I have shared my SpyShelter settings with my users on numerous occasions, but I have not yet devoted myself to this completely new thread, in which I would gather this fragmentary information. I was asked a few days ago to do it, and I wonder why I have not done so far Smile It's possible that two things affected it
- the program has been developing its functionalities over the years and thus expanded the offered options, which gave rise to further experience
- in addition, it has been designed so that certain settings are not immediately obvious and some functions (labo rather possibilities) are discovered for their own use alone or thanks to discussions with others.

Okay, that's right - the information below is based on the latest release, or version 11.3 in the SpyShelter Firewall ... this is important, because the Firewall version from the Premium version has two additional functions, namely the firewall module and the application start control module . This information is on the program's page in the version's comparison table, but I know from experience that the functionalities mentioned in such comparisons are often only a password for the user ... sometimes only a marketing one. In the case of this program are serious things, but more on that later. I would like to say one more thing ... properly stipulate ... the settings presented below are not options suggested ... the best ... the one real and revealed ... absolutely NOT to be treated like that! These are my own settings, such as they suit me, and for obvious reasons, not everyone is needed or sufficient as such .

I will start the review in a natural order, in line with the order of the tabs / modules from left to right.

PROTECTION
This is the main screen and the situation is rather simple ... all protection is included and does not require a comment.

RULES
General - it's like a summary ... list ... all our decisions on received messages / warnings, and sometimes the result of conscious changes in the rules already in place ... two things important in my list, which illustrates the following two pictures:
- there are several blocking rules, which results either from received alerts or from later modifications to earlier rules (numbers for blocked activities can be found in the settings on the list of monitored actions) (Figure 1)
- the rules also show the permissions for all actions for selected processes ... in addition to security applications, we also find programs to control the system and the processes used multifunction device (it happened that I went "on the easy side" because I wanted to save the creation of detailed rules for programs I have known for years and which I trust, or which I needed immediately, and the installation mode at startup did not give the expected results - no further alerts (Figure 2)

Application Execution Control - this module is present only in the version with firewall, and it is used to supervise which application can be launched and which block (the process is important, not its action ... so we have in some way the functionality of anti-malware programs exe).

It is difficult to suggest anything here, but it is definitely worth paying attention to what the superior processes of so-called "parents" (in the upper window) are shown to us as child processes ("children") in the bottom window. Usually this is a list of processes that we can somehow explain to ourselves, e.g. in the case of the list for the Explorer.exe process or for the file manager (for me FreeCommender.exe ) ... if we find something disturbing, then the fastest way is the position delete, but it's probably better to check what the process is about and if so it can be run by a specific other parent process.
It is worth paying attention to the entry on the bottom list marked only with the asterisk " * " as in the example below ... these are rules created automatically by SS, and mean any file from any location ... and here is the danger just because in the extreme case without further alert, it allows opening a file, i.e. a pest. I mostly threw such entries, I left only for known applications or those that I wanted to block (by other processes) ... as below (Figure 3)

[Picture: 4tFWao3.jpg]

LOG WINDOW

There are no settings here, there is simply a list of detected actions and decisions made. Not much can be done with this list, and it seems that a good idea could be reported by users adding the possibility of creating a rule from such a single entry, which can be done in some other applications of this type ... the developer's decision so far is no, but I hope you have to Smile

RESTRICTED APPS

List of limited applications - this function is very important to me and I can only complain that so little popularized. It allows you to limit the permissions of selected processes and thus minimize specific system modifications by these processes ... also allows you to impose restrictions on areas of "increased risk" on the disk, i.e. on connected portable drives, files downloaded from the network, on foreign documents , for collected program installers coming from various sources.
It is important enough to be described in detail in the help file of the program

> Quote:
> This function:
> - Automatically blocks all dangerous actions
> - Increases the chances of protection against attacks using holes in popular programs (eg Internet browsers).
> - Limits access to system files and registry.
> - Limits access to capturing keys, creating screenshots
> - Prevents malware from increasing your own privileges

We create the list of such locations / applications ourselves, because only we know what we need ... what I find on my screen can be seen on the summary screen below (Figure 4).

A short comment yet:
- the list includes vulnerable applications that are often used to perform an attack on the system ... among them web browsers, a PDF program and a system notebook

- as the locations I have on the list removable drives (it allows to avoid unauthorized launch of executable files) and two folders, one of which is intended for downloaded files (Download) and the other one (Instalki) is my program archive
- each item we can temporarily remove restrictions using the "Run as unlimited" command available from the mouse button
- "mysterious" W and S markings in separate columns signify the permissions granted for a given process / location for:
W is recording the image from the camera
S is sound recording
the default stamp in the column is " - " or lock, and we can change it to " + " or allow using the mouse button menu at a given position. For me, as you can see, all items have a lock.
A small tip - if you are going to update applications from a limited list ... install some plugins to them, it will be better to run them in unlimited mode , which allows us to command from the right mouse button. Then the necessary modifications will be implemented without limitations of the restricted mode localization.

Folders with write access - the list of locations that can be found in this tab results from the fact that by placing restrictions on applications / locations, we must in most cases add the possibility of recording for them. This is necessary because the applications can not work properly without it, and the folders for specific files without the function of saving new data in it lose the right reason.
A few notes here:
- adding subsequent applications / processes to the limited list, it is necessary to remember that in most cases we need to add the ability to write to the native folders of these programs or related temporary file folders ... it's so much simpler that SpyShelter asks when adding an application message about accepting adding the possibility to the indicated folder
- while adding own folders, we must add the option of writing to them manually
- some of the folders ... especially those related to the system ... we have the mouse context menu (so-called special folders), and we can add external disks as a general category (without specific drive names) and any chosen folder.
For me, it looks like in Fig. 5

[Picture: J0R1vUq.jpg]

File access violations - here we can find a list of processes that as limited attempts to access the forbidden locations and a list of these locations. It can be so important that if necessary (for the correct operation of the application) we can add the ability to write to such a selected item.
On the screenshot (Figure 6) you can see an example list of locations (along with files that were to be changed) after a test disabling the write capability for the portable Firefox native folder

Executed as restricted - here we find a list of processes that work as limited ... for the purposes of the description I have included a PDF viewer (1 process), Firefox (2 processes) and Chrome (6 processes), and each of them can be terminated if necessary ( Fig. 7).

[Image: hn1H16H.jpg]

FIREWALL

Network Zones - the firewall is another module / function that distinguishes the firewall version from "Premium" and replaces its "Secure Internet" module ( " AntiNetworkSpy" ) while providing much more functionality. On the first tab we can see a list of detected networks with the attribute of trust assigned to it - I have only one home network that I use on a daily basis, but if the laptop is used in different places, additional items should appear on the list.
My home network is assigned the "Unspecified" category, which means that we will be notified when we try to establish a new connection (if the set security level and established automatic permissions for selected trusted providers do not allow it automatically).

Network Activity - on this tab we can see all processes that are connected to the network and transfer statistics for them, but that's not all that we can find in this function. Cluttering in the selected position gives us a new window with a list of specific connections / addresses (name and IP address) also with transfer data ... whereas starting the menu with the right mouse button on the selected address gives us additional possibilities, among others blocking by server name or by IP (you can see it on the screen below). In addition, clicking on the headings of the speed columns with the right button allows you to select the current or average speed from the menu (Figure 8).

OK ... it was about the settings, and now the moment about the rules. For me, they result from the response to the displayed alerts and my own later modifications, and especially from the use of the so-called group rule. SpyShelter allows you to create a rule pattern that after saving can be used for any chosen process - for me, this rule blocks traffic in both directions for applications that in my opinion do not require access to the network. We create such a rule in the advanced options window ( "Create rules for a component" ) by selecting "select" in the top box - in the new window, "create" command - in the rule window we define the parameters we need and we approve changes in each closed window. From now on, the name of our new rule appears in the rules selection menu (additional info in the help file for SS). The application of this new rule gives us in the list of rules a new action marked with the number 59 with the name "Custom network rule 'NAME' assigned to the module" Firewall "(Figure 9) ... what interesting rules with this number will not be found in the list of monitored actions ... we have number 58, and then immediately 60 Smile

Another curiosity related to the firewall and change of program settings - if we disable all protection modules outside the firewall (you can not turn off all the main slider "Protection status", and then turn on "Firewall" ... you have to disable each module separately from status and firewall) we will have an active option to monitor actions assigned to the firewall. On their list (Figure 10), we find action No. 53 "Launching the application" ... and thanks to this action we will have an application with the basic anti-exe function from SpyShelter, i.e. allowing and blocking the application of certain applications, which we can of course expand with the functionality resulting from from the "Application launch control" function (see above "Rules")

[Image: P8TEeHD.jpg]

KEYSTROKE ENCRYPTION

Process Filter - is a program function whose role is to encrypt the characters typed from the keyboard, and thus protect against the interception of our data by possible pests. This particular module allows you to determine the way of filtering ... maybe simpler - determining ... processes in which this encryption is to take place. We have 4 options available:
- enabling encryption for all processes - it can cause problems in cooperation with processes that do not tolerate it, that's why we have another option ...
- encryption for all except for those indicated on the list - it is a list built-in, to which we can add any processes indicated by us, in which we do not want encryption (this setting recommended by the manufacturer) ... if this list is too much for us, we ...
- encryption only in selected processes - here we indicate only those processes in which we want to encrypt (the rest will be deprived of it), which allows us to indicate only processes prone to data interception like browsers, text editors, communicators, etc.
- disabling encryption - no explanations needed.
For me there is a designated "second" level, ie no encryption for exceptions ... as seen on the screenshot (Figure 11) to the built-in list, I added two important and life-saving security applications for me - Shadow Defender and Keriver 1-Click.

By the way of adding processes - in addition to the indication of the process in the system file manager, we can use the unique ... because the functionality of the process manager exists only in this module. The list of running processes starts the "Select process from list" command . And here digression, which was already raised in proposals for changes in the program - probably all of the HIPS / BB type programs I know have ... and had ... a module in which processes and even services were indicated, which allowed without the use of additional tools to control the work of the system, and in addition, sometimes set rules for them. For now, the function of such an SS does not have, but maybe someday we will wait Smile

Advanced - this is a tab with advanced features that should be changed only when fully aware of the changes made, because they have a significant impact on the entire functionality. For me, there is no major interference here and this module looks like a screenshot (Figure 12)
- lack of Asian language support and notifications
- change of the level of protection against hooks to "Better protection mode"

[Picture: YTcz6h6.jpg]

SETTINGS
General - we finally got to the first tab in the settings module ... I do not remember what the default settings are, so now it's hard for me to say how changed my relation is to them. I will discuss a few things from the illustrations (Figure 13), which I want to point out:
A - SpyShelter starts with me at the start of the system, but I also marked launching as a service (so-called early start), which gives the possibility to run the application protecting the system from being loaded and regardless of user accounts ... this has an impact on security, because the pests processes even acting in autostart will start later and thus can be detected or blocked by the SS.
B - I do not check at the start if there is a new version and therefore the program will not update automatically ... it results from the principle I adopted that nothing will update

me automatically and everything is downloaded manually. SpyShelter is so important to me that I follow subsequent changes and versions and decide whether to enter them immediately or with delay ... or even at all. Similarly with every other application ... I do not have an AV in my system so I do not have a problem updating the signatures.
If this is the default setting ... do not change it, because it will be safer for most people.
C - * RESTRICTED * appears on the taskbar next to the application name of the application running as limited ... because I am using this function, I have this option enabled.
D - if I am already deciding on the installation mode ... which in itself can be dangerous, because I have no control over the actions being performed ... I allow to create rules in this mode - some of them will remain as a fixed rule, and some will be sure removed when clearing rules, because it applies to temporary actions that have no equivalent in a normally working system. I run the installation mode rarely and thus I do not see a threat to myself, but I should warn against its excessive use .

Security - one of two very tabs with settings related to the protection being carried out ... in my case (Figure 14) "without madness" at first glance, but I have some important remarks and I put them below:
A - the option "Digitally signed applications" is the choice of how SS applications are treated digitally, and de facto tells us about the chosen level of protection ... my level of "ask user" means that any suspicious action will trigger a message that you need reply. Someone may think that this is some paranoia, but that's not true ... after so many years of uninterrupted work on this machine and therefore a large collection of created rules, the vast majority of activities in the system no longer requires any of my interventions - which was to be allowed - it is allowed, and what is prohibited - is already prohibited. The messages appear during basically only updating or testing new programs or their subsequent versions, and this is not that troublesome.
The default protection level set during the installation is "Automatically allow - a high level of protection" and I would recommend it to everyone less advanced ... if someone thinks that the number of messages is still too big ... irritating ... stressful even (yes ... in such situations, there may be stress and fear that our decision will be right and if we do not "break" something in the system), I advise that you temporarily work for a limited period of time to work at a low level of protection or automatically allow Microsoft applications . "Temporarily" does not mean (for everyday use) weeks or longer ... it should not last more than a few days ... it should be remembered that this program is used to control system and application work, so it is in our interest to exercise this control Smile
By the way, one more note - SpyShelter does not have so-called learning mode, i.e. automatic creation of permanent rules during operation ... the only similar one is the installation mode which I mentioned earlier.

[Image: BkNtIKy.jpg]

B - file / folder protection function is another option important for me offered by the program ... it works in a way different from the restrictions on processes / folders, that is, does not limit the actions of "outside" files covered by them, but controls the access "from outside" through processes. The list of my locations is visible on the screenshot (Figure 15) and as you can see, the three folders have the category "Personal", which means that
- any attempt to access a new application to a file in these folders and

- any attempt to open a new file type by an application that could already have been running there on other files
will trigger an access message.
This feature not only limits the access of unnecessary applications to our sensitive / protected data, but above all it can be an effective mechanism of protection against pests, such as ransomware.
C - SpyShelter has a built-in "factory" option to scan uncertain files / processes on the VirusScann website. Jotti (available in the alert window during installation, detection of a new action, but also from the context menu of the right mouse button), but also allows you to use another local AV scanner, which can be more convenient ... trustworthy ... for some users.
In my program, I added the Emsisoft Emergency Kit as an additional scanner (Figure 16).
D - I have disabled the option of closing SS processes from the level of the process manager ... this setting increases the protection of the program itself and should block attempts to close the protective application by external processes ... by pests also.
E - the field is empty, because I use only one account in the system - with administrator privileges.
F - the function of automatic blocking of suspicious applications is like supplementing the anti-exe functionality and automatically adds the suspicious process / its action to blocked rules. This setting works well in our everyday activities, but it's better to turn it off if we're installing something new, because something can go wrong. The way we work and the effects of inclusion of this function visible to us can be interesting and inspiring ... if anyone wants to explore the topic and possibly test I can post a link to the post, among others in this topic
https://safegroup.pl/thread-4263-post-21...#pid218516
G - the option field is empty, which means that I care more about protection than compatibility with other applications ... you have to try yourself if this setting does not conflict with any programs on your systems.

[Image: PuI1Dpu.jpg]

As for the rest of the settings
- I did not set additional protection for selected entries in the registry, I do not have my own trusted certificates, I do not exclude applications trying to install hooks for monitoring connections (action No. 33)
- I do not protect my settings with a password
- I do not run the virtual keyboard to login
I do not feel such need Smile

Advanced - on this tab (Fig. 17) we find, among other things, settings that "overclock" SpyShelter's protective capabilities, allowing him, among others, for automatic operation in certain situations
A - the inclusion of this option affects the behavior of processes for which we receive alerts in the form of an alert
* ending child processes causes that not only the process about which we have information in the alert is closed, but also all others for which it is a superior ... motivating process
* ending all events closes all processes with the same path, because the virus may not run just one process with the given name ... an example of such a multiplication process can be even a Chrome browser that runs several processes under the name Chrome.exe .

B - this option supports protection against threats from pests operating from removable disks ... in my case it is a complementary function of imposing limitations on removable drives (I mentioned earlier about this).
C - the option of "hard hooks" basically should be turned on when we want to strengthen the operation of the SS against other applications with which it may possibly conflict ... in my case it is included, although now I have nothing else from such applications except for Shadow Defender. It's possible that I once turned on just in case, while testing some other programs ... maybe ExeRadar Pro? ... some sandbox? ... I do not know Smile
D - I have this option enabled, but its operation is not about the level of security, but rather blocking notifications when drivers that do not exist are detected eg during installation or update
E - both notifications are turned on, because I want to know if any of these automatic decisions are made ... I can check this later in the log list, but here I receive information on a regular basis in the form of a notification (by the way the next notification in the form of sound does not applies, so the field is empty)
G - here we choose drivers for firewall support ... are system drivers and everything that uses them on Vista and above should be based on WFP (Windows Filtering Platform).

List of monitored actions - illustration (Figure 18) shows me a modified list, which I explain below
A - there are changes ... in the entire column "Allow automatically" the selection is set to "No" (default is at all "Yes" ) and each field next to the number in the column "Action code" is empty (selected by default)
B - there is no selection, i.e. there are no automatic permissions for applications with digital signatures on white lists (those built into the program and those that we ourselves create)
As far as in point B as if there is nothing to explain, because it's about a high degree of sensitivity and thus protection, in point. And my decision may be incomprehensible ... so I explain. The default settings mean that you only have to select one field - this is from point B - to properly disable monitoring all actions from the list against applications from the trusted white list. My settings "obstruct" this task and make it rather impossible as a result of some accidental action ... that's why I manually edited each decision to "No" and unchecked each box to remain empty.

[Image: 2MbbunS.jpg]

ABOUT
Here (picture 19) we have only one view without tabs and we will find features / options quite obvious in it, but I will pay attention to three things:
And - "Tips" ... read them carefully and let them become the main guideline for you not only when working with this program, but with any other intended for protection ... let them permanently come to your principles and good practices in everyday use computer.
B - use the help file, because it is the first and basic information base that will give you knowledge about the operation of the program and also the first help in difficult moments when you do not know how to act. Pressing the "Help" button will connect to the website in Polish
https://www.spyshelter.com/usersmanual/polish/

but remember that even without access to the network you have a local help file , which is located in the SpyShelter installation folder - it is called help.chm and will allow you to use the updated version of the guide.
C - here we can check manually and according to the need (without going to the manufacturer's website), if there is a newer version. Of course, if you have automatic checking turned on, you do not have to do it here.

[Picture: 4AXwIy9.jpg]

Useful links
https://safegroup.pl/thread-10869.html
https://avlab.pl/producent/spyshelter
https://www.dobreprogramy.pl/Polskie-dob...60495.html

---
updated:
06.11 - I have a small technical problem on my machine, so I decided to publish part of the article ... just in case. The rest will be added and published as a continuation, not a separate part. Let me know what the visibility of the pictures is.
13.11 - I added the next part (firewall, encryption) and changed the graphics into a collective, which is due to some technical limitations ... I hope it will be OK.
November 22 - I added a description of two modules of the Settings ... the rest in progress.
27/11 - I added the rest of the issues.
28/11 - I have changed the way graphics are pasted - now they are also visible to users who have not logged in, I have added useful links.