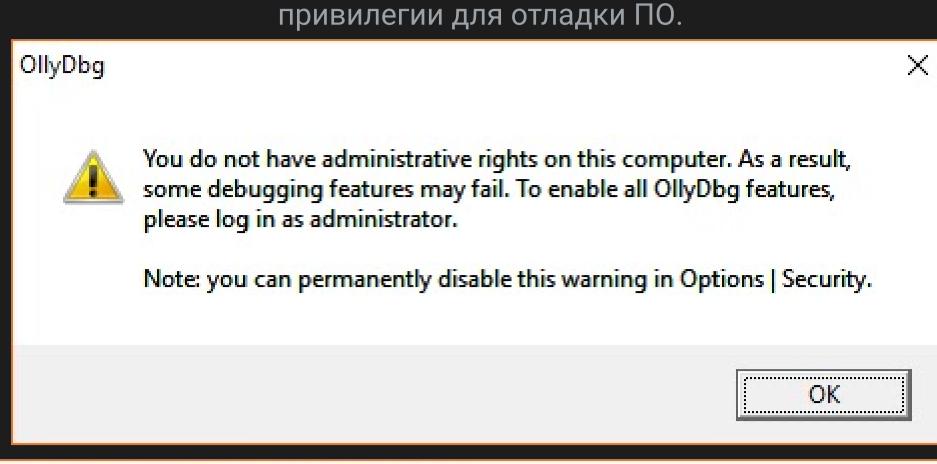


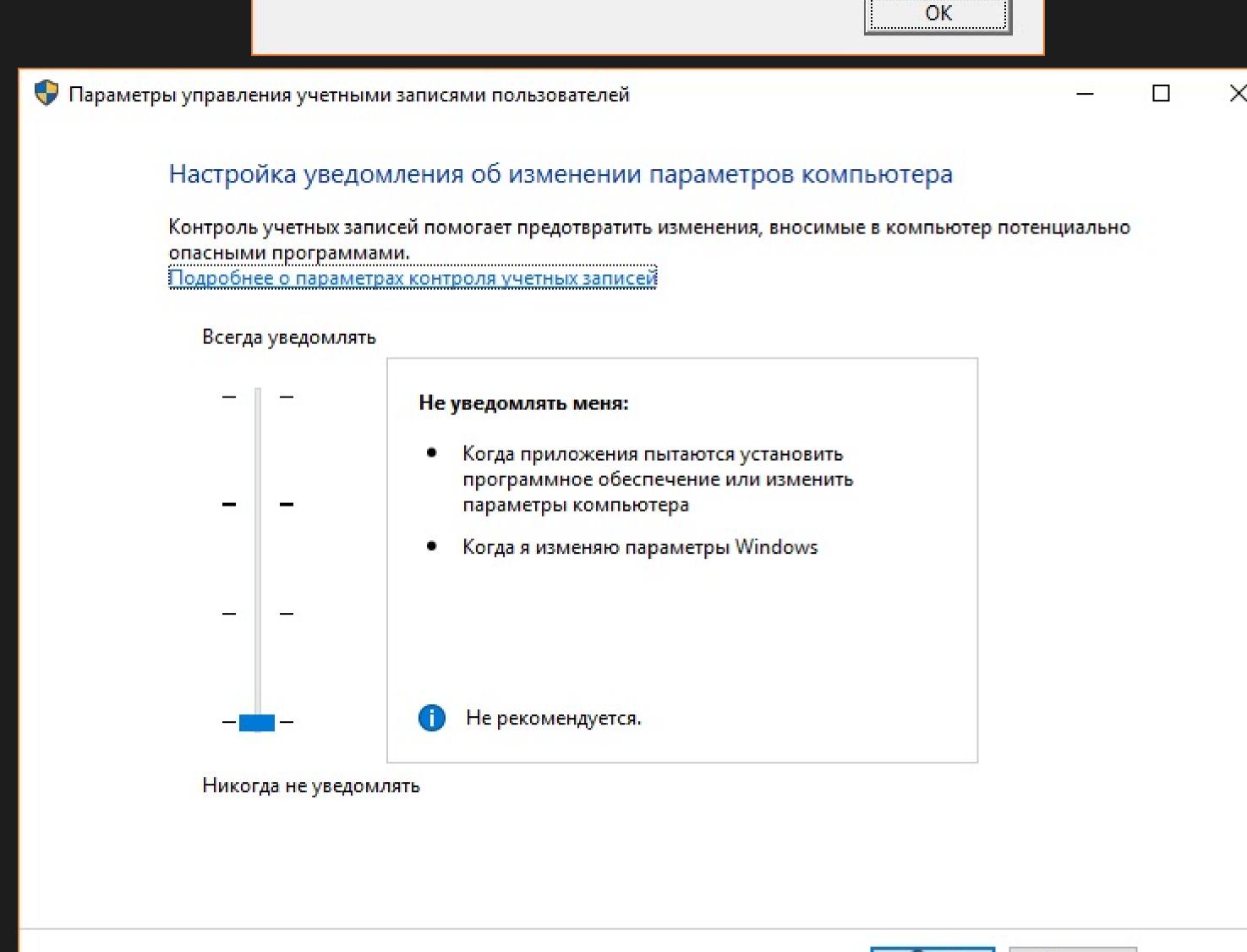
Повышение административных привилегий - Windows 10

A STATE OF THE PERSON AS A STATE OF THE PERSON

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

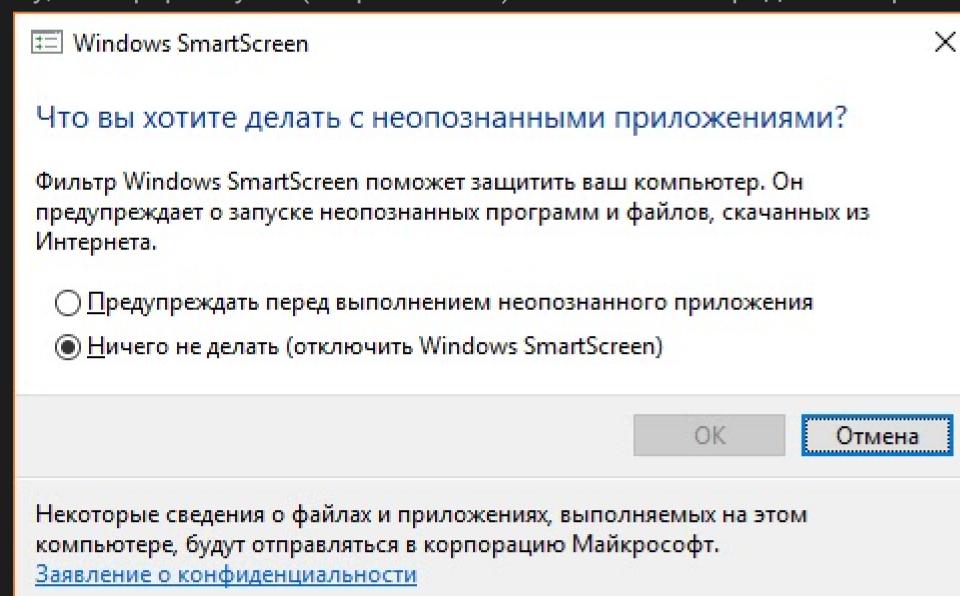




И вот, уже к моменту выхода Windows 10, стала использоваться параллельно другая технология - **Smart Screen**. Ее суть тоже довольна проста - препятствовать запуску тех приложений, которые майкрософт считает херовыми. Чаще всего это касалось бинарников для вин98 или 95. Это такой, своего рода, блэклист,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

Отмена

Не определено



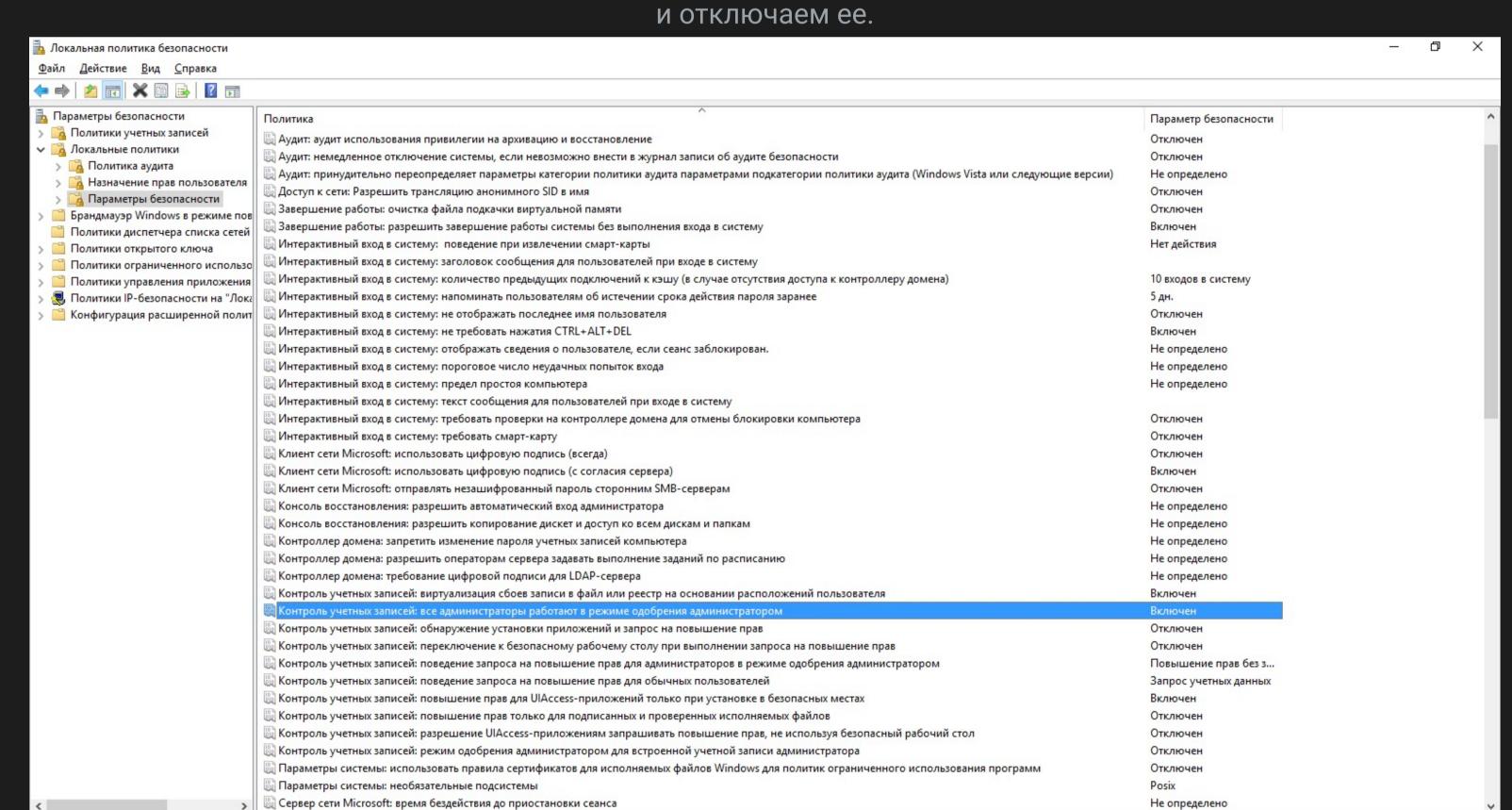
Стоит учесть, что всех проблем это не решит, так как программа может не запуститься уже на уровне загрузчика, но это уже вопрос правки и РЕ формата. Это решаемо.

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"



После этого нас встретит небольшой алерт, означающий, что **UAC** полностью вырублен. Локальная политика безопасности Файл Действие Вид Справка (- - | <u>*</u> | Параметры безопасности Параметр безопасности 🔀 Политики учетных записей 🗟 DCOM: Ограничения компьютера на доступ в синтаксисе SDDL (Security Descriptor Definition Language) Не определено Покальные политики 👸 DCOM: Ограничения компьютера на запуск в синтаксисе SDDL (Security Descriptor Definition Language) Не определено > Политика аудита Аудит: аудит доступа глобальных системных объектов Отключен Назначение прав пользователя 🖟 Аудит: аудит использования привилегии на архивацию и восстановление Отключен > 🔀 Параметры безопасности Аудит: немедленное отключение системы, если невозможно внести в журнал записи об аудите безопасности Отключен 🧻 Брандмауэр Windows в режиме пов 🖟 Аудит: принудительно переопределяет параметры категории политики аудита параметрами подкатегории политики аудита (Windows Vista ... 🛮 Не определено Политики диспетчера списка сетей 💹 Доступ к сети: Разрешить трансляцию анонимного SID в имя Политики открытого ключа Завершение работы: очистка файла подкачки виртуальной 📖 Завершение работы: разрешить завершение работы системы без выполнения входа в систему Включен 📔 Политики управления приложения 🌏 Политики IP-безопасности на "Лока Нет действия 📖 Интерактивный вход в систему: поведение при извлечении смарт-карты 🖟 Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему Конфигурация расширенной полит 📓 Интерактивный вход в систему: количество предыдущих подключений к кэшу (в случае отсутствия доступа к контроллеру домена) 10 входов в систему 🛍 Интерактивный вход в систему: напоминать пользователям об истечении срока действия пароля заранее 🔛 Интерактивный вход в систему: не отображать последнее имя пользователя Отключен 🛍 Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL Включен 🕍 Интерактивный вход в систему: отображать сведения о пользователе, если сеанс заблокирован. Не определено 🗓 Интерактивный вход в систему: пороговое число неудачных попыток входа Не определено 🕍 Интерактивный вход в систему: предел простоя компьютера Не определено 👸 Интерактивный вход в систему: текст сообщения для пользователей при входе в систему 🔊 Интерактивный вход в систему: требовать проверки на контроллере домена для отмены блокировки компьютера Отключен 📓 Интерактивный вход в систему: требовать смарт-карту 🕍 Клиент сети Microsoft: использовать цифровую подпись (всегда) Отключен 👸 Клиент сети Microsoft: использовать цифровую подпись (с согласия сервера) Включен 📓 Клиент сети Microsoft: отправлять незашифрованный пароль сторонним SMB-серверам Отключен 💹 Консоль восстановления: разрешить автоматический вход администратора Не определено 👸 Консоль восстановления: разрешить копирование дискет и доступ ко всем дискам и папкам 📓 Контроллер домена: запретить изменение пароля учетных записей компьютера Не определено 📓 Контроллер домена: разрешить операторам сервера задавать выполнение заданий по расписанию Не определено 🖟 Контроллер домена: требование цифровой подписи для LDAP-сервера Не определено 🖟 Контроль учетных записей: виртуализация сбоев записи в файл или реестр на основании расположений пользователя Включен Отключен 🛍 Контроль учетных записей: переключение к безопасному рабочему столу при выполнении запроса на повышение прав Отключен 🖺 Контроль учетных записей: поведение запроса на повышение прав для администраторов в режиме одобрения администратором Повышение прав без з... Перезагрузите компьютер для 📓 Контроль учетных записей: поведение запроса на повышение прав для обычных пользователей Запрос учетных данных отключения контроля учетных запис 👸 Контроль учетных записей: повышение прав для UIAccess-приложений только при установке в безопасных местах Включен 📓 Контроль учетных записей: повышение прав только для подписанных и проверенных исполняемых файлов Отключен 📓 Контроль учетных записей: разрешение UIAccess-приложениям запрашивать повышение прав, не используя безопасный рабочий стол Отключен Центр безопасности и обслуживания 闏 Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора Отключен

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:

Не удается открыть приложение Калькулятор невозможно открыть, используя встроенную учетную запись администратора. Войдите с другой учетной записью и попробуйте еще раз. Закрыть

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.