

Win7 установка и анализ средств защищенности

Установка: запускаем iso файл, ждём. Всё. (Драйвера все на месте, если нет, закидываем с флешки)

Русской раскладки изначально нет, поэтому идём в панель управления -> смена раскладки клавиатуры и добавляем русскую раскладку.

1. Учетные записи пользователей и контроль учетных записей (UAC)

Типы учетных записей:

- Администратор (полный доступ).
- Обычный пользователь (ограниченные права).

Контроль учетных записей (UAC):

- Регулирует уровень уведомлений при изменении системных параметров (4 уровня настройки).
- Отключается через: Панель управления -> Учетные записи -> Изменить параметры UAC.

2. Защитник Windows (Windows Defender)

Встроенный неполноценный антивирус.

Настройки:

- Режим реального времени.
- Планирование сканирования.
- Исключение файлов/папок.

3. Брандмауэр Windows

Фильтрация входящего/исходящего трафика.

Настройки:

- Включение/отключение.
- Правила для программ и портов.
- Настройка профилей (частная/общественная сеть).

4. Центр обновления Windows (Windows Update)

Автоматические/ручные обновления.

Настройки параметров обновлений.

Путь: Панель управления -> Центр обновления Windows.

5. Шифрование и защита данных

BitLocker:

- Шифрование всего диска или отдельных разделов.
- Использование TPM-модуля (если есть).

Путь: Панель управления -> Система и безопасность -> BitLocker.

6. Политики безопасности (Local Security Policy)

Основные настройки:

- Парольная политика (сложность, срок действия).
- Политика блокировки учетной записи.
- Настройки аудита (логирование событий).
- Права пользователей (например, запрет доступа к USB).

7. Защита от вредоносных программ

Рекомендуется установка стороннего антивируса (например, Kaspersky, Avast).

Интеграция с Защитником Windows.

8. Настройки безопасности браузера (Internet Explorer)

Уровни безопасности для зон (Интернет, локальная сеть и т.д.).

Фильтр SmartScreen (блокировка фишинга).

Управление надстройками.

9. Родительский контроль

Ограничение времени работы за ПК.

Блокировка программ/игр по рейтингу.

Настройка через Панель управления -> Учетная запись пользователей и семейная безопасность -> Родительский контроль.

10. Сетевые настройки безопасности

Выбор типа сети (Домашняя/Общественная/Рабочая).

Отключение общего доступа к файлам в публичных сетях.

Настройка VPN (если используется).

11. Резервное копирование и восстановление

Создание точек восстановления системы.

Настройка архивации данных (Панель управления -> Архивация и восстановлении).

12. Аудит и мониторинг

Просмотр журналов событий (eventvwr.msc).

Настройка аудита доступа к файлам (через Политики безопасности).

13. Дополнительные меры

Отключение ненужных служб (через services.msc).

Очистка автозагрузки (через msconfig).

Использование стандартных учетных записей вместо административных для повседневных задач.