

СПО «АККОРД- Win64 К»

Инструкция по исключению возможности запуска системных команд LogOff, Shutdown и др. (наследование ПРД от группы)

> Москва 2020

В данной инструкции приведены сведения о том, как исключить для пользователя возможность запуска системных команд типа Logoff, Shutdown и т.п. при использовании дискреционного метода с формированием списка контролируемых процессов.

1. Запустить программу «Настройка комплекса «Аккорд» (Пуск-> Программы-> Аккорд-> Настройка комплекса Аккорд).

В главном окне программы в поле «Механизмы разграничения доступа» установить флаги в строках «Дискреционный», «Контроль процессов» и «Наследование ПРД от группы» (рисунок **1**).

🚰 Настройка Комплекс СЗИ НСД «Аккорд	q-Win64-K» — □ X
<u>Ф</u> айл <u>К</u> оманды <u>П</u> араметры По <u>м</u> ощь	
日 🍡 帝 📔	
Состояние: Аккорд установлен: Да Мягкий режим: Выключен Версия AcRun.sys: 5.0.10.73 Версия AcGina.dll: 4.0.29	При старте: Спрашивать разрешение: Перезагрузка при ошибках: Автоматический логин в ОС:
Механизмы разграничения доступа: Дискреционный Мандатный Контроль процессов	Синхронизация: С базой пользователей NT: 🗹 Удалять незарег, пользователей: 🗌
 Наследование ПРД от группы ТМ-контроллер: Использовать страницу ТМ: 	Журнал команд: Просмотр
Использовать страницу ТМ:	Просмотр

Рисунок 1 - Главное окно программы настройки комплекса «Аккорд»

2. В меню «Параметры» выбрать пункт «Дополнительные опции...» На вкладке «Разное» открывшегося окна установки дополнительных опций убрать флаг «Использовать полный путь процесса» (рисунок 2).

🚹 Дополни	тельные опции			×
Контроль	Режим сессии	Разное	Данные конфигура	ции
- Разное: Число	проходов, при очи	істке файл	юв:	2
Очища	ть файлы, начиная	я с уровня	Общедоступно	\sim
🗹 Очи	щать файл подкач	ки		
🗌 Выв	зодить на экран с	ообщения	оНСД	
🗌 Мяг	кий режим			
Исп	юльзовать полны	й путь про	цесса	
🗹 3an	исывать в журнал	і логическ	ие имена дисков	
🗹 Печ	атать гриф прило:	жения в за	аголовке окна	
-Храните	ель экрана:			
🗌 Бло	кировать USB уст	ройства		
Текст	в хранителе экран	на:		
Принять				Отмена

Рисунок 2 - Убрать опцию «Использовать полный путь процесса»

3. На вкладке «Режим сессии» окна установки дополнительных опций установить флаг «Завершать сессию только полной перезагрузкой» (рисунок 3).

3

дополни	тельные опц				^
Контроль	Режим сесс	ии Раз	ное	Данные конфигураці	ии
- Режим с	сессии				
Вручнук)	∼ Pe>	ким	старта системы защиты	ı
				5. P. 1	
Ц Испо	льзовать пров	зерку под	линн	ости сеанса Windows	
🗌 Запр	етить загрузку	у ОС в Бе	зопа	сном режиме	
Пере	ключение мон	итора в т	екст	овый режим при старте	
🗹 Испо	льзовать полн	юе имя в	учёт	ных записях Windows N	т
🗹 Заве	ршать сессию	только п	олна	й перезагрузкой	
Вести ж	урналы в: [D:VAccord	.x64\		
🗌 Пока	зывать меню	экспорта	а жур	налов в трэе	
1024	Ограничив	ать разм	ер ж	урнала (МВ)	
Наимен	ование АС:				
🗌 Изме	нить экран вх	ода в сис	тем	ł	

4

Рисунок 3 – Установка опции «Завершать сессию только полной перезагрузкой»

4. Завершить работу приложения с сохранением изменений.

5. Запустить утилиту «Редактор прав доступа» (Пуск-> Программы-> Аккорд-> Редактор прав доступа). В поле «Программная среда» установить в строке «Детальность журнала» значение «Сбор статистики», выбрав его из выпадающего списка (рисунок 4). Удаляем в Разделении доступа — Объекты и Процессы (рисунок 5).

🔒 🏖 🗙 🔎 😂 🏗	🛛 🖉 🖛 🗍 🕹 📲					
🗐 🛃 Администраторы	Идентификация/Аутентиф	рикация				
Гл.Администратор	Полное имя	Gerojo	••••			
Э 🛃 Обычные	Идентификатор	01 000056F343CE 45				
	Пароль	Не назначен				
	Вход в систему					
	Параметры пароля	0+30+3+Только Супервизор				
	Временные ограничения	Нет … Блокирован	Г			
	Подконтрольный	Г				
	Г Чровень доступа пользов					
	Уровень доступа	Общедоступно []				
	Программная среда	1	~			
	Стартовая задача	<u>e</u>	-			
	Детальность журнала	Сбор статистики	•			
	Гашение экрана	И CTRL+F12 ALT+F12 5				
	Опции	Результаты И/А				
	01000000	11110000				
	Контроль целостности	Разграничение доступа				

Рисунок 4 - Установка детальности журнала «Сбор статистики»

Редактирование правил разграничения доступа для DOCTOR	_		×
Объекты Процессы			
Объеклы	Права	goemy	na
INSERT DELETE ENTER	F2	[ESC
Новый Удалить Редактировать 🚭 USB/SD	Сохранит	ь	гмена 🗎

Рисунок 5 — Очищаем содержимое Объекты и Процессы

6. Перезагрузить компьютер.

5

7. Войти в ОС под учетной записью пользователя (при запуске будет оповещение о специальном режиме работы комплекса «Аккорд»). Запустить процессы, необходимые для выполнения должностных обязанностей пользователя. Завершить сеанс пользователя. Выйти из ОС. Повторить данную процедуру несколько раз, для получения подробной статистики.

8. Войти в ОС под учетной записью администратора.

9. Запустить программу LogBase.exe (по умолчанию — C:\Accord.x64\LogBase.exe). Выбрать файлы журнала предыдущих сеансов под учетной записью пользователя (рисунок 6). Запустить из меню Команды — Запуск AcProc.

🚰 LogBase - Работа с	журналами пользователей		_		×
Файл Команды ?					
• 11 🚳	\checkmark				
SUPERVISOR	Имя журнала	Дата/время входа	Дата/время вы	жода	
DUCTOR	20201214170102.LOW	14.12.2020 / 17:01:02	14.12.2020 / 17	:04:16	
C:\Accord.x64\					

Рисунок 6 – Выбор журнала для формирования списка

В появившемся окне (рисунок 7) отметить только необходимые (для работы пользователя) процессы (вкладка 'Процессы') и нажать кнопку <Экспортировать>. Т.о появится файл *.prd в котором будут прописаны все процессы используемые пользователем (рисунок 8).

Анализатор журналов			_	×
Файл тюмощь Файл журнала: С:\Accord.x64\2021	01214170102.LOW			
Имя пользователя: DOCTOR				
Процессы Объекты ОБЩИЙ_РЕС	JPC			
Процессы	Категории доступа			~
ACRUNNT.EXE	Общедоступно			
APPLICATIONFRAMEHOST.EXE	Общедоступно			
BACKGROUNDTASKHOST.EXE	Общедоступно			
BDEUISRV.EXE	Общедоступно			
BROWSER_BROKER.EXE	Общедоступно			
CALCULATOR.EXE	Общедоступно			
CMD.EXE	Общедоступно			
CONHOST.EXE	Общедоступно			
CTFMON.EXE	Общедоступно			
DLLHOST.EXE	Общедоступно			
EXPLORER.EXE	Общедоступно			
FILECOAUTH.EXE	Общедоступно			
FONTDRVHOST.EX	Общедоступно			
GFXDOWNLOADWRAPPER.EXE	Общедоступно		_	
GOOGLECBASHHANDLEB EXE	Общелостипно			×
Снять все Очистить спис	ок Общий ресурс Эк	спортиров	зать	

Рисунок 7 – Выбор процессов для контроля

10. Нажать кнопку "Экспортировать". При нажатии кнопки появляется окно, в котором следует указать путь, имя файла и нажать кнопку <Сохранить> (рисунок 8).

йл Помощь				
йл журнала: C:\Accord.x64\20201224185615.LOW				
а пользователя: USER3				
less lesson l				
роцессы Объекты ОБЩИИ_РЕСЭРС				
роцессы	🛂 Сохранение файла .PRD		×	Категории доступа
ACRUNNT.EXE		-		Общедоступно
ANYDESK.EXE	Папка: Accord.x64	• + E		Общедоступно
AUDIODG.EXE	14ua ^	Л ата и	-	Общедоступно
C:VASMVALCUNNE F.EXE		дата из	Michen M	Общедоступно
C:\PROGRAM FILES (X86)\ANYDESK\ANYDESK.EXE	Backup	24.12.2	020 18:38	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\CONFIGSERVICE.EXE	Identifiers	16.12.2	020 15:33	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\SUSERVICE.EXE	Vista	16.12.2	020 15:33	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\SUSETSCHED.EXE	Wallpapers	16.12.2	020 15:33	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\TVSU.EXE	AccordUpdate.prd	18,10,2	016 13:30	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\TVSUCOMMANDLAUN	(Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\TVSUKERNEL.EXE			-	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\TVSUSHIM.EXE	Имя файла: USER3.prd		Сохранить	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\UACSDK.EXE				Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\UNCSERVER.EXE	Тип файла: ПРД СЗИ НСД "Аккорд" (* prd)	•	Отмена	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\UNCSETTING.EXE	and an and a second		13	Общедоступно
C:\PROGRAM FILES (X86)\MICROSOFT\EDGEUPDATE\MICROSOFTEDGEUPD	ATE.EXE			Общедоступно
C:\PROGRAM FILES (X86)\MICROSOFT\EDGE\APPLICATION\MSEDGE.EXE				Общедоступно
C:\PROGRAM FILES (X86)\OPENOFFICE 4\PROGRAM\SOFFICE.BIN				Общедоступно
C:\PROGRAM FILES (X86)\OPENOFFICE 4\PROGRAM\SOFFICE.EXE				Общедоступно
C:\PROGRAM FILES (X86)\VMWARE\VMWARE WORKSTATION\VMWARE-TRA	W.EXE			Общедоступно
C:\PROGRAM FILES (X86)\VMWARE\VMWARE WORKSTATION\VMWARE-UNI	TY-HELPER.EXE			Общедоступно
C:\PROGRAM FILES (X86)\VMWARE\VMWARE WORKSTATION\VMWARE.EXE				Общедоступно
C:\PROGRAM FILES\ERL7.3\ERTS-7.3\BIN\EPMD.EXE				Общедоступно
C:\PROGRAM FILES\ERL7.3\ERTS-7.3\BIN\ERL.EXE				Общедоступно
C:\PROGRAM FILES\ERL7.3\ERTS-7.3\BIN\ERLSRV.EXE				Общедоступно
C:\PROGRAM FILES\ERL7.3\ERTS-7.3\BIN\INET_GETHOST.EXE				Общедоступно
C:\PROGRAM FILES\ERL7.3\LIB\OS_MON-2.4\PRIV\BIN\WIN32SYSINFO.EXE				Общедоступно

Рисунок 8 – Сохранение файла .PRD

11. Выйти из приложения Анализатор журналов.

12. Запустить утилиту «Редактор прав доступа». Выбрать пользователя, нажать на него правой кнопкой мыши. Отметить «Импорт ПРД» (рисунок 9). Появится окно выбора файла со списком процессов (рисунок 10).

ACED32 Pega	ктор базы пользователе	Администратор й ПАК "Аккорд"		×
	▶ 😂 🏗	● ● & 4		
Админист Да Даминист Даминист Даминист Даминист Даминист Дамин	граторы дминистратор	-Идентификация/Аутентиф Полное имя	рикация	
📃 🔜 🧟 USB		мдентификатор	01 000056F343CE 45	
	Переименование	вроль	Не назначен	
	• Переместить	юд в систему араметры пароля	0+30+3+Только Супервизор	
	Импорт ПРД Экспорт ПРД	ременные ограничения	Нет Блокирован	
	Импорт из *.atf Экспорт в *.atf	ровень доступа пользов	ателя	
L		Уровень доступа	Общедоступно []	
		Программная среда Стартовая задача		à
		Детальность журнала	Сбор статистики	
		Гашение экрана	и ctrl+f12ALT+f125	<u> </u>
		01000000		
		Контроль целостности	Разграничение доступа	_
		Пнет	Ш Доступ к объектам	<u> </u>

Рисунок 9 – Импорт ПРД

		S 1		
дминистраторы Эполь	Идентификация/А	утентификац	ия	
I л.Администратор	Полное имя	Geo	nio 📕	x
Папка: Accord.x64			G 🖻 🖻	
Backup				
Identifiers				
Wallpapers				
AccordUpdate.prd				
AcWs32.prd				
EVERTUNE.DIG				
USER3.prd			OTYPH	
USER3.prd Имя файла: USER3.prd			Откры	пъ
USER3.prd Имя файла: USER3.prd Тип файла: Файлы ПРД			• Отме	пъ
USER3.prd Имя файла: USER3.prd Тип файла: Файлы ПРД			• Отме	на

Рисунок 10 – Выбор файла со списком процессов

13. Выбрать нужный файл .prd. и нажать кнопку <Открыть>.

В появившемся окне установить флаг «Для процессов» и нажать кнопку <Импорт> (рисунок 11). В окне со списком импортированных процессов (рисунок 12) отметить строку «Заменить».

йл Команды ?] 🏖 🗙 🔎 🔛 🎼 🗍	• • & 4	
Администраторы а Гл.Администратор Параметры импорта	фикация/Аутентификация имя Geroio ×	
Вход в систему Параметры пароля Временные ограничения Разграничение доступа Для объектов Пля процессов	Разное Поции Результаты И/А Программная среда Стартовая задача Детальность журнала Гашение экрана	
СТRL-F СТRL-С Полная Сброс	Импорт Отмена	- - -
Опцин 01000	000 ···· Результаты И/А 11110000 ль целостности Разграничение доступа	••

Рисунок 11 – Выбор параметров импорта

Список процессов —		×
 ACRUNNT.EXE APPLICATIONFRAMEHOST.EXE AUDIODG.EXE BACKGROUNDTASKHOST.EXE BDEUISRV.EXE BROWSER_BROKER.EXE CALCULATOR.EXE CALCULATOR.EXE COMPPKGSRV.EXE CONHOST.EXE CONHOST.EXE CONHOST.EXE CTFMON.EXE CTFMON.EXE DLLHOST.EXE DWM.EXE EXPLORER.EXE FILECOAUTH.EXE FILECONFIG.EXE IBREFOY.EXE 		~
Снять всё		
 Объединить П Использовать ПРД как у объекта из Заменить 	файла	
OK	Отмен	ia

Рисунок 12 - Окно со списком импортированных процессов

14. Переходим в Разделение доступа — Процессы и проверяем импортированные процессы, в случае необходимости можно их скорректировать (рисунок 13)

Редактирование правил разграничения доступа для DOCTOR	_		×
Объекты Процессы			
Процессы			^
ACRUNNT.EXE			
APPLICATIONFRAMEHOST.EXE			
AUDIODG.EXE			
BACKGROUNDTASKHOST.EXE			
BDEUISRV.EXE			
BROWSER_BROKER.EXE			
CALCULATOR.EXE			
CHROME . EXE			
COMPPKGSRV.EXE			
CONHOST . EXE			
CSRSS.EXE			
CTFMON.EXE			
DLLHOST.EXE			
DWM.EXE			
EXPLORER . EXE			×
INSERT DELETE ENTER	F2	E	SC
Новый Удалить Редактировать 🚓 USB/SD	Сохранит	ъОт	мена

Рисунок 13 - Окно со списком импортированных процессов

15. Установить запрет на запуск процесса Shutdown.exe можно следующим образом: в главном окне утилиты ACED32 (рисунок 4) нажать кнопку справа в поле «Разграничение доступа» для группы Обычные, найти в списке Shutdown.exe, нажать кнопку <Редактировать> (Enter) и в появившемся окне атрибутов доступа поле «Прочее» оставить пустым (рисунок 14).

ибуты доступа к объектам		
DUbytu goctyfia k o6bekram SgrmEnclave.dll A SgrmEnclave_se SgrmLpac.exe SgrmLpac.exe SgrmLpac.exe Shacet.dll SharedPCCSP.dl SharedPcCSP.dl ShareHost.dll ShareHost.dll ShareMost.dll ShareMost.dll ShareMost.dll ShellSyle.dll Shellsyle.dll Shina dll Shina dll	 Имя объекта: С:\Windows\System Тип объекта: Файл Операции с файлами Я Открыть для чтения Я Открыть для записи С Создание О Удаление N Переименование V Видимость О Эмуляция записи 	n32\shutdown.exe Операции с папками ✓ М Создание ✓ Е Удаление ✓ Б Переход ✓ п Переименование Регистрация Г п При чтении Г w При записи Прочее Г X Запуск программ
shimgvw.dll shlwapi.dll shpafact.dll shrpubw.exe shsetup.dll shrvcs.dll shunimpl.dll shunimpl.dll	Наследование прав доступа С 0 Нет С 5 На все подкаталоги С 1 Только на следующий уровень СТRL-С СТRL-R СТRL Сборос Чтение Полни	F F2 ESC эй Сохоанить Закони

Рисунок 14 – Окно атрибутов доступа к объектам

16. Сменить детализацию журнала пользователя на значение «Низкая» (рисунок 15).

13						
🖺 АСЕD32 Редактор базы пользователей ПАК "Аккорд" — 🗌 🗙						
Файл Команды ?						
🖃 🛁 Администраторы	ы Идентификация/Аутентификация					
👘 🔏 Общинистратор	Полное имя	· · · · · · · · · · · · · · · · · · ·				
	Шипка	01 000033332080 D5 ···				
LOCALADM	Пароль	Назначен				
	Вход в систему					
	Параметры пароля	8+5+3+Супервизор и пользователь …				
	Временные ограничения	Нет 🛄 Блокирован 🗖				
	Подконтрольный					
уровень доступа пользователя						
	Уровень доступа	Общедоступно []				
	Программная среда					
	Стартовая задача	<u>i</u>				
	Детальность журнала	Низкая 💌				
	Гашение экрана	И СТВL+F12 ALT+F12 5				
	Опции	Результаты И/А				
	0000000	11110000				
	Контроль целостности	Разграничение доступа				
	Нет	Доступ к объектам				

Рисунок 15 – Установка низкого уровня детальности журнала пользователя

17. Выйти из приложения ACED32. Перезагрузить компьютер.