

СПО «АККОРД- Win64 К»

Инструкция по исключению возможности запуска системных команд LogOff, Shutdown и др.

> 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» и «Контроль процессов» (рисунок 1).

Состояние: Аккорд установлен: Нет Мягкий режим: Выключен Версия AcRun.sys: Не запущен Версия AcGina.dll: Не запущен	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: 🗌
Паследование ПРД от группы ТМ-контроллер: Использовать страницу ТМ: 0 🐳	Журнал команд: 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 установить флаг «Использовать полный путь процесса» (рисунок 2).

Разное:				
	and a second			
Число проходов, при очистке файлов:	-			
Очищать файлы, начиная с уровня: Общедоступно	4			
🗌 Очищать файл подкачки				
🗌 Выводить на экран сообщения о НСД				
Поврана на экран сообщения от год				
Использовать полный путь процесса				
🗹 Записывать в журнал логические имена дисков				
🖂 Печатать гриф приложения в заголовке окна				
Хранитель экрана:				
Блокировать USB устройства				
Tokot b upply togo ok polici				

Рисунок 2 - Установка опции «Использовать полный путь процесса»

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

	Режим сессии	Разное	Данные конфигурации	
Режим с	ессии			
Вручную	(Режим	старта системы защиты	
Ucnov	пьзовать проверн этить загрузку О(ключение монито пьзовать полное	к у подлинн С в Безопа ра в текст имя в учёт	юсти сеанса Windows оном режиме овый режим при старте ных записях Windows NT	
Завер	шать сессию тол	ько полно	й перезагрузкой	
Вести жу	рналы в: С: 🖓	ccord.x64		E
	зывать меню эко	порта жур	налов в трэе	
Пока				
🗌 Пока	Ограничивать	размер ж	урнала (МВ)	
Пока 0	Ограничивать рвание АС:	размер ж	урнала (МВ)	

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).

🕞 🏖 🗙 🔎 😂 🔚	🛛 🖉 🖛 🗍 🗞 📲	
🗄 🛃 Администраторы	Идентификация/Аутентиф	рикация
Гл.Администратор	Полное имя	Gerojo
В бычные	Идентификатор	01 000056F343CE 45
	Пароль Не на	Не назначен
USERUSB	Вход в систему	
	Параметры пароля	0+30+3+Только Супервизор
	Временные ограничения	Нет Блокирован (
	Подконтрольный	Г
		279.07
	эровень доступа пользов	
	эровень доступа	
	Программная среда	1
	Стартовая задача	9
	Детальность журнала	Сбор статистики
	Гашение экрана	И CTRL+F12ALT+F125
	Опции	Результаты И/А
	01000000	11110000
	Контроль целостности	Разграничение доступа

Рисунок 4 - Установка детальности журнала «Сбор статистики»

6. Перезагрузить компьютер.

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.

8. Войти в ОС под учетной записью администратора.

9. Запустить программу AcProc.exe (Пуск-> Программы-> Аккорд-> Создание списка процессов из журналов регистрации). Выбрать файл журнала предыдущего сеанса под учетной записью пользователя. В появившемся окне отметить только необходимые (для работы пользователя) процессы и нажать кнопку <Общий ресурс>. Далее по выбранному файлу журнала происходит поиск объектов, к которым выбранный процесс обращался с запросами, и если поиск завершается успешно, то во вкладке «Общий ресурс» появляются соответствующие объекты (рисунок 5). При необходимости скорректировать этот список.

Васе - Работа с усурналами пользовате		
督 Анализатор журналов	— [
Файл Помощь		
Файл журнала: [C:\Accord.x64\2020 Имя пользователя: USER3	1224191654.LOW	
Процессы Объекты ОБЩИЙ_РЕСУ	PC	
Процессы	Категории доступа	^
ACRUNNT.EXE	Общедоступно	
ANYDESK.EXE	Общедоступно	
AUDIODG.EXE	Общедоступно	
C:\ASM\ACCONNET.EXE	Общедоступно	
C:\PROGRAM FILES (X86)\ANYD	Общедоступно	
C:\PROGRAM FILES (X86)\LENO	Общедоступно	
CAPBOGBAM FILES (\$86)VENO	Общелостипно	~
Снять все Очистить списо	к Общий ресурс Экспортировать	

Рисунок 5 – 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 6).

іл Помощь			
йл журнала: C:\Accord.x64\20201224185615.LOW			
а пользователя: USER3			
роцессы Объекты ОБЩИЙ_РЕСУРС			
роцессы	Соуранение файла PRD	×	Категории доступа
ACRUNNT.EXE	Сохранение фанла л но	~	Обшедостипно
ANYDESK.EXE	Папка: Accord x64	▼ ← € [*] ■	Общедоступно
AUDIODG.EXE	· · · · · · · · · · · · · · · · · · ·		Общедоступно
C:VASMVACCONNET.EXE	Имя	Дата изменения	Общедоступно
C:\PROGRAM FILES (X86)\ANYDESK\ANYDESK.EXE	Backup	24.12.2020 18:38	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\CONFIGSERVICE.EXE	Identifiers	16.12.2020 15:33	Общедоступно
CVPROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\SUSERVICE.EXE	Vista	16 12 2020 15:33	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\SUSETSCHED.EXE	Wallpaperr	16 12 2020 15:33	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\TVSU.EXE		10.10.2016 12.20	Общедоступно
C:\PROGRAM FILES (X86)\LENOVO\SYSTEM UPDATE\TVSUCOMMANDLAUN	Accordopdate.prd	18.10.2010 13:30	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			Общедоступно
: \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
:\PROGRAM FILES (X86)\OPENOFFICE 4\PROGRAM\SOFFICE.EXE			Общедоступно
C:\PROGRAM FILES (X86)\VMWARE\VMWARE WORKSTATION\VMWARE-TRA	Y.EXE		Общедоступно
C:\PROGRAM FILES (X86)\VMWARE\VMWARE WORKSTATION\VMWARE-UNI	TY-HELPER.EXE		Общедоступно
:\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\W/IN32SYSINFO.EXE			Обшедостипно

Рисунок 6 – 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 7). Появится окно выбора файла со списком процессов (рисунок 8).

🛃 Администра 🕱 Гл.Адмі	I			
ПЛАЦМІ	торы	Идентификация/Аутентиф	рикация	
USBAD	мім	Полное имя	Gerojo	
🛃 Обычн		- ^М дентификатор	01 000056F343CE 45	
<u>&</u> `	синхронизировать	ароль	Не назначен	••
8 U1 [Переименование	KOR B CHCTEMU		
⇒ [Переместить	араметры пароля	0+30+3+Только Супервизор	
-	Импорт ПРД	ременные ограничения	, Нет ··· Блокирован	F
3	Экспорт ПРД			1
	Ампорт из *.atf	одконтрольный		
	Экспорт в *.atf	ровень доступа пользов	ателя	
		Уровень доступа	Общедоступно []	
		Программная среда		
		Стартовая задача	1	ê
		Детальность журнала	Сбор статистики	•
		Гашение экрана	И CTRL+F12ALT+F125	
		Опции	Результаты И/А	_
				1.0

Рисунок 7 – Импорт ПРД

	X 🎤 🔤 🟥		1		
- 🛃 Aa	министраторы Гл.Администратор	Идентификация/Ауте Полное имя	нтификация Geroio	X	
- <u>-</u>	Импорт файла				
	Папка: Accord.x64		• G	12 19 💷	
	Backup				
	Identifiers				
	Vista				ван
	AccordUpdate.prd				
	AcWs32.prd				-
	EVERYONE.prd				
	USER3.prd				
	Имя файла: USER3.prd			Открыть	
	Имя файла: USER3.prd			Открыть	
	Имя файла: USER3.prd Тип файла: Файлы ПРД		•	Открыть Отмена	
	Имя файла: USER3.prd Тип файла: Файлы ПРД			Открыть Отмена	
	Имя файла: USER3.prd Тип файла: Файлы ПРД	101000000		Открыть Отмена	
	Имя файла: USER3.prd Тип файла: Файлы ПРД	101000000 Контроль целостност		Открыть Отмена 11110000	ступа

Рисунок 8 – Выбор файла со списком процессов

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

6

В появившемся окне установить флаг «Для процессов» и нажать кнопку <Импорт> (рисунок 9). В окне со списком импортированных процессов (рисунок 10) отметить строку «Заменить».

8° X ₽ 😂 🏝	
💁 Администраторы 📆 Гл.Администратор	Идентификация/Аутентификация Полное имя Баккір
Параметры импорта	× –
Вход в систему Параметры пароля Временные ограничения	Разное П Опции П Результаты И/А
Разграничение доступа Для объектов Г Для процессов	Программная среда Стартовая задача Детальность журнала Гашение экрана
CTRL-F CTRL-C Полная Сброс	Импорт Отмена
	Опции Результаты И/А

Рисунок 9 – Выбор параметров импорта

Файл Коман	дактор базы пользоват ды ?	елей ПАК "Аккорд"			
Админ	 Список процессов ACRUNNT.EXE ANYDESK.EXE AUDIODG.EXE 		- 0	×	
⊟— <mark>—</mark> В Обыч —— В Ц	C:\ASM\ACCONNET. C:\PROGRAM FILES C:\PR	EXE (X86)\LENOVO\SYSTEM UPDATE (X86)\LENOVO\SYSTEM UPDAT	CONFIGSER SUSERVICE. SUSETSCHE TVSU.EXE TVSUCOMM. TVSUKERNE TVSUSHIM.E UNCSERVEF UNCSERVEF UNCSERVEF UNCSERVEN SUNCSETTEN CATION/MSED	VICE.EXE EXE D.EXE ANDLAU L.EXE XE EXE G.EXE G.EXE	р ирован Г
	Снять всё С Объединить Г С Заменить	Использовать ПРД как у объем	та из файла		
	ОК		0	гмена	
		Контроль целостности	• Разгр	аничение до уп к объект	ам

Рисунок 10 - Окно со списком импортированных процессов

14. Установить запрет на запуск процесса Shutdown.exe можно следующим образом: в главном окне утилиты ACED32 (рисунок 4) нажать кнопку справа в поле «Разграничение доступа», найти в списке Shutdown.exe, нажать кнопку <Редактировать> (Enter) и в появившемся окне атрибутов доступа поле «Прочее» оставить пустым (рисунок 11).

грибуты доступа к объектам		3
SgmEnclave.dll A SgmEnclave_se SgmLpac.exe SgmLpac.exe Shacet.dll SharedPCCSP.dl SharedPcCSP.dl SharedRealitySv ShareHost.dll ShareHost.dll ShareHost.dll ShareHost.dll ShareHost.dll ShareHost.dll ShareHost.dll ShareHost.dll SharedRealityList ShareHost.dll SharedRealityList ShareHost.dll SharedRealityList SharedRealit	Имя объекта: С:\Windows\System Тип объекта: Файл Операции с файлами Г В Открыть для чтения Г В Открыть для чтения Г W Открыть для записи С Создание Г D Удаление Г N Переименование Г V Видимость Г О Эмуляция записи	32\shutdown.exe Операции с папками ✓ М Создание ✓ Е Удаление ✓ С Переход ✓ п Переименование Регистрация Г При чтении Г w При записи Прочее Г Х Запуск программ
	Наследование прав доступа С 0 Нет С 5 На все подкаталоги С 1 Только на следующий уровень СТRL-С СТRL-R СТRL- Сброс Чтение Полны	F F2 ESC й Сохранить Закрыть

Рисунок 11 – Окно атрибутов доступа к объектам

15. Сменить детализацию журнала пользователя на значение «Низкая» (рисунок 12).

16. Выйти из приложения ACED32. Перезагрузить компьютер.

a 🖀 🗙 🔎 😂 🛍	⊅ ⇒ & 4	I	
- 🛃 Администраторы	Идентификация/Аутенти	фикация	
Гл.Администратор	Полное имя	Gerojo	
Обычные	Идентификатор	01 000056F343CE 45	
	Пароль	Не назначен	
USERUSB	Вход в систему		
	Параметры пароля	0+30+3+Только Супервизор	
	Временные ограничения	Нет … Блокирован	Г
	Подконтрольный	Г	
	Г-Уровень доступа пользов	вателя	
	Уровень доступа	Общедоступно []	••••
	Программная среда		
	Стартовая задача		è
	Детальность журнала	Низкая	•
	Гашение экрана	И CTRL+F12 ALT+F12 5	
	Опции	Результаты И/А	
	01000000	11110000	
	Контроль целостности	Разграничение доступа	

Рисунок 12 – Установка низкого уровня детальности журнала пользователя