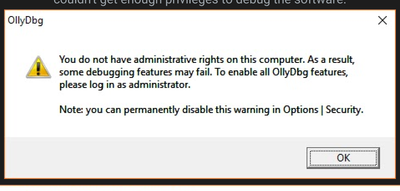
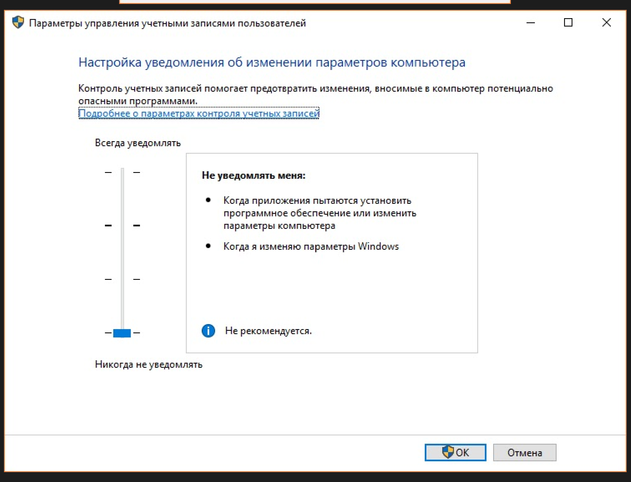
Administrative Privilege Escalation - Windows 10

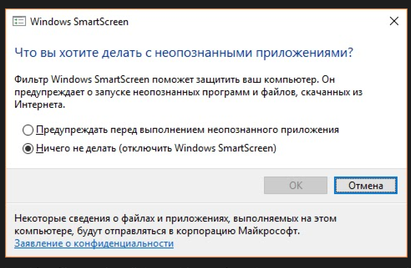
February 21, 2017

Since the days of whists, Microsoft introduced such a protective system as **UAC** (User Account Control). and editing / creating values in the registry. On the one hand, all this is fine, but on the other hand, this fucking thing was constantly annoying when trying to install normal software. We do not consider malware and all sorts of downloaders. Naturally, QUS could be safely turned off by setting the lowest level of protection But it only worked on Vista and 7, and as a result, we couldn't get enough privileges to debug the software.

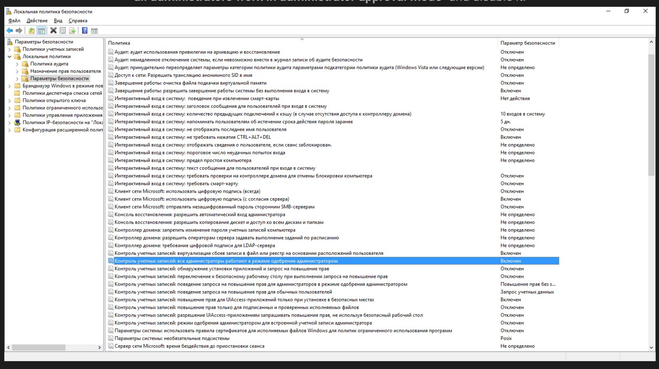




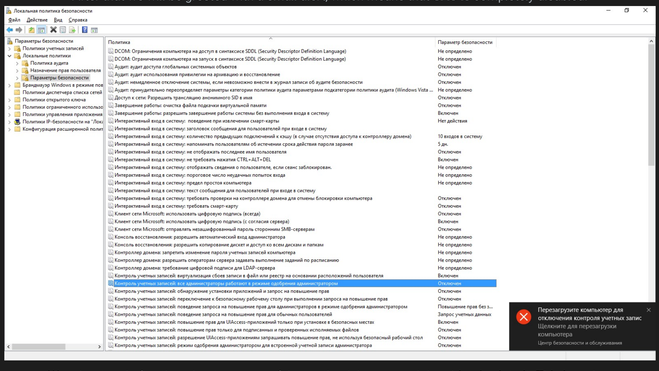
And now, by the time Windows 10 was released, another technology began to be used in parallel - **Smart Screen** .
Its essence is also quite simple - to prevent the launch of those applications that Microsoft considers crappy. Most often it concerned binaries for Win98 or 95. This is a kind of blacklist, but based not on the list, but on the PE format (theoretically). simply.



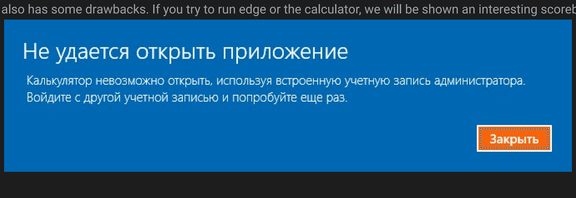
It is worth considering that this will not solve all the problems, since the program may not start already at the bootloader level, but this is already a matter of editing and the PE format.
But we still do not receive privileges and the debugger does not work properly - we receive again the same message + the dragndrop does not work.
But this is also solvable: D
To do this, we will open **Local Security Policies** .
Go to the **Local Policies -> Security Settings** section and find in the list a policy with the heading "**User Account Control: all administrators work in administrator approval mode**" and disable it.



After that we will be greeted with a small alert, which means that **UAC is** completely disabled.



We reboot and after the reboot we can safely use the debugger and drop binaries into it. This is a plus.
But it also has some drawbacks. If you try to run edge or the calculator, we will be shown an interesting scoreboard:



And, it would seem, why the browser and the calculator need the privileges of the built-in administrator (the same privileged disabled account, which we usually used through Computer Management in the Administration section of the Control Panel). It's hard to say a bug, feature or vulnerability. That's all.