-сайтами на странице результатов поиска, отображаются цветные значки безопасности. Цвет этого значка соответствует рейтингу безопасности сайта.

Пользователи могут посмотреть отчет о веб-сайте, чтобы узнать подробнее о конкретных угрозах. Отчеты о веб-сайтах доставляются с сервера рейтингов McAfee GTI и содержат приведенную ниже информацию.

McAfee GTI сохраняет рейтинги веб-сайтов и отчеты для модуля контроль Интернета. Если модуль контроль Интернета настроен на проверку загруженных файлов, сканер использует информацию о репутации файлов, предоставляемую McAfee GTI, для проверки наличия подозрительных файлов. Сканер отправляет отпечатки образцов (хэши) на центральный сервер баз данных, размещенный в McAfeeLabs, чтобы определить, являются ли образцы вредоносными. Благодаря отправке хэшей обнаружение может стать доступным до момента публикации McAfeeLabs обновленного файла содержимого. Можно настроить EndpointSecurity на использование прокси-сервера, чтобы получать сведения о репутации McAfee GTI из модуля Общие параметры

2.5. Призначення, основні функції та принципи роботи модуля “Адаптивний захист від загроз”.

Обзор модуля Адаптивная защита от угроз

Адаптивная защита от угроз (ATP) McAfee® EndpointSecurityMcAfeeEndpointSecurity® – это дополнительный модуль EndpointSecurity, который проверяет содержимое в среде вашего предприятия и определяет, какие действия следует предпринять, на основе репутации файлов, правил и пороговых значений репутации.

Адаптивная защита от угроз предоставляет следующие преимущества.

• Быстрое обнаружение и защита от угроз безопасности и вредоносных программ.

• Возможность узнать, какие системы или устройства уже скомпрометированы и как угроза распространяется в вашей среде.

• Возможность немедленно ограничить, заблокировать или очистить определенные файлы или сертификаты на основе репутации угрозы и ваших критериев риска.

• Интеграция с проверкой RealProtect позволяет выполнять автоматизированный анализ репутации в облаке и клиентских системах.

• Интеграция с McAfee® AdvancedThreatDefense и McAfee GTI в режиме реального времени для обеспечения подробной оценки и предоставления данных о классификации вредоносных программ. Такая интеграция позволяет реагировать на угрозы и предоставлять общий доступ к информации в вашей среде.

Чтобы получить дополнительные источники анализа угроз и расширить функциональность, можно развернуть сервер McAfee® ThreatIntelligenceExchange (TIE). За подробной информацией обратитесь к реселлеру или торговому представителю.

Основные функции модуля Адаптивная защита от угроз

Основные функции модуля Адаптивная защита от угроз направлены на защиту вашего предприятия от файлов с неизвестной репутацией, обнаружение вредоносных шаблонов и исправление ложных положительных результатов.

Защита

Обеспечьте защиту своего предприятия путем блокировки или ограничения файлов с неизвестной репутацией, используя функции модуля Адаптивная защита от угроз, которые представлены ниже.

• Обработка файлов на основе репутации – модуль Адаптивная защита от угроз предупреждает о появлении неизвестного файла в среде

. Вместо отправки информации о файле в McAfee для анализа модуль Адаптивная защита от угроз может немедленно заблокировать этот файл.

• Интеграция с сервером TIE – сервер TIE (при наличии) предоставляет информацию о количестве систем, в которых запускался файл. AdvancedThreatDefense помогает определить, представляет ли файл угрозу.

• Динамическое ограничение приложений – позволяет запускать неизвестные файлы в контейнере, ограничивая их возможные действия.

Когда компания впервые использует файл с неизвестной репутацией, модуль Адаптивная защита от угроз может запустить его в контейнере. Правила ограничения определяют, какие действия не могут совершать ограниченные приложения. Динамическое ограничение приложений также ограничивает процессы, когда они загружают PE-файлы (переносные исполняемые файлы) и библиотеки DLL (динамически подключаемые библиотеки), которые понижают репутацию процесса.

Обнаружение вредоносных шаблонов и программ в памяти благодаря представленным ниже функциям модуля

Адаптивная защита от угроз.

• Проверка RealProtect – выполняет автоматический анализ репутации.

RealProtect проверяет подозрительные файлы и операции в клиентской системе и обнаруживает вредоносные шаблоны, используя методы машинного обучения. Проверки RealProtect на основе клиента и на основе

облака включают в себя проверку DLL, позволяющую не допустить загрузку доверенными процессами недоверенных файлов PE и DLL.

Исправление

Очистка файлов и устранение ложных положительных результатов с помощью описанных ниже функций модуля

Адаптивная защита от угроз.

• Очистка файлов – модуль Адаптивная защита от угроз может очищать файлы, когда репутация файла достигает установленного порога.

• Исключения пользовательских файлов – если пользовательский файл является доверенным, но по умолчанию имеет репутацию зараженного, он блокируется Вы можете исключить его из проверок или изменить репутацию файла, сделав его доверенным, и разрешить его запуск в организации без запроса обновленного DAT-файла у McAfee.

Принцип работы Адаптивная защита от угроз

Адаптивная защита от угроз получает информацию о репутации из локального кэша репутации, с сервера TIE и McAfee GTI, чтобы определить способ обработки файлов в клиентской системе.

1. Если система управляемая, администратор настраивает параметры Адаптивная защита от угроз в McAfeeePO и запускает ее в клиентской системе.

2. Пользователь открывает файл в клиентской системе. Адаптивная защита от угроз проверяет наличие файла в локальном кэше репутации.

3. Если файла нет в локальном кэше репутации, Адаптивная защита от угроз отправляет запрос на получение сведений о репутации (при наличии) на сервер TIE.

4. Если сервер TIE недоступен или файл отсутствует в базе данных сервера TIE, Адаптивная защита от угроз отправляет запрос репутации в McAfee GTI.

5. В зависимости от репутации файла и параметров Адаптивная защита от угроз: ◦ Файл разрешается открыть. ◦ Файл блокируется. ◦ Разрешается запуск файла в контейнере. ◦ Пользователю предлагается выполнить действие.

6. McAfee GTI присылает актуальную информацию о репутации файла на сервер TIE.

7. Сервер TIE обновляет базу данных и отправляет обновленную информацию о репутации во все системы с включенной Адаптивная защита от угроз для немедленной защиты вашей среды.

8. Адаптивная защита от угроз записывает сведения в журнал.

Обзор функций

Управление доступом с помощью репутации файлов и сертификатов

Репутация файлов и сертификатов основана на их содержимом и свойствах. Параметры модуля Адаптивная защита от угроз определяют, будут ли элементы заблокированы или разрешены в вашей среде, на основе уровней репутации. В зависимости от необходимой оптимизации правил для конкретных типов систем возможны три уровня безопасности. Каждый уровень связан с конкретными правилами, которые определяют вредоносные и подозрительные файлы и сертификаты.

• Продуктивность – системы с большим количеством изменений, частой установкой и удалением доверенных программ и частыми обновлениями. Примерами таких систем служат компьютеры, используемые в разработке. Для этой настройки используется меньшее количество правил.

Пользователи видят минимум блокировок и запросов действий при обнаружении новых файлов.

• Сбалансированность – стандартные корпоративные системы, которые изменяются нечасто. Для этой настройки используется большее количество правил. Пользователи видят большее количество блокировок и запросов действий.

• Безопасность – системы, управляемые ИТ-отделом, с тщательным контролем и минимумом изменений. Примерами выступают системы, которые имеют доступ к критической или конфиденциальной информации в финансовых или правительственных учреждениях. Эта настройка также используется для серверов. Для этой настройки используется максимальное количество правил. Пользователи видят максимальное количество блокировок и запросов действий. При определении уровня безопасности обратите внимание на тип системы и интенсивность блокировки и запросов действий для пользователей. Принцип определения репутации Для определения репутации файла или сертификата Адаптивная защита от угроз использует проверку перед выполнением и отслеживание после выполнения.

При попытке запустить файл с определенной репутацией на вашем компьютере Адаптивная защита от угроз может отобразить запрос о дальнейших действиях. Запрос отобразится только в том случае, если Адаптивная защита от угроз установлена и настроена на отображение запроса.

Прим.: Адаптивная защита от угроз использует системный значок на панели задач McAfee для отображения запросов. В системах, доступ к которым осуществляется только с помощью удаленного рабочего стола, значок на панели задач не запускается и запросы не отображаются. Чтобы обойти эту проблему, добавьте UpdaterUI.exe в сценарий входа. Администратор настраивает пороговое значение репутации, при котором

отображается запрос. Например, если пороговое значение репутации "Неизвестно", EndpointSecurity выдает запросы для всех файлов с репутацией "Неизвестно" и ниже.

Если вы не выбрали определенный параметр, Адаптивная защита от угроз выполнит действие по умолчанию, заданное администратором.

Сообщение с запросом, тайм-аут и действие по умолчанию зависят от конфигурации Адаптивная защита от угроз.

Прим.: В Windows 8 и 10 используются всплывающие уведомления – всплывающие сообщения с предупреждениями и запросами. Щелкните всплывающее уведомление, чтобы отобразить уведомление в режиме рабочего стола.

1. (Необязательно) При появлении запроса введите сообщение для администратора. Например, используйте сообщение, чтобы описать файл или объяснить ваше решение о разрешении или блокировании в системе.

2. Выберите Разрешить или Заблокировать.

Результат

Адаптивная защита от угроз действует на основании вашего выбора или действия, заданного по умолчанию, и закрывает окно с запросом.

3 РОЗРОБЛЕННЯ ВАРІАНТА ТЕХНОЛОГІЇ ЗАХИСТУ КІНЦЕВИХ ТОЧОК КОРПОРАТИВНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ

3.1. Технологія застосування модуля “Попередження загроз”

Управление предотвращение угроз

Администратор может указывать параметры предотвращение угроз для предотвращения доступа угроз, а также настраивать проверки.

Настройка исключений Модуль предотвращение угроз позволяет тонко настраивать защиту, указывая элементы для исключения. Например, вам необходимо исключить некоторые типы файлов, чтобы сканер не блокировал файл, используемый базой данных или сервером. Заблокированный файл может привести к сбою базы данных или сервера либо к возникновению ошибок.

Чтобы повысить производительность проверок при доступе и по требованию,рекомендуетсяиспользовать систему исключения из проверки, а не функцию добавления файлов и папок в исключения.

Исключения в списках исключений являются взаимоисключающими. Каждое исключение оценивается отдельно от других в списке.

Защита точек доступа к системе

Предотвращение проникновения угроз в клиентскую систему является передним краем защиты от вредоносных программ. Защита доступа предотвращает нежелательные изменения на управляемых компьютерах, ограничивая доступ к определенным файлам, общим ресурсам, разделам и параметрам реестра, процессам и службам.

Модуль "Защита доступа" блокирует доступ к элементам и создает о них отчеты с помощью правил, определенных McAfee и пользователем (иначе именуемых пользовательскими правилами). Модуль Защита доступа сравнивает требуемое действие со списком правил и предпринимает действие, указанное правилом.

Для регистрации попыток доступа к файлам, общим ресурсам, разделам и параметрам реестра, а также процессам и службам, необходимо включить функцию защиты доступа.

Способы проникновения угроз в систему

Угрозы проникают в систему через различные точки доступа.

Точка доступа	Описание
Макрос	Документы, созданные в текстовых редакторах, а также электронные таблицы.
Исполняемые файлы	Кажущиеся безвредными программы вместе с ожидаемым содержимым могут содержать и вирусы. Наиболее часто файлы таких программ имеют расширение .EXE, .COM, .VBS, .BAT, .HLP и .DLL.
Сценарии	Сценарии, связанные с веб-страницами и электронной почтой, такие как ActiveX и JavaScript, могут содержать вирусы.
Сообщения системы IRC (Internet Relay Chat)	Файлы, отправленные с этими сообщениями, могут включать вредоносное содержимое. Например, процессы автоматического запуска могут содержать червей и «троянских коней».
Файлы справки обозревателя и приложений	При загрузке этих файлов справки в систему могут проникать встроенные вирусы и исполняемые файлы.
Электронная почта	Юмористическме материалы, игры и изображения, вложенные в сообщения электронной почты.
Сочетание выше перечисленных способов	Изощренные разработчики вредоносных программ одновременно используют все эти способы проникновения и даже встраивают одну вредоносную программу в другую для доступа к управляемому компьютеру.

Предотвращение угроз с помощью функции «Защита доступа»

Защита доступа предотвращает потенциальные угрозы, управляя действиями с учетом правил защиты, определенных McAfee и пользователем.

предотвращение угроз предоставляет защиту доступа по следующему простому принципу.

В случае возникновения угрозы

В случае запуска пользователем или процессом действия:

1. Функция «Защита доступа» выполняет проверку этого действия в соответствии с определенными правилами.

2. Если действие нарушает правило, «Защита доступа» управляет этим действием, основываясь на информации в настроенных правилах.

3. Защита доступа обновляет файл журнала, создает его и отправляет событие на управляющий сервер, если система является управляемой.

Пример угрозы доступа

1. Пользователь загружает из Интернета допустимую (не вредоносную) программу MyProgram.exe.

2. Пользователь запускает программу MyProgram.exe, запуск происходит в обычном режиме.

3. Затем программой MyProgram.exe запускается дочерний процесс под именем AnnoyMe.exe.

4. AnnoyMe.exe выполняет попытку внести в операционную систему изменения, чтобы его загрузка всегда выполнялась при запуске системы.

5. «Защита доступа» обрабатывает запрос и сопоставляет действие с существующим правилом блокировки и отправки отчета.

6. Защита доступа запрещает модификацию операционной системы программе AnnoyMe.exe и регистрирует сведения о такой попытке в журнале. Защита доступа также создает и отправляет предупреждение на управляющий сервер.

Сведения о правилах защиты доступа

Используйте правила защиты доступа, определенные McAfee и пользователями, чтобы защитить точки доступа к системе.

Правила, определенные McAfee, всегда имеют приоритет в отношении правил, определенных пользователями.

Исключения

На уровне правила включения и исключения действуют для этого правила. На уровне политики исключения действуют для всех правил. Исключения можно не настраивать.

Настройка правил защиты доступа, определенных McAfee

Правила, определенные McAfee, предотвращают изменение часто используемых файлов и настроек.

Подготовка

Режим интерфейса Клиент EndpointSecurity должен быть настроен на Полный доступ, или же вы должны войти в систему как администратор.

Предоставляются следующие возможности:

• Изменение настроек блокировки и создания отчетов для этих правил.

• Добавление исключенных и включенных исполняемых файлов в эти правила.

Недоступные действия:

• Удаление этих правил.

• Изменение файлов и настроек, защищенных с помощью этих правил.

• Добавление субправил или имен пользователей в эти правила.

Блокировка атак с переполнением буфера

Защита от эксплойтов запрещает атакам с переполнения буфера выполнять произвольный код. Эта функция отслеживает вызовы API в режиме пользователя, совершаемые в результате переполнения буфера.

В случае обнаружения соответствующие сведения записываются в журнал активности, отображаются в клиентской системе и, если настроена соответствующая опция, отправляются на управляющий сервер.

Компонент предотвращение угроз использует файл содержимого функции предотвращения действий средств использования уязвимостей для защиты таких приложений, как MicrosoftInternetExplorer, MicrosoftOutlook, OutlookExpress, MicrosoftWord и MSN Messenger.

Атаки с переполнением буфера

Злоумышленники используют атаки с переполнением буфера, чтобы запускать исполняемый код путем переполнения буфера с фиксированным объемом памяти, зарезервированного для процесса ввода. Этот код позволяет злоумышленнику проникнуть в систему целевого компьютера или повредить хранящиеся там данные.

Большой процент атак с использованием вредоносных программ составляют атаки с переполнением буфера, направленные на перезапись информации в смежных ячейках памяти во фрейме стека.

Существует два типа атак с переполнением буфера:

• Атаки на стек: объекты стековой памяти используются для хранения введенных пользователем данных. Это наиболее распространенный тип атак.

• Атаки на динамическую память: заполняется память, зарезервированная для программы. Это довольно редкий вид атак.

Объект стековой памяти фиксированного размера пуст и находится в состоянии ожидания ввода данных пользователем. Когда пользователь вводит в программу данные, они сохраняются в верхней части стека и им назначается обратный адрес блока памяти. При обработке стека введенные пользователем данные отправляются на обратный адрес, указанный программой.

Ниже приводятся этапы атаки на стек с переполнением буфера.

1. Переполнение стека. При написании программы для данных резервируется определенный объем памяти. При записи данных, объем которых превышает зарезервированное в стеке пространство, происходит переполнение стека. Это вызывает проблему, только если введенные данные являются вредоносными.

2. Использование переполнения. Программа ожидает ввода данных пользователем. Если злоумышленник вводит исполняемую команду, которая превышает размер стека, эта команда сохраняется за пределами зарезервированного пространства.

3. Запуск вредоносной программы. Команда не выполняется автоматически, если она превышает размер буфера стека. Сначала в результате переполнения буфера происходит сбой программы. Если злоумышленник предоставил обратный адрес блока памяти, указывающий на вредоносную команду, то программа пытается выполнить восстановление, используя обратный адрес. Если обратный адрес является допустимым, вредоносная команда выполняется.

4. Использование разрешений. Вредоносная программа теперь запускается с теми же разрешениями, что и приложение, в отношении которого совершена атака. Поскольку программы обычно выполняются в режиме ядра или с разрешениями, унаследованными от учетной записи службы, теперь злоумышленник может получить полный контроль над операционной системой.

Принцип работы сигнатур

Сигнатуры предотвращения действий средств использования уязвимостей – это набор правил, которые сравнивают поведение с известными атаками и выполняют определенное действие в случае

обнаружения совпадения. McAfee предоставляет сигнатуры в обновлениях содержимого предотвращения действий средств использования уязвимостей.

Сигнатуры защищают конкретные приложения, определенные в списке Правила защиты приложений. В случае обнаружения атаки предотвращение действий средств использования уязвимостей может остановить поведение, запущенное посредством атаки

. При обновлении файла содержимого предотвращения действий средств использования уязвимостей также обновляется список сигнатур (при необходимости).

Пользователь может изменить параметры действия этих сигнатур, но не может добавить, удалить или каким-либо образом изменить эти сигнатуры. Чтобы защитить определенные файлы, общие ресурсы, разделы реестра, параметры реестра, процессы и услуги, необходимо создать настраиваемые правила защиты доступа.

Действия

Действие – это то, что предотвращение действий средств использования уязвимостей выполняет при запуске сигнатуры.

• Блокировка – предотвращает операцию.

• Отчет – разрешает выполнение операции и отправляет отчет по событию.

Если не выбран ни один из вариантов, сигнатура отключается – предотвращение действий средств использования уязвимостей разрешает выполнение операции и не отправляет отчет по событию.

Файл содержимого предотвращения действий средств использования уязвимостей автоматически устанавливает действие для сигнатур с учетом уровня серьезности. Пользователь может изменить действие определенной

сигнатуры в разделе Сигнатуры настроек Предотвращение действий средств использования уязвимостей. Любые изменения, внесенные в действия сигнатур, сохраняются после обновления содержимого.

Правила поведения

Правила поведения блокируют атаки "нулевого дня" и поддерживают нормальную работу приложений и операционной системы. Эвристические правила поведения определяют рамки допустимого поведения. Все действия, выходящие за эти рамки, рассматриваются как подозрительные и инициируют ответ. Например, согласно правилу поведения, доступ к HTML-файлам может быть разрешен только процессам веб-сервера. Если другой процесс попытается получить доступ к файлам HTML, предотвращение действий средств использования уязвимостей выполнит указанное действие. Такой механизм защиты (внутреннее и внешнее экранирование) гарантирует безопасность приложений и их данных, а также не позволяет использовать одни приложения для атаки на другие.

Кроме того, правила поведения не допускают переполнения буфера и последующего выполнения кода, что является одним из самых распространенных видов атак. Уровни серьезности Каждая сигнатура имеет уровень серьезности, назначенный по умолчанию. Он указывает на серьезность возможных последствий атаки.

• Высокий – сигнатуры, обеспечивающие защиту от явных угроз и злонамеренных действий. Эти сигнатуры относятся к явным средствам использования уязвимостей и в большинстве своем не основаны на поведении.

Осторожно: Чтобы предотвратить проникновение в систему атак средства использования уязвимости, необходимо установить сигнатуры с уровнем серьезности Высокий и применить средство Блокировка на каждом узле.

• Средний – поведенческие сигнатуры, не позволяющие приложениям выходить за рамки своей прикладной оболочки (подходит для клиентов, защищающих веб-серверы и серверы Microsoft SQL Server 2000).

Совет: Рекомендация. На критических серверах для сигнатур с уровнем серьезности Средний выберите параметр Блокировка после точной настройки.

• Низкий – поведенческие сигнатуры, экранирующие приложения. Внешнее экранирование – это блокировка приложений и ресурсов системы, в результате которой их нельзя изменить.

Установка параметра Блокировка для сигнатур с уровнем серьезности Низкий повышает безопасность системы, но требует дополнительных настроек.

• Информационный – сигнатуры, уведомляющие об изменении системной конфигурации, что может сигнализировать о несущественном риске для безопасности или о попытке доступа к важным системным данным. События этого уровня, как правило, происходят при нормальной работе системы и не свидетельствуют об атаке.

• Отключено – сигнатуры, отключенные в файле содержимого предотвращения действий средств использования уязвимостей.

Правила защиты приложений и принципы их работы

Правила защиты приложений определяют исполняемые файлы, которые отслеживаются для сигнатур предотвращения действий средств использования уязвимостей. Если исполняемый файл не включен в список, он не отслеживается.

Сигнатуры предотвращения действий средств использования уязвимостей бывают двух классов:

• Сигнатуры переполнения буфера обеспечивают защиту памяти, отслеживая пространство в памяти, используемое процессами.

• Сигнатуры API отслеживают вызовы API между процессами, которые выполняются в пользовательском режиме и ядре.

Содержимое для модуля предотвращения действий средств использования уязвимостей, предоставляемое McAfee, включает список защищаемых приложений. Модуль предотвращение угроз отображает эти приложения в разделе Правила защиты приложений настроек предотвращения действий средств использования уязвимостей.

Чтобы поддерживать защиту в актуальном состоянии, обновления для предотвращения действий средств использования уязвимостей заменяют определенные McAfee правила защиты приложений в настройках предотвращения действий средств использования уязвимостей с помощью последних правил защиты приложений.

Пользователь может включить, отключить, удалить или изменить состояние включения для определенных McAfee правил защиты приложений. Кроме того, можно создавать и дублировать собственные правила защиты приложений. Любые изменения, внесенные в эти правила, сохраняются и после обновления содержимого.

Если список включает конфликтующие правила защиты приложений, правила с Состоянием включения параметра Исключение имеют преимущество над параметром Включение

Исключения из предотвращения действий средств использования уязвимостей и принцип их работы

Ложные положительные результаты возникают, когда обычные действия в процессе работы пользователя интерпретируются как атака.

Чтобы избежать подобных ситуаций, нужно создать исключения для действий, инициирующих ложные положительные результаты.

Исключения позволяют сократить число предупреждений о ложных положительных результатах, минимизировать поток ненужных данных и гарантировать, что все предупреждения будут соотноситься с действительными угрозами безопасности.

Приведем пример. В ходе тестирования клиент распознал сигнатуру "Java – Creationofsuspicious ļOHV inTempfolder". Эта сигнатура показывает, что приложение Java пытается создать файл в папке WindowsTemp. Событие, запускаемое этой сигнатурой, приводит к созданию предупреждения, так как приложение Java может использоваться для загрузки вредоносной программы в папку WindowsTemp. В данном случае это может быть признаком внедрения троянского коня. Но если процесс создает файлы в папке Temp в рамках обычных рабочих операций, например, сохраняя файл с помощью приложения Java, создайте исключение, чтобы разрешить это действие.

Если предотвращение действий средств использования уязвимостей будет нарушено, с событием будет связан отдельный процесс и, возможно, модуль вызывающего объекта, API или сигнатура. Если есть основания полагать, что нарушение является ложным положительным результатом, то можно добавить исключение, указав один или несколько таких идентификаторов

. В управляемых системах исключения из предотвращения действий средств использования уязвимостей, созданные в Клиент EndpointSecurity, не отправляются в McAfeeePO и могут быть перезаписаны при развертывании обновленной политики администратором. Настройте глобальные исключения в политике Предотвращение действий средств использования уязвимостей в McAfeeePO

. При указании исключений следует учитывать следующее:

• Каждое исключение применяется независимо. Несколько исключений можно связать друг с другом с помощью логического оператора OR, чтобы при совпадении с любым из указанных исключений событие нарушения не возникало.

• Необходимо указать хотя бы один параметр из следующих: Процесс, Модуль вызывающего объекта, API или Сигнатура.

• Исключения, в которых задан Модуль вызывающего объекта или API, не применяются в функции предотвращения выполнения данных.

• Для исключений типа Процесс необходимо указать по меньшей мере один идентификатор: Имя файла или путь, Хэш MD5 или Подписавший.

• Если указать несколько идентификаторов, то применяться будут все.

• Если указать несколько идентификаторов, которые не соответствуют друг другу (например, имя файла и хэш MD5 не применяются к одному и тому же файлу), исключение считается недействительным.

• Исключения не зависят от регистра символов.

• Подстановочные знаки можно использовать во всех полях, кроме поля хэша MD5.

• При добавлении в исключение идентификаторов подписей оно будет применяться только к процессу в указанных подписях. Если идентификаторы подписей не указаны, исключение применяется к процессу во всех подписях.

3.2. Технологія застосування модуля “ Міжмережевий екран”.

Принцип работы групп правил брандмауэра

Используйте группы правил брандмауэр, чтобы упорядочить правила брандмауэра и упростить управление. Группы правил брандмауэр не влияют на то, как брандмауэр обращается с содержащимися в них правилами; брандмауэр попрежнему обрабатывает правила сверху вниз.

брандмауэр обрабатывает настройки группы раньше, чем настройки правил, принадлежащих к этой группе. Если в настройках имеется противоречие, настройки группы имеют приоритет.

Настройка учета местоположения для групп

брандмауэр позволяет настраивать для группы и ее правил учет местоположения и создавать изоляцию соединения. Параметры группы Местоположение и Сетевые параметры позволяют настроить группы таким образом, чтобы в них учитывался выбор сетевого адаптера. Используйте группы сетевого адаптера, чтобы применять правила, зависящие от выбора адаптера, к компьютерам с несколькими сетевыми интерфейсами. После включения статуса местоположения и имени местоположения параметры разрешенных подключений для каждого сетевого адаптера могут включать:

Местоположение:

• Необходима доступность McAfeeePO

• Суффикс DNS, специфический для соединения

• IP-адрес шлюза по умолчанию

• IP-адрес сервера DHCP

• Сервер DNS, отвечающий за преобразование URL-адресов

• IP-адрес сервера-источника WINS

• IP-адрес сервера-получателя WINS

• Доступность домена (HTTPS)

• Раздел реестра Сети:

• IP-адрес локальной сети

• Типы соединений

Если к одному соединению применимы правила двух групп с учетом местоположения, брандмауэр использует обычный приоритет и первой обрабатывает группу, стоящую в начале списка правил. Если в первой группе отсутствуют соответствующие правила, обработка правил продолжается.

Когда брандмауэр сопоставляет параметры группы с учетом местоположения с параметрами активного подключения, применяются правила из данной группы. Правила рассматриваются как небольшой набор правил и используется обычный приоритет. Если некоторые правила не соответствуют перехваченному трафику, брандмауэр их игнорирует.

Если выбран этот параметр...	То...
Включить учет местоположения	Требуется указать имя местоположения.
Необходима доступность McAfee ePO	McAfee ePO доступен, а полное доменное имя сервера было задано.
Локальная сеть	IP-адрес адаптера должен совпадать с одним из элементов списка.
Суффикс DNS, специфический для соединения	Суффикс DNS у адаптера должен соответствовать одному из элементов списка.
Шлюз по умолчанию	IP-адрес шлюза адаптера по умолчанию должен соответствовать хотя бы одному из элементов списка.
Сервер DHCP	IP-адрес сервера DHCP у адаптера должен соответствовать хотя бы одному из элементов списка.
Сервер DNS	IP-адрес сервера DNS у адаптера должен соответствовать любому из элементов списка.
Сервер-источник WINS	IP-адрес сервера-источника WINS у адаптера должен соответствовать хотя бы одному из элементов списка.
Сервер-получатель WINS	IP-адрес сервера-получателя WINS у адаптера должен соответствовать хотя бы одному из элементов списка.
Доступность домена (HTTPS)	Указанный домен должен быть доступен при использовании HTTPS.

Группы правил брандмауэр и изоляция соединения

Используйте изоляцию соединения для групп, чтобы закрыть для нежелательного трафика доступ к указанной сети.

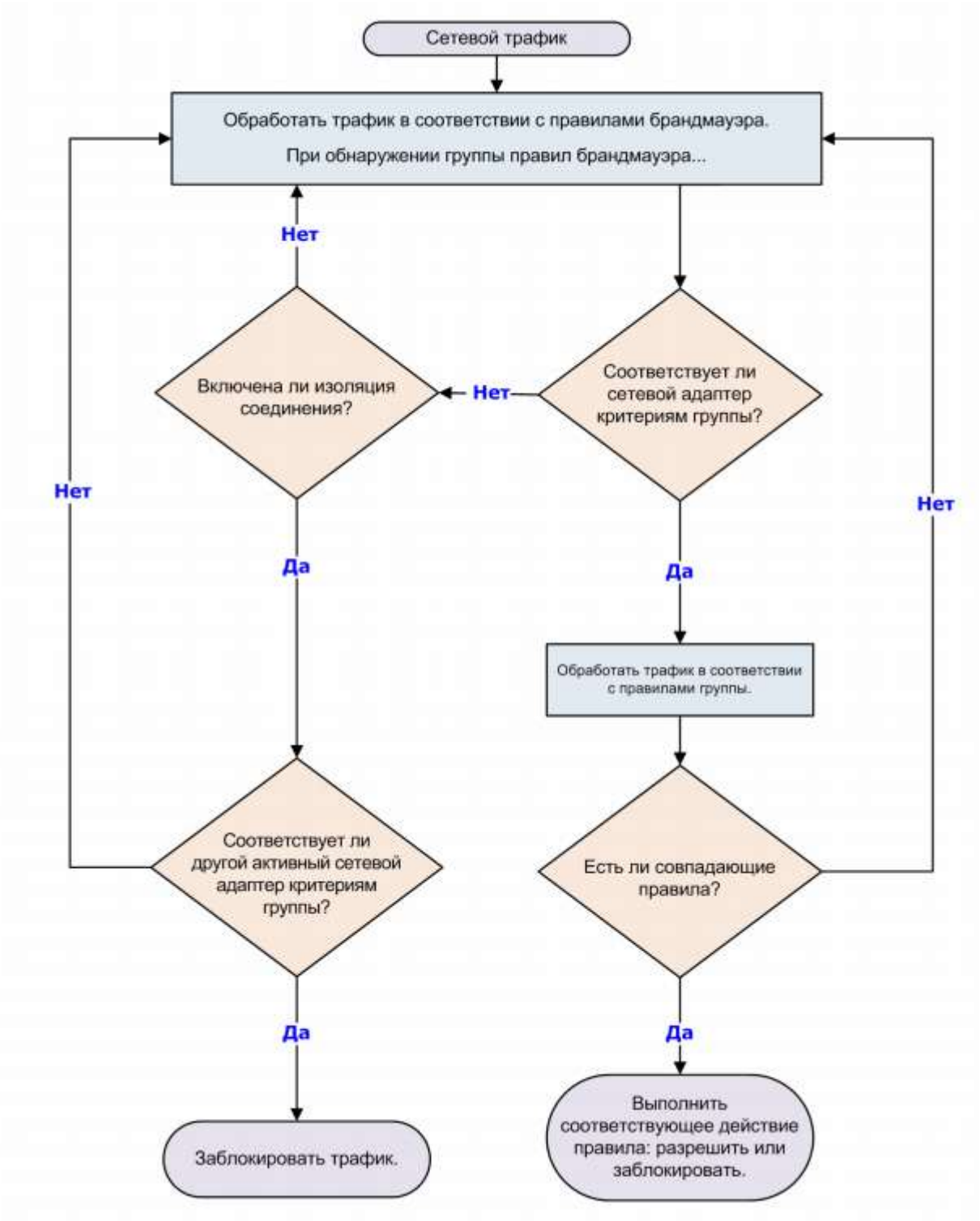
Когда для данной группы включена изоляция соединения, а активный сетевой адаптер соответствует критериям группы, брандмауэр обрабатывает только тот трафик, который соответствует следующим условиям:

• Разрешающие правила, находящиеся выше данной группы в списке правил брандмауэра

• Критерии группы

Остальной трафик блокируется.

Прим.: Ни одна группа, для которой включена изоляция соединения, не может иметь связанные параметры передачи или исполняемые файлы.



В качестве примеров использования изоляции сетевого соединения рассмотрим две настройки: корпоративная среда и отель. В списке действующих правил брандмауэра правила и группы расположены в следующей очередности:

1. Правила основного соединения

2. Правила соединения с виртуальной частной сетью

3. Группа правил соединения с корпоративной локальной сетью

4. Группа правил соединения с виртуальной частной сетью

Пример: изоляция соединения с корпоративной сетью

Обработка правил подключения выполняется до тех пор, пока не обнаруживается группа правил соединения с корпоративной локальной сетью. Эта группа включает в себя следующие настройки:

• Тип подключения = Проводное

• Суффикс DNS, специфический для подключения = mycompany.com

• Шлюз по умолчанию

• Изоляция соединения = Включена

Компьютер оснащен адаптером локальной сети и адаптером беспроводной сети. Компьютер подключается к корпоративной сети с помощью проводного соединения. Однако интерфейс беспроводной связи также активен, поэтому компьютер также подключается к зоне беспроводного доступа, находящейся за пределами офиса. Компьютер подключается к обеим сетям, поскольку правила основного доступа находятся в самом начале списка правил брандмауэра. Соединение с проводной локальной сетью активно и соответствует критериям соединения с корпоративной локальной сетью. Брандмауэр обрабатывает трафик, проходящий по локальной сети, но поскольку включена изоляция соединения, весь остальной трафик, проходящий не по локальной сети, блокируется.

Пример: изоляция соединения в отеле

Обработка правил соединения выполняется до тех пор, пока не обнаруживается группа правил соединения с виртуальной частной сетью. Эта группа включает в себя следующие настройки:

• Тип подключения = Виртуальное

• Суффикс DNS, специфический для подключения = vpn.mycompany.com

• IP-адрес = адрес, входящий в диапазон адресов концентратора виртуальной частной сети

• Изоляция соединения = Включена

Общие правила соединения разрешают установить временную учетную запись в отеле для доступа в Интернет. Правила соединения с виртуальной частной сетью разрешают подключение к туннелю виртуальной частной сети и его использование. После установки туннеля клиент виртуальной частной сети создает виртуальный адаптер, соответствующий критериям группы правил соединения с виртуальной частной сетью. Брандмауэр разрешает только трафик в туннеле виртуальной частной сети и основной трафик на самом адаптере. Попытки других посетителей отеля получить доступ к компьютеру через проводную или беспроводную сеть блокируются.

брандмауэр выполняет как фильтрацию, так и проверку пакетов с контролем состояния.

Фильтрация пакетов с контролем состояния представляет собой отслеживание данных протоколов TCP/UDP/ICMP с контролем состояния на транспортном уровне 4 и ниже в сетевом стеке OSI. Каждый пакет подвергается обследованию. Если проверенный пакет соответствует существующему разрешающему правилу брандмауэра, его передача разрешается, а в таблице состояний создается соответствующая запись. В таблице состояний динамически отслеживаются соединения, ранее

сопоставленные с набором статических правил, и отражается текущее состояние соединения по протоколам TCP/UDP/ICMP. Если проверенный пакет соответствует существующей записи в таблице состояний, его передача разрешается без дополнительной проверки. Если соединение закрывается или истекает срок его действия, его запись удаляется из таблицы состояний.

Проверка пакетов с контролем состояния представляет собой процесс фильтрации пакетов с контролем состояния и отслеживания команд на уровне приложений 7 в сетевом стеке OSI. Это сочетание позволяет четко определить состояние соединения компьютера. Доступ к командам уровня приложения позволяет безошибочно выполнять проверку и обеспечивать защиту протокола FTP.

Таблица состояний Firewall

Брандмауэр с контролем состояния имеет таблицу состояний, в которой динамически хранятся данные об активных соединениях, созданных разрешающими правилами.

В каждой записи определяется соединение с учетом следующих факторов:

• Протокол — предварительно определенный способ связи между службами; в частности, протоколы TCP, UDP и ICMP.

• IP-адреса локального и удаленного компьютеров – каждому компьютеру назначается уникальный IP-адрес. Протокол IPv4, текущий стандарт для IP-адресов, разрешает адреса длиной 32 бита, тогда как протокол IPv6, новый стандарт, разрешает адреса длиной 128 бит. Многие операционные системы, в том числе WindowsVista и более поздние версии Windows, поддерживают протокол IPv6. брандмауэр поддерживает оба стандарта.

• Номера портов локального и удаленного компьютеров — компьютер отправляет и получает данные служб, используя пронумерованные порты. Например, служба HTTP обычно доступна по порту 80, а FTP — по порту 21. Номера портов могут находиться в диапазоне 0–65535.

• Идентификатор процесса — уникальный идентификатор процесса, связанный с трафиком соединения.

• Метка времени — время последнего входящего или исходящего пакета, связанного с соединением.

• Время ожидания — временной предел (в секундах), по истечении которого запись удаляется из таблицы, если не получен пакет, соответствующий соединению. Время ожидания для соединений TCP принудительно применяется, только если соединение не установлено.

• Направление — направление трафика (входящий или исходящий), инициировавшего создание записи. После установки соединения двунаправленный трафик разрешается даже правилами для одного направления, при условии, что запись соответствует параметрам соединения в таблице состояний.

Вопросы по таблице состояний

• В случае изменения набора правил брандмауэра все активные соединения проверяются на соответствие новому набору правил. Если соответствующее правило не найдено, запись о соединении удаляется из таблицы состояний.

• Если адаптер получает новый IP-адрес, брандмауэр распознает новую конфигурацию и удаляет все записи в таблице состояний с неверным локальным IP-адресом.

• Когда процесс завершается, все записи в таблице состояний, связанные с процессом, удаляются.

Принцип работы фильтрации пакетов с контролем состояния

Фильтрация с контролем состояния включает обработку пакета с использованием двух наборов правил: набора настраиваемых правил брандмауэра и набора динамических правил брандмауэра или таблицы состояний.

Настраиваемые правила имеют два возможных действия:

• Разрешить — передача пакета разрешена и в таблицу состояний вносится соответствующая запись.

• Заблокировать — передача пакета блокируется и запись в таблицу состояний не вносится.

Записи в таблице состояний появляются в результате сетевой активности и отображают состояние сетевого стека. Каждое правило в таблице состояний имеет только одно действие, Разрешить, поэтому передача любого пакета, соответствующего правилу из таблицы состояний, автоматически разрешается

. Процесс фильтрации включает следующие этапы:

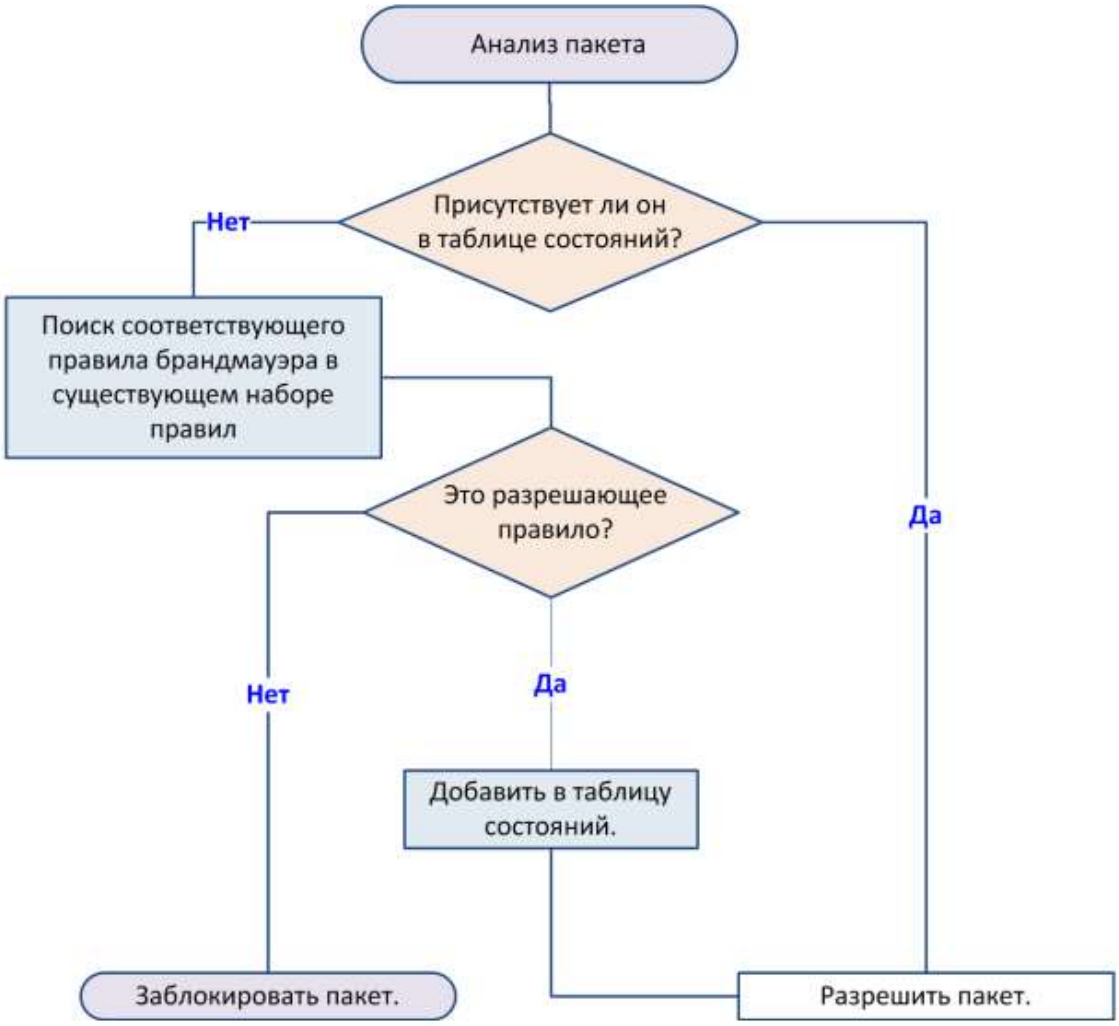
1. Брандмауэр сопоставляет входящий пакет с записями в таблице состояний. Если пакет соответствует любой из записей в таблицы, то его передача немедленно разрешается. Если нет, то проверяется весь список настраиваемых правил брандмауэра. Прим.: Пакет считается соответствующим записи в таблице состояний, если у них соответствуют

такие элементы, как «Протокол», «Локальный адрес», «Локальный порт», «Удаленный адрес» и «Удаленный порт».

2. Если пакет соответствует разрешающему правилу, его передача разрешается, а в таблице состояний создается соответствующая запись.

3. Если пакет соответствует блокирующему правилу, его передача блокируется.

4. Если пакет не соответствует ни одному из настраиваемых правил, его передача блокируется.



Принцип проверки пакетов с контролем состояния

Проверка пакетов с контролем состояния объединяет фильтрацию с контролем состояния и доступ к командам на уровне приложений, что обеспечивает защиту таких протоколов, как FTP.

В протоколе FTP используется два типа соединения: управление для команд и данные для информации. При соединении клиента с сервером FTP:

• Устанавливается канал управления на порте адресата FTP под номером 21.

• В таблице состояний создается соответствующая запись. Если включен параметр Использовать проверку протокола FTP, брандмауэр выполняет проверку с контролем состояния для всех пакетов, поступающих по каналу контроля FTP через порт 21.

Когда канал управления открыт, клиент поддерживает связь с сервером FTP. Брандмауэр анализирует команду PORT в пакете и создает в таблице состояний вторую запись, чтобы разрешить соединение для передачи данных.

Когда сервер FTP находится в активном режиме, он открывает соединение для передачи данных; в пассивном режиме это соединение инициирует клиент. Когда сервер FTP принимает первую команду передачи данных (LIST), он открывает соединение для передачи данных в сторону клиента и осуществляет передачу. После завершения передачи канал данных закрывается.

Комбинация соединения для управления и соединения для передачи данных называется сеансом. Динамические правила FTP иногда называются правилами сеанса. Сеанс считается установленным до тех пор, пока запись о канале управления этого сеанса не будет удалена из таблицы состояний. Если во время проведения периодической очистки таблицы будет удалена запись о канале управления сеанса, то впоследствии будут удалены и все записи о соединении для передачи данных

3.3. Технологія застосування модуля “ Контроль Інтернету”.

Принцип работы EndpointSecurity

EndpointSecurity перехватывает угрозы, следит за общей работоспособностью системы и составляет отчеты по обнаружениям и состоянию. Для выполнения этих задач клиентское программное обеспечение устанавливается в каждую систему.

Как правило, пользователь устанавливает один или несколько модулей EndpointSecurity в клиентские системы, управляет обнаружениями и настраивает параметры, которые определяют принцип работы функций продукта.

McAfeeePO

Развернуть модули McAfee® ePolicyOrchestrator® (McAfee® ePO™) в клиентских системах и управлять ими можно с помощью EndpointSecurity.

Каждый модуль включает в себя расширение и пакет ПО, которые устанавливаются на сервер McAfeeePO. Затем McAfeeePO развертывает ПО в клиентских системах. (McAfeeePOOn-Premises)

Клиентское программное обеспечение обменивается данными с McAfee® Agent с помощью McAfeeePO, чтобы получать обновления продукта, отчеты и конфигурацию политик, а также чтобы принудительно применять эти политики.

Модули клиента

Клиентское программное обеспечение защищает системы благодаря регулярным обновлениям, непрерывному отслеживанию и подробной отчетности.

Это ПО отправляет данные об обнаружениях на компьютерах пользователей на сервер McAfeeePO. Эти данные используются при

составлении отчетов об обнаружениях и проблемах безопасности на вашем компьютере.

Сервер TIE и Data Exchange Layer

ПриисполъзованиимодуляАдаптивнаязащитаотугрозплатформа Endpoint Security интегрируетсяс McAfee® Threat Intelligence Exchange (TIE) и McAfee® Data Exchange Layer (DXL). Эти дополнительные продукты позволяют пользователям локально управлять репутацией файлов и мгновенно предоставлять общий доступ к информации по всей среде.

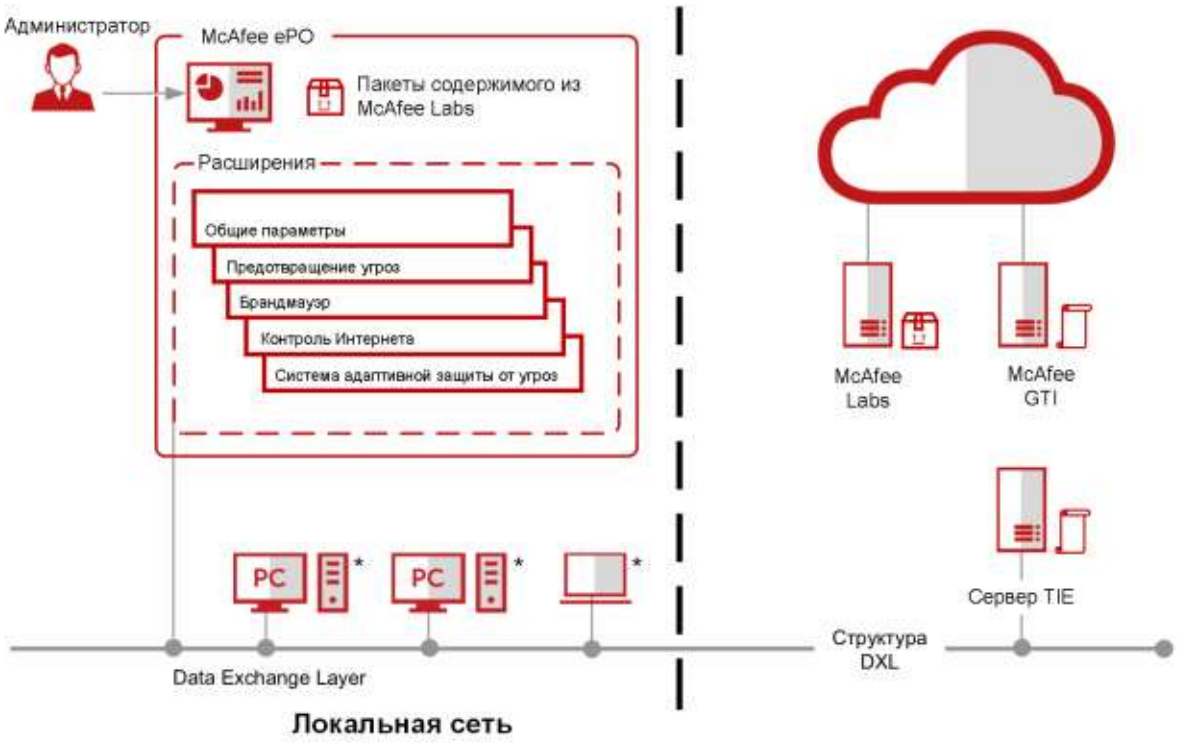
McAfee GTI

Модули предотвращение угроз, брандмауэр, контроль Интернета и Адаптивная защита от угроз отправляют запрос McAfee® GlobalThreatIntelligence™ (McAfee GTI), чтобы получить информацию о репутации и определить, как следует обрабатывать файлы в клиентской системе.

McAfeeLabs

Клиентское программное обеспечение обменивается данными с McAfeeLabs, чтобы получать файлы содержимого и обновления ядра. McAfeeLabs регулярно выпускает обновленные пакеты содержимого.

Принцип работы



* Модули клиента: "Общие параметры", "Предотвращение угроз", "Брандмауэр", "Контроль Интернета" и "Система адаптивной защиты от угроз"

Как обеспечить актуальность средств защиты

Регулярное обновление EndpointSecurity позволяет защитить компьютеры пользователей от самых новых угроз. Клиентское программное обеспечение соединяется с локальным или удаленным сервером McAfeeePO либо напрямую с сайтом в Интернете, чтобы выполнить обновление. EndpointSecurity проверяет наличие следующих обновлений.

• Обновление файлов содержимого, используемых для обнаружения угроз. Файлы содержимого содержат описание угроз, например вирусов и шпионских программ. С обнаружением новых угроз эти описания обновляются.

• Обновления компонентов программного обеспечения, например разного рода исправления.

Обзор модуля контроль Интернета

контроль Интернета в McAfeeEndpointSecurity отслеживает поиск в Интернете и просмотр веб-страниц на клиентских компьютерах. Модуль защищает от угроз на веб-страницах и в загрузках файлов.

Команда McAfee анализирует все веб-сайты и на основании результатов проверки присваивает им цветовые рейтинги безопасности. Цвет отражает уровень безопасности веб-сайта.

контроль Интернета использует эти результаты проверки для определения угроз в Интернете. ПО, установленное в клиентской системе, предоставляет дополнительные функции, которые отображаются в окне браузера и в результатах поиска для уведомления пользователей.

Развернуть модуль контроль Интернета в клиентских системах и управлять им можно с помощью McAfeeePO.

Параметры позволяют контролировать доступ к сайтам в соответствии с их рейтингом безопасности, типом содержимого, а также URL-адресом и доменным именем.

Основные функции модуля контроль Интернета

Основные функции модуля контроль Интернета направлены на защиту ваших систем от веб-угроз, обнаружение угроз и исправление ошибок, связанных с загрузкой файлов

Защита

Описанные ниже функции модуля контроль Интернета помогут вам защитить системы от вредоносных веб-сайтов и загрузок

Список блокировок и разрешений – предотвращает посещение пользователями определенных URL-адресов или доменов либо всегда разрешает доступ к сайтам, важным для вашего бизнеса.

Блокировка веб-категорий и действий на основе рейтинга – рейтинги безопасности и веб-категории, определенные McAfee, используются для контроля доступа пользователей к сайтам, страницам и загрузкам.

Безопасный поиск – автоматическая блокировка опасных сайтов из результатов поиска на основании их рейтинга безопасности.

Самозащита – запрещает пользователям отключать подключаемый модуль контроль Интернета, а также удалять или изменять файлы, разделы реестра, значения реестра, службы и процессы модуля контроль Интернета.

Обнаружение

Описанные ниже функции модуля контроль Интернета помогут вам обнаруживать вредоносные веб-сайты.

Кнопка контроль Интернета в окне браузера – в подключаемом модуле контроль Интернета отображается кнопка, указывающая рейтинг безопасности сайта. Нажмите эту кнопку, чтобы получить больше информации о сайте.

Значок контроль Интернета на страницах результатов поиска – отображается возле каждого сайта из списка. Цвет значка указывает на рейтинг безопасности сайта. Наведите курсор на этот значок, чтобы получить больше информации о сайте.

Отчеты сайта – в них содержатся подробные сведения о том, каким образом был вычислен рейтинг безопасности на основе типов обнаруженных угроз, результатов проверок и других данных.

Панели управления и мониторы – отображают статистику операций модуля контроль Интернета, включая посещения и загрузки с сайтов по рейтингу, тип содержимого, а также список блокировок и разрешений.

Запросы и отчеты – предоставление подробной информации о событиях в браузере модуля контроль Интернета с возможностью ее сохранения в отчетах.

Исправление

Описанные ниже функции модуля контроль Интернета позволяют выполнять отслеживание и настройку.

Взаимная блокировка с другими продуктами McAfee – автоматически отключает модуль контроль Интернета, если он обнаруживает устройство интернет-шлюза или если установлено McAfee® ClientProxy, а также в режиме перенаправления.

Проверка загружаемых файлов – модуль контроль Интернета отправляет файлы в модуль предотвращение угроз для проверки. В случае обнаружения угрозы модуль предотвращение угроз отвечает настроенным действием (например, очисткой) и уведомляет пользователя.

Панели управления и мониторы – отслеживают операции, чтобы понять, какие действия в Интернете вы выполняете, и затем используют эту информацию для настройки параметров модуля контроль Интернета.

Исключения – предотвращают назначение рейтинга для определенных IP-адресов и их блокировку модулем контроль Интернета.

Принцип работы модуля контроль Интернета

Модуль контроль Интернета запрашивает у McAfee GTI информацию о репутации, чтобы определить, какие действия следует предпринимать при навигации по URL-адресам.

1. Администратор настраивает параметры модуля контроль Интернета в McAfeeePO и принудительно применяет политику в клиентской системе.

2. Пользователь заходит на веб-сайт или получает доступ к его ресурсам.

3. Модуль контроль Интернета запрашивает репутацию URL-адреса у McAfee GTI.

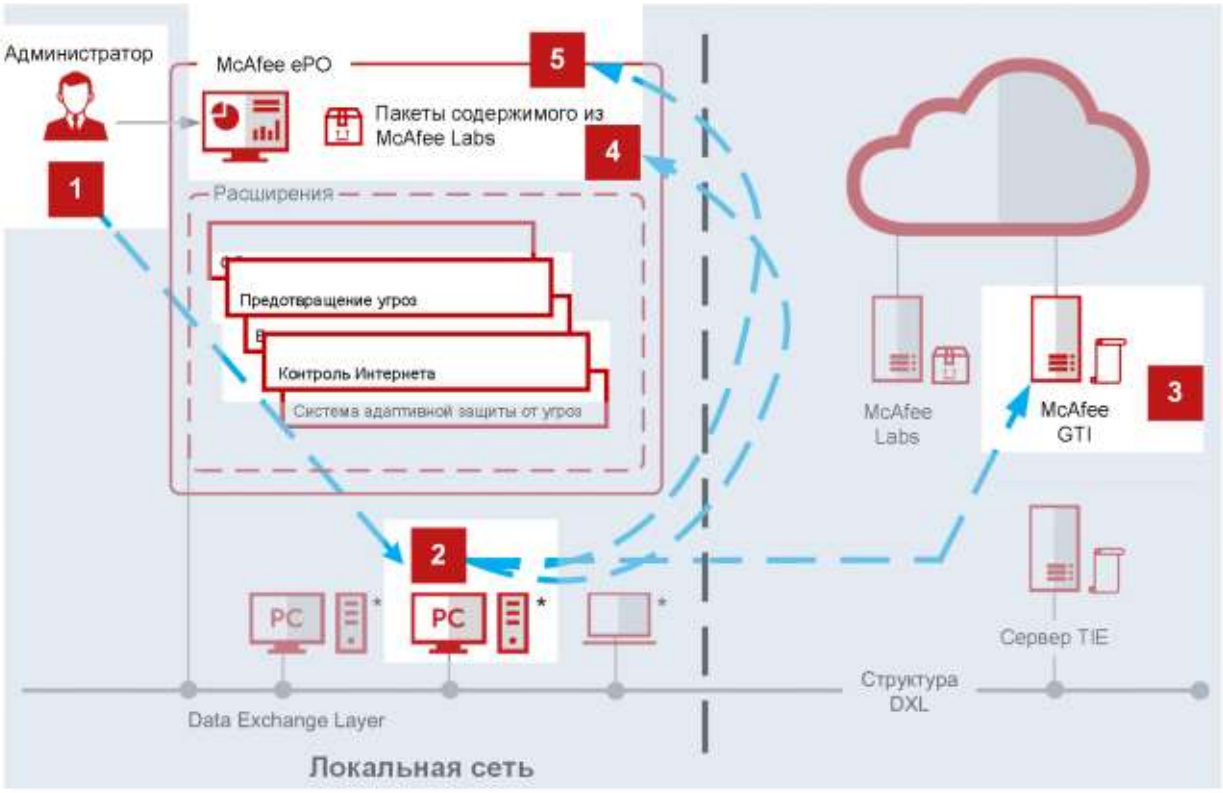
Если репутация URL-адреса зеленого цвета, модуль контроль Интернета разрешает перейти по этому URL-адресу и отображает страницу. В противном случае модуль контроль Интернета переходит на страницу блокировки или предупреждения, в зависимости от настроек.

Если репутация URL-адреса не имеет рейтинга, но соответствует категории в McAfee GTI, модуль контроль Интернета разрешает или блокирует переход по URL-адресу в зависимости от настроек Действия на основе содержимого.

4. Если это запрос на загрузку файлов, а файл не имеет репутации вредоносного, то модуль контроль Интернета разрешает загрузку, даже если URL-адрес имеет репутацию вредоносного. Если репутация файла неизвестна, контроль Интернета отправляет файл в модуль предотвращение угроз, чтобы проверить его сканером по требованию. Модуль предотвращение угроз сравнивает файл с файлом содержимого AMCore. Если его содержимое соответствует сигнатуре или хэшу, загрузка файла блокируется. В другом случае файл загружается.

5. Модуль Модуль контроль Интернета регистрирует сведения, а затем создает событие и отправляет его в McAfeeePO.

Принцип работы



* Модули клиента: "Общие параметры", "Предотвращение угроз", "Брандмауэр", **"Контроль Интернета"** и "Система адаптивной защиты от угроз"

Модуль контроль Интернета и McAfeeClientProxy

Когда модуль контроль Интернета отключен из-за наличия ClientProxy, который выполняет перенаправление:

модуль контроль Интернета игнорирует действия, связанные с рейтингом и принудительным применением;

элементы управления браузером модуля контроль Интернета отключаются.

На странице Состояние Клиент EndpointSecurity для модуля контроль Интернета отображается состояние Отключен.

На странице Параметры Клиент EndpointSecurity указано, что модуль контроль Интернета отключен, поскольку обнаружен ClientProxy.

Использование модуля "Контроль Интернета" в клиентской системе

Включение подключаемого модуля контроль Интернета из браузера в клиентской системе

В зависимости от настроек необходимо вручную включить подключаемый модуль контроль Интернета, чтобы получать уведомления о небезопасных веб-страницах при их просмотре и поиске.

Подготовка

Модуль контроль Интернета должен быть включен в параметрах.

Подключаемые модули также называют дополнениями в Edge, Chrome и Firefox и надстройками в InternetExplorer.

В InternetExplorer и Chrome при первом запуске может быть предложено включить подключаемые модули. Самые актуальные сведения см. в статье базы знаний KB87568.

Процедура

Включите подключаемый модуль, выполнив соответствующие действия в браузере.

Edge	Если расширение контроль Интернета не включается автоматически, выполните указанные ниже действия. 1. В меню выберите Расширения. 2. Переведите переключатель Контроль Интернета в Endpoint Security в положение Вкл.
Chrome	Когда отобразится соответствующий запрос, щелкните Включить расширение. Если Chrome не предложит вам включить подключаемый модуль контроль Интернета, включите его вручную, выполнив следующие действия: 1. Нажмите Параметры → Расширения. 2. Щелкните Включить, чтобы активировать контроль Интернета.
Firefox	Если Firefox не предложит вам включить дополнение контроль Интернета, включите его вручную, выполнив следующие действия: 1. Выберите в меню Дополнения → Расширения. 2. Щелкните Включить, чтобы активировать контроль Интернета.
Internet Explorer	• При отображении запроса нажмите кнопку Включить. • Если доступно несколько подключаемых модулей, нажмите Выбрать надстройки, а затем нажмите Включить для панели инструментов модуля контроль Интернета. • Чтобы сделать это вручную, выберите в меню пункт Управление дополнениями, выберите Контроль Интернета в Endpoint Security, а затем щелкните Включить. **Примечание:** В Internet Explorer при отключении панели инструментов контроль Интернета предлагается также отключить подключаемый модуль контроль Интернета. Подключаемый модуль контроль Интернета остается включенным, даже когда панель инструментов не отображается, если параметры политики запрещают удалять и отключать подключаемый модуль.

Получение информации о просматриваемом веб-сайте

Вы можете получить информацию о веб-сайте с помощью кнопки контроль Интернета в браузере. В разных браузерах кнопка работает по-разному.

Модуль контроль Интернета должен быть включен.

Подключаемый модуль контроль Интернета должен быть включен в браузере.

В настройках Параметры должен быть отключен параметр Скрыть панель инструментов в браузере клиента.

Процедура

(Только для InternetExplorer) Откройте сводные сведения о рейтинге безопасности для веб-сайта: наведите курсор на кнопку в браузере

Откройте меню:

Edge **Chrome** **Firefox**	Нажмите кнопку  в адресной строке.
Internet Explorer	Нажмите кнопку на панели инструментов.

3. Просмотрите подробные сведения о веб-сайте, включая результаты анализа, рейтинг и категорию:

a. Выберите в меню пункт Просмотреть отчет о веб-сайте. В новом окне браузера откроется страница Центр угроз McAfee.

b. В разделе Поиск в библиотеке выберите URL/адрес веб-сайта.

c. Введите имя веб-сайта и щелкните Перейти.

Получение информации о сайте из результатов поиска

Подробные сведения о сайте, включая данные о рейтинге и категории, можно получить на странице результатов поиска.

Управление модулем "Контроль Интернета" в клиентской системе

Включение модуля контроль Интернета и настройка его параметров в клиентской системе

Можно включить модуль контроль Интернета и настроить его параметры из Клиент EndpointSecurity.

Подготовка Установите для режима интерфейса Клиент EndpointSecurity значение Полный доступ или войдите в Клиент EndpointSecurity как администратор.

Действие	Инструкции	Примечания
Перевод панели инструментов модуля контроль Интернета в браузере в скрытый режим без отключения защиты. (только Internet Explorer)	Выберите Скрыть панель инструментов в браузере клиента.	
Разрешение для пользователей запускать Internet Explorer с параметром командной строки `-extoff`. (Управляемые системы) (только Internet Explorer)	Выберите Разрешить пользователю запускать Internet Explorer в режиме без расширений.	**Внимание:** В режиме отключенных расширений Internet Explorer не загружает *никакие* расширения и надстройки. Хотя модуль контроль Интернета включен в системе, он не загружается в браузер, и система будет уязвимой для угроз.
Отслеживание событий браузера.	Настройте параметры в разделе Ведение журнала событий.	
Блокировка или отображение предупреждения для неизвестных URL-адресов.	На вкладке Принудительное применение действия выберите действие (Заблокировать, Разрешить или Предупредить) для сайтов, еще не проверенных McAfee GTI.	
Проверка файлов перед загрузкой.	В разделе Принудительное применение действия установите флажок Включить проверку файлов для загрузок файлов, а затем выберите уровень риска McAfee GTI для блокировки.	Если пользователи указывают полный URL-адрес файла, имеющего репутацию не вредоносного, контроль Интернета разрешает загрузку файла, даже если сайт заблокирован.

Действие	Инструкции	Примечания
Добавление дополнительных сайтов в локальную частную сеть.	На вкладке Исключения в разделе Укажите IP-адреса или их диапазоны, которые необходимо исключить из рейтинга контроля Интернета или блокировки нажмите Добавить и введите внешний IP-адрес или диапазон.	
Блокировка подозрительных сайтов в результатах поиска.	На вкладке Безопасный поиск выберите Включить безопасный поиск, выберите поисковую систему, а затем укажите, необходимо ли блокировать ссылки на подозрительные сайты.	Функция Безопасный поиск автоматически отфильтровывает вредоносные сайты из результатов поиска на основании рейтинга их безопасности. контроль Интернета использует Yahoo в качестве поисковой системы по умолчанию и поддерживает функцию Безопасный поиск только в Internet Explorer. При изменении поисковой системы по умолчанию необходимо перезапустить браузер, чтобы изменения вступили в силу. В следующий раз при запуске Internet Explorer модуль контроль Интернета отобразит всплывающее окно с предложением использовать функцию безопасного поиска McAfee с указанной поисковой системой. В версиях браузера Internet Explorer, в которых эта поисковая система заблокирована, всплывающее окно безопасного поиска не отображается.

Указание действий на основе рейтинга и блокировка доступа к вебсайтам на основе веб-категории в клиентской системе

Можно указать действия, которые необходимо применить к сайтам и загрузкам файлов на основе рейтингов безопасности. Кроме того, можно блокировать или разрешать сайты в каждой веб-категории.

Установите для режима интерфейса Клиент EndpointSecurity значение Полный доступ или войдите в Клиент EndpointSecurity как администратор.

3.4. Технологія застосування модуля “Адаптивний захист від загроз”.

Использование модуля "Система адаптивной защиты от угроз" в клиентской системе

Ответные действия при определении репутации файла

При попытке запустить файл с определенной репутацией на вашем компьютере Адаптивная защита от угроз может отобразить запрос о дальнейших действиях. Запрос отобразится только в том случае, если Адаптивная защита от угроз установлена и настроена на отображение запроса.

Прим.: Адаптивная защита от угроз использует системный значок на панели задач McAfee для отображения запросов. В системах, доступ к которым осуществляется только с помощью удаленного рабочего стола, значок на панели задач не запускается и запросы не отображаются. Чтобы обойти эту проблему, добавьте UpdaterUI.exe в сценарий входа.

Администратор настраивает пороговое значение репутации, при котором отображается запрос. Например, если пороговое значение репутации "Неизвестно", EndpointSecurity выдает запросы для всех файлов с репутацией "Неизвестно" и ниже.

Если вы не выбрали определенный параметр, Адаптивная защита от угроз выполнит действие по умолчанию, заданное администратором.

Сообщение с запросом, тайм-аут и действие по умолчанию зависят от конфигурации Адаптивная защита от угроз.

Прим.: В Windows 8 и 10 используются всплывающие уведомления – всплывающие сообщения с предупреждениями и запросами. Щелкните всплывающее уведомление, чтобы отобразить уведомление в режиме рабочего стола.

task_mcafee

1. (Необязательно) При появлении запроса введите сообщение для администратора. Например, используйте сообщение, чтобы описать файл или объяснить ваше решение о разрешении или блокировании в системе.

2. Выберите Разрешить или Заблокировать.

Разрешить	Разрешение использовать файл.
Заблокировать	Блокировка файла в системе.

Чтобы указать Адаптивная защита от угроз не повторять запрос для этого файла, выберите Запомнить это решение.

Результат

Адаптивная защита от угроз действует на основании вашего выбора или действия, заданного по умолчанию, и закрывает окно с запросом.

Проверка состояния подключения

Чтобы определить, получает ли модуль Адаптивная защита от угроз в клиентской системе сведения о репутации файлов с сервера TIE или McAfee GTI, перейдите на страницу Сведения с информацией о Клиент EndpointSecurity.

1. ОткройтеКлиент Endpoint Security.

2. В меню Действие выберите Сведения.

3. Щелкните Адаптивная защита от угроз в левой части экрана. В поле Состояние подключения указано одно из следующих значений для Адаптивная защита от угроз:

Возможно подключение к анализу угроз – подключение к серверу TIE для получения сведений о репутации корпоративного уровня.

Возможно подключение только к McAfee GTI – подключение к McAfee GTI для получения сведений о репутации глобального уровня.

Управление модулем "Система адаптивной защиты от угроз" в клиентской системе

Обработка ложных положительных результатов с помощью файлов Extra.DAT

Когда Адаптивная защита от угроз определяет, что обнаружение – это ложный положительный результат, McAfeeLabs выпускает отрицательный файл Extra.DAT, чтобы скрыть обнаружение.

Прим.: Файлы ExtraDAT для определенных угроз можно загрузить со страницы Обновления безопасности McAfeeLabs.

Адаптивная защита от угроз поддерживает использование только одного файла Extra.DAT одновременно. Если необходимо использовать отрицательный и положительный файлы Extra.DAT для модуля предотвращение угроз, пользователь может запросить объединенный файл в McAfeeLabs

Каждый файл Extra.DAT имеет встроенную дату истечения срока действия. При загрузке файла Extra.DAT эта дата сравнивается с датой сборки содержимого AMCoreContent, установленного в системе. Если дата сборки содержимого AMCore идет позже даты истечения срока действия файла ExtraDAT, такой файл ExtraDAT считается недействительным. Он больше не загружается и не используется модулем. В ходе следующего обновления файл Extra.DAT удаляется из системы.

Если следующее обновление содержимого AMCore включает в себя сведения из файла ExtraDAT, файл ExtraDAT удаляется. Endpoint Security сохраняетфайлы Extra.DAT впапке c:\Program Files\Common Files\McAfee\Engine\content\avengine \extradat.

Загрузка файла Extra.DAT в клиентскую систему

Загрузите файл ExtraDAT и активируйте его для системы с помощью Клиент EndpointSecurity.

Установите для режима интерфейса Клиент EndpointSecurity значение Полный доступ или войдите в систему как администратор

1. ОткройтеКлиент Endpoint Security.

2. В меню Действие выберите Загрузить Extra.DAT.

3. Щелкните Обзор, перейдите в папку, в которую вы загрузили файл Extra.DAT, затем щелкните Открыть.

4. Нажмите Применить.

Результат

Сведения об обнаруженных угрозах, содержащиеся в файле ExtraDAT, вступают в силу немедленно.

Динамическое ограничение приложений

Динамическое ограничение приложений позволяет настроить запуск в контейнере для приложений с определенной репутацией.Ограниченные приложения не могут выполнять некоторые действия в соответствии с правилами ограничения.

В зависимости от порога репутации Адаптивная защита от угроз потребует от функции динамического ограничения приложений запустить приложение в контейнере.

Эта технология позволяет пользователю оценивать неизвестные и потенциально опасные приложения, разрешая им запуск в среде, но ограничивая при этом их действия. Пользователи могут пользоваться приложениями, однако приложения могут работать не так, как ожидалось,

поскольку динамическое ограничение приложений блокирует определенные действия. Если пользователь решит, что приложение безопасно, он сможет настроить Адаптивная защита от угроз EndpointSecurity или сервер TIE так, чтобы приложение работало в обычном режиме. Использование динамического ограничения приложений

1. Включите Адаптивная защита от угроз и укажите порог репутации для срабатывания функции динамического ограничения приложений в разделе Параметры.

2. Настройте определенные McAfee правила ограничения и исключения в настройках функции Динамическое ограничение приложений.

Мониторинг активности модуля "Система адаптивной защиты от угроз" в клиентской системе

Поиск недавних действий в журнале событий

В журнале событий Клиент EndpointSecurity отображаются все события, которые произошли в системе, защищенной McAfee.

task_mcafee

1.ОткройтеКлиент Endpoint Security.

2.В левой части страницы щелкните Журнал событий. На странице отображаются все события, зарегистрированные программой EndpointSecurity в системе за последние 30 дней. Если Клиент EndpointSecurity не может связаться с диспетчером событий, он показывает сообщение об ошибке связи. В этом случае для просмотра журнала событий необходимо перезагрузить систему.

3.Выберите событие в верхней панели, чтобы просмотреть его подробности в нижней панели. Чтобы изменить относительный размер панелей, нажмите значок переплета и перетащите его между панелями.

4.На странице журнала событий можно сортировать, фильтровать и перезагружать события, а также выполнять их поиск.

5.Найдите необходимые сведения в журнале событий. По умолчанию на странице журнала событий отображается 20 событий. Чтобы отображать больше событий, выберите параметр Количество событий на страницу в раскрывающемся списке

Имена и расположения файлов журналов Адаптивная защита от угроз

В файлы журнала активности, ошибок и отладки записываются события, происходящие в системах, защищенных с помощью EndpointSecurity.

Все файлы журналов активности и отладки хранятся в следующем расположении по умолчанию:

Все модули хранят сведения об ошибках в едином файле EndpointSecurityPlatform_Errors.log.

Включение журнала отладки для любого модуля также позволяет активировать ведение журнала отладки модуля Общие параметры для таких функций, как самозащита.

Табл. 1: Файлы журнала

Модуль	Функция или технология	Имя файла
Адаптивная защита от угроз		AdvancedThreatProtection_Activity.log
		AdvancedThreatProtection_Debug.log
	Динамическое ограничение приложений	DynamicApplicationContainment_Activity.log
		DynamicApplicationContainment_Debug.log
Общие параметры	Ошибки	EndpointSecurityPlatform_Errors.log Содержит журналы ошибок для всех модулей.

ВИСНОВКИ

В магістерській роботі проведено дослідження та аналіз проблеми забезпечення захисту кінцевих точок корпоративної інформаційної системи, встановлена сутність завдань захисту кінцевих точок корпоративної інформаційної системи.

Проаналізовано існуючі технології захисту кінцевих точок корпоративної інформаційної системи та обрано рішення Mc Afee Endpoint Security.

Визначено методи та засоби забезпечення захисту кінцевих точок корпоративної інформаційної системи, які реалізовані в McAfeeEndpointSecurity.

Встановлено основні функції та принципи роботи реалізації захисту кінцевих точок корпоративної інформаційної системи в McAfeeEndpointSecurity.

Технологія та програмне забезпечення McAfeeEndpointSecurity - це розширюване комплексне рішення для забезпечення кібербезпеки, яке захищає сервери, комп'ютерні системи, ноутбуки та планшети від відомих і невідомих загроз. Ці загрози включають в себе шкідливі програми, підозрілі з'єднання, небезпечні веб-сайти і завантажені файли.

Встановлено, що Mc Afee Endpoint Security забезпечує роботу декількох технологій для забезпечення безпеки, які обмінюються даними в режимі реального часу, щоб аналізувати загрози і захищати від них.

McAfeeEndpointSecurity складається з наступних модулів безпеки:

- модуль Запобігання загрозам – не дозволяє загрозам проникнути в систему, автоматично перевіряє файли при доступі і виконує цільові перевірки на наявність шкідливих програм в клієнтських системах;

- міжмережевий екран– відстежує обмін даними між комп'ютером і ресурсами в мережі і в Інтернеті. Перехоплює підозрілі повідомлення;

- модульКонтроль Інтернету – відстежує пошук і перегляд сторінок в Інтернеті в клієнтських системах і блокує вебсайти та завантаження в залежності від рейтингу і вмісту безпеки;

- модуль Адаптивний захист від загроз – аналізує вміст в корпоративному середовищі користувача і визначає, які дії виконувати, використовуючи дані про репутацію файлів, правила і граничні значення репутації. Модуль Адаптивний захист від загроз – це додатковий модуль EndpointSecurity.

У модулі Загальні параметри можна налаштувати загальні функції, наприклад захист інтерфейсу і реєстрацію подій в журналі. Цей модуль встановлюється автоматично при установці будь-якого іншого модуля. Всі модулі інтегруються в єдиний інтерфейс McAfeeEndpointSecurity в клієнтській системі. Кожен модуль працює в комплексі з іншими і автономно, щоб забезпечити кілька рівнів захисту.

Встановлено принцип роботи McAfeeEndpointSecurity, який полягає в перехопленні загрози, відстежуванні за загальним станом системи і складанні звітів за виявленням і станом.

У роботі запропоновано варіант топології системи захисту кінцевих точок корпоративної інформаційної системи підприємства.Для виконання цих завдань клієнтське програмне забезпечення має встановлюватися в кожну окрему систему – актив корпоративної інформаційної системи. На активах корпоративної інформаційної системи встановлюється один або кілька модулів рішення McAfeeEndpointSecurity, налаштовуються функції і здійснюється керуваннявиявленнями. Зазвичай клієнтське програмне

забезпечення працює у фоновому режимі і не вимагає ніяких дій з боку користувача.

Таким чином, реалізація технології захисту кінцевих точок (активів) корпоративної інформаційної системи на основі рішення McAfeeEndpointSecurity забезпечить ефективний захист інформації та кібербезпекукорпоративної інформаційної системи підприємства.