Система защиты от запуска вредоносного ПО и от модификации санкционированных исполняемых объектов СЗ "Панцирь+" (краткое описание и инструкция по эксплуатации)

Сведение о разработчике и поставщике программы СЗ "Панцирь+". ООО "Научно-производственное предприятие "Информационные технологии в бизнесе" (ООО "НПП "ИТБ"), тел.: (812) 324-27-71, e-mail: info@npp-itb.spb.ru, http://www.npp-itb.spb.ru.

Общие сведения о программе: СЗ "Панцирь+":

1. **"Система защиты "Панцирь+" (СЗ "Панцирь+")". Свидетельство о регистрации программы для ЭВМ №2013616107 от 26.06.2013.**
2. **Программой СЗ "Панцирь+" реализовано запатентованное техническое решение «Система контроля доступа к файлам на основе их автоматической разметки». Патент №2524566 от 05.06.2014.**

Введение. Сегодня уже ни для кого не секрет, что одну из наиболее актуальных угроз компьютерной безопасности составляет внедрение на компьютер и запуск вредоносного ПО. Подавляющая часть компьютерных атак, в конечном счете, сводится к решению именно этой задачи. Существуют различные способы внедрения и запуска вредоносных программ, основанные, как на реализации различных технических приемов, в том числе, на эксплуатации уязвимостей в ОС и приложениях, так и на использовании методов социальной инженерии.

Технология защиты от запуска вредоносного ПО.

Задача защиты - не позволять несанкционированно (без ведома пользователей, без их осознанного решения) запускать (исполнять) на компьютере файлы, созданные пользователями (в том числе, несанкционированно от их имени) в процессе эксплуатации системы. Решение. Любой создаваемый интерактивным пользователем файл автоматически размечается СЗ - ему сопоставляется учетная информация создавшего файл субъекта доступа (имя учетной записи и процесса - полнопутевое имя исполняемого файла процесса). При обращении к любому файлу на исполнение (в том числе, и системой), СЗ анализируется, был ли создан этот файл в процессе эксплуатации системы (размечен ли он). Если это так, то автоматическое исполнение (запуск) подобного файла блокируется, пользователю выдается соответствующее уведомление. При этом пользователю предлагается проанализировать причину подобного несанкционированного события по журналу событий и решить, санкционирован ли этот файл для последующего исполнения. Если нет, то пользователь сможет удалить этот файл из проводника СЗ, если да, то удалить его разметку, переведя тем самым файл в разряд санкциониированных для исполнения, и впоследствии запускать его.Универсальность решения достигается тем, что проводимая процедура анализа никак не связана с каким-либо анализом файла, в том числе, с типом его расширения. Перехватывается системный запрос на запись, соответственно на исполнение - именно подобным образом идентифицируется исполняемый файл. Принципиальным является и то, что перехватываются не запросы на открытие файла для записи и исполнения, а непосредственно запись и исполнение, что сводит к минимуму ложные срабатывания средства защиты. Универсальность решения обеспечивается и тем, что при реализации данной технологии защиты не важен способ занесения (внедрения) вредоносной программы (исполняемого файла) на защищаемый компьютер - загрузка из интернета, почтовое вложение (в архиве, либо нет), копирование с внешнего накопителя и т.п. - любым способом записанный на защищаемый компьютер файл будет автоматически размечен, и в отношении него будет действовать защита от

несанкционированного исполнения. Не важным также является и то, каким образом злоумышленником скрывается свойство исполнимости файла.
В рамках реализации данной технологии, СЗ «Панцирь+» решаются следующие задачи защиты:
- Контроль (разметка) создаваемых интерактивными пользователями на компьютере файлов в процессе работы системы, автоматическое предотвращение запуска (в том числе и системными правами) создаваемых файлов. СЗ осуществляет аудит создания и попыток исполнения создаваемых файлов.
- Предотвращение запуска программ с внешних файловых накопителей (аудит подобных попыток запуска СЗ не ведется, о запрете запрошенного доступа на исполнение к внешнему накопителю пользователь уведомляется штатным сообщением ОС).

Технология защиты от модификации санкционированных исполняемых файлов.

Описанная выше технология обеспечивает невозможность запуска несанкционированно установленной на компьютер программы, при этом санкционировано установленные исполняемые объекты (файлы) остаются уязвимы, поскольку они могут быть модифицированы, удалены, переименованы. Все подобные действия не приведут к запуску вредоносной программы, но могут сказаться на работоспособности (корректности работы) ОС и приложений. Задача защиты - не позволять несанкционированно (без ведома пользователей, без их осознанного решения) модифцировать санкционированные исполняемые файлы ОС и приложений.
Для защиты исполняемых объектов от несанкционированной модификации, удаления, переименования в СЗ реализована следующая технология защиты, также основанная на автоматической разметке файлов, но в данном случае, уже не создаваемых в процессе работы пользователей, а установленных ранее - исполняемых. Любой исполненный (не размеченный, как созданный, в противном случае, он не сможет быть исполнен) файл СЗ автоматически размечается - ему сопоставляется учетная информация исполнившего файл субъекта доступа (имя учетной записи и процесса - полнопутевое имя исполняемого файла процесса).
Примечание. Чтобы отделить создаваемый файл от исполняемого, в разметку включается признак типа файла, отображаемый при обзоре соответствующей пиктограммой.
При обращении к любому файлу интерактивным пользователем на модификацию/удаление/переименование, СЗ анализируется, был ли он размечен, как исполняемый. Если это так, подобный доступ к исполняемому файлу блокируется, пользователю предлагается решить, санкционирован ли этот файл для изменения. Если нет, то пользователь сможет проанализировать причину подобного несанкционированного события по журналу событий, приняв далее необходимые меры; если же да, то удалить его разметку, переведя тем самым файл в разряд санкциониированных для модификации, удаления, переименования, и впоследствии изменить его. Универсальность решения опять же достигается тем, что проводимая процедура анализа никак не связана с каким-либо анализом файла, в том числе, с типом его расширения. Перехватывается системный запрос на исполнение, соответственно на модификацию/удаление/переименование - именно подобным образом идентифицируется исполняемый файл. Принципиальным является и то, что перехватываются не запросы на открытие файла для исполнения, модификацию/удаление/переименование, а непосредственно контролируемые действия, что сводит к минимуму ложные срабатывания средства защиты.
Примечание. Для автоматической разметки исполняемых объектов ОС и приложений, рекомендуется после ввода СЗ в действие, по крайней мере, один раз запустить критичные к модификации приложения.
В рамках реализации данной технологии, СЗ «Панцирь+» решаются следующая задача защиты:

- Контроль (разметка) исполненных на компьютере файлов ОС и приложений в процессе работы системы, автоматическое предотвращение несанкционированной модификации/удаления/переименование исполняемых файлов. СЗ осуществляет аудит исполнения и попыток модификации/удаления/переименование исполняемых файлов.

Дополнительная защита.

- Защита от обхода реализуемых СЗ правил доступа к файловым объектам, за счет несанкционированного получения интерактивными пользователями системных прав (атака на повышение привилегий). Реализована следующая технология защиты. СЗ фиксирует, каким интерактивным пользователем осуществлен запуск каждого приложения. В случае если приложение обращается к файловому объекту не под учетной записью запустившего его пользователя, а под системной учетной записью, любой доступ к любому файловому объекту данному приложению СЗ блокируется.
- Самозащита. Файлы СЗ защищены от несанкционированного доступа к ним с целью удаления и модификации.

Программно-аппаратные требования.

СЗ "Панцирь+" может использоваться с ОС Microsoft Windows Vista и выше (32-х и 64-х битные - различные дистрибутивы ПО СЗ) с файловой системой NTFS (обязательное условие). Разметка файлов создается и хранится в дополнительных атрибутах NTFS. Требований к аппаратным средствам не предъявляется.

Инструкция по эксплуатации.

Установка СЗ. Для установки СЗ необходимо запустить файл "cfp (версия ПО - 32х или 64-х).exe" из состава дистрибутива и далее следовать рекомендациям программы-установщика. В результате установки программы (после перезагрузки компьютера) на панели задач появится соответствующий ярлык СЗ (буква "*П*"). Если он отображается красным цветом – СЗ запущена, серым – остановлена, красным на желтом фоне – в журнале аудита СЗ есть непрочитанные сообщения (появившиеся после последнего открытия журнала аудита). СЗ запускается в системе автоматически при каждом включении (перезагрузке) компьютера.

Органы управления. При нажатии на значок СЗ на панели задач "*П*" правой кнопкой мыши откроется меню управления, рис.1. В данном меню можно выбрать одно из следующих действий: убрать защиту, открыть журнал аудита, открыть программу обзора разметки файлов на компьютере, задать список особых процессов.

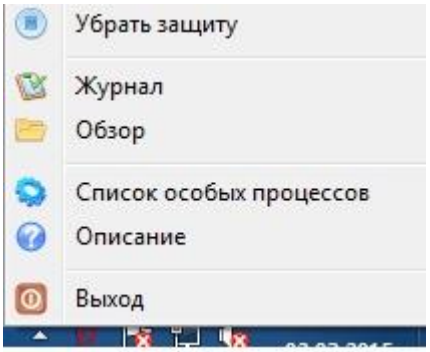


Рис.1. Меню управления СЗ

Внимание. При выборе "Убрать защиту" СЗ переходит в пассивный режим, разметка создаваемых и исполняемых файлов не производится, разграничений и контроля доступа к файлам не осуществляется. Компьютер находится под угрозой запуска вредоносных программ и несанкционированной модификации санкционированных исполняемых файлов!

При выборе "Убрать защиту" значок СЗ на панели задач отобразится серым цветом. Для запуска СЗ следует нажать на ярлык "*П*" СЗ правой кнопкой мыши и в открывшемся меню выбрать "Включить защиту".

Удаление СЗ. Удаление программы осуществляется штатными средствами Windows через меню "Программы", вкладка "Удаление программы".

Внимание. Для разметки файлов СЗ используются создаваемые программой резервные поля атрибутов доступа NTFS (хранимые в альтернативных потоках). Поэтому при работе с созданными Вами (размеченными СЗ) файлами на других компьютерах (где не установлена СЗ), либо после удаления СЗ на Вашем компьютере, созданная СЗ разметка файлов не будет сказываться на работе с ними.

Предварительная настройка, штатный режим эксплуатации. Никакой настройки СЗ производить не требуется. Запущенная программа в полном объеме автоматически решает свои задачи. До тех пор, пока не наступит нештатный режим, Вам беспокоиться не о чем!

Примечание. Для того чтобы разметились исполняемые файлы критичных к несанкционированной модификации приложений, требуется, по крайней мере, один раз их запустить на компьютере после установки СЗ.

Нештатный режим, угроза несанкционированного доступа. Нештатный режим наступает при выявлении СЗ попытки несанкционированного доступа к размеченным файлам. При этом ярлык СЗ на панели задач "*П*" окрашивается в желтый цвет, пользователю выдается соответствующее уведомление, рис.2.

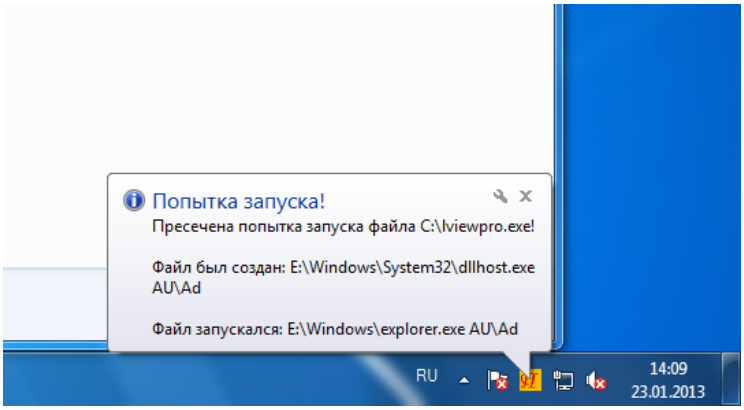


Рис.2. Уведомление пользователя о попытке несанкционированного доступа к размеченному файлу

Вы можете проигнорировать это уведомление и работать далее (СЗ свое дело сделала, попытка запуска несанкционированной программы, либо несанкционированной модификации исполняемого файла была предотвращена), а можете проанализировать нештатную ситуацию. Для этого требуется открыть меню, рис.1, и выбрать в нем "Журнал", откроется журнал событий, рис.3.

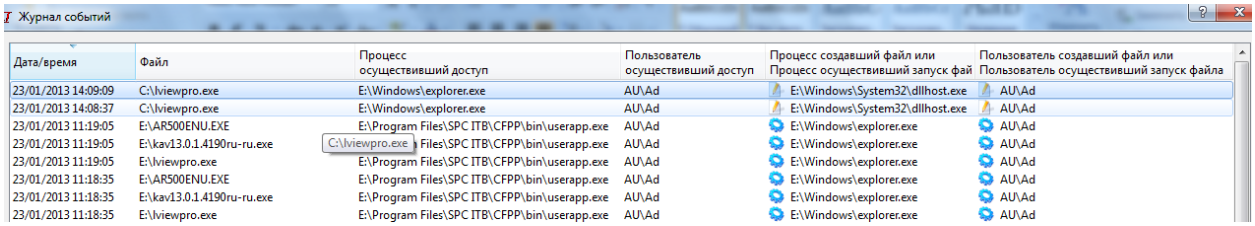


Рис.3. Журнал событий

Журнал событий имеет следующую структуру:
- "Дата/время" (временные характеристики регистрации события);
- "Файл" (полнопутевое имя размеченного файла, несанкционированная попытка доступа к которому была предотвращена СЗ);
- "Процесс, осуществивший доступ" (полнопутевое имя исполняемого файла процесса, совершившего несанкционированную попытку исполнения размеченного созданного файла, либо модификацию/удаление/переименование размеченного исполняемого файла);
- "Пользователь, осуществивший доступ" (имя пользователя (учетной записи) которым (от лица которого), совершена попытка несанкционированного доступа к размеченному файлу);
- "Процесс, создавший файл или процесс, осуществивший запуск файла" (полнопутевое имя исполняемого файла процесса, создавшего файл, к которому запрашивается несанкционированный доступ на исполнение или полнопутевое имя исполняемого файла процесса, исполнившего ранее файл, к которому запрашивается несанкционированный доступ на модификацию/удаление/переименование);
- "Пользователь, создавший файл или пользователь, осуществивший запуск файла" (имя пользователя (учетной записи) которым (от лица которого), создан файл, к которому запрашивается несанкционированный доступ на исполнение или имя пользователя (учетной записи), исполнившего ранее файл, к которому запрашивается несанкционированный доступ на модификацию/удаление/переименование).

Примечание. Тип размеченного файла – созданный в процессе работы пользователя, либо исполняемый, несанкционированный доступ к которому предотвращается СЗ, отображается соответствующей пиктограммой в журнале событий, см. рис.3.

СЗ позволяет изменять предустановленные параметры журнала событий из меню, представленного на рис.4, запускаемого по правой кнопке мыши из журнала событий, см. рис.3.

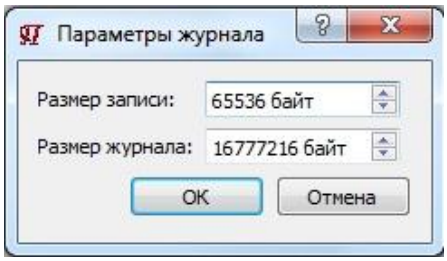
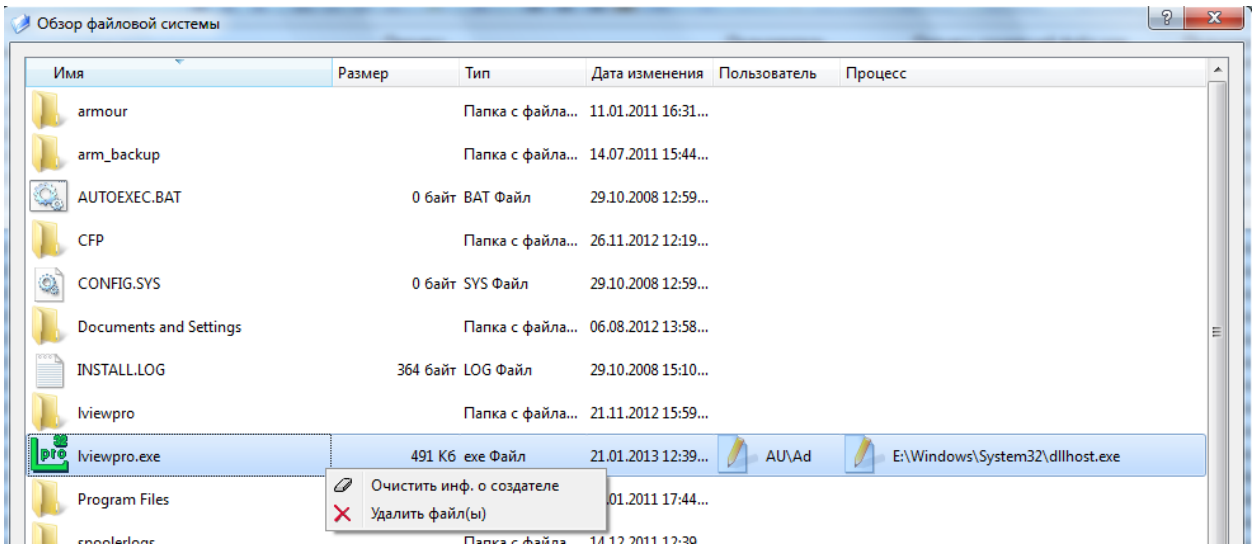


Рис.4. Задание параметров журнал событий

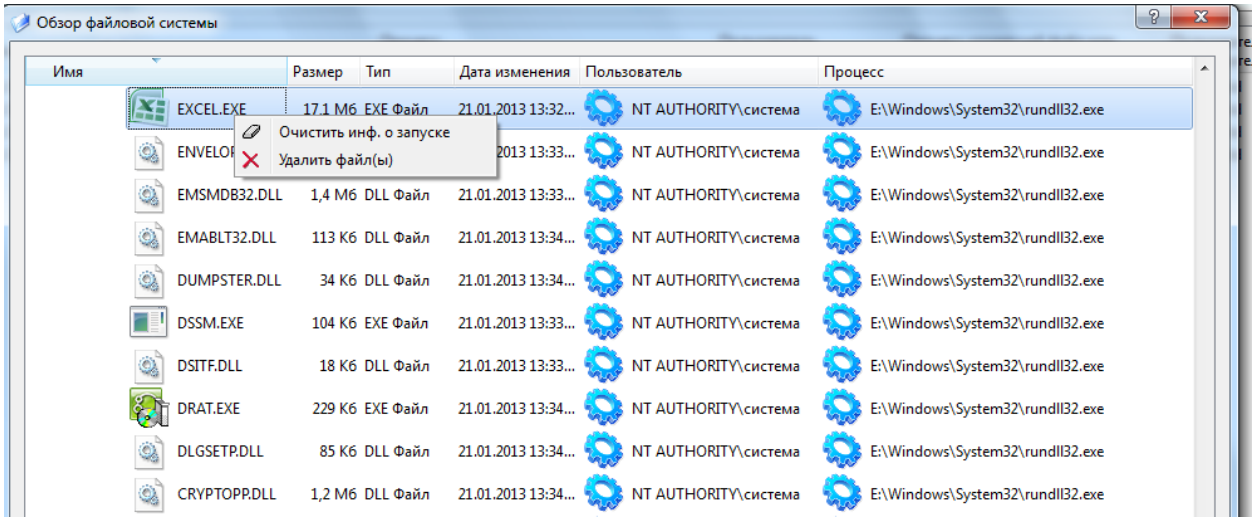
При превышении заданного размера журнала событий, каждая новая запись будет размещаться на месте (вместо) наиболее ранней записи в журнале.

Каковы Ваши дальнейшие действия?

1. В отношении размеченного файла, к которому осуществлена попытка несанкционированного доступа. Выберите левой кнопкой требуемый файл в поле "файл" журнала событий, см. рис.3. Откроется программа СЗ обзора файловой системы, см. рис. 5, с отображением разметки выбранного Вами файла.



1) Отображение созданного файла



2) Отображение размеченного исполняемого файла

Рис.5. Программа СЗ обзора файловой системы.

Здесь также используется соответствующая пиктограмма, для указания типа файла - на рис. 4.1 отображен размеченный СЗ созданный файл, на рис.4.2 размеченный СЗ исполняемый файл.

Выбрав правой кнопкой мыши требуемый файл, Вы получите возможность, либо его удаления, либо удаления его разметки, рис.5. При удалении разметки файла (выбрать "Очистить инф. о создателе", рис.5.1, соответственно, «Очистить инф. о запуске», рис.5.2), Вы, тем самым, переводите файл в категорию санкционированных для исполнения (созданный файл), либо модификации/удаления/переименования (исполняемый файл). Впоследствии, не отключая СЗ, данный файл можно будет благополучно исполнять, либо соответственно модифицировать/удалять/переименовывать.

Внимание! Проводник «Обзор файловой системы», рис. 5, запускается с правами текущего пользователя. Поэтому для удаления исполняемого файла, или файла созданного в каталоге, защищаемом ОС, из проводника СЗ пользователю может

быть отказано (это не распространяется на удаление разметки подобных файлов). Воспользуйтесь в этом случае для удаления файла штатным проводником ОС.

Примечание. Подобный подход к созданию проводника СЗ «Панцирь+» обусловлен тем, что СЗ призвана усиливать безопасность ОС, а не ослаблять ее, предоставляя пользователям возможности, противоречащие политике безопасности, реализуемой ОС (в частности, при запуске проводника СЗ с системными правами, пользователь (соответственно с правами интерактивного пользователя) получил бы возможность удаления любого файла из защищаемых ОС каталогов).

2. В отношении процесса, которым осуществлена попытка несанкционированного доступа к размеченному файлу. Выбрав двойным нажатием левой кнопки мыши требуемый процесс в поле "Процесс, осуществивший доступ" журнала событий, либо в поле "Процесс создавший файл, либо процесс, осуществивший запуск файла", см. рис.3, Вы откроете программу обзора ФС, где будет отображен исполняемый файл выбранного Вами процесса с его разметкой (поскольку он уже исполнялся), см. рис.5.2.

По правой кнопке мыши Вы можете удалить выбранный исполняемый файл соответствующего процесса, либо удалить его разметку, рис.5.2.

Работа с особыми процессами. Некоторый процессы, которые в СЗ относятся к категории «особых», предполагают в рамках штатного функционирования модификацию исполняемых (отмеченных СЗ, как исполняемые) файлов и создание новых файлов для последующего их санкционированного исполнения в системе. В первую очередь, к особым можно отнести процессы, ответственные за автоматическое обновление системы и приложений, которое, в большинстве случаев происходит без ведома пользователя. В штатном режиме функционирования (без дополнительных настроек) подобное обновление СЗ выполнить не позволит. Как к этому относиться и что делать?

Нужно понимать, что в случае разрешения некоторому процессу – критичному процессу, в системе модифицировать исполняемые файлы и/или создавать файлы, которые далее будет разрешено выполнять, Вы тем самым создаете «канал несанкционированного доступа», который может быть использован злоумышленником для запуска вредоносного ПО. С этой целью может быть использована уязвимость критичного процесса, подмена виртуального канала связи, используемого разработчиком соответствующего ПО для автоматических обновлений, и т.д.. Как следствие, разрешать автоматическое обновление имеет смыл только тех приложений, разработчик которых гарантирует безопасность обновлений, им реализованы соответствующие меры защиты. Прежде чем разрешить автоматическое обновление того или иного приложения, поинтересуйтесь, как его разработчик обеспечивает безопасность такого обновления.

Если никак, то лучше отказаться от подобной возможности, а все необходимые Вам обновления осуществлять локально при отключенной СЗ. Для того, чтобы при этом журнал событий не наполнялся не несущими для Вас никакой информации сообщениями (о запрете соответствующих автоматических обновлениях Вы и так знаете), можно использовать фильтр регистрируемых сообщений. Фильтр сообщений запускается по правой кнопки мыши из журнала событий, см. рис.6, и имеет вид, представленный на рис.7.

В данном фильтре можно задать файловые объекты (в том числе, используя соответствующие маски) предотвращенный СЗ несанкционированный доступ к которым не будет регистрироваться в журнале событий.

Для задания нерегистрируемого СЗ события (файла, каталога, маски) следует в поле "Не сообщать при запуске следующих объектов", рис.7, выбрать по правой кнопки мыши меню добавления (задания), удаления, редактирования подобного объекта. При добавлении (редактировании) объекта откроется меню "Новое имя", рис.8, в котором вручную, либо с использованием соответствующих обзоров, можно ввести объект (при

необходимости, соответствующим образом затем его скорректировав, например, задав его маской).

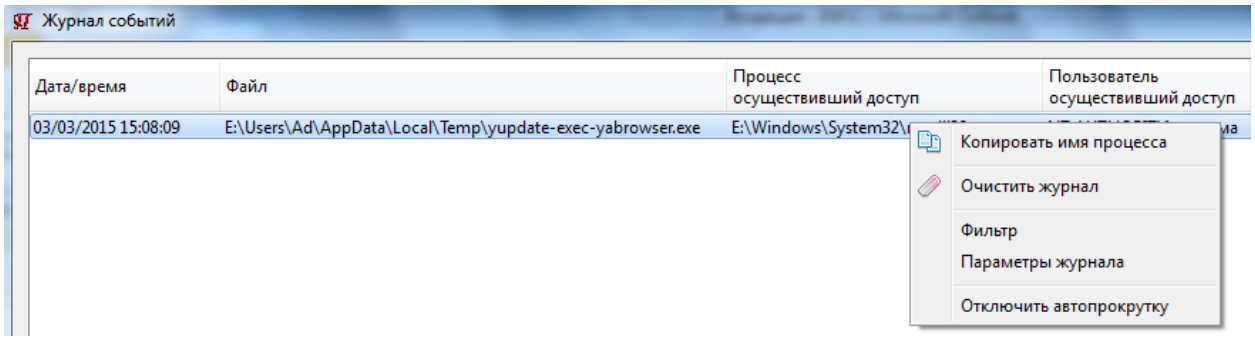


Рис.6. Запуск фильтра сообщений

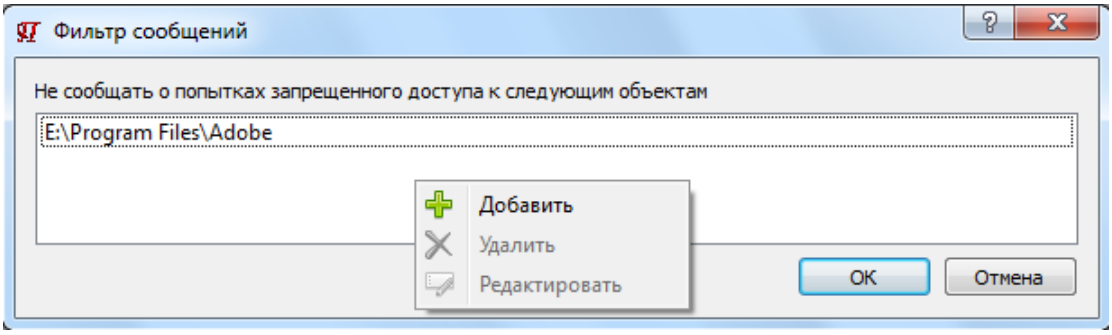


Рис.7. Фильтр сообщений

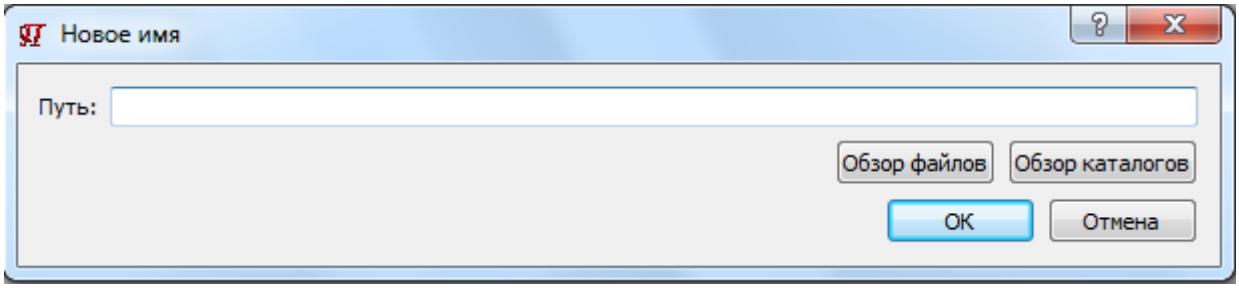


Рис.8. Меню задания нерегистрируемых событий в фильтре сообщений

В случае, если Вы уверены в безопасности проводимых разработчиком ПО автоматических обновлений, Вы можете отнести процесс, ответственный за обновление того или иного ПО (полнопутевое имя его исполняемого файла Вы узнаете из журнала событий, см. рис.3) к категории «особых» в СЗ. С этой целью в меню управления, см. рис.1, требуется выбрать «Список особых процессов», в результате чего откроется интерфейс с отображенным в нем списком заданных особых процессов с заданными для них исключениями, см. рис.9.

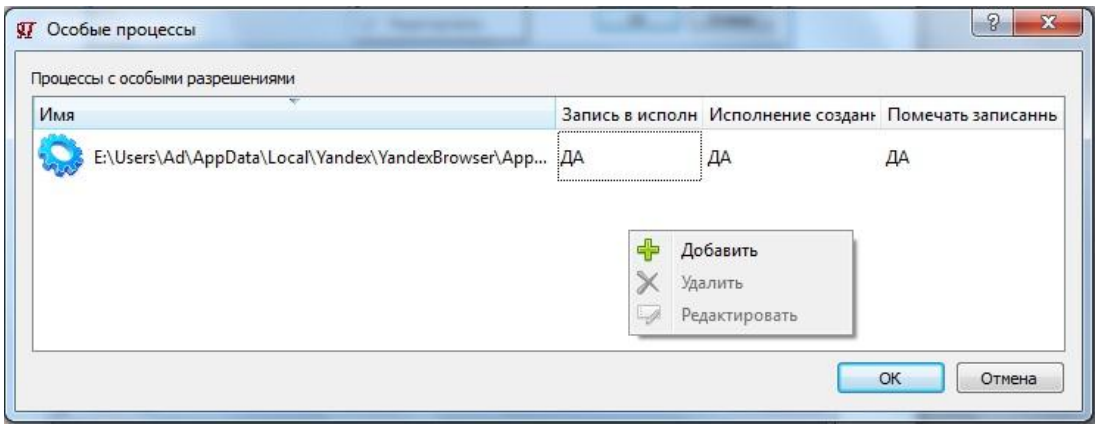


Рис.9. Интерфейс отображения списка заданных особых процессов с заданными для них исключениями

Особые процессы и правила для них задаются из меню, представленного на рис.10, запускаемого по правой кнопки мыши из интерфейса «Особые процессы, см. рис.9.

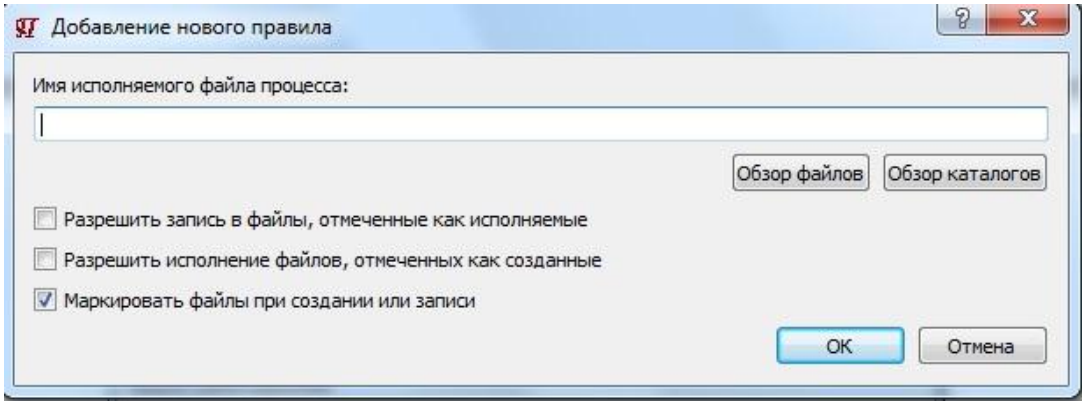


Рис.10. Меню задания особого процесса и правила для него

Особый процесс рекомендуется задавать полнопутевым именем его исполняемого файла (хотя возможно и применение соответствующих масок), которое может быть введено вручную, с использованием соответствующих обзоров, а так же по средством копирования из журнала событий, см. рис.6.

Примечание. Имя процесса может быть скопировано из любого поля журнала событий, см. рис.6, в которых отображены имена процессов (нужно по правой кнопке мыши запустить соответствующее меню, см. рис.6 при наведении курсора на требуемое имя процесса).

Для особого процесса существует возможность задания следующих исключающих правил (если задано одновременно несколько правил, то они будут действовать одновременно), см. рис.10:

- «Разрешить запись в файлы, отмеченные как исполняемые». Процессу разрешается запись в исполняемые (размеченные СЗ, как исполняемые) файлы – их модификация, удаление, переименование. При модификации исполняемого файла его разметка не меняется. Для этого необходимо установить соответствующий флаг;
- «Разрешить исполнение файлов, отмеченных как созданные». Процессу разрешается исполнять создаваемые (размеченные СЗ, как создаваемые) файлы. Для этого необходимо установить соответствующий флаг;

- «Маркировать файлы при создании или записи». **Исходно флаг установлен СЗ**. При создании процессом нового файла, этот файл не размечается, если модифицируется файл, размеченный СЗ, как создаваемый, его исходная разметка не изменяется. Для этого необходимо **убрать** соответствующий флаг.

Для того, чтобы процессу, ответственному за автоматическое обновление какого-либо ПО, разрешить выполнить обновление в полном объеме, для этого процесса требуется задать два правила - установить флаг «Разрешить запись в файлы, отмеченные как исполняемые» и убрать флаг «Маркировать файлы при создании или записи».

СЗ предоставляет возможность просмотра, при необходимости, удаления произведенной СЗ разметки файлов. Для запуска программы обзора файловой системы СЗ следует воспользоваться командой "Обзор" в меню управления СЗ, см. рис.1. Откроется интерфейс программы обзора/удаления разметки файлов, рис.11.

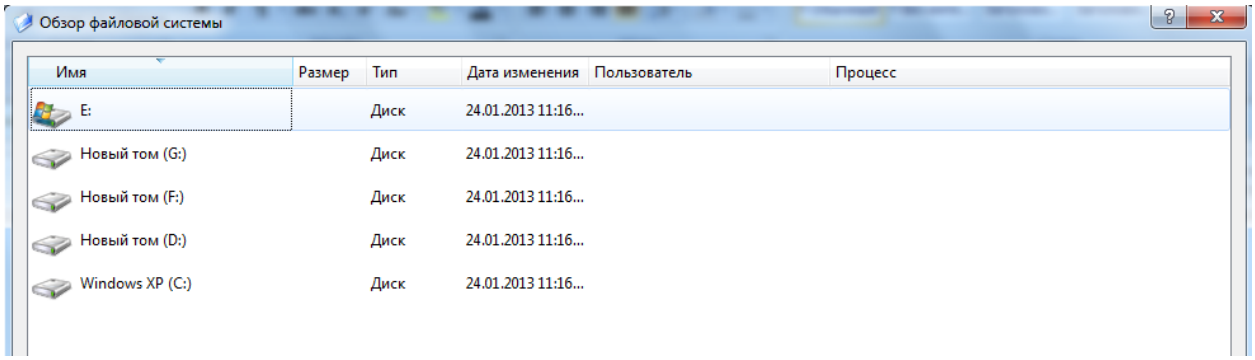


Рис.11. Интерфейс программы обзора/удаления разметки файлов

Используя данную программу, можно посмотреть, какие файлы, в каких папках размечены. Здесь также используется соответствующая пиктограмма, для указания типа файла (используется тот же обзор, что проиллюстрирован на рис.5 - на рис. 5.1 отображен созданный файл, на рис.5.2 размеченный СЗ исполняемый файл).

Выбрав правой кнопкой мыши файл, Вы получите возможность, либо его удаления, либо удаления его разметки, рис.5. При необходимости, используя данную программу, можно удалить разметку всех файлов в выбранном каталоге, либо на выбранном диске. Для этого следует выбрать интересующий Вас объект (логический диск, каталог, подкаталог), в котором необходимо удалить разметку файлов, и по правой кнопке мыши выбрать соответствующее меню. Откроется предложение очистить (удалить) разметку файлов в выбранном объекте, см. рис.12, соответственно, информацию о создателе (для создаваемых файлов), или/и информацию о запуске (для исполняемых файлов).

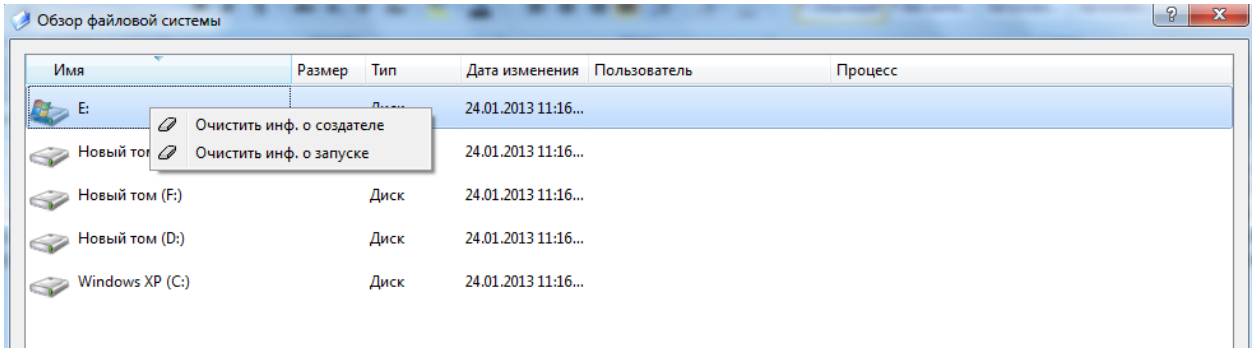


Рис.12. Меню удаления разметки файлов в выбранном объекте

При удалении разметки файлов в объекте следует учитывать необходимость удаления (задавать при необходимости) разметки файлов в подкаталогах выбранного каталога, либо в каталогах и подкаталогах выбранного логического диска, рис.13.

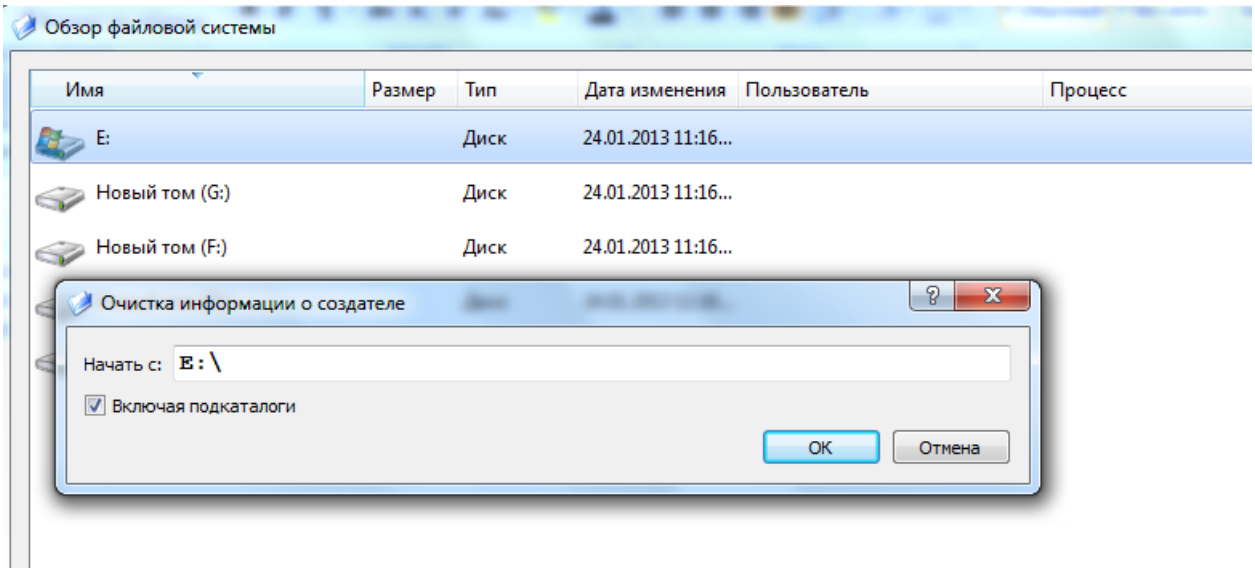


Рис.13. Задание параметров очистки разметки файлов в выбранном объекте

Заключение. Естественно, ПО СЗ "Панцирь+" не является панацеей от всех бед, связанных с информационной безопасностью Вашего компьютера. СЗ решает лишь определенный круг задач защиты компьютера, при этом решает наиболее актуальные на сегодняшний день задачи защиты максимально эффективно! Установив на своем компьютере данное ПО, Вы можете быть уверены в том, что несанкционированная Вами программа не будет запущена, вне зависимости от того, как она была внедрена на Ваш компьютер! Не будут и несанкционированно модифицированы исполняемые объекты ОС и приложений, используемые Вами при работе! А это, не мало!

Со своими замечаниями и пожеланиями
Вы можете обратиться к разработчикам СЗ
по адресу: info@npp-itb.spb.ru.
Любое Ваше замечание и/или комментарий будут с благодарностью
восприняты, рассмотрены и учтены в дальнейшем развитии СЗ "Панцирь+"!

Коллектив разработчиков ООО "НПП "ИТБ"