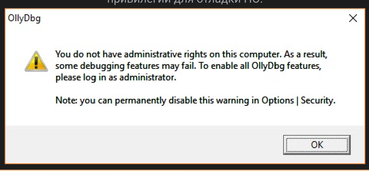
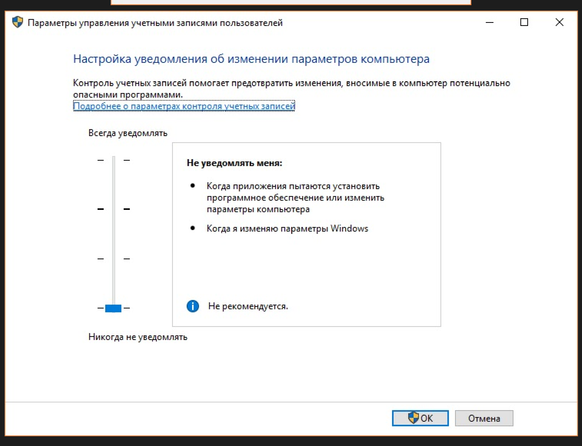
Повышение административных привилегий - Windows 10

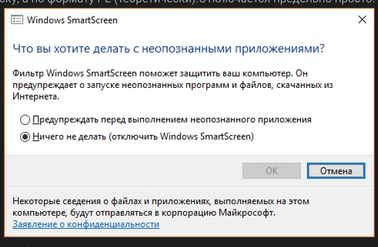
февраля 21, 2017

Майкрософт еще со времен висты ввели такую защитную систему как **UAC** (Контроль учетных записей).Если доступно объяснить суть, то сия система определяла имеющиеся на носителях инсталляторы и препятствовала их прямому выполнению, так как они затрагивали как и файловую систему, так и осуществляли установку драйверов и правки/создание значений в реестре.С одной стороны все это прекрасно, но с другой эта хуета постоянно заебывала при попытке установки нормального софта.Мы не рассматриваем малвари и всякие даунлоадеры.Естественно, что КУЗ можно было спокойно выключить, выставив самый низкий уровень защиты.Но это срабатывало только на висте и семерке.Как следствие мы не могли получить достаточные привилегии для отладки ПО.

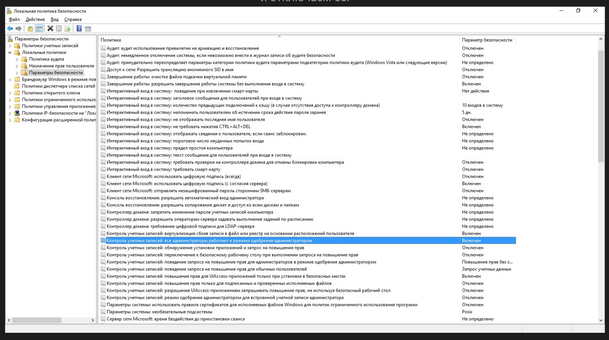




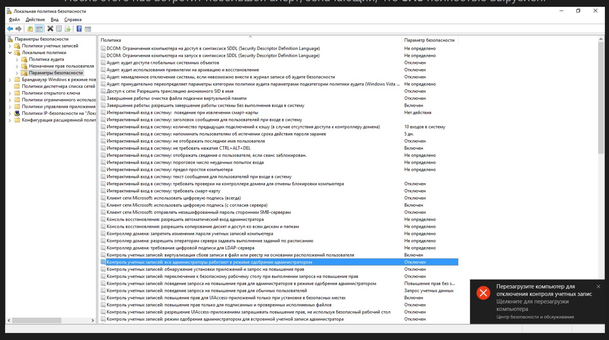
И вот, уже к моменту выхода Windows 10, стала использоваться параллельно другая технология - **Smart Screen**. Ее суть тоже довольна проста - препятствовать запуску тех приложений, которые майкрософт считает херовыми.Чаще всего это касалось бинарников для вин98 или 95.Это такой, своего рода, блэклист, но основанный не по списку, а по формату PE (теоретически).Отключается предельно просто.



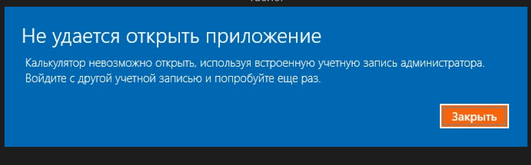
Стоит учесть, что всех проблем это не решит, так как программа может не запуститься уже на уровне загрузчика, но это уже вопрос правки и PE формата.Это решаемо.
Но привилегий мы все равно не получаем и отладчик должным образом не работает - мы получаем снова тоже сообщение + не работает драгндроп.
Но это тоже решаемо :D
Для этого мы откроем **Локальные политики безопасности**.
Переходим в раздел **Локальные политики -> Параметры безопасности** и находим в списке политику с заголовком **"Контроль учетных записей: все администраторы работают в режиме одобрения администратором"** и отключаем ее.



После этого нас встретит небольшой алерт, означающий, что **UAC** полностью вырублен.



Перезагружаемся и после перезагрузки можем спокойно юзать отладчик и дропать в него бинарники.Это плюс. Но без минусов тоже не обошлось.Если попытаться запусть edge или калькулятор, то нам покажут интересное табло:



И, казалось бы, а зачем браузеру и калькулятору привилегии встроенного администратора (та самая привилегированная отключенная учетка, которую мы обычно задействовали через Управление компьютером в разделе Администрирования из Панели управления).Баг, фича или уязвимость - трудно сказать.На этом все.