DOI: 10.22184/1992-4178.2022.220.9.108.111

Углубление самоконтроля контрольно-проверочной аппаратуры изделий систем управления: параметры оболочки пользователя

С. Белов[1]

УДК 004.42 + 53.087.4 + 004.514 | ВАК 2.2.8

Ранее освещался вопрос защиты контрольно-проверочной аппаратуры (далее – КПА) изделий систем управления (далее – ИСУ) от злоумышленников в части копирования аппаратуры и программного обеспечения [1]. Однако дальнейшее изучение проблемы показало, что она оказалась глубже: существуют операторы, нарушающие правила работы с КПА, указанные в ТУ, и изменяющие параметры операционной системы КПА. Для предотвращения этого была создана оболочка КПА, дающая доступ оператору только к ярлыкам программ, но операторы научились обходить эту оболочку. В результате работоспособность КПА нарушается вплоть до состояния необходимости ремонтных работ.

ВВЕДЕНИЕ

Поставляемые заказчику комплекты КПА содержат технические условия в составе конструкторской документации. В них описана четкая последовательность работы с КПА от момента сборки конструкции до нажатия кнопки запуска программы самоконтроля КПА или программы контроля ИСУ. Последовательность работы с программой самоконтроля и программой ИСУ указаны в соответствующих ТУ, что тоже регламентирует четкий алгоритм взаимодействия оператора с ними, вплоть до «нажать и отпустить левую кнопку мыши».

Проблема была обнаружена после того, как заказчик, спустя примерно 10 лет эксплуатации, направил КПА на платный ремонт к изготовителю. При анализе КПА были обнаружены проблемы работоспособности плат управления, проявления которых создавали полную уверенность в неисправности физического характера. Однако платы не работали исключительно по причине скрытого нарушения работоспособности операционной системы (далее – ОС). Как только ОС была переустановлена с теми же версиями драйверов плат – часть плат заработала исправно.

С учетом того, что аналогичные КПА на территории разработчика со сроком эксплуатации 12 лет таких проблем никогда не содержали (на протяжении срока эксплуатации ОС не переустанавливалась), был сделан вывод об изменении свойств или состава операционной системы пользователями КПА, работавшими с ней у заказчика – нарушение правил эксплуатации КПА как результат действий, не указанных в инструкциях ТУ (также предполагается, что на данной КПА играли в Quake 2).

Так как данный факт недоказуем – претензии заказчику предъявлять нельзя. Однако можно принять ряд мер, направленных на то, чтобы оператор был максимально ограничен в возможностях использования КПА, оставаясь строго в рамках ТУ.

ТЕКУЩАЯ СИТУАЦИЯ С ПО КПА И КОНЦЕПЦИЯ ЗАЩИТЫ КПА ОТ ПОЛЬЗОВАТЕЛЯ-ЗЛОУМЫШЛЕННИКА

Требуется ввести термин «оболочка КПА» как обозначение программы, блокирующей пользователю возможности выхода на рабочий стол и работы с файлами ОС. У КПА для разных ИСУ, являющихся собственной разработкой различных подразделений предприятия, такие оболочки разные, но они одинаковы для всех КПА, создаваемых в одном подразделении. Независимо от качества оболочек и их разнообразия, КПА очень просто взламывается с помощью загрузки со стороннего диска (например, miniWindows XP в составе Hiren"s Boot CD v.15.2 [2]). В этом случае не удается предотвратить ущерб, максимум – зафиксировать факт его нанесения.

[1] АО «ГосНИИП», ведущий инженер, for-work2016@mail.ru.

Текущая оболочка КПА была написана в 2004 году и представляла собой имитацию кнопки «Пуск» ОС, ее панели задач и системного трея. Оболочка при глубоком тестировании показала ряд недостатков:

- существует последовательность действий, при которых библиотека перехвата нажатий клавиш, встроенная в оболочку, перестает работать. Как следствие, становится доступен вызов диспетчера задач по Ctrl + Alt + Del, закрытие оболочки, запуск Explorer.exe – получение доступа к ОС;
- несмотря на то, что библиотека в данном случае выполняет защитную функцию, она была стороннего производства. С учетом особенностей ее работы (клавиатурный перехватчик), она может быть рассмотрена как программная закладка в соответствии со ст. 138.1 УК РФ с дополнениями 308-ФЗ от 2 августа 2019 года [3] или противоречить внутренним правилам предприятия;
- очень простой и незашифрованный пароль разработчика, штатно завершающий оболочку и запускающий Explorer.exe;
- все настройки содержатся в исходном коде. Значит, при изменении состава кнопок, названий кнопок или путей к файлам порождается уникальная версия оболочки. Контроль версий при этом не ведется, маркеры принадлежности к определенному ИСУ или КПА отсутствуют;
- оболочка завершала работу после запуска ПО контроля ИСУ и запускалась при выходе из ПО контроля ИСУ. Обоснованием такого решения стало то, что оболочка содержала в себе несколько высокочастотных таймеров, делавших высоковероятным ее влияние на ПО контроля ИСУ. Отключением оболочки во время работы ПО обеспечивалось освобождение ресурсов системы, устранение влияния ПО друг на друга и в первую очередь – предотвращение временны́х задержек при работе ПО контроля ИСУ;
- невозможность корректного запуска оболочки в только что установленной ОС (недостаток сторонних библиотек).

В связи с этим формируется концепция защиты КПА от злоумышленника:

- доработать оболочку КПА по критерию максимальной защищенности от возможности ее выключения, в том числе доработать так, чтобы оболочка не мешала ПО контроля ИСУ и запускалась на любой конфигурации ОС;
- главная задача: разработать в самоконтроле КПА тест, проверяющий целостность файлов и настроек оболочки КПА, а также самой ОС. Если злоумышленник совершит нарушение, изменив конфигурацию, самоконтроль КПА не пройдет, ОТК заказчика данную КПА не аттестует. Заказчику придется вызывать платно разработчиков для устранения проблемы (или даже транспортировать КПА к разработчикам за свой счет), ожидать окончания ремонта. Таким образом, заказчику становится выгодно подавлять таких злоумышленников, проводя разъяснительные беседы и поиск виновных;
- для проверки работоспособности оболочки требуется как минимум вынести ее настройки в отдельный файл, с целью их последующего анализа. При этом можно повысить удобство использования оболочки, позволяя редактировать настройки без необходимости перекомпиляции ее исполняемого файла, установки языка программирования и поиска исходного кода. А раз затрагивается вопрос удобства использования – реализовать возможность установки, ремонта и анализа оболочки специалистом, не являющимся ни программистом, ни электроником.

КОНЦЕПЦИИ ДОРАБОТКИ ОБОЛОЧКИ КПА

Внешний вид оболочки было решено оставить почти без изменений: меню «Пуск», список запускающих ПО кнопок-ярлыков, окно завершения работы, окно смены пароля.

Защита оболочки от ее закрытия:

- отказ от любого вида хуков (технологий, изменяющих стандартное поведение компонентов информационной системы) как стороннего ПО с неизвестными алгоритмами работы;
- организация взаимодействия оболочки с реестром ОС и политиками безопасности ОС как с отлаженным функционалом ОС;
- мимикрия оболочки под системный процесс, неотличимый в диспетчере задач от оригинального, если каким-то образом будет получен доступ к диспетчеру задач. Антивирусы не видят оболочку как потенциально опасное ПО;
- поиск уязвимостей в ПО контроля ИСУ по критерию возможности сторонних действий в ОС, отличных от ТУ;

- обеспечение способности обрабатывать в пароле непечатные клавиши (например, NumLock). Код клавиши записывается в пароль при нажатии, но не отображается на экране: подсмотреть пароль на экране невозможно. Стандартные пароли, независимо от их уровня сложности, в себе такого символа никогда не содержат, разгадать пароли с NumLock практически невозможно;
- применение многозначного шифрованного неизменяемого пароля принудительного выхода из оболочки разработчиком, вводимого в определенном месте после определенных действий.

Меры по достижению максимальной совместимости оболочки с программой контроля ИСУ:

- отказ от всех таймеров, кроме ApplicationEvents как компонента, потребляющего минимум ресурсов (без нажатия клавиш T=1 с, без нажатия клавиши T=1 мкс, с нажатием клавиши T=8 мкс);
- отказ от кнопок в панели задач, возникающих при запуске ПО и исчезающих при его закрытии;

Таблица 1. Параметры реестра для изменения оболочкой КПА и проверки самоконтролем КПА

Параметр, тип параметра	Путь параметра	Значения параметра	Решаемая задача	Результат	Примечание
Scancode Map, REG_BYNARY	HKLM\ SYSTEM\ ControlSet001\ Control\ Keyboard Layout	00 00 00 00 00 00 00 00 03 00 00 00 36 00 38 00 36 00 38 E0 00 00 00 00	Переназначение клавиш Alt и Alt Gr на правый Shift	Блокировка комбинации Ctrl+Alt+Del	Правый Shift, обычно, вообще не используется
NoViewContextMenu, REG_DWORD	HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ Explorer	0x00000001	Блокировка контекстного меню проводника	Устранение уязвимости в ПО контроля ИСУ при открытии файлов телеметрии	Доступ к свойствам файла и к изменению открывающего приложения – позволяет запустить Explorer.exe
DisableTaskMgr, REG_DWORD	HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Policies\ System	0x00000001	Блокировка диспетчера задач	Кнопка диспетчера задач неактивна	Ctrl+Shift+Escape также не сработает
Shell, REG_SZ	HKCU\ Software\ Microsoft\ Windows NT\ CurrentVersion\ Winlogon	Путь к исполняемому файлу оболочки	Подмена файла, запускаемого ОС автоматически при старте	Запуск оболочки вместо Explorer.exe	Много лишних библиотек не будет загружено. Run и RunOnce не сработают
Название оболочки	HKCU\ Software\ Microsoft\ Windows\ CurrentVersion\ Run	Путь к исполняемому файлу оболочки	Автоматический запуск оболочки	Запуск оболочки после Explorer.exe	Для диагностики: как те или иные программы (в том числе Explorer.exe) влияют на ПО контроля ИСУ

- присвоение максимально низкого приоритета работы;
- исключение ресурсоемких функций по критериям нагрузки на процессор и времени их выполнения.

Удобство использования:

- вынесение настроек программы в ini-файл. Время создания / изменения ini-файла является при этом триггером его взлома;
- наличие возможности изменения настроек вручную специалистом / разработчиком. В дальнейшем, если не выставить настройки в умолчания, тест в самоконтроле КПА пройден не будет;
- наличие возможности динамического создания кнопок и их разделителей в ini-файле;
- введение в состав перечня настроек опции отключения ограничений, а также запуска Explorer.exe вместе с оболочкой – для диагностических и ремонтных работ разработчика;
- использование двух паролей выхода из оболочки: фиксированного пароля разработчика и изменяемого пароля куратора КПА у заказчика. Таким образом, в рамках разных КПА будут разные пароли куратора, но разработчик может обойти их с помощью пароля фиксированного и вводимого в секретном месте (например, вообще не имеющем отношения к оболочке: в программе контроля ИСУ, в поле ввода номера ИСУ).

КОНЦЕПЦИИ ДОРАБОТКИ ПО САМОКОНТРОЛЯ КПА

Внешний вид и алгоритм выполнения тестов: тест оболочки КПА и параметров ОС – первый. При тесте «не норма» окрашивать тест красным цветом и отражать статус теста в протоколе самоконтроля.

Совместимость оболочки КПА с тестом в самоконтроле КПА: ini-файл с настройками должен быть составлен по правилам, поддерживаемым обеими программами. В том числе, по правилам шифрования этого файла (использование MD5, AES, магических чисел, псевдослучайных чисел, полностью самописного алгоритма, комбинации алгоритмов и т. д.).

РЕАЛИЗАЦИЯ КОНЦЕПЦИЙ ДОРАБОТКИ ОБОЛОЧКИ КПА И РАЗРАБОТКИ ТЕСТА САМОКОНТРОЛЯ КПА

Параметры реестра для оболочки КПА, их значения и особенности указаны в табл. 1. Данная таблица получена экспериментально, часть возможностей взята из [4].

Требуется отдельное выполнение команд

- secedit.exe /refreshPolicy MACHINE_POLICY /enforce,
- secedit.exe /refreshPolicy USER_POLICY /enforce: обновление политик безопасности ОС без ее перезагрузки.

Итог: мгновенное срабатывание NoViewContextMenu.

Алгоритм теста КПА с учетом доработанной оболочки КПА:

- проверить наличие файлов оболочки КПА, включая файл настроек;
- проверить дату и время создания и изменения файла настроек;
- открыть файл настроек, проверить настройки на соответствие необходимым;
- проверить наличие ключей реестра и их значения на соответствие необходимым и сопоставить их с настройками оболочки КПА;
- убедиться, что оболочка КПА запущена;
- убедиться в отсутствии процесса Explorer.exe;
- проверка прочих параметров ОС по выбору разработчика.

ЗАКЛЮЧЕНИЕ

В настоящий момент измененная оболочка КПА успешно протестирована и установлена на КПА заказчика.

Пока не обнаружено способа разрушить оболочку без применения сторонних загрузочных носителей. Но теперь разрушения с применением таких носителей успешно фиксируются тестом КПА.

ЛИТЕРАТУРА

1. **Белов С.** Углубление самоконтроля контрольно-проверочной аппаратуры изделий систем управления: уточнения и дополнения по предыдущим материалам // ЭЛЕКТРОНИКА: Наука, Технология, Бизнес. 2022. № 8. С. 104–108.
2. **Речицкий А.** Спустя 6 лет вышла новая версия легендарного аварийного дистрибутива Hiren's BootCD / Ставрополь: Хабр, 2018 г. [Электронный ресурс] URL: https://habr.com/ru/post/415593.
3. Федеральный закон от 2 августа 2019 года № 308-ФЗ «О внесении изменения в ст. 138.1 Уголовного кодекса Российской Федерации». М.: Кремль, 2019.
4. **Honeycutt J.** Microsoft Windows 2000 Registry Handbook / England, London: Que Publishing (Pearson Education), 2000.