Практична робота №2

Тема: Настроювання параметрів локальної політики безпеки в операційній системі.

Мета:

навчальна: навчитися налаштовувати операційну систему для безпечного користування, опанувати методи та способи захисту ОС;

розвиваюча: навчитися діяти згідно інструкції, розвивати логічне мислення, аналізувати свою діяльність та робити висновки;

виховна: виховувати комп'ютерну грамотність;

Обладнання: ПК за операційною системою Windows 10.

Теоретичні відомості:

Кожен користувач повинен піклуватися про безпеку свого комп'ютера. Для цього часто вмикають брандмауер Windows, встановлюють антивірус і інші захисні інструменти, але цього не завжди вистачає. Вбудований засіб операційної системи «Локальна політика безпеки» дозволить кожному вручну оптимізувати роботу облікових записів, мереж, редагувати відкриті ключі та виконати інших дій, пов'язані з налагодженням захищеного функціонування ПК.

Хід роботи

1. Оберіть вірні рекомендації, щодо використання паролю:

- ☐ використовувати пароль завдовжки не менше 10 символів;
- ☐ пароль повинен бути якомога меншим, що б його легко можна було запам'ятати;
- ☐ суміщати в паролі символи верхнього і нижнього регістру, цифри та інтервали;
- ☐ бажано використовувати лише цифри;
- ☐ використовувати один і той же пароль на різних ресурсах;
- ☐ уникати слів, які мають змістовне значення;
- ☐ уникати використання особистої інформації;
- ☐ пароль бажано зберігати записаним у надійному місці;
- ☐ запам'ятовувати, а не записувати пароль.

2. Брандмауер – це _____

_____

_____

_____

3. Групова політика в операційній системі дає можливість _____

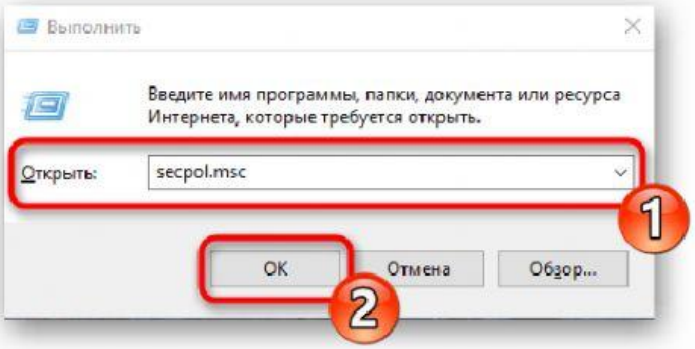
_____

_____

_____

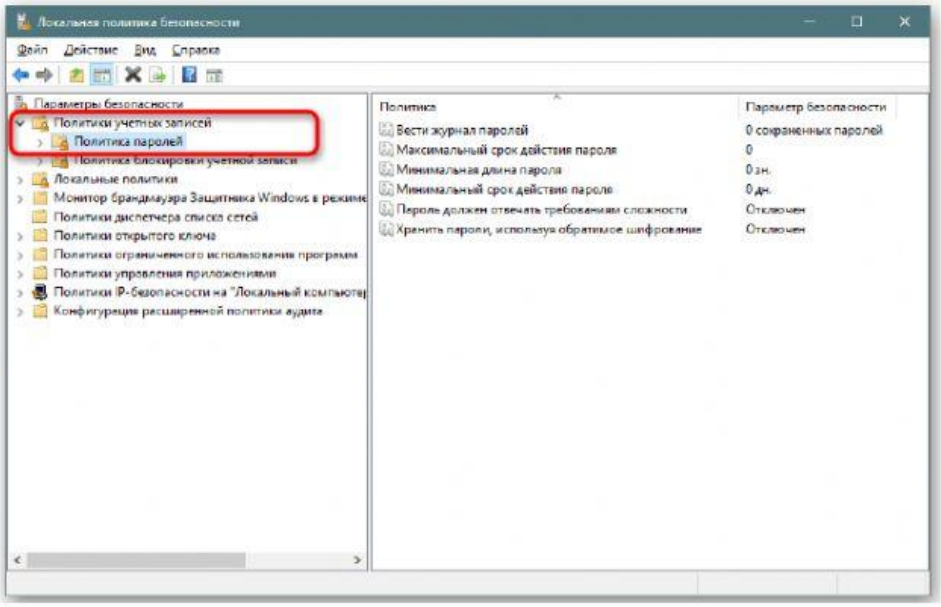
4. Відкриваємо *Локальну політику безпеки* в Windows 10.

Відкрийте *Виконати*, затиснувши комбінацію клавіш *Win + R*. У полі напишіть secpol.msc, після чого натисніть на клавішу *Enter* або клацніть на *OK*.

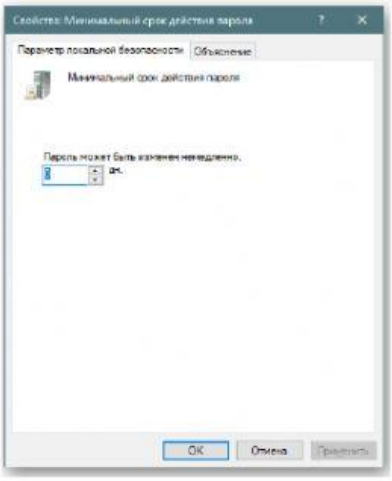


5. Налаштування політики облікових записів.

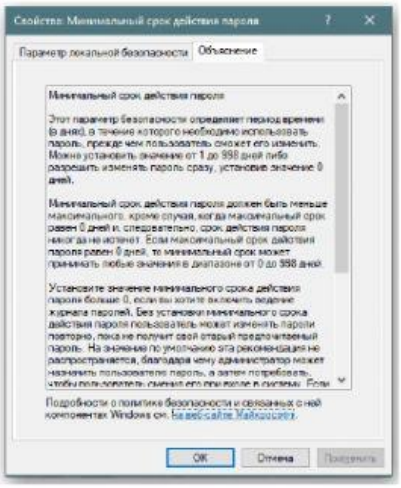
Розгорніть *Політика облікових записів* і відкрийте розділ *Політика паролів*. Справа відображається список властивостей, кожен з яких відповідає за обмеження або виконання дій. Наприклад, в пункті *Мінімальна довжина пароля* можна вказати кількість знаків, а в *Мінімальний термін дії пароля* – кількість днів на блокування його зміни.



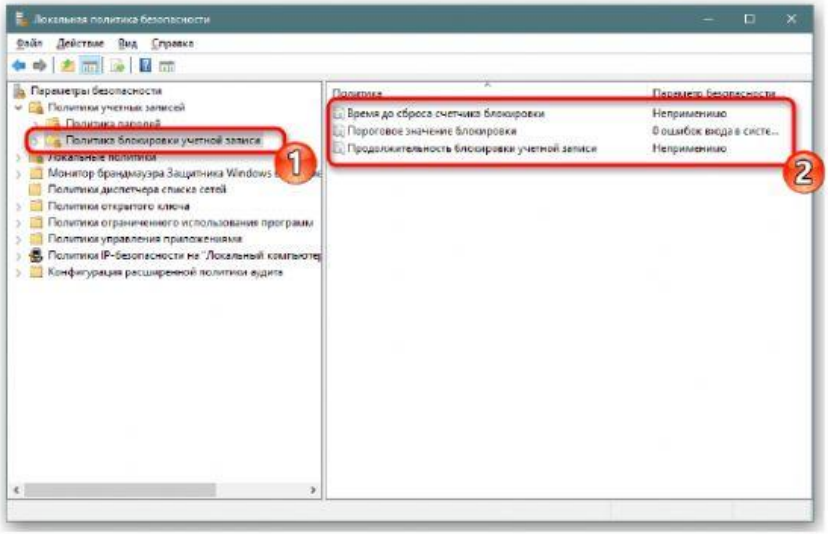
Двічі клацніть на одному з параметрів, щоб відкрити окреме вікно з властивостями. Як правило, тут присутня обмежена кількість налаштувань. Наприклад, в *Мінімальний термін дії пароля* можливо тільки виставити кількість днів.



У вкладці *Пояснення* знаходиться детальний опис кожного параметра від розробників. Зазвичай воно розписано досить широко, але більша частина інформації очевидною, тому її можна опустити, виділивши тільки основні моменти особисто для себе.



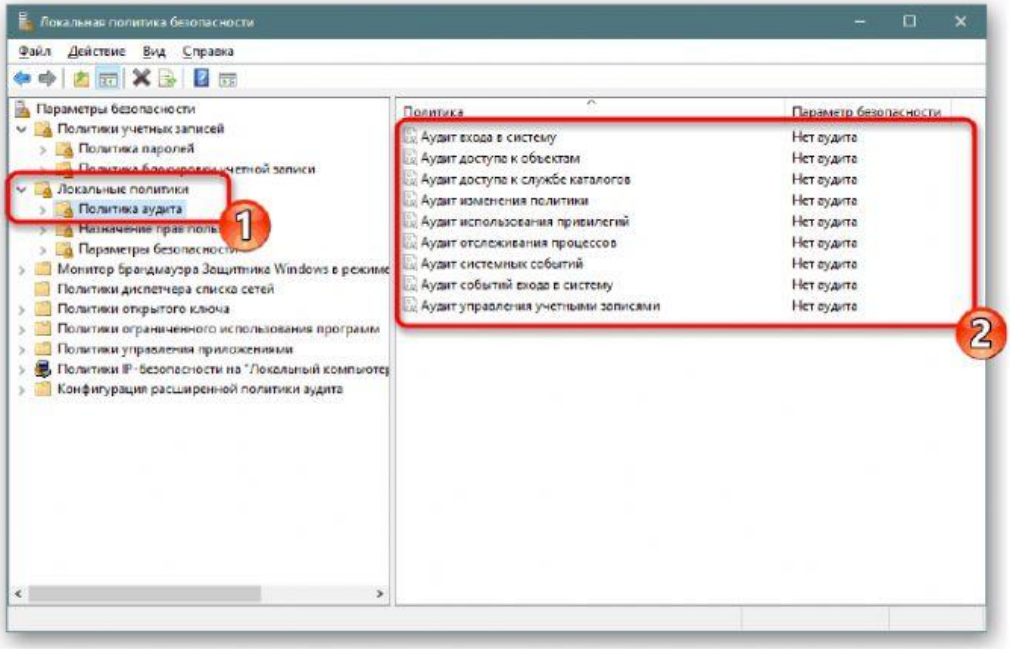
У папці *Політика блокування облікового запису* присутній три політики. Тут доступна установка часу до скидання лічильника блокування, порогове значення блокування (кількість помилок введення пароля при вході в систему) і тривалість блокування профілю користувача.



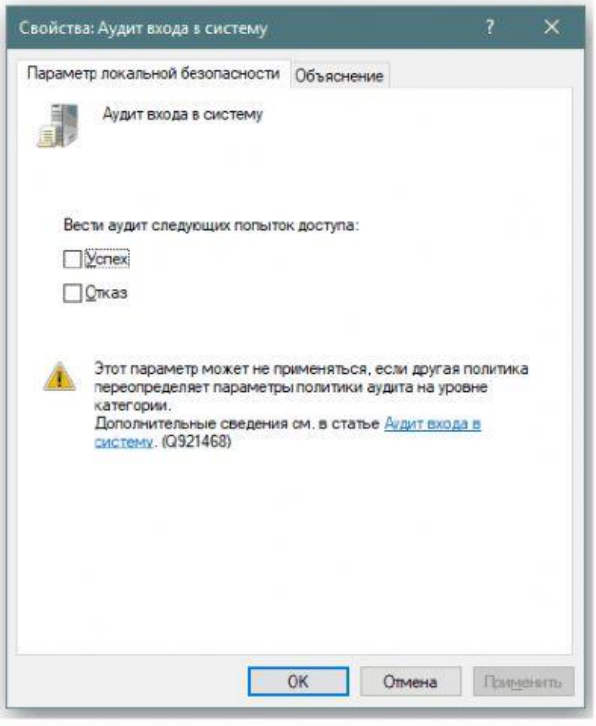
6. Локальні політики.

У розділі *Локальні політики* зібрано відразу кілька груп параметрів: *Політика аудиту, Призначення прав користувачу, Параметри безпеки.*

Аудит – процедура спостереження за діями користувача з подальшим занесенням їх в журнал подій і безпеки.

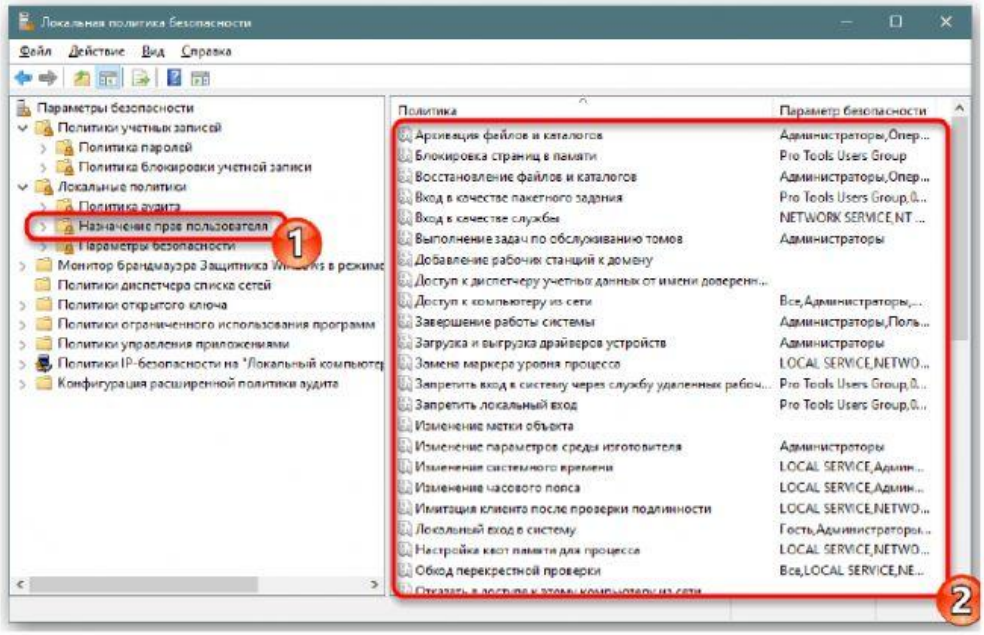


Якщо встановлено значення *Ні аудиту*, дії відслідковуватися не будуть. У властивостях ж на вибір надається два варіанти – *Відмова* і *Успіх*. Оберіть пункт на одному з них або відразу на обох, щоб зберігати успішні і перервані дії.

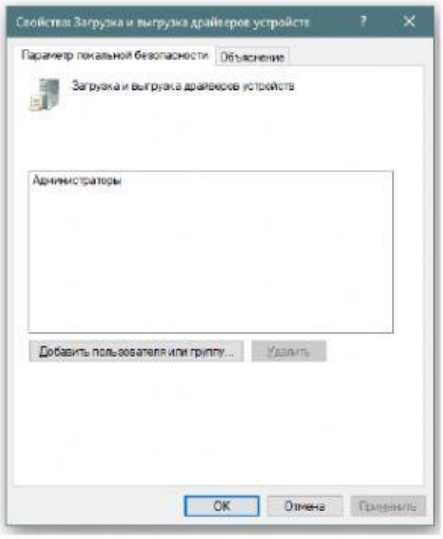


У папці *Призначення прав користувача* зібрані налаштування, що дозволяють надати групам користувачів доступ для виконання певних процесів, наприклад, вхід в

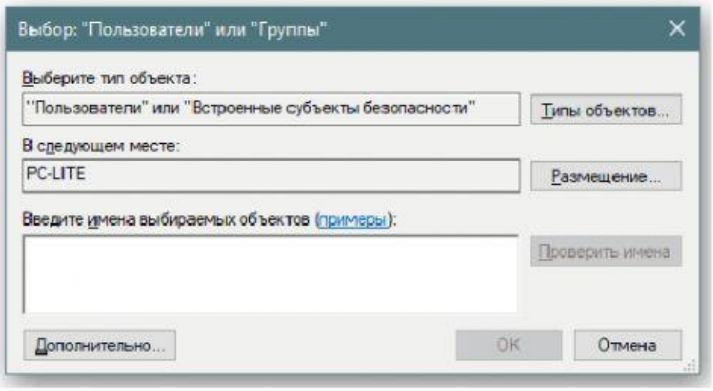
якості служби, можливість підключення до інтернету, установка або видалення драйверів пристроїв і багато іншого. Ознайомтеся з усіма пунктами і їх описом.



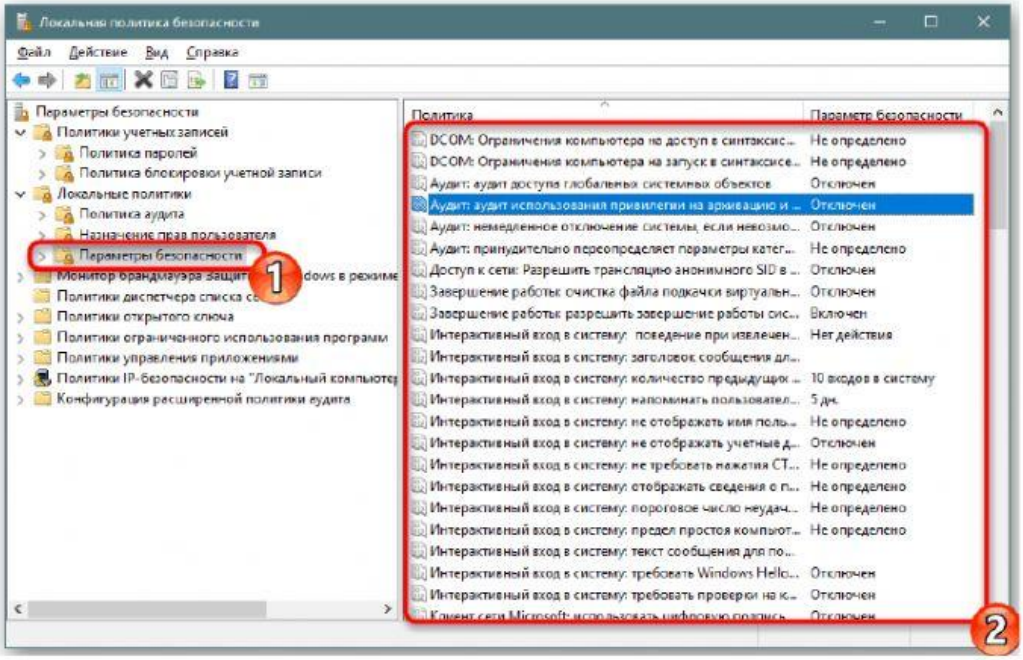
У *Властивості* вказаний перелік груп користувачів, яким дозволено здійснення заданої дії.



В окремому вікні відбувається додавання груп користувачів або певних облікових записів з локальних комп'ютерів. Потрібно лише вказати тип об'єкта і його розміщення, а після перезавантаження комп'ютера всі зміни вступлять в силу.

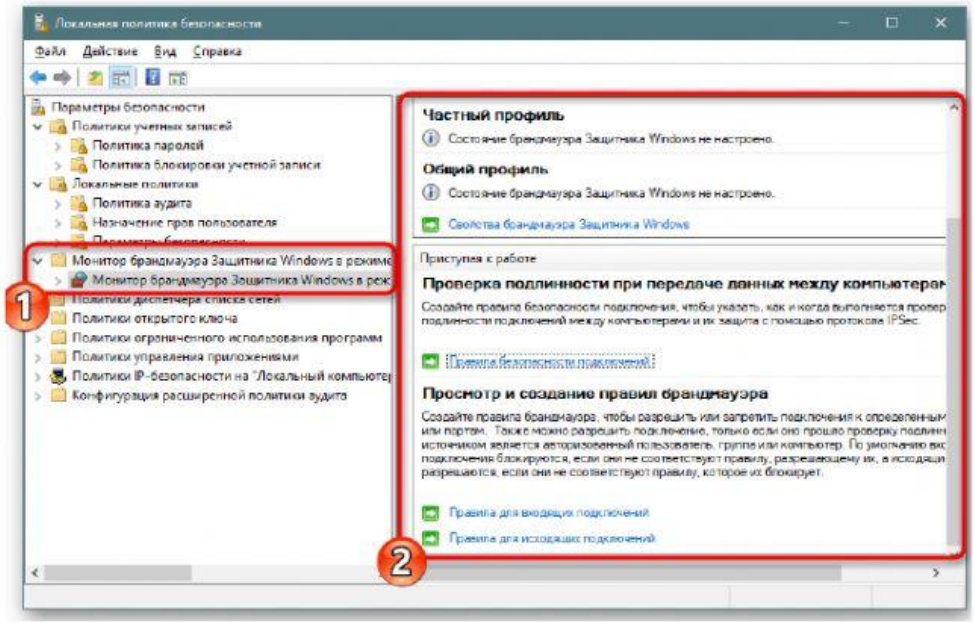


Розділ *Параметри безпеки* присвячений забезпеченню захищеності двох попередніх політик. Тобто тут можна налаштувати аудит, який буде відключати систему при неможливості додавання відповідного запису аудиту у журнал, або ж встановити обмеження на кількість спроб введення пароля. Параметрів тут налічується більше тридцяти. Умовно їх можна розділити на групи – інтерактивний вхід в систему, контроль облікових записів, мережевий доступ, пристрої та мережева безпека. У властивостях можливо активувати або відключати кожну з цих налаштувань.



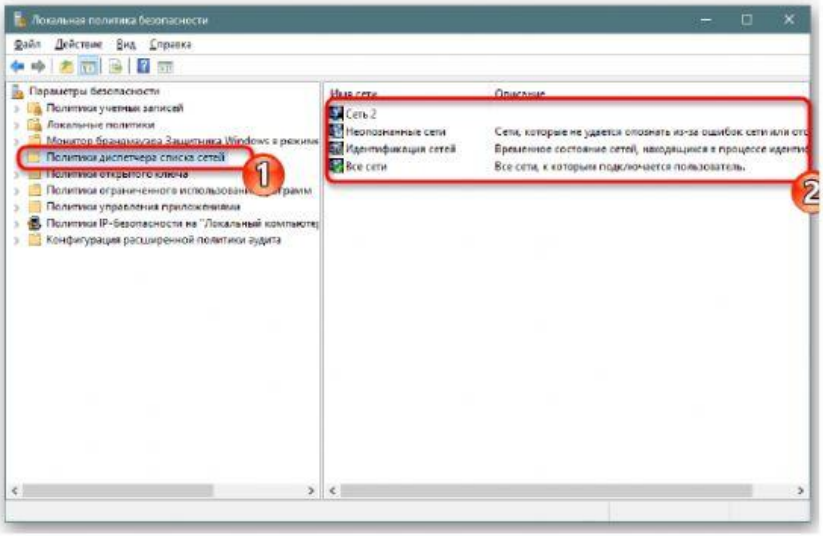
7. Монітор брандмауера для програми Windows Defender

У *Монітор брандмауера Захисника Windows в режимі підвищеної безпеки* є створення правил для програм, портів або зумовлених з'єднань. Тут можливо блокувати або дозволяти підключення, вибравши при цьому мережу і групу. У цьому ж розділі відбувається визначення типу безпеки підключення.



8. Політики диспетчера списку мереж

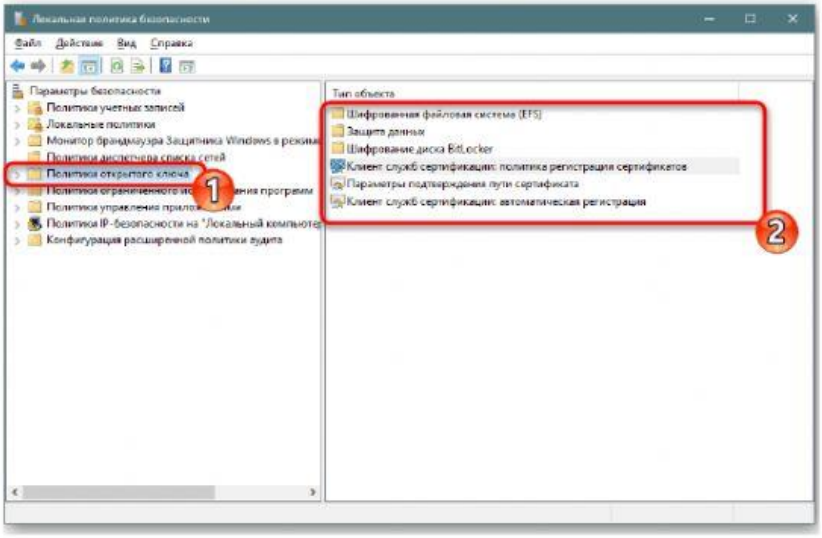
У папці *Політики диспетчера списку мереж* кількість параметрів залежить від активних і доступних інтернет-з'єднань. Наприклад, пункт *Невідомі мережі* або *Ідентифікація мереж* буде присутній завжди, а *Мережа 1*, *Мережа 2* і так далі – в залежності від реалізації мережевого оточення.



У властивостях можна вказати ім'я мережі, додати дозвіл для користувачів, встановити власний значок або задати розташування. Все це доступно для кожного параметра і має застосовуватися окремо. Після виконання змін потрібно їх застосовувати і перезавантажувати комп'ютер, щоб вони вступали в силу. Іноді може знадобитися і перезавантаження роутера.

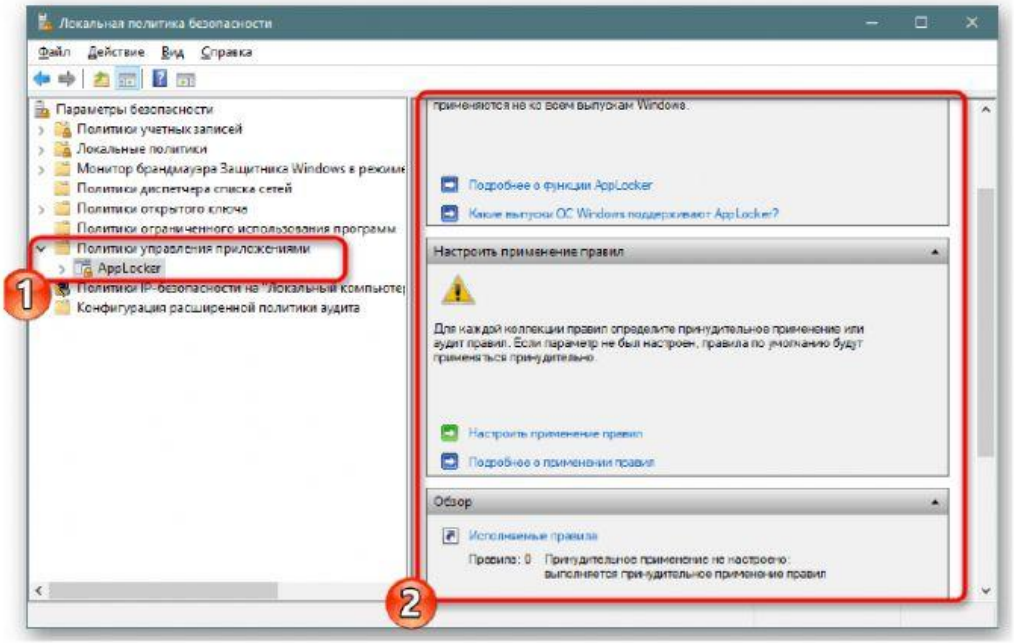
9. Політики відкритого ключа

Розділ *Політики відкритого ключа* найчастіше використовується на комп'ютерах на підприємстві, де для здійснення криптографічних операцій або інших захищених маніпуляцій задіяні відкриті ключі і центри специфікацій. Все це дозволяє гнучко проводити контроль взаємодії між пристроями, забезпечивши стабільну і безпечну мережу.

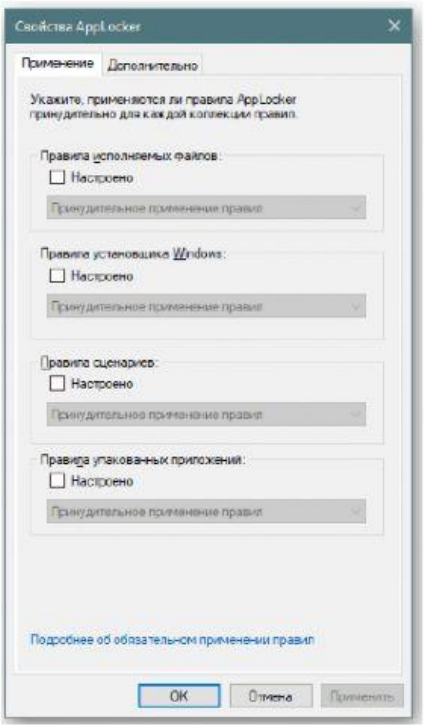


10. Політики управління додатками

У *Політики управління додатками* знаходиться інструмент *AppLocker*, що містить різноманітні функції і налаштування, що дозволяють регулювати роботу з програмами. Наприклад, дозволяє створити правило, яке обмежує запуск всіх програм, окрім зазначених, або встановити обмеження на зміну файлів програмами, задавши окремі аргументи і виключення.



В меню *Властивості* застосування правил налаштовується для колекцій. Наприклад, виконувані файли, інсталятор Windows, сценарії і упаковані програми. Кожне значення може застосовуватися примусово, в обхід інших обмежень *Локальної політики безпеки*.

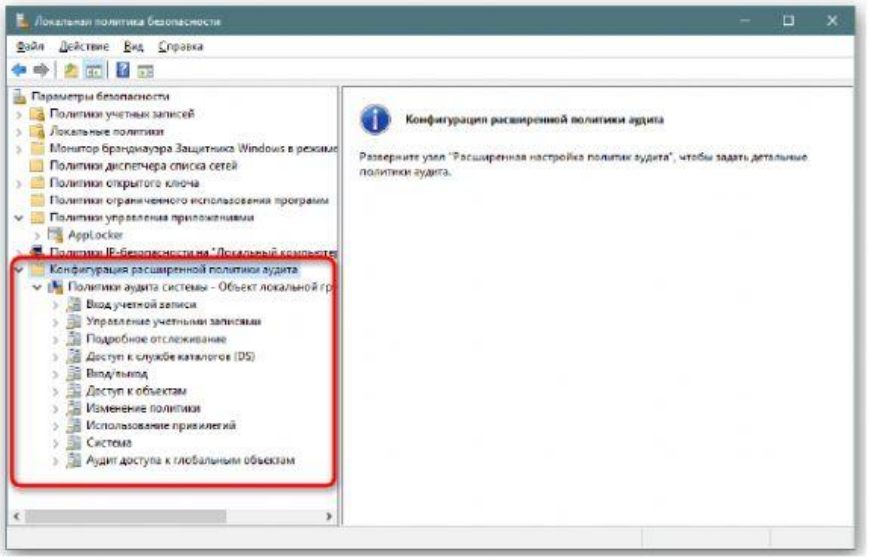


11. Політики IP-безпеки на «Локальний комп'ютер»

Налаштування в розділі *Політики IP-безпеки на «Локальний комп'ютер»* мають деяку схожість з тими, що доступні в веб-інтерфейсі роутера. Наприклад, включення шифрування трафіку або його фільтрація. Користувач сам створює необмежену кількість правил через вбудований *Майстер створення* та вказує там методи шифрування, обмеження на передачу і прийом трафіку, а також активує фільтрацію по IP-адресами (дозвіл або заборона на підключення до мережі).

12. Конфігурація розширеної політики аудиту

У розділі *Конфігурація розширеної політики аудиту* винесені додаткові та більш ширші параметри щодо аудитів – створення / завершення процесів, зміни файлової системи, реєстру, політик, управління групами облікових записів користувачів, додатків та багато іншого.



! У локальній політиці безпеки в Windows 10 присутні багато корисних параметрів, що дозволяють організувати гарний захист системи. АЛЕ раджу перед внесенням певних змін уважно вивчити опис самого параметра, щоб зрозуміти його принцип роботи. Редагування деяких правил іноді призводить до серйозних проблемам роботи операційної системи.

ВИСНОВКИ ПО РОБОТІ: _____

_____

_____

_____

_____