ОСОБОЕ КОНСТРУКТОРСКОЕ БЮРО
СИСТЕМ АВТОМАТИЗИРОВАННОГО ПРОЕКТИРОВАНИЯ

ГОСУДАРСТВЕННАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ

УТВЕРЖДЕН
37222406.26.20.40.140.091 90-ЛУ

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «АККОРД-Win64 К»

РУКОВОДСТВО АДМИНИСТРАТОРА

37222406.26.20.40.140.091 90

АННОТАЦИЯ

Настоящий документ является руководством по управлению механизмами защиты специального программного обеспечения средств защиты информации от несанкционированного доступа (СПО СЗИ НСД) «Аккорд-Win64 K» (ТУ 26.20.40.140-091-37222406-2020) (далее по тексту – СПО «Аккорд-Win64 K», «Аккорд-Win64 K», СПО «Аккорд», «Аккорд») и предназначен для конкретизации задач и функций должностных лиц организации (предприятия, фирмы), планирующих и организующих защиту информации в системах и средствах информатизации на базе СВТ с применением СПО «Аккорд-Win64 K».

В документе приведены основные функции администратора безопасности информации, порядок установки прав доступа пользователей к информационным ресурсам, организации контроля работы СВТ с внедренными средствами защиты и другие сведения необходимые для управления защитными механизмами СПО «Аккорд-Win64 K».

Для лучшего понимания и использования защитных механизмов СПО «Аккорд-Win64 K» рекомендуется предварительно ознакомиться с комплектом эксплуатационной документации, а также принять необходимые защитные организационные меры, рекомендуемые в документации.

Применение защитных мер СПО «Аккорд-Win64 K» должно дополняться общими мерами предосторожности и физической безопасности СВТ.

СОДЕРЖАНИЕ

1. Содержание работы Администратора безопасности информации по применению СПО «Аккорд» 9
1.1. Планирование применения СПО «Аккорд» 9
1.2. Установка и настройка СПО «Аккорд» 11
1.3. Эксплуатация СПО «Аккорд» 12
1.4. Снятие защиты 12
2. Основные механизмы реализации защитных функций СПО «Аккорд» 14
2.1. Требование идентификации и аутентификации 14
2.2. Требование гарантии проектирования 14
2.3. Требование реализации дискреционного механизма разграничения доступа 17
2.4. Требование по реализации мандатного принципа контроля доступа 20
2.5. Требование управления потоками информации 23
2.6. Требование регистрации событий 23
2.7. Требование очистки памяти 25
3. Некоторые особенности действия атрибутов и подготовки ПРД 27
4. Примеры ПРД для типовых ситуаций разграничения доступа 29
4.1. Пример 1. Субъекту разрешено работать в каталоге C:\DOC 29
4.2. Пример 2. Пользователю на диске будут видны и доступны только явно описанные каталоги 29
4.3. Пример 3. Разрешено работать только с файлами и только в выделенном каталоге 30
4.4. Пример 4. Применение атрибутов наследования 31
4.5. Пример 5. То же, но пользователю нельзя удалять файлы 31
4.6. Пример 6. У пользователя полный доступ к директории на диске D 32
4.7. Пример 7. Конфиденциальное делопроизводство 32
4.8. Пример 8. То же, что и пример 7, но разрешен доступ только к корню диска A 33
4.9. Пример 9. То же, но пользователь может читать все файлы, размещенные на A 34
4.10. Пример 10. Установка атрибутов файлов 34
4.11. Пример 11. Установка атрибутов для выделенных программ 35
4.12. Пример 12. Запрет доступа к файлам 36
4.13. Пример 13. Анализ ресурсов 36
4.14. Пример 14. Использование атрибута «О» 37
4.15. Пример 15. Описание сетевого ресурса 37

4.16. Пример 16. Создание изолированной программной среды (ИПС) в ОС Windows..... 39
4.17. Пример 17. Регистрация вывода документа на печатающее устройство 41
5. Правовые аспекты применения СПО «Аккорд» 43
6. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА..... 44
Приложение 1. Рекомендации по организации службы информационной безопасности..... 45
Приложение 2. Операции, фиксируемые подсистемой регистрации СПО «Аккорд» 47
Приложение 3. Список событий СПО «Аккорд-Win64 К», регистрируемых в системном журнале ОС..... 49
Приложение 4. Сообщения об ошибках СПО «Аккорд-Win64 К» 51
Приложение 5. Перечень нормативных документов, используемых при организации защиты информации 52
Приложение 6. Список файлов ОС Windows 7 x32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К»..... 54
Приложение 7. Список файлов ОС Windows 7 x64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К»..... 56
Приложение 8. Список файлов ОС Windows 8.1 x 64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К» 59
Приложение 9. Список файлов ОС Windows 8.1 x 32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К» 62
Приложение 10. Список файлов ОС Windows 10 x64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К» 65
Приложение 11. Список файлов ОС Windows 10 x32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К» 68
Приложение 12. Список файлов ОС Windows Server 2003 R2 x32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К» 70
Приложение 13. Список файлов ОС Windows Server 2003 R2 x64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 К» 73
Приложение 14. Список файлов ОС Windows Server 2012 R2, рекомендуемых для контроля целостности при СПО «АККОРД – Win64 К»..... 76

Приложение 15. Список файлов ОС Windows Server 2016, рекомендуемых для контроля целостности при СПО «АККОРД – Win64 K»..... 87

ПРИНЯТЫЕ ТЕРМИНЫ И СОКРАЩЕНИЯ

Администратор БИ	– администратор службы безопасности информации
Имя_пользователя	– имя, под которым пользователь зарегистрирован в системе
Идентификатор	- специальное устройство, содержащее уникальный признак пользователя, с которым зарегистрированный пользователь входит в систему и который используется системой для определения его прав, а также для регистрации факта доступа и характера выполняемых им работ или предоставляемых ему услуг
Объект доступа	– под объектом доступа понимается один из перечисленных ресурсов СВТ: диск, каталог, файл, раздел или ключ реестра, процесс (задача), драйвер устройства.
Параметры пользователя	– идентифицирующие признаки пользователя (имя, данные для идентификации, пароль) и его права по доступу к ресурсам СВТ в соответствии с его полномочиями
Пользователь	– субъект доступа к объектам (ресурсам) СВТ
ПРД	– правила разграничения доступа
Предъявить идентификатор	- приложить идентификатор к контактному устройству съемника информации, либо вставить идентификатор в USB-порт компьютера, либо ввести данные с клавиатуры (в зависимости от типа используемого идентификатора)
Удаление пользователя	– удаление имени, под которым пользователь зарегистрирован в системе, из списка зарегистрированных пользователей в СПО «Аккорд-Win64 K»
Синхронизация параметров пользователя	– сопоставление БД пользователей подсистемы разграничения доступа с учетными записями пользователей Windows
Создать пользователя	– зарегистрировать пользователя в подсистеме разграничения доступа
Сообщения	– информация, выводимая на дисплей, которая сообщает о действиях пользователя, о состоянии программы и нормально завершенных действиях, сбоях в системе и др.
Число проходов при удалении	– количество проходов случайной последовательности по содержимому файла при его удалении

ВВЕДЕНИЕ

Специальное программное обеспечение (СПО) «Аккорд-Win64 K» (ТУ 26.20.40.140-091-37222406-2020) - это простое, но чрезвычайно эффективное средство, используя которое можно надежно защитить от несанкционированного доступа информацию на СВТ (серверах и рабочих станциях), функционирующих под управлением 64-битных ОС Windows 7, Windows 8, Windows 8.1, Windows Server 2012 Enterprise Edition R2, Windows 10 Professional, Windows Server 2016 Enterprise Edition, Windows Server 2019 или 32-битных ОС Windows 7, Windows 8, Windows 8.1, Windows 10 Professional, без переделки ранее приобретенных программных средств.

СПО «Аккорд-Win64 K» реализует:

- механизм дискреционного контроля доступа;
- механизм мандатного[1] контроля доступа;
- механизм защиты ввода и вывода на отчуждаемый физический носитель информации и соотнесения пользователя с устройством;
- механизм идентификации и аутентификации пользователей;
- механизм регистрации системных событий;
- механизм контроля целостности.

СПО «Аккорд» - это лишь хороший инструмент, позволяющий службе безопасности информации (администратору БИ) значительно проще и надежнее решать одну из стоящих перед ней задач – защиту от НСД к СВТ и информационным ресурсам АС, разграничение доступа к объектам доступа.

Использование СВТ с внедренными средствами защиты СПО «Аккорд-Win64 K» не требует изменения существующего программного обеспечения. Необходимо лишь квалифицированное применение СПО «Аккорд-Win64 K» – правильная установка, настройка и эксплуатация в соответствии с принятыми на предприятии ПРД и обеспечение организационной поддержки.

Как показывает практика довольно длительного применения СПО семейства «Аккорд», часто трудности заключаются в отсутствии у большинства пользователей (организаций, фирм и т.д.) установленного порядка и четких правил разграничения доступа к защищаемым ресурсам. Поэтому именно выяснение того, что и кому в СВТ доступно, а что нет, и какие действия с доступными ресурсами разрешено выполнять, а какие нет, является основным содержанием необходимой организационной поддержки.

Для выполнения этих задач, а также для обеспечения непрерывной организационной поддержки работы применяемых программно-технических средств защиты информации, в том числе и СПО «Аккорд», необходима специальная служба безопасности информации (СБИ), в небольших

---

[1] В рамках настоящего документа под мандатным принципом контроля доступа понимается принцип контроля доступа на основе иерархических меток

организациях и подразделениях - администратор безопасности информации (администратор БИ). На СБИ (администратора БИ) возлагаются задачи по осуществлению единого руководства, организации применения средств защиты и управления ими, а также контроля за соблюдением всеми категориями пользователей требований по обеспечению безопасности информационных ресурсов автоматизированных систем. Правовой статус СБИ, обязанности и некоторые рекомендации по организации СБИ приведены в Приложении 1.

Для эффективного применения СПО «Аккорд» и поддержания требуемого уровня защищенности СВТ необходимы:

- физическая охрана СВТ и его ресурсов;
- периодическое тестирование средств защиты СПО «Аккорд»;
- разработка и ведение учетной и объектовой документации (инструкция администратора, инструкций пользователей, журнал учета отчуждаемых носителей пользователей и др.). Все разработанные учетные и объектовые документы должны быть согласованы, утверждены у руководства и доведены до сотрудников (пользователей). Это необходимо для того, чтобы План защиты организации (предприятия, фирмы и т.д.) и действия СБИ (администратора БИ) получили юридическую основу.
- прием в эксплуатацию СПО «Аккорд» оформляется актом в установленном порядке, в формуляре на СПО «Аккорд» (37222406.26.20.40.140.091 ФО) администратором БИ делается соответствующая отметка.

1. Содержание работы Администратора безопасности информации по применению СПО «Аккорд»

Основным содержанием работы администратора БИ по применению СПО «Аккорд» являются следующие мероприятия:

- планирование применения СПО «Аккорд»;
- организация установки СПО «Аккорд» и настройка его защитных средств в соответствии с установленными ПРД;
- эксплуатация СВТ с внедренным СПО «Аккорд», в т.ч., организация контроля за правильностью применения защитных механизмов СПО «Аккорд»;
- снятие защиты.

1.1. Планирование применения СПО «Аккорд»

Планирование применения СПО «Аккорд» осуществляется с учетом общей политики обеспечения безопасности в организации (на предприятии, фирме и т.д.). Основное содержание этой политики должно отражаться в Плане защиты организации (предприятия и т.д.) - документе, отражающем также подходы к защите информации и фиксирующем состояние защищаемой автоматизированной системы. В части защиты информации в него целесообразно включать сведения о характере и составе обрабатываемой информации, составе технических и программных средств АС (СВТ), возможных угрозах системе и наиболее вероятных способах их реализации, описание выбранных методов и средств защиты от этих угроз, правила разграничения доступа к информационным ресурсам и другие вопросы.

Для настройки средств защиты СПО «Аккорд» в соответствии с разработанными и утвержденными в организации ПРД администратору БИ необходимо предварительно выяснить и отразить в плане защиты следующие характеристики защищаемой системы (СВТ):

- перечень задач, решаемых структурными подразделениями организации (сотрудниками) с использованием АС (СВТ);
- детальный перечень используемых при решении каждой задачи программ;
- детальный перечень используемых при решении каждой задачи (совместно используемых несколькими задачами) данных с указанием мест их размещения, режимов обработки и правил доступа к ним;
- конфигурацию СВТ с указанием перечня используемых технических средств (принтеров, сканеров и т.д.) и их характеристик;
- при использовании СПО «Аккорд» для защиты ЛВС - подробный перечень имеющихся в защищаемой сети серверов, рабочих станций и т.д. с указанием их состава, конфигурации, характеристик используемых технических средств и мест их размещения;

- перечень размещенных на СВТ (каждой рабочей станции ЛВС и каждом файловом сервере) системных и прикладных программ, файлов и баз данных;
- перечень установленных на СВТ (рабочих станциях и серверах) программных средств защиты (СКЗИ и СЗИ НСД);
- списки пользователей СВТ с указанием решаемых ими задач из общего перечня задач и предоставленных им (в соответствии с их обязанностями) полномочий по доступу в СВТ (рабочим станциям, серверам ЛВС) и информационным ресурсам.

На этапе организации системы защиты и применения СПО «Аккорд» необходимо, исходя из целей защиты СВТ и ее специфики, разработать ряд документов, определяющих:

- порядок и правила предоставления, изменения и утверждения конкретным должностным лицом необходимых полномочий по доступу к ресурсам СВТ;
- порядок организации учета, выдачи, использования и хранения съемных магнитных носителей информации, содержащих резервные копии программ и данных и т.п.;
- порядок обновления используемых версий, приема в эксплуатацию новых системных и прикладных программ на защищаемых СВТ (рабочих станциях, серверах) - кто обладает правом разрешения таких действий, кто осуществляет, кто контролирует, и что при этом они должны делать - гарантирующий их безопасность и отсутствие РПВ;
- порядок использования, хранения и контроля целостности программных продуктов;
- порядок замены и ремонта средств вычислительной техники на защищаемой СВТ (в АС) - кто обладает правом разрешения таких действий, кто их осуществляет, кто контролирует, и что при этом они должны делать;
- порядок и периодичность анализа системных журналов регистрации и принятия мер по зарегистрированным несанкционированным действиям пользователей СВТ.

Для реализации впоследствии возможности создания любому пользователю изолированной программной среды (ИПС) необходимо, чтобы вышеназванные документы и правила разграничения доступа к ресурсам гарантировали:

- исключение возможности доступа непривилегированных пользователей к находящихся в СВТ инструментальным и технологическим программам, с помощью которых можно проанализировать работу СЗИ и предпринять попытки их «взлома» и обхода, внедрения разрушающих программных воздействий (РПВ);
- исключение возможности разработки программ в защищенном контуре СВТ (системы);
- исключение возможности несанкционированной модификации и внедрения несанкционированных программ;

- жесткое ограничение круга лиц, обладающими расширенными или неограниченными полномочиями по доступу к защищаемым ресурсам.

С учетом вышеизложенного необходимо также разработать и внести необходимые изменения во все организационно-распорядительные документы (положения о подразделениях, функциональные обязанности сотрудников, инструкции пользователей и т.д.) по вопросам информационной безопасности и правилам работы на СВТ (в АС) с внедренными средствами защиты СПО «Аккорд», действиям в случае возникновения нештатных ситуаций.

1.2. Установка и настройка СПО «Аккорд»

Администратор БИ организует установку СПО «Аккорд» в соответствии с принятой в организации политикой информационной безопасности и осуществляет контроль за качеством ее выполнения.

Порядок установки и настройки СПО «Аккорд» в соответствии с конфигурацией СВТ содержится в «Руководстве по установке» (37222406.26.20.40.140.091 98).

ВНИМАНИЕ! Установка СПО «Аккорд» должна проводиться в присутствии администратора БИ.

ВНИМАНИЕ! Следует помнить, что драйвер AcXAllow.sys (Запрет доступа к общим ресурсам) выключает ВЕСЬ входящий трафик на РС.

В настоящем разделе рассматривается порядок настройки защитных механизмов СПО «Аккорд» в соответствии с правилами разграничения доступа (ПРД) к информации, принятыми в организации (на предприятии, фирме и т.д.).

Содержанием этой работы является назначение пользователям СВТ полномочий по доступу к ресурсам в соответствии с разработанными (и возможно уточненными в ходе настройки СПО «Аккорд») организационно-распорядительными документами.

Полномочия пользователей по доступу к ресурсам АС (СВТ) назначаются с помощью программы ACED32.EXE[2] путем соответствующей настройки:

- средств идентификации и аутентификации пользователей с учетом необходимой длины пароля и времени его жизни, ограничением времени доступа субъекта к СВТ;
- механизма управления доступом к ресурсам с использованием атрибутов доступа, которые устанавливаются администратором БИ в соответствие каждой паре «субъект доступа - объект доступа» при регистрации пользователей исходя из их функциональных обязанностей;
- механизма функционального замыкания программной среды пользователей средствами защиты СПО «Аккорд»;

[2] Описание программы и порядок ее применения см. в документе «Установка правил разграничения доступа. Программа ACED32» (37222406.26.20.40.140.091 97), поставляемом в комплекте эксплуатационной документации на комплекс

- механизмов управления стандартными процедурами печати, процедурами ввода/вывода на отчуждаемые носители информации;
- дополнительных защитных механизмов, таких как блокирование экрана и клавиатуры в случаях, в которых могут реализовываться угрозы информации, а также подачи соответствующих звуковых и визуальных сигналов при попытках несанкционированного доступа к СВТ и его ресурсам.

1.3. Эксплуатация СПО «Аккорд»

При эксплуатации СПО «Аккорд» администратор БИ решает следующие задачи:

- поддерживает средства защиты СПО «Аккорд» в работоспособном состоянии и контролирует правильность их работы;
- производит изменения в настройке средств защиты СПО «Аккорд» на основании и в полном соответствии с изменениями правил разграничения доступа. Они могут быть вызваны различными причинами, например, изменением состава пользователей, их должностных и функциональных обязанностей, расширением номенклатуры используемых технических и программных средств, задач и т.п.
- осуществляет текущий контроль за работой пользователей СВТ с внедренными средствами защиты СПО «Аккорд»;
- анализирует содержимое журнала регистрации событий, формируемого средствами СПО «Аккорд», и на этой основе вырабатывает предложения по совершенствованию защитных механизмов, реализуемых средствами СПО «Аккорд», принимает необходимые меры по совершенствованию системы защиты информации в целом;
- опционально для управления из единого интерфейса использует дополнительное ПО ("Консоль администрирования СЗИ").

ВНИМАНИЕ! Непрерывная организационная поддержка функционирования средств защиты СПО «Аккорд» предполагает обеспечение строгого соблюдения всеми пользователями требований СБИ (администратора БИ).

1.4. Снятие защиты

Снятие (отключение) средств защиты СПО «Аккорд» может потребоваться для установки на жесткий диск компьютера какого-либо нового программного обеспечения - операционной системы, прикладного ПО и т.д.

ВНИМАНИЕ! Снятие защиты разрешено только администратору БИ (супервизору).

Для снятия защиты администратору БИ необходимо отключить подсистему разграничения доступа:

1) Загрузить СВТ и войти в систему с параметрами администратора БИ.

2)Запустить программу ACSETUP.EXE из каталога C:\ACCORD.X64 (C:\ACCORD.NT – для 32-битных ОС) и выполнить процедуру идентификации администратора БИ.

Если идентификация прошла успешно, то на экране появляется диалоговое окно программы настройки СПО «Аккорд».

3)В пункте меню «Команды» программы настройки СПО «Аккорд» следует выбрать подпункт «Снятие» и выполнить действия, рекомендуемые программой. После выполнения команды «Снятие» подсистема разграничения доступа будет отключена и при следующей загрузке не будет активироваться. Каталог ACCORD.X64 (C:\ACCORD.NT – для 32-битных ОС) остается на жестком диске. При необходимости можно полностью деинсталлировать СПО «Аккорд». Для этого в панели управления следует выбрать «Программы и компоненты», найти и выделить строку «Комплекс СЗИ НСД Аккорд-Win64 К», далее выполнить команду «Удалить».

2. Основные механизмы реализации защитных функций СПО «Аккорд»

2.1. Требование идентификации и аутентификации

В соответствии с нормативными документами, комплекс средств защиты (КСЗ) должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность данных для идентификации субъекта - осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам недентифицированных пользователей и пользователей, чья подлинность при аутентификации не подтвердилась.

Реализация

1) Идентификация должна выполняться труднокопируемым уникальным идентификатором до загрузки операционной системы.

2) Аутентификация должна выполняться с обеспечением защиты от раскрытия пароля - по крайней мере, пароль должен быть достаточной длины, и проверяться он должен также до загрузки операционной системы (ОС).

3) Должен обеспечиваться контроль целостности программ и данных и на его основе - защита от несанкционированных модификаций программ и данных;

4) В составе средств защиты от НСД должны быть средства, позволяющие обеспечить контроль запуска задач, и на этой основе - функциональное замыкание информационных систем с исключением возможности несанкционированного выхода в ОС.

2.2. Требование гарантии проектирования

На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:

- непротиворечивые правила изменения ПРД;
- правила работы с устройствами ввода и вывода;
- формальную модель механизма управления доступом.

Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданным принципам разграничения доступа.

Реализация

Описание попыток НСД в среде Windows

Попытки несанкционированного доступа могут быть проведены через:

1) Операции файловой системы.

Подобные операции наиболее часто встречаются при работе с Windows. К ним относятся попытки чтения, записи, модификации и т.д. файлов и каталогов локального или сетевого СВТ. Отсутствие контроля над такими попытками позволяет неавторизованному пользователю получить доступ к любой информации, находящейся в СВТ.

2) Операции работы с реестром Windows.

Эти операции предоставляют возможность для несанкционированного доступа и нарушения целостности системы (подмена системных файлов, внедрение вредоносных программ). Перехватив операции работы с реестром Windows, можно анализировать запросы и пресекать попытки НСД.

3) Загрузка модулей и запуск программ.

Перехватив загрузку модулей, можно отследить/запретить загрузку сторонних модулей (EXE, DLL, VXD, SYS) в системе, что позволит избежать подмены системных модулей. Перехватив запуск исполняемых модулей, можно отследить/запретить запуск сторонних процессов в системе, что позволит избежать запуска вредоносных программ.

Работа драйвера ACRUN.SYS

Операционные системы Windows имеют двухуровневую архитектуру:

1) Системный уровень (kernel mode) - имеет доступ к аппаратному уровню либо через порты ввода/вывода, либо через зарезервированные области памяти;

2) Пользовательский уровень (user mode) - обычно не имеет прямого доступа к аппаратному уровню, а доступ к системному уровню осуществляется через *системные вызовы*.

Пользователь имеет доступ только ко второму уровню – пользовательскому. Очевидно, что контроль доступа к ресурсам лучше осуществлять на системном уровне. Единственный способ заставить код исполняться в kernel mode - это поместить этот код в драйвер. Драйвер – это фактически часть ядра ОС со всеми вытекающими отсюда последствиями.

Таким образом, загрузив свой драйвер и перехватив, к примеру, операции файловой системы, появится возможность:

1) перехватывать операции создания, открытия, чтения, записи в любой файл (у нас привилегии ядра системы);

2) перехватывать операции сканирования каталогов;

3) перенаправлять файловые операции (например, перенаправить вывод в log-файл).

В нашем драйвере перехват доступа к файловой системе выполнен путем перехвата системных вызовов ядра; перехватываются следующие системные функции:

- ZwCreateFile – создание или открытие существующих объектов (файлов, папок, драйверов…);

- ZwOpenFile - открытие существующих объектов (файлов, папок, драйверов…);
- ZwCreateSection – создание нового процесса Win32;
- ZwSetInformationFile – переименование объектов, удаление объектов;
- ZwDeleteFile - удаление объектов;
- ZwWriteFile – запись информации в объект;
- ZwQueryDirectoryFile – просмотр содержимого папки;
- ZwSetSystemTime – установка системного времени, даты;
- ZwDeleteKey – удаление ключа реестра;
- ZwOpenKey – открытие ключа реестра;
- ZwCreateKey – создание ключа реестра;
- ZwDeleteValueKey – удаление переменной реестра;
- ZwSetValueKey – установка значения переменной реестра;
- ZwQueryValueKey – чтение значения переменной реестра;
- ZwClose – закрытие объекта;
- ExFreePool, ExFreePoolWithTag – освобождение памяти.

Почти все подобные вызовы (Zw*) имеют в теле функции следующее:

```
mov eax, NumberFunction
lea edx, [esp+04h]
int 2eh,
```

где NumberFunction есть номер вызываемой функции в таблице системных сервисов, которая находится по адресу, содержащемуся в глобальной переменной KeServiceDescriptorTable. Данная переменная указывает на следующую структуру:

```
typedef struct SystemServiceDescriptorTable
{
SSD SystemServiceDescriptors[4];
} SSDT, *LPSSDT;
Ниже приводятся описания остальных структур:
typedef VOID *SSTAT[];
typedef unsigned char SSTPT[];
typedef SSTAT *LPSSTAT;
typedef SSTPT *LPSSTPT;
typedef struct SystemServiceDescriptor
{
LPSSTAT lpSystemServiceTableAddressTable;
```

```
ULONG dwFirstServiceIndex;
ULONG dwSystemServiceTableNumEntries;
LPSSTPT lpSystemServiceTableParameterTable;
} SSD, *LPSSD;
```

DescriptorTable на которую указывает KeServiceDescriptorTable доступна из KernelMode.

Базовые сервисы ядра находятся в KeServiceDescriptorTable->SystemServiceDescriptors[0].

Каждый элемент таблицы представляет собой структуру типа SSD, которая содержит следующие данные:

- lpSystemServiceTableAddressTable - массив адресов функций, которые вызываются при соответствующем вызове сервиса ядра;
- dwFirstServiceIndex - стартовый индекс в таблице адресов функций;
- dwSystemServiceTableNumEntries - количество сервисов;
- lpSystemServiceTableParameterTable - массив байт, содержащих количество байт, которое необходимо выделить на стеке для передачи параметров в функцию.

Таким образом, чтобы перехватить сервис ядра, достаточно заменить в KeServiceDescriptorTable> SystemServiceDescriptors[0] в массиве lpSystemServiceTableAddressTable нужный адрес на свой.

2.3. Требование реализации дискреционного механизма разграничения доступа

КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Для каждой пары (субъект - объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов. Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.). Должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

Реализация

Для реализации дискреционного механизма разграничения доступа необходимо по крайней мере конкретизировать термины, используемые в формальном описании. При этом целесообразно исходить из того, что полученная модель должна, с одной стороны, быть понятна пользователю, с другой - не ограничивать пользователя в реализации процедур разграничения доступа и как можно ближе соответствовать особенностям архитектуры технических средств компьютера и особенностям операционной системы. С этой точки зрения необходимо определить, что целесообразно выбрать в качестве объектов разграничения доступа и какие допустимые типы доступа целесообразно использовать.

Обсуждая этот вопрос, отметим, что в качестве объектов в большинстве ОС используются: Диски – каталоги (папки) - файлы (задачи).

Выбор типов доступа целесообразно связать с функциями ОС, посредством которых осуществляется доступ к ресурсам. Перехват вызовов этих функций позволит реализовать ПРД для явных действий пользователя.

Реализация ПРД для скрытых действий пользователя может быть осуществлена за счет ограничения перечня задач, которые пользователь имеет право запускать. Это означает, что средства ПРД должны содержать возможность явного и недвусмысленного описания перечня задач, запуск которых разрешен пользователю, и средств контроля за использованием этих задач. Формирование перечня должно осуществляться администратором БИ в порядке, предусмотренном для формирования и изменения ПРД.

В СПО «Аккорд» дискреционные правила разграничения доступа устанавливаются присвоением объектам доступа атрибутов доступа. Установленный атрибут означает, что определяемая атрибутом операция может выполняться над данным объектом. В СПО применяются следующие атрибуты:

- R - открытие файлов для чтения;
- W - открытие файлов для записи;
- O - подмена атрибута R атрибутами RW на этапе открытия файла;
- C - создание файлов;
- D - удаление файлов;
- N - переименование файлов и подкаталогов;
- V - видимость файлов;
- M - создание каталогов;
- E - удаление каталогов;
- n – переименование каталогов;
- G - доступность данного каталога (т.е. переход к нему);
- X - исполнение задач;
- S - наследование подкаталогами атрибутов родительского каталога.

Установленные атрибуты определяют важнейшую часть ПРД пользователя. От правильности выбора и установки атрибутов во многом зависит эффективность работы СЗИ. В этой связи администратор службы безопасности

информации должен ясно представлять, от чего и как зависит выбор атрибутов, назначаемых объектам, к которым имеет доступ пользователь. Как минимум, необходимо изучить принцип разграничения доступа с помощью данных атрибутов, а также особенности работы программных средств, которые будут применяться пользователем при работе.

ВНИМАНИЕ! Если ACED32 в окне «Атрибуты доступа к объектам» не выводит в дереве объектов необходимые ключи реестра, то эти ключи можно прописать вручную в поле «Имя объекта» (подробнее см. документ «Установка правил разграничения доступа. Программа ACED32»).

Специальная программа – редактор прав доступа - позволяет администратору БИ для каждой пары субъект - объект определить:

Для дисков:

- доступность, т.е. пользователю доступны только те логические диски, которые явно описаны в ПРД;

Для каталога:

- доступность (переход к данному каталогу);
- видимость (данный каталог будет виден пользователю из файловых оболочек типа Windows Commander или Explorer);
- наследование подкаталогами атрибутов каталога;

Для содержимого каталога:

- создание подкаталогов;
- удаление подкаталогов;
- переименование подкаталогов;
- открытие файлов для записи;
- открытие файлов для чтения;
- создание файлов;
- переименование файлов;
- удаление файлов;
- видимость файлов;
- «фиктивное» открытие файлов для записи;

Для задач:

- исполнение;

Дополнительно могут определяться права доступа к отдельным файлам (с указанием полного пути доступа) - эти права будут обеспечиваться в безусловном порядке, даже если файл расположен в каталоге, доступа к которому данный пользователь не имеет, или атрибуты доступа для файла отличны от атрибутов каталога, в котором он находится. Предусмотрено определение следующих прав:

- открытие файлов для записи;

- открытие файлов для чтения;
- создание файлов;
- удаление файлов;
- переименование файлов;
- видимость файлов;
- «фиктивное» открытие файлов для записи;
- запуск задач.

Существует также и «черный список». Это файлы или каталоги, которые присутствуют в списке объектов, для которых не установлен **ни один** атрибут доступа. Объекты, описанные в «черном списке», становятся недоступными пользователю, даже если они расположены в каталогах, к которым пользователь имеет доступ. В «черный список» можно включать также логические имена устройств и драйверы устройств. Эти объекты после такого описания становятся недоступны пользователю. Таким образом осуществляется соотнесение пользователю доступных ему устройств.

Кроме этого, в подсистеме дискреционного доступа реализованы два дополнительных атрибута, предназначенных для регистрации обращения пользователя к отдельным ресурсам. Атрибут «r» - определяет регистрацию операций чтения для отдельного объекта, атрибут «w» - регистрацию операций записи. Использование этих атрибутов целесообразно в случае, когда администратору безопасности необходимо иметь информацию обо всех случаях обращения (даже санкционированных) к критичным ресурсам, а не только сообщения об НСД.

2.4. Требование по реализации мандатного принципа контроля доступа

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.). Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая

классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;

- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В КСЗ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом должен контролироваться не только единичный акт доступа, но и потоки информации.

Реализация

Разграничение доступа с использованием мандатного механизма управления доступом СПО «Аккорд» осуществляется путем присвоения (задания) объектам доступа категории доступа (грифа), которые характеризуются уровнем доступа от 0 (самый низкий) до 15 (максимальный). Установленный для объекта доступа гриф является его меткой конфиденциальности.

Пользователям и процессам (опционально) присваиваются категории доступа (уровни допуска), также изменяющиеся от 0 до 15. Доступ пользователя или процесса возможен только тогда, когда его уровень допуска не ниже грифа объекта доступа.

Категории доступа могут быть поименованы как уровни секретности либо другим, более удобным для Администратора БИ образом.

Для активации мандатного механизма разграничения доступа необходимо в файле ACCORD.INI в секции **[ACED]** установить ключ **MandatoryAccess=Yes**. Если в мандатный механизм необходимо ввести контроль доступа процессов тогда, в этой же секции необходимо установить ключ **CheckProcess=Yes**.

Названия и количество категорий (меток конфиденциальности) задаются в файле ACCORD.INI в секции **[MANDATORY].** По умолчанию в СПО «Аккорд» определены 5 категорий конфиденциальности (секретности):

```
Level0=Общедоступно
Level1=ОБЩИЙ_РЕСУРС
Level2=Конфиденциально
Level3=Секретно
```

Level4=Совершенно секретно

Администратор БИ имеет право изменять названия и количество категорий конфиденциальности - но не более 15-ти. С увеличением номера категории повышается конфиденциальность данных. Далее необходимо установить уровень допуска пользователей. Это делается с помощью программы ACED32 - пункт меню «Команды», далее «Уровень доступа». После этого Администратор БИ может назначать как для каталогов, так и для отдельных файлов требуемые уровни доступа.

Проверка прав доступа субъекта (пользователя или процесса) к какому-либо объекту доступа (ресурсу СВТ либо АС) осуществляется в следующем порядке:

1)Проверяется, имеет ли пользователь права на доступ, установленные дискреционным механизмом СПО «Аккорд».

2)Если пользователю установлены права по доступу дискреционным механизмом СПО «Аккорд», то проверяется уровень допуска пользователя и гриф (метка конфиденциальности) объекта доступа (ресурса СВТ либо АС).

3)Доступ будет разрешен только в том случае, если уровень допуска пользователя больше либо равен грифу (метке конфиденциальности) объекта доступа (ресурса СВТ либо АС).

В СПО «Аккорд» реализована дополнительная функция, позволяющая устанавливать уровень доступа исполняемому процессу, когда он загружается в оперативную память. Исполняемому файлу (программе) присваивается метка конфиденциальности (уровень доступа) как объекту на диске СВТ. При этом файл (программа) будет запускаться только пользователем с определенным уровнем допуска.

После успешной загрузки в оперативную память исполняемый файл (программа) получает метку уровня доступа как субъект доступа, который работает с объектами (ресурсами). В этом случае проверка доступа к ресурсу осуществляется в следующем порядке:

1)Проверяется, имеет ли пользователь право на доступ в соответствии с дискреционным механизмом.

2)При наличии дискреционных прав доступа пользователя средствами мандатного механизма СПО «Аккорд» проверяется уровень его допуска и гриф (метка конфиденциальности) объекта доступа (ресурса).

3)Если доступ разрешен, то проверяется, имеет ли текущий процесс уровень допуска больше либо он равен уровню доступа объекта (ресурса), к которому обратился пользователь с помощью этого процесса.

4)Доступ будет разрешен только в случае успешного выполнения трех вышеописанных проверок.

При такой реализации механизма управления потоками информации обработка информации определенного уровня конфиденциальности выполняется только с помощью выделенных программ (процессов).

2.5. Требование управления потоками информации

Должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

Реализация

В СПО «Аккорд» реализован механизм управления потоками информации, основанный на принципах мандатного разграничения доступа (п.2.3). При такой реализации механизма управления потоками информации обработка информации определенного уровня конфиденциальности выполняется только с помощью выделенных программ (процессов).

Как для каталогов, так и для отдельных файлов может быть установлена метка конфиденциальности, а каждому пользователю присваивается метка уровня доступа. Администратор БИ в файле конфигурации ACCORD.INI может установить или отключить флаг использования мандатного управления доступом. Если механизм мандатного доступа включен, то пользователь получит доступ только к тем объектам, метка конфиденциальности которых не выше уровня доступа субъекта (пользователя).

В СПО «Аккорд» реализована дополнительная функция, которая позволяет установить уровень доступа процессу в оперативной памяти. Таким образом, исполняемый файл (программа) имеет метку конфиденциальности, как объект на диске СВТ, и может запускаться только пользователем с определенным уровнем доступа, а после загрузки в оперативную память получает метку уровня доступа как субъект, который работает с объектами, имеющими соответствующую метку конфиденциальности. При такой реализации механизма управления потоками информации обработка информации определенного уровня конфиденциальности выполняется только с помощью выделенных программ (процессов). При этом процессу автоматически присваиваются атрибуты доступа, которые запрещают запись информации на носитель, метка конфиденциальности которого ниже уровня доступа процесса.

2.6. Требование регистрации событий

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизмов;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией, а также регистрировать все попытки доступа и действия выделенных пользователей (администраторов защиты и т.п.).

Обсуждение

Представляется нецелесообразным постоянно осуществлять полномасштабную регистрацию всех попыток доступа всех пользователей ко всем ресурсам - в первую очередь, из-за высоких накладных расходов. В то же время вполне представимы ситуации, при которых необходима полная трассировка событий. В частности, именно такой способ следует применять, изучая, какие ресурсы требует новая программа - перед тем, как передать ее для эксплуатации пользователям. В этой связи целесообразно выделить несколько уровней детальности журнала. Установку уровня детальности для пользователя следует поручить администратору БИ в порядке, предусмотренном для установки и изменения ПРД.

Реализация

Как для каталогов, так и для отдельных файлов может быть установлена опция регистрации доступа к каталогу и его содержимому в регистрационном журнале. Регистрация осуществляется в следующем порядке:

- для каждого пользователя администратор БИ устанавливает уровень детальности журнала - низкая, средняя, высокая;
- для любого уровня детальности в журнале отражаются параметры регистрации пользователя, доступ к устройствам, запуск задач, попытки нарушения ПРД, изменения ПРД (в частности, изменение паролей);
- для среднего уровня детальности в журнале отражаются дополнительно все попытки доступа к защищаемым дискам, каталогам и отдельным файлам, а также попытки изменения некоторых системных параметров - даты, времени и др.;
- для высокого уровня детальности в журнале отражаются дополнительно все попытки доступа к содержимому защищаемых каталогов.

Кроме этого, предусмотрен механизм принудительной регистрации доступа к объектам. Для этого введены два дополнительных атрибута, а именно:

- r - фиксировать в журнале все попытки доступа к объекту на чтение;
- w - фиксировать в журнале все попытки доступа к объекту на запись.

Используя эти атрибуты, администратор может обеспечить регистрацию событий, важных для поддержания необходимого уровня информационной безопасности.

Программа LogView.EXE позволяет осуществить просмотр, вывод на печать и архивацию журнала регистрации событий СПО «Аккорд». Журнал отображается в виде таблицы. Каждая строка таблицы соответствует одному событию, зарегистрированному в журнале.

Журнал содержит следующую информацию:

- дата и точное время регистрации события;
- детальность журнала, установленная на момент регистрации события;
- имя рабочей станции;
- тип операции - в таблице выводится краткая аббревиатура;
- объект доступа - в таблице выводится полное наименование объекта доступа. Объектом доступа может быть файл, каталог, диск, устройство. Если событием является изменение прав доступа - в этом поле отображаются обновленные Права доступа;
- результат события. При положительном завершении события результат – «OK», при отрицательном - регистрируется несанкционированный доступ (НСД) или ошибка доступа;
- имя Процесса - программа, осуществляющая доступ к объекту в момент регистрации события. Для удобства просмотра и анализа информации можно выполнять фильтрацию по одному или нескольким полям таблицы. В Приложении 2 приведен справочник, который содержит как краткое, так и полное наименование операций, регистрируемых подсистемой регистрации.

2.7. Требование очистки памяти

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации. КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении).

Обсуждение

Если с внешней памятью все ясно, то с оперативной есть проблемы. В частности - средствами DOS блок памяти выделяется задаче, и сама задача своими средствами может захватывать блоки памяти. При реализации функций очистки памяти важно очищать как то, так и другое.

Реализация

В СПО «Аккорд». осуществляется перехват функций освобождения памяти и завершения задачи. Именно при этом и выполняется очистка оперативной памяти (освобождаемого блока). Очистка внешней памяти на локальных и сетевых дисках выполняется опционно.

Соответствующая опция - **«Число проходов при удалении»** - количество проходов случайной последовательности по содержимому файла на диске при его удалении, устанавливается администратором БИ при создании ПРД пользователя.

Опционный механизм применен в связи с тем, что очистка внешней памяти требует определенных временных затрат, которые не всегда (исходя из значимости защищаемых ресурсов) оправданы.

Атрибуты устанавливаются с помощью редактора ПРД к СВТ и информационным ресурсам АС. Редактор описан в документе «Установка правил разграничения доступа. Программа ACED32.» (37222406.26.20.40.140.091 97).

3. Некоторые особенности действия атрибутов и подготовки ПРД

Часто перед нормальной попыткой открыть существующий файл программы выполняют просмотр содержимого каталога. В этом случае, если атрибут «V» не установлен, функции FindFirst и FindNext возвратят результат «ошибка». В некоторых случаях (при некорректной установке атрибутов) это может быть источником коллизий.

Отметим, что все атрибуты, кроме атрибута «G», относятся к содержимому каталога. Атрибут «G» относится к собственно каталогу.

При написании программ хорошим тоном считается, когда программа создает «временные» файлы в каталоге, имя которого хранится в переменной окружения TEMP. Например, ОС Windows и все программы для Windows фирмы Microsoft вначале пытаются найти переменную окружения TEMP и при успехе используют данный каталог для размещения промежуточных данных. Применительно к «Аккорд» можно рекомендовать следующее: Если у вас задана переменная окружения TEMP, то доступ к этому каталогу должен быть максимально полным (следует исключить лишь атрибут «X»- запуск программ).

Отдельно стоит рассмотреть применение атрибута «O». Введение этого атрибута связано с тем, что ряд программ открывают файл на чтение и запись, хотя реально используют только операции чтения. В этом случае пользователю приходится разрешать Права доступа и на чтение, и на запись, что потенциально может служить источником информационных угроз. Чтобы избавиться от этой опасности, можно «разнести» данные по специальным каталогам. Это вполне возможный путь, однако, его применение приводит к усложнению «Плана защиты» и увеличению количества каталогов. Введенный в СЗИ «Аккорд» атрибут «O» позволяет решить задачу другим методом, а именно: атрибут «O» подменяет (для задачи) атрибут "R" на совокупность атрибутов «R» и «W». При этом операция открытия файла проходит нормально, а попытка записи в этот файл классифицируется как НСД. Решение о применении для описания ПРД пользователей атрибута «O» принимается администратором БИ в том случае, когда файл по плану защиты должен быть доступен пользователю только для чтения, а применяемая для обработки данных программа пытается открыть этот файл и на чтение, и на запись. Анализ ситуации может быть выполнен путем изучения журнала при тестировании программного обеспечения, планируемого для включения в состав программных средств АС.

Некоторые редакторы текстов (в частности, Microsoft Word и «Лексикон») сохраняют при редактировании информацию в файлах, имя которого отличается от имени редактируемого файла (указанные редакторы заменяют первый символ имени на символ «тильда» - волнистая линия). Если нет возможности не использовать такие редакторы, то необходимо по крайней мере проследить, чтобы эти файлы оставались недоступными для пользователей, не имеющих на это полномочий.

Обратите внимание на доставку информации в виде исполняемого файла - не важно, в каком виде осуществляется доставка - по сети, с помощью отчуждаемого носителя и др. Очень часто именно такой способ используется для внедрения программных закладок, и очень часто покушения такого рода оказываются успешными. Вариант воздействия, выведший из строя не одну BBS - посылка архивированного файла, содержащего несколько Gb нулей. В архивированном виде такой файл занимает весьма немного места, а при раскрытии очень быстро занимает все пространство диска.

Для того, чтобы избежать неприятностей такого рода, нужно запрещать запуск задач из всех каталогов, кроме тех, в которых хранятся проверенные модули. Следует также обратить внимание на использование отчуждаемых носителей - как в плане разрешения на использование (далеко не каждому пользователю это необходимо), так и в плане регистрации и учета.

4. Примеры ПРД для типовых ситуаций разграничения доступа

ВНИМАНИЕ! Правила разграничения доступа (ПРД), приведенные в настоящем руководстве – это лишь примеры использования атрибутов доступа, а не описание политики безопасности. В каждом конкретном случае администратор БИ должен описывать реальные ресурсы АС (СВТ)

Будем считать, что физический диск на компьютере разбит на два логических диска. Как на диске C, так и на D размещены каталоги, доступ к которым могут иметь разные пользователи. Программные средства в основном размещены на диске C.

4.1. Пример 1. Субъекту разрешено работать в каталоге C:\DOC

В этом случае ПРД для пользователя должны содержать следующий перечень атрибутов:

Права доступа[3]:

C:\	[R				V			G		X	S]
C:\ACCORD.X64\	[R				V			G		X	0]
C:\DOC\	[R	W	C	D	N	V	M	E	G	X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		0]

Пояснения: при этом весь диск C:\ доступен только для чтения, в каталоге C:\ACCORD.X64\ разрешено чтение файлов и запуск программ, каталог C:\DOC\ доступен полностью. К каталогу ...\TEMP\ следует всегда задавать полный доступ, за исключением, разве что, запуска программ - часто он требуется для размещения временных файлов прикладных задач. Файлы AUTOEXEC.BAT и CONFIG.SYS полностью недоступны (“скрытые” файлы).

4.2. Пример 2. Пользователю на диске будут видны и доступны только явно описанные каталоги

Права доступа[4]:

C:\	[R	W	C	D	N	V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]

[3)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

[4)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

C:\DOC\	[R	W	C	D	N	V	M	E	G	X	0]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]

Каталог C:\NORTON\ описан, так как из него запускаются задачи – по крайней мере, NC.EXE, но в нем запрещено удаление и переименование файлов. Корневой каталог описан **без наследования** прав доступа. Именно такой вариант ПРД предоставляет пользователю доступ только к явно описанным каталогам и файлам – остальные ресурсы недоступны и невидимы из любых файловых оболочек.

Обратите внимание - при таких атрибутах видны и доступны файлы, размещенные в корневом каталоге диска C:. Для того, чтобы эти файлы были недоступны пользователю, из описания корневого каталога нужно удалить атрибут «V».

Однако такой вариант неприемлем при работе с Windows, т.к. данная операционная система производит чтение и запись нескольких файлов, размещенных в корневом каталоге. Вот пример описания прав доступа для работы с Windows.

Права доступа[5]:

C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]
C:\DOC\	[R	W	C	D	N	V	M	E	G	X	0]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\PROGRAM FILES\	[R	W	C			V	M	E		X	S]
C:\RECYCLED\	[R	W	C			V	M	E		X	S]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]
C:\WINDOWS\	[R	W	C	D	N	V	M	E	G	X	S]

Вот теперь мы получили то, что хотели.

4.3. Пример 3. Разрешено работать только с файлами и только в выделенном каталоге

В этом случае пользователю необходимо запретить запуск задач, создание и удаление подкаталогов.

Права доступа[6]:

C:\	[R	W	C			V	M	E	G	X	0]

[5] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

[6] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

C:\ACCORD.X64\	[R					V			G	X	0]
C:\DOC\	[R	W	C	D	N	V			G		0]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]

Теперь можно вернуться к Примеру 1 и убедиться, что создать каталоги можно, но увидеть их, перейти к ним и вообще работать с ними будет трудновато - по крайней мере, до тех пор, пока администратор БИ не установит вновь созданным каталогам необходимые атрибуты.

4.4. Пример 4. Применение атрибутов наследования

Есть и более простой способ - установить для разрешенного каталога атрибут наследования прав доступа.

Права доступа[7]:

C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]
C:\DOC\	[R	W	C	D	N	V	M	E	G		S]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]

Теперь с подкаталогами проблем быть не должно.

4.5. Пример 5. То же, но пользователю нельзя удалять файлы

Права доступа[8]:

C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]
C:\DOC\	[R	W	C		N	V	M	E	G		S]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]

Аналогичным образом можно проверить действие других атрибутов и сочетаний атрибутов. Этот эксперимент наверняка наведет на мысли об оптимальном применении разграничения доступа в Вашей ситуации.

---

[7] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

[8] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

4.6. Пример 6. У пользователя полный доступ к директории на диске D

Основные параметры:

- Идентификатор: G2.
- Права администратора: Нет.
- Детальность журнала: Низкая.

Права доступа[9]:

C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]
D:\	[R	W					M	E	G		0]
D:\HHH\	[R	W	C	D	N	V	M	E	G	X	S]

4.7. Пример 7. Конфиденциальное делопроизводство

Обычно задача конфиденциального делопроизводства ставится так. Пользователю поручено исполнить документ, взяв исходные материалы из указанной ему директории, и передать готовый документ в другую указанную ему директорию. Это означает, что мы должны определить для пользователя различные права доступа к директориям. Так, из одной директории пользователь может только копировать файлы (и, естественно, ознакомиться с ними), но не может ни редактировать их, ни удалять. В другой («своей») директории он может обрабатывать документы без ограничений, а в третью директорию может только записывать готовые материалы.

Пусть для исполнения документа выделен каталог ...\HHH\, а пользователь с разными правами может использовать подкаталоги A1, A2 и A3. Эта задача реализуется следующими атрибутами:

Основные параметры

- Идентификатор: G2.
- Права администратора: Нет.
- Детальность журнала: Низкая.

Права доступа[10]:

C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]

[9)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

[10)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

```
C:\NORTON\          [R  W  C           V  M  E        X  0]
C:\TEMP\            [R  W  C  D  N  V  M  E  G        S]
D:\                 [R  W              M  E  G        0]
D:\HHH\             [                     G        0]
D:\HHH\A1\          [R                 V  G        0]
D:\HHH\A2\          [R  W  C  D  N  V  M  E  G        S]
D:\HHH\A3\          [   W  C           V  G        0]
```

Из этого примера ясно, что перед включением некоторого программного средства в перечень используемых в системе разграничения доступа нужно его особенности изучить. Изучение может основываться на использовании высокого уровня детальности журнала и анализе результатов. После того как станет ясно, какие ресурсы требует то или иное программное средство, необходимо на основе анализа выявить, имеются ли возможности для нарушения ПРД и можно ли создать такие ПРД, которые обеспечат требуемый уровень безопасности информации. Только вслед за этим администратор БИ может принять решение о возможности применения тех или иных средств. Некоторые рекомендации по формированию ПРД при использовании наиболее распространенных программных средств обработки информации приведены в соответствующем разделе ниже.

4.8. Пример 8. То же, что и пример 7, но разрешен доступ только к корню диска A

В этом случае атрибуты могут быть такими:

Права доступа[11]:

```
A:\                 [R                 V        G        0]
C:\                 [R  W  C           V  M  E  G     X  0]
C:\ACCORD.X64\      [R                 V        G     X  0]
C:\NORTON\          [R  W  C           V  M  E        X  0]
C:\TEMP\            [R  W  C  D  N  V  M  E  G        S]
D:\                 [R  W              M  E  G        0]
D:\HHH\             [                     G        0]
D:\HHH\A1\          [R                 V  G        0]
D:\HHH\A2\          [R  W  C  D  N  V  M  E  G        S]
D:\HHH\A3\          [   W  C           V  G        0]
```

[11)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

4.9. Пример 9. То же, но пользователь может читать все файлы, размещенные на A

Это означает, что пользователю должны быть доступны все подкаталоги, т.е. нужно установить атрибут наследования “S”.

Права доступа[12]:

A:\	[R					V			G		S]
C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]
D:\	[R	W					M	E	G		0]
D:\HHH\	[								G		0]
D:\HHH\A1\	[R					V			G		0]
D:\HHH\A2\	[R	W	C	D	N	V	M	E	G		S]
D:\HHH\A3\	[	W	C			V			G		0]

4.10. Пример 10. Установка атрибутов файлов

Как уже отмечалось, дополнительно могут определяться Права доступа к отдельным файлам - с приоритетом, даже если файл расположен в каталоге, доступа к которому данный пользователь не имеет. Рассмотрим задачу, аналогичную приведенной в примере 9, но с тем отличием, что исходный материал для исполнения документа расположен в файле C:\BOOK\BOOK.DOC.

Этот материал должен быть доступен пользователю, но другие файлы из того же каталога должны быть недоступны. В этом случае атрибуты могут быть такими:

Права доступа[13]:

A:\	[R					V			G		S]
C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G	X	0]
C:\BOOK\BOOK.DOC	[R	W	C			V					]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]
D:\	[R	W	C	D	N		M	E	G		0]
D:\HHH\	[								G		0]

[12)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

[13)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

D:\HHH\A1\	[R					V			G		0]
D:\HHH\A2\	[R	W	C	D	N	V	M	E	G		S]
D:\HHH\A3\	[	W	C			V			G		0]

В результате работы монитора разграничения доступа при установленных таким образом атрибутах пользователь не сможет увидеть исходный файл (т.к. не описан каталог BOOK), но вполне может скопировать его командой copy c:\book\book.doc d:\hhh\a2\c1\book.doc

Обратите внимание на наличие атрибутов W, C и V. Функции, соответствующие этим атрибутам, используются встроенной командой DOS «COPY», и в этой связи установка их является обязательной. Чтобы избавиться от таких неоднозначностей, вместо команды «COPY» лучше использовать специально подготовленную программу. Если Вы используете не command.com, а другой интерпретатор командной строки, то перечень атрибутов может быть другим. Так, для NDOS достаточно атрибутов R и V - он написан корректней.

Естественно, на аналогичном принципе можно построить и запись в заранее определенный файл.

4.11. Пример 11. Установка атрибутов для выделенных программ

Предусмотрена также возможность установки разрешения на исполнение задач, размещенных в выделенном файле, - выделенных задач. Пусть необходимо запустить утилиту TMTEST. Для этого установим следующие атрибуты:

Права доступа[14]:

A:\	[R					V			G		S]
C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G		0]
C:\ACCORD.X64\TMTEST.EXE	[					V				X	]
C:\BOOK\BOOK.DOC	[R	W	C			V					]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]
D:\	[R	W	C	D	N		M	E	G		0]
D:\HHH\	[								G		0]
D:\HHH\A1\	[R					V			G		0]
D:\HHH\A2\	[R	W	C	D	N	V	M	E	G	X	S]
D:\HHH\A3\	[	W	C			V			G		0]

[14] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

В данном примере из каталога C:\ACCORD.X64\ разрешен запуск только программы TMTEST.EXE.

Обратите внимание - кроме атрибута «X» необходимо установить и «V». Это связано с особенностями запуска задач (функция FindFirst).

4.12. Пример 12. Запрет доступа к файлам

Пусть пользователю A4 запрещен доступ к файлам с расширением .BAT и .SYS, размещенным в корневом каталоге диска C:. в этом случае ПРД выглядят так:

Основные параметры:

- Идентификатор: A4.
- Права администратора: Нет.
- Детальность журнала: Низкая.

Права доступа[15]:

C:\	[R	W	C			V	M	E	G		X	0]
C:\ACCORD.X64\	[R					V			G		X	0]
C:*.BAT	[											]
C:*.SYS	[											]
C:\DOC\	[R	W	C		N	V	M	E	G			S]
C:\NORTON\	[R	W	C			V	M	E			X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G			S]

4.13. Пример 13. Анализ ресурсов

Перед тем как включить в АС новое программное средство, администратор БИ должен изучить его особенности в части доступа к ресурсам. Не исключено, что требуемые ресурсы не позволят применять изучаемые программы в составе АС, или, возможно, возникнет необходимость пересмотреть «План защиты».

Для анализа ресурсов целесообразно установить в программе «ACED32» для некоторого пользователя высокий уровень детальности журнала и полный доступ к каталогам и файлам, провести сеанс работы с изучаемым программным средством, а затем посредством программы «LOGVIEW» изучить требуемые для работы программы ресурсы. Необходимо помнить, что объем журналов при высоком уровне детальности будет очень большим, и в этой связи сеанс работы должен быть не слишком длинным. Лучше, в случае необходимости, изучение провести несколькими небольшими сеансами.

[15)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

4.14. Пример 14. Использование атрибута «O»

Пусть в состав АС включена некоторая специализированная процедура копирования информации mycopy.exe (естественно, это только пример). Пусть, также по Плану защиты пользователю доступны каталоги, как в примере 7. Попытаемся воспользоваться этой процедурой при следующих установленных атрибутах:

Права доступа[16]:

C:\	[R	W	C			V	M	E	G	X	0]
C:\ACCORD.X64\	[R					V			G		0]
C:\NORTON\	[R	W	C			V	M	E		X	0]
C:\TEMP\	[R	W	C	D	N	V	M	E	G		S]
D:\	[R	W	C	D	N		M	E	G		0]
D:\HHH\	[								G		0]
D:\HHH\A1\	[R					V			G		0]
D:\HHH\A2\	[R	W	C	D	N	V	M	E	G		S]
D:\HHH\A3\	[	W	C			V			G		0]

Воспользуемся для копирования имеющейся в АС программой mycopy d:\hhh\a1\test.txt d:\hhh\a2\test.tst

При этом будет выдано сообщение об ошибке - о невозможности открыть файл. Изменим теперь атрибуты доступа, а именно, в части описания прав доступа к каталогу d:\hhh\a1:

D:\HHH\A1\	[R					V		O	G		0]

При этом процедура будет успешно выполнена.

4.15. Пример 15. Описание сетевого ресурса

Иллюстрацию использования сетевых ресурсов продемонстрируем на задаче, аналогичной приведенной в примере 7. Здесь, однако, каталоги размещаются на сервере, а пользователи имеют различные права. Приводимая цепочка показывает, как можно организовать конфиденциальное делопроизводство в сети. Необходимо обратить внимание на описание каталогов, расположенных на сервере.

Пользователь: A1

Основные параметры:

- Идентификатор: A1.

---

[16] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

- Права администратора: Нет.
- Детальность журнала: Низкая.

Права доступа[17]:

C:\	[R	W	C			V	M	E	G	X	O	S]
D:\	[R	W	C	D	N	V	M	E	G	X	O	0]
\SERVER\VOL2\	[								G			0]
\SERVER\VOL2\A1\	[R					V			G	X	A	0]
\SERVER\VOL2\A2\	[R	W	C	D	N	V	M	E	G	X	O	0]
\SERVER\VOL2\A3\	[	W	C			V			G		O	0]

Пользователь: A2

Основные параметры:

- Идентификатор: A2.
- Права администратора: Нет.
- Детальность журнала: Низкая.

Права доступа:

C:\	[R	W	C			V	M	E	G	X	O	S]
D:\	[R	W	C	D	N	V	M	E	G	X	O	S]
\SERVER\VOL2\	[								G			0]
\SERVER\VOL2\A1\	[R					V			G	X	A	0]
\SERVER\VOL2\A2\	[R	W	C	D	N	V	M	E	G	X	O	0]
\SERVER\VOL2\A3\	[	W	C			V			G		O	0]

Пользователь: A3

Основные параметры:

- Идентификатор: A3
- Права администратора: Нет
- Детальность журнала: Низкая

Права доступа:

C:\	[R	W	C			V	M	E	G	X	O	S]
D:\	[R	W	C	D	N	V	M	E	G	X	O	S]
\SERVER\VOL2\	[								G			0]
\SERVER\VOL2\A3\	[R					V			G	X	A	0]
\SERVER\VOL2\A4\	[R	W	C	D	N	V	M	E	G	X	O	0]
\SERVER\VOL2\A5\	[	W	C			V			G		O	0]

---

17) на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

Примечание: чтобы дать пользователю полный доступ ко всем сетевым ресурсам, нужно в описании каталогов ввести символ « \ » и дать полный доступ – [RWCDNVMEGXO S]. В этом случае доступ определяется только настройками сетевого администрирования.

4.16. Пример 16. Создание изолированной программной среды (ИПС) в ОС Windows

Windows обладает достаточно обширным набором функций и утилит для изменения конфигурации и подключения новых устройств и ресурсов. С одной стороны, эти функции облегчают работу квалифицированному пользователю, но с другой - могут служить источником НСД. Наиболее эффективным способом создания ИПС является создание «белого» списка процессов с помощью мандатного механизма разграничения доступа с контролем процессов и динамического контроля целостности файлов из этого списка (см. Приложение 2 документа «Установка правил разграничения доступа. Программа ACED32» 37222406.26.20.40.140.091 97), как используя, так и не используя утилиту Actskmng.exe.

При использовании мандатного механизма в редакторе прав доступа ACED32.EXE автоматически включаются в список ПРД все задачи, которые в данный момент находятся в памяти. В дальнейшем этот список может корректироваться администратором на основе информации в журнале регистрации. Пользователь (или операционная система в сеансе этого пользователя) не сможет в процессе работы запустить процесс, который пытается получить доступ к ресурсу, но не включен в этот список, или его уровень доступа ниже метки доступа ресурса. Процессу можно назначить уровень доступа таким образом, чтобы обрабатывать данные (объекты) с определенной меткой доступа пользователь смог только процессами (задачами) с определенным уровнем доступа.

Доступ к пользовательским каталогам и файлам следует прописать в соответствии с полномочиями, установленными для данного пользователя (с использованием дискреционного или мандатного метода). Доступ к файлам и папкам операционной системы описывается так, чтобы обеспечить работоспособность системы, но исключить возможность несанкционированного изменения. После перезагрузки компьютера и входа в систему зарегистрированного пользователя запустится ОС Windows, в которой пользователь может работать только в разрешенных каталогах и только с установленным ПО. ПРД в этом случае могут выглядеть так[18]:

Пользователь: MAIN_USER

- Права администратора: Нет
- Детальность журнала: Низкая

[18)] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

37222406.26.20.40.140.091 90

----------Объекты----------

A:\	[R VO G S]	Общедоступно
C:\	[R VO G X0]	Общедоступно
C:\ACCORD.X64\	[S]	Общедоступно
C:\BOOT.INI	[ ]	
C:\DOCUMENTS AND SETTINGS\	[RWCDNV MEGn XS]	Общедоступно
C:\PROGRAM FILES\	[R VO G XS]	Общедоступно
C:\PROGRAM FILES\MICROSOFT OFFICE\	[R V G S]	Общедоступно
C:\PROGRAM FILES\MICROSOFT OFFICE*.DLL	[R V X]	
C:\PROGRAM FILES\MICROSOFT OFFICE*.EXE	[R V X]	
C:\RECYCLED\	[RWCDNV MEGn S]	Общедоступно
C:\WINNT\	[R VO G XS]	Общедоступно
C:\WINNT\SYSTEM32\ACCESS.CPL	[ ]	
C:\WINNT\SYSTEM32\ACCORD.SCR	[R V X]	
C:\WINNT\SYSTEM32\ACGINA.DLL	[R V X]	
C:\WINNT\SYSTEM32\ACRUNVDD.DLL	[R V X]	
C:\WINNT\SYSTEM32\ACRUNVDD.EXE	[R V X]	
C:\WINNT\SYSTEM32\ALSNDMGR.CPL	[ ]	
C:\WINNT\SYSTEM32\APPWIZ.CPL	[ ]	
C:\WINNT\SYSTEM32\AUTOEXEC.NT	[R]	
C:\WINNT\SYSTEM32\AZIAHLP.DLL	[R V X]	
C:\WINNT\SYSTEM32\BDEADMIN.CPL	[ ]	
C:\WINNT\SYSTEM32\DESK.CPL	[ ]	
C:\WINNT\SYSTEM32\DRIVERS\ACRUN.SYS	[ ]	
C:\WINNT\SYSTEM32\FAX.CPL	[ ]	
C:\WINNT\SYSTEM32\HDWWIZ.CPL	[ ]	
C:\WINNT\SYSTEM32\IAMCPL.CPL	[ ]	
C:\WINNT\SYSTEM32\INETCPL.CPL	[ ]	
C:\WINNT\SYSTEM32\INTL.CPL	[ ]	
C:\WINNT\SYSTEM32\IRPROPS.CPL	[ ]	
C:\WINNT\SYSTEM32\JOY.CPL	[ ]	
C:\WINNT\SYSTEM32\MAIN.CPL	[ ]	
C:\WINNT\SYSTEM32\MMSYS.CPL	[ ]	
C:\WINNT\SYSTEM32\NCPA.CPL	[ ]	
C:\WINNT\SYSTEM32\NWC.CPL	[ ]	
C:\WINNT\SYSTEM32\ODBCCP32.CPL	[ ]	
C:\WINNT\SYSTEM32\POWERCFG.CPL	[ ]	
C:\WINNT\SYSTEM32\STICPL.CPL	[ ]	
C:\WINNT\SYSTEM32\SYSDM.CPL	[ ]	

C:\WINNT\SYSTEM32\TELEPHON.CPL	[ ]	
C:\WINNT\SYSTEM32\TIMEDATE.CPL	[ ]	
C:\WINNT\SYSTEM32\TMATTACH.DLL	[R V X]	
C:\WINNT\SYSTEM32\TMDRV32.DLL	[R V X]	
C:\WINNT\TEMP\	[RWCDNV MEGn S]	Общедоступно
D:\	[R VO G 0]	Общедоступно
D:\OPEN_DOC\	[RWCDNV MEGn S]	Секретно
E:\	[R V G 0]	
E:\RECYCLED\	[RWCDNV MEGn S]	
E:\SYSTEM VOLUME INFORMATION\	[RW V G S]	

----------Процессы----------

```
ACCORD.SCR          [Общедоступно]
ACRUNNT.EXE         [Общедоступно]
AUTOCHK.EXE         [Общедоступно]
CSRSS.EXE           [Общедоступно]
EXPLORER.EXE        [Общедоступно]
INTERNAT.EXE        [Общедоступно]
LSASS.EXE           [Общедоступно]
MPNOTIFY.EXE        [Общедоступно]
NDDEAGNT.EXE        [Общедоступно]
OSA.EXE             [Общедоступно]
PSTORES.EXE         [Общедоступно]
REALPLAY.EXE        [Общедоступно]
RPCSS.EXE           [Общедоступно]
SERVICES.EXE        [Общедоступно]
SETUP.EXE           [Общедоступно]
SMSS.EXE            [Общедоступно]
SPOOLSS.EXE         [Общедоступно]
SYSTEM              [Общедоступно]
SYSTRAY.EXE         [Общедоступно]
TASKMGR.EXE         [Общедоступно]
USERINIT.EXE        [Общедоступно]
WINLOGON.EXE        [Общедоступно]
WINWORD.EXE         [Секретно]
_AVPCC.EXE          [Общедоступно]
```

Пользователь сможет работать с документами в каталоге D:\OPEN_DOC только средствами WinWord и не может изменить конфигурацию системы.

4.17.Пример 17. Регистрация вывода документа на печатающее устройство

Пользователь: MAIN_USER[19]

- Права администратора: Нет.

---

[19] на примере 64-битной ОС. Для 32-битной ОС вместо каталога C:\ACCORD.X64 – каталог C:\ACCORD.NT

- Стартовый каталог: C:\.
- Детальность журнала: Низкая.

A:\	[R	W	C	D	N	V	O	M	E	G	X	S]
C:\	[R	W				V	O			G	X	0]
C:\ACCORD.X64\	[R	W				V	O			G		S]
C:\DRWEB\	[R	W				V	O			G		S]
C:\MSOFFICE\	[R	W	C	D	N	V	O	M	E	G	X	S]
C:\PROGRAM FILES\	[R	W	C	D	N	V	O	M	E	G	X	S]
C:\TEMP\	[R	W	C	D	N	V	O	M	E	G		S]
C:\WINNT\	[R	W	C	D	N	V	O	M	E	G	X	S]

Для регистрации вывода документа на печатающее устройство и маркировки конфиденциального документа нужно установить подсистему контроля печати и включить пользователю опцию «Активировать контроль печати».

Для регистрации только факта вывода документа на печатающее устройство достаточно установить атрибут W (регистрация записи) в списке атрибутов объекта C:\WINNT\SPOOL\PRINTERS\.

5. Правовые аспекты применения СПО «Аккорд»

Специальное программное обеспечение средств защиты информации от несанкционированного доступа «Аккорд-Win64 K» и сопутствующая документация защищены законом России об авторских правах, а также положениями Международного Договора. Любое использование СПО «Аккорд» в нарушение закона об авторских правах или в нарушение положений ЭД на СПО «Аккорд» будет преследоваться ОКБ САПР в силу наших возможностей.

Авторские права на данное изделие, в том числе аппаратные средства и специальное ПО, принадлежат ОКБ САПР, Россия, 115114, г. Москва, 2-й Кожевнический пер., д.12, эт.2, пом.1, к.21, тел. (495) 994-72-62, факс: (495) 234-03-10, E-mail: okbsapr@okbsapr.ru.

ОКБ САПР разрешает Вам делать архивные копии программного обеспечения «Аккорд» для использования потребителем, приобретшим СПО «Аккорд» в установленном порядке. Ни при каких обстоятельствах программное обеспечение «Аккорд» не распространяется между другими предприятиями (фирмами) и лицами.

Удалять в продукции СПО «Аккорд» уведомление об авторских правах ни при каких обстоятельствах не допускается.

Применение средств СПО «Аккорд» для других целей возможно только при наличии письменного согласия ОКБ САПР.

Отметим, что предыдущие ограничения не запрещают Вам распространять Ваши собственные исходные коды или модули, связанные с применением программного обеспечения СПО «Аккорд». Однако, тот, кто получает от Вас такие исходные коды или модули, должен приобрести собственную копию нашего программного обеспечения, чтобы на законном основании использовать его и иметь сертификат соответствия.

ОКБ САПР гарантирует исправность физических экземпляров аппаратуры и документации, поставляемых в составе СПО «Аккорд», согласно формуляру на СПО «Аккорд».

Мы просим пользователя при обнаружении ошибок или дефектов направить нам подробный отчет о возникших проблемах, который позволит найти и зафиксировать проблему.

СПО «Аккорд» поставляется по принципу «as is», т.е. ОКБ САПР ни при каких обстоятельствах не предусматривает никакой компенсации за Ваши дополнительные убытки, включая любые потери прибыли, потери сохранности или другие убытки вследствие аварийных ситуаций или их последствий, убытки, которые могут возникнуть из-за использования или невозможности использования СПО «Аккорд».

При покупке и применении СПО «Аккорд» предполагается, что Вы знакомы с данными требованиями авторов разработки и изготовления СПО «Аккорд» и согласны с положениями настоящего раздела.

6. ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

В случае необходимости консультации ЗАО «ОКБ САПР» предлагает без дополнительной оплаты с понедельника по пятницу с 10-00 до 18-00 (по московскому времени) обращаться по телефонам:

+7 (495) 994-49-96

+7 (495) 994-49-97

+7 (926) 235-89-17

+7 (926) 762-17-72

или по адресам электронной почты:

help@okbsapr.ru

support@okbsapr.ru

Наш адрес в Интернете http://www.okbsapr.ru/.

Приложение 1. Рекомендации по организации службы информационной безопасности

Ответственными за защиту информации в АС (СВТ) являются все руководители и отдельные пользователи (операторы) в пределах их служебной компетенции.

Для непосредственной организации и обеспечения функционирования системы защиты информации как компонента АС, в организации (на предприятии, фирме) должны быть предусмотрены специальные органы или ответственные лица - служба безопасности информации (СБИ) или администратор безопасности информации.

Сотрудники СБИ (администратор БИ) помимо безупречной репутации и полного доверия со стороны руководства организации должны обладать определенным уровнем знаний и навыков в области вычислительной техники, достаточным для ясного понимания всех видов угроз программно-информационным ресурсам АС (СВТ) и необходимым для грамотного управления и эффективного применения средств защиты.

Организационно-правовой статус СБИ (администратора БИ)

- СБИ (администратор БИ) должны подчиняться тому лицу, которое в данной организации несет персональную ответственность за соблюдение правил обращения с защищаемой информацией;
- сотрудники службы (администратор БИ) должны иметь право доступа во все помещения, где установлена аппаратура АС, и право прекращать автоматизированную обработку информации при наличии или угрозе утечки защищаемой информации;
- руководителю СБИ (администратору БИ) должно быть предоставлено право запрещать включение в число действующих новые элементы компонентов АС, если они не отвечают требованиям защиты информации;
- службе БИ (администратору БИ) должны обеспечиваться все условия, необходимые для выполнения своих функциональных обязанностей;
- численность службы должна быть достаточной для выполнения перечисленных выше функций, при этом штатный состав не должен иметь (по возможности) других обязанностей, связанных с функционированием АС;
- создаваемая структура защиты информации в СВТ при применении СПО «Аккорд» должна поддерживаться механизмом установления полномочий пользователям СВТ и управлением их доступом к информационным ресурсам. Для этого СБИ (администратор БИ) разрабатывает и вводит в действие установленным в организации порядком организационно-правовые документы по применению СВТ с внедренными средствами защиты с учетом действующих нормативных и законодательных документов.

Обязанности администратора БИ по применению СПО «Аккорд»:

1) На основе «Плана защиты», введенного в организации, разрабатывать таблицы разграничения доступа к защищаемым ресурсам, вводить (при

установке СПО «Аккорд») полномочия пользователей и корректировать их в ходе эксплуатации СВТ.

2) Устанавливать СПО «Аккорд» в СВТ и организовывать ее эксплуатацию с внедренными средствами защиты.

3) Тщательно анализировать процессы функционирования программ, которые будут закреплены за пользователями, в соответствии с этим создавать для каждого из них изолированную программную среду исполнения задачи, исходя из их функциональных обязанностей.

ВНИМАНИЕ! Нежелательно, чтобы программы, закрепленные за пользователями, имели возможность доступа к дискам по абсолютным секторам, возможность прямого редактирования памяти.

4) Обучать пользователей правилам обработки защищаемой информации, контролировать правильность применения ими средств защиты СПО «Аккорд» и оказывать помощь в части организации работы на СВТ с внедренным СПО «Аккорд».

5) Выявлять возможные каналы НСД к информации при применении СПО «Аккорд», готовить предложения по их устранению.

6) Систематически анализировать состояние СПО «Аккорд» и его отдельных средств, периодически проводить их тестирование и проверку защитных функций СПО «Аккорд», о чем делать отметку в формуляре.

7) Регулярно анализировать содержание системного журнала и разрабатывать меры по исключению неправильного применения СПО «Аккорд» пользователями.

ВНИМАНИЕ! Администратор должен довести до пользователей распоряжение о запрете снятия задач с выполнения при помощи выключения питания или нажатия на клавишу <RESET>.

8) Разрабатывать и вводить установленным порядком необходимую учетную и объектовую документацию (инструкции пользователям и др.).

9) Разрабатывать и утверждать в установленном порядке систему мер и действий на случай непредвиденных обстоятельств (заражение объекта ВТ новым типом вируса, фактов НСД к информации, нарушения правил функционирования системы защиты и т.д.).

10) В период профилактических работ на СВТ снимать при необходимости СПО «Аккорд» с эксплуатации, о чем делать отметку в формуляре.

11) Принимать меры при попытках НСД к защищаемой информации и нарушении правил функционирования системы защиты. Обязанности администратора БИ должны быть отражены в «Инструкции администратора безопасности информации», утвержденной соответствующим должностным лицом.

Приложение 2. Операции, фиксируемые подсистемой регистрации СПО «Аккорд»

В таблице 1 приведена расшифровка кодов событий журнала регистрации СПО «Аккорд».

Таблица 1 – Расшифровка кодов событий СПО «Аккорд»

Код события	Расшифровка кода события
Коды событий файлов и каталогов	
ChangeDir	Смена каталога
ChMod	Установка/смена атрибутов
CloseFile	Закрытие файла
CreateDir	Создание каталога
CreateFile	Создание файла
DeleteDir	Удаление каталога
DeleteFile	Удаление файла
DriveAccess	Доступ к диску
Exec	Запуск программы
Exit	Завершение программы
OpenFile	Открытие файла
RenameDir	Переименование каталога
RenameFile	Переименование файла
Search	Поиск файла/каталога
SetDate	Установка системной даты
SetTime	Установка системного времени
Traverse	Проверка существования пути
Коды событий ключей реестра	
RegCloseKey	Закрытие ключа реестра
RegCreateKey	Создание ключа реестра
RegCreateValue	Создание переменной в ключе реестра
RegDeleteKey	Удаление ключа реестра
RegDeleteValue	Удаление переменной из ключа реестра
RegEnumKey	Поиск ключей реестра
RegEnumValue9	Поиск переменных в ключе реестра
RegOpenKey0	Открытие ключа реестра
RegQueryValue	Чтение переменной из ключа реестра
RegSetValue	Изменение значения переменной в ключе реестра
Коды событий хранителя экрана	
SSOffAtAdmin ScreenSaver	Разблокировка с помощью данных для идентификации администратора АРМ АБИ
SSOffAtRemoute ScreenSaver	Разблокировка с АРМ АБИ
SSOffAtTM ScreenSaver	Разблокировка с помощью данных для идентификации
SSOffBadTM	Попытка разблокировать не теми данными для идентификации, которыми осуществлялась блокировка
SSOnAtHotKey ScreenSaver	Блокировка с помощью клавиатуры
SSOnAtRemoute ScreenSaver	Блокировка с АРМ АБИ
SSOnAtTimeout 0 ScreenSaver	Блокировка по времени неактивности
SSTimeDisable	Выключен временной контроль ScreenSaver-а
SSTimeEnable	Включен временной контроль ScreenSaver-а

Коды событий проверки файлов	
EndCheck	Конец проверки списка файлов
EndUpdate	Конец обновления списка файлов
FileCheck	Проверка файла
GetPrivateKey	Получение секретного ключа
StartCheck	Начало проверки списка файлов
StartUpdate	Начало обновления списка файлов
TotalEDS	Подпись списка файлов
TotalHash	Хэш списка файлов

Приложение 3. Список событий СПО «Аккорд-Win64 K», регистрируемых в системном журнале ОС

События СПО «Аккорд», регистрируемые в системном журнале ОС, возможные причины их возникновения и порядок действий в случае появления сообщения отражены в таблице 2.

Таблица 2 – События СПО «Аккорд», регистрируемые в системном журнале ОС

Сообщение	Возможные причины возникновения сообщения	Порядок действий в случае появления сообщения
Не найден ключевой лицензионный файл!	Отсутствует ключевой файл лицензии	1) Необходимо запустить тест для проверки работы контроллера (TmExplor.exe); 2) прислать значение полей «S/N» и «UID» по адресу электронной почты key@okbsapr.ru; 3) производственный отдел сформирует файл лицензии и отправит его заказчику; 4) полученный файл скопировать в каталог с установленными файлами СЗИ «Аккорд» под именем «accord.key»
Неверный ключевой файл лицензии!	Файл лицензии поврежден (т.е. имеются повреждения подписи, даты создания файла лицензии, серийного номера и т.д.)	1) Необходимо сообщить о повреждении файла лицензии и прислать поврежденный файл по адресу электронной почты key@okbsapr.ru; 2) производственный отдел сформирует корректный файл лицензии и отправит его заказчику; 3) полученный файл нужно скопировать в каталог с установленными файлами СЗИ «Аккорд» под именем «accord.key»
Истек срок действия лицензии!	Срок действия файла лицензии истек	1) Необходимо сообщить о том, что срок действия лицензии истек, а также прислать имеющийся файл по адресу электронной почты key@okbsapr.ru; 2) производственный отдел сформирует корректный файл лицензии и отправит его заказчику; 3) полученный файл нужно скопировать в каталог с установленными файлами СЗИ «Аккорд» под именем «accord.key»
Ключевой файл лицензии не подходит для этого продукта!	Имеющийся файл лицензии предназначен для другого продукта	1) Необходимо сообщить о том, что файл лицензии не предназначен для СПО «Аккорд-Win64 K», а также прислать имеющийся файл по адресу электронной почты key@okbsapr.ru; 2) производственный отдел сформирует корректный файл лицензии и отправит его заказчику; 3) полученный файл нужно скопировать в каталог с установленными файлами СЗИ «Аккорд» под именем «accord.key»
Неверная сигнатура ключевого файла	Поврежден файл лицензии (например, при намеренном	1) Необходимо сообщить о повреждении файла лицензии, а также прислать поврежденный файл по адресу электронной почты key@okbsapr.ru;

лицензии!	изменении срока действия лицензии со стороны пользователя или файл поврежден при копировании в каталог с установленным СЗИ «Аккорд»)	2) производственный отдел сформирует корректный файл лицензии и отправит его заказчику; 3) полученный файл нужно скопировать в каталог с установленными файлами СЗИ «Аккорд» под именем «accord.key»
Ключевой файл лицензии не подходит для этой операционной системы!	Файл лицензии предназначен для ПО «Аккорд-NT» или «Аккорд-2000». Данный файл лицензии предназначен для использования на ОС Windows NT/2000/XP	1) Необходимо сообщить тип используемого ПО СПО «Аккорд», а также прислать имеющийся файл по адресу электронной почты key@okbsapr.ru; 2) производственный отдел сформирует корректный файл лицензии и отправит его заказчику; 3) полученный файл нужно скопировать в каталог с установленными файлами СЗИ «Аккорд» под именем «accord.key»
Лицензия истекает через XXX[1] дней!	Срок действия файла лицензии истекает через XXX дней	1) Необходимо сообщить об истечении срока действия лицензии и прислать имеющийся файл по адресу электронной почты key@okbsapr.ru; 2) производственный отдел сформирует корректный файл лицензии и отправит его заказчику; 3) полученный файл нужно скопировать в каталог с установленными файлами СЗИ «Аккорд» под именем «accord.key»

[1)] «XXX» - количество дней

Приложение 4. Сообщения об ошибках СПО «Аккорд-Win64 K»

Сообщения об ошибках, причины их появления и методы устранения приведены в таблице 1.

Таблица 3 – Сообщения об ошибках СПО «Аккорд-Win64 K»

Сообщение на экране	Причины появления сообщения	Порядок действий
«Ошибка чтения ключа!»	Ошибка чтения данных из идентификатора	Нажать кнопку <OK>, повторить операцию. Если ошибка повторится, сгенерировать новый ключ
«Ошибка запуска программы [ErrCode=193]»	Запуск программы AcTskMng.EXE с установленным параметром WaitEndTask=Yes	Присвоить параметру WaitEndTask значение «No». Затем выполнить запуск программы AcTskMng.EXE
«Ошибка создания ключа!»	Ошибка записи информации в идентификатор	Нажать кнопку <OK>. Повторить операцию

Приложение 5. Перечень нормативных документов, используемых при организации защиты информации

1) Федеральный закон от 21 июля 1993 года № 5485-I (с изменениями и дополнениями от 6 октября 1997 года № 131-ФЗ) «О государственной тайне».

2) Федеральный закон от 4 июля 1996 г. №85-ФЗ «Об участии в международном информационном обмене».

3) Федеральный закон от 8 августа 2001 г. № 128-ФЗ «О лицензировании отдельных видов деятельности».

4) Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи».

5) Федеральный закон от 7 июля 2003 г. №126-ФЗ «О связи».

6) Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации».

7) Федеральный закон от 27 июля 2006 г. №153-ФЗ «О персональных данных».

8) Указ Президента Российской Федерации от 19 февраля 1999 г. № 212 «Вопросы Государственной технической комиссии при Президенте Российской Федерации».

9) «Доктрина информационной безопасности Российской Федерации», утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр.-1895.

10) Указ Президента Российской Федерации от 17 декабря 1997 г. № 1300 «Концепция национальной безопасности Российской Федерации» в редакции Указа Президента Российской Федерации от 10 января 2000 г. №24.

11) Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Перечень сведений конфиденциального характера».

12) Указ Президента Российской Федерации от 6 октября 1998 г. № 1189 «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена».

13) Постановление Правительства Российской Федерации от 3 ноября 1994 г. №1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти».

14) Постановление Правительства Российской Федерации от 11 февраля 2002 г. №135 «О лицензировании отдельных видов деятельности».

15) Постановление Правительства Российской Федерации от 30 апреля 2002 г. №290 «О лицензировании деятельности по технической защите конфиденциальной информации».

16) «Сборник руководящих документов по защите информации от несанкционированного доступа», Гостехкомиссия России, Москва, 1998 г.

17) ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

18) ГОСТ Р 50922-96 «Защита информации. Основные термины и определения».

19) ГОСТ Р 51583-2000 «Порядок создания автоматизированных систем в защищенном исполнении».

20) ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний».

21) ГОСТ Р ИСО 7498-2-99 «Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».

22) ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем».

23) ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированных систем».

24) ГОСТ 35.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

25) ГОСТ Р ИСО\МЭК 9126- 90 «Информационная технология. Оценка программной продукции. Характеристика качества и руководства по их применению».

26) ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации».

27) РД Гостехкомиссии России «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля недекларированных возможностей», Москва, 1999 г.

Приложение 6. Список файлов ОС Windows 7 x32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\System32\advapi32.dll
\Windows\System32\aelupsvc.dll
\Windows\System32\apphelp.dll
\Windows\System32\audiosrv.dll
\Windows\System32\authui.dll
\Windows\System32\authz.dll
\Windows\System32\bcrypt.dll
\Windows\System32\BFE.DLL
\Windows\System32\cdd.dll
\Windows\System32\cfgmgr32.dll
\Windows\System32\ci.dll
\Windows\System32\crypt32.dll
\Windows\System32\cryptbase.dll
\Windows\System32\cryptsp.dll
\Windows\System32\cryptsvc.dll
\Windows\System32\cscsvc.dll
\Windows\System32\devrtl.dll
\Windows\System32\dhcpcore.dll
\Windows\System32\dhcpcore6.dll
\Windows\System32\dnsrslvr.dll
\Windows\System32\dps.dll
\Windows\System32\dui70.dll
\Windows\System32\duser.dll
\Windows\System32\es.dll
\Windows\System32\esent.dll
\Windows\System32\gdi32.dll
\Windows\System32\gpapi.dll
\Windows\System32\gpsvc.dll
\Windows\System32\HotStartUserAgent.dll
\Windows\System32\lmhsvc.dll
\Windows\System32\mmcss.dll
\Windows\System32\MMDevAPI.dll
\Windows\System32\msctf.dll
\Windows\System32\MsCtfMonitor.dll
\Windows\System32\mssrch.dll
\Windows\System32\msvcrt.dll
\Windows\System32\mswsock.dll
\Windows\System32\msxml6.dll
\Windows\System32\ncobjapi.dll
\Windows\System32\netprofm.dll

\Windows\System32\nlasvc.dll
\Windows\System32\nsi.dll
\Windows\System32\ole32.dll
\Windows\System32\oleaut32.dll
\Windows\System32\PeerDist.dll
\Windows\System32\PlaySndSrv.dll
\Windows\System32\propsys.dll
\Windows\System32\radardt.dll
\Windows\System32\RpcRtRemote.dll
\Windows\System32\rpcss.dll
\Windows\System32\rsaenh.dll
\Windows\System32\samsrv.dll
\Windows\System32\schedsvc.dll
\Windows\System32\sechost.dll
\Windows\System32\setupapi.dll
\Windows\System32\shell32.dll
\Windows\System32\shlwapi.dll
\Windows\System32\srvsvc.dll
\Windows\System32\sxs.dll
\Windows\System32\taskcomp.dll
\Windows\System32\tquery.dll
\Windows\System32\trkwks.dll
\Windows\System32\ubpm.dll
\Windows\System32\umpnpmgr.dll
\Windows\System32\umpo.dll
\Windows\System32\usp10.dll
\Windows\System32\UXInit.dll
\Windows\System32\uxsms.dll
\Windows\System32\uxtheme.dll
\Windows\System32\wbemcomn.dll
\Windows\System32\wbem\fastprox.dll
\Windows\System32\wbem\repdrvfs.dll
\Windows\System32\wbem\wbemcore.dll
\Windows\system32\wbem\wmiprvse.exe
\Windows\System32\wbem\wmiutils.dll
\Windows\System32\wdiasqmmodule.dll
\Windows\System32\wevtsvc.dll
\Windows\System32\winmm.dll
\Windows\System32\winsrv.dll
\Windows\System32\winsta.dll
\Windows\System32\wlanapi.dll
\Windows\System32\wlansvc.dll
\Windows\System32\wlgpclnt.dll
\Windows\System32\wpdbusenum.dll
\Windows\System32\xmllite.dll

Приложение 7. Список файлов ОС Windows 7 x64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\System32\advapi32.dll
\Windows\System32\aelupsvc.dll
\Windows\System32\AudioEng.dll
\Windows\System32\AUDIOKSE.dll
\Windows\System32\audiosrv.dll
\Windows\System32\authui.dll
\Windows\System32\authz.dll
\Windows\System32\basesrv.dll
\Windows\System32\bcrypt.dll
\Windows\System32\bcryptprimitives.dll
\Windows\System32\BFE.DLL
\Windows\System32\cdd.dll
\Windows\System32\cfgmgr32.dll
\Windows\System32\CI.dll
\Windows\System32\comctl32.dll
\Windows\System32\crypt32.dll
\Windows\System32\cryptbase.dll
\Windows\System32\cryptsp.dll
\Windows\System32\cryptsvc.dll
\Windows\System32\cscsvc.dll
\Windows\System32\devobj.dll
\Windows\System32\devrtl.dll
\Windows\System32\dhcpcore.dll
\Windows\System32\dhcpcore6.dll
\Windows\System32\dnsrslvr.dll
\Windows\System32\dps.dll
\Windows\System32\dui70.dll
\Windows\System32\duser.dll
\Windows\System32\dwmcore.dll
\Windows\System32\es.dll
\Windows\System32\esent.dll
\Windows\System32\fdPnp.dll
\Windows\System32\FirewallAPI.dll
\Windows\System32\FntCache.dll
\Windows\System32\fundisc.dll
\Windows\System32\FXSST.dll
\Windows\System32\gpapi.dll
\Windows\System32\gpsvc.dll
\Windows\System32\HotStartUserAgent.dll

\Windows\System32\iertutil.dll
\Windows\System32\inetpp.dll
\Windows\System32\IPHLPAPI.DLL
\Windows\System32\lmhsvc.dll
\Windows\System32\localspl.dll
\Windows\System32\lpk.dll
\Windows\System32\mmcss.dll
\Windows\System32\MMDevAPI.dll
\Windows\System32\MPSSVC.dll
\Windows\System32\msctf.dll
\Windows\System32\MsCtfMonitor.dll
\Windows\System32\mssrch.dll
\Windows\System32\msvcrt.dll
\Windows\System32\mswsock.dll
\Windows\System32\msxml6.dll
\Windows\System32\ncobjapi.dll
\Windows\System32\ncsi.dll
\Windows\System32\netcfgx.dll
\Windows\System32\netprofm.dll
\Windows\System32\nlasvc.dll
\Windows\System32\nsi.dll
\Windows\System32\ole32.dll
\Windows\System32\oleaut32.dll
\Windows\System32\PeerDist.dll
\Windows\System32\PlaySndSrv.dll
\Windows\System32\PrintIsolationProxy.dll
\Windows\System32\radardt.dll
\Windows\System32\rpcrt4.dll
\Windows\System32\rpcss.dll
\Windows\System32\rsaenh.dll
\Windows\System32\samsrv.dll
\Windows\System32\sechost.dll
\Windows\System32\setupapi.dll
\Windows\System32\shell32.dll
\Windows\System32\shlwapi.dll
\Windows\System32\SPInf.dll
\Windows\System32\srvsvc.dll
\Windows\System32\ssdpapi.dll
\Windows\System32\ssdpsrv.dll
\Windows\System32\sxs.dll
\Windows\System32\sysmain.dll
\Windows\System32\taskcomp.dll
\Windows\System32\tquery.dll

\Windows\System32\trkwks.dll
\Windows\System32\ubpm.dll
\Windows\System32\umpnpmgr.dll
\Windows\System32\umpo.dll
\Windows\System32\upnp.dll
\Windows\System32\urlmon.dll
\Windows\System32\usbmon.dll
\Windows\System32\usp10.dll
\Windows\System32\UXInit.dll
\Windows\System32\uxsms.dll
\Windows\System32\uxtheme.dll
\Windows\System32\wbemcomn.dll
\Windows\system32\wbem\fastprox.dll
\Windows\system32\wbem\repdrvfs.dll
\Windows\system32\wbem\wbemcore.dll
\Windows\system32\wbem\WmiPrvSE.exe
\Windows\system32\wbem\wmiutils.dll
\Windows\System32\wdiasqmmodule.dll
\Windows\System32\wevtapi.dll
\Windows\System32\wevtsvc.dll
\Windows\System32\winmm.dll
\Windows\System32\winsrv.dll
\Windows\System32\winsta.dll
\Windows\System32\wlanapi.dll
\Windows\System32\wlgpclnt.dll
\Windows\System32\wow64.dll
\Windows\System32\wow64cpu.dll
\Windows\System32\ws2_32.dll
\Windows\System32\WSDMon.dll
\Windows\System32\xmllite.dll

Приложение 8. Список файлов ОС Windows 8.1 x 64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\System32\advapi32.dll
\Windows\System32\aelupsvc.dll
\Windows\System32\AudioEng.dll
\Windows\System32\AUDIOKSE.dll
\Windows\System32\audiosrv.dll
\Windows\System32\authui.dll
\Windows\System32\authz.dll
\Windows\System32\basesrv.dll
\Windows\System32\bcrypt.dll
\Windows\System32\bcryptprimitives.dll
\Windows\System32\BFE.DLL
\Windows\System32\cdd.dll
\Windows\System32\cfgmgr32.dll
\Windows\System32\CI.dll
\Windows\System32\comctl32.dll
\Windows\System32\crypt32.dll
\Windows\System32\cryptbase.dll
\Windows\System32\cryptsp.dll
\Windows\System32\cryptsvc.dll
\Windows\System32\cscsvc.dll
\Windows\System32\devobj.dll
\Windows\System32\devrtl.dll
\Windows\System32\dhcpcore.dll
\Windows\System32\dhcpcore6.dll
\Windows\System32\dnsrslvr.dll
\Windows\System32\dps.dll
\Windows\System32\dui70.dll
\Windows\System32\duser.dll
\Windows\System32\dwmcore.dll
\Windows\System32\es.dll
\Windows\System32\esent.dll
\Windows\System32\fdPnp.dll
\Windows\System32\FirewallAPI.dll
\Windows\System32\FntCache.dll
\Windows\System32\fundisc.dll
\Windows\System32\FXSST.dll
\Windows\System32\gpapi.dll
\Windows\System32\gpsvc.dll
\Windows\System32\iertutil.dll

\Windows\System32\inetpp.dll
\Windows\System32\IPHLPAPI.DLL
\Windows\System32\lmhsvc.dll
\Windows\System32\localspl.dll
\Windows\System32\lpk.dll
\Windows\System32\mmcss.dll
\Windows\System32\MMDevAPI.dll
\Windows\System32\MPSSVC.dll
\Windows\System32\msctf.dll
\Windows\System32\MsCtfMonitor.dll
\Windows\System32\mssrch.dll
\Windows\System32\msvcrt.dll
\Windows\System32\mswsock.dll
\Windows\System32\msxml6.dll
\Windows\System32\ncobjapi.dll
\Windows\System32\ncsi.dll
\Windows\System32\netcfgx.dll
\Windows\System32\netprofm.dll
\Windows\System32\nlasvc.dll
\Windows\System32\nsi.dll
\Windows\System32\ole32.dll
\Windows\System32\oleaut32.dll
\Windows\System32\PeerDist.dll
\Windows\System32\PlaySndSrv.dll
\Windows\System32\PrintIsolationProxy.dll
\Windows\System32\radardt.dll
\Windows\System32\rpcrt4.dll
\Windows\System32\rpcss.dll
\Windows\System32\rsaenh.dll
\Windows\System32\samsrv.dll
\Windows\System32\sechost.dll
\Windows\System32\setupapi.dll
\Windows\System32\shell32.dll
\Windows\System32\shlwapi.dll
\Windows\System32\SPInf.dll
\Windows\System32\srvsvc.dll
\Windows\System32\ssdpapi.dll
\Windows\System32\ssdpsrv.dll
\Windows\System32\sxs.dll
\Windows\System32\sysmain.dll
\Windows\System32\taskcomp.dll
\Windows\System32\tquery.dll
\Windows\System32\trkwks.dll

\Windows\System32\ubpm.dll
\Windows\System32\umpnpmgr.dll
\Windows\System32\umpo.dll
\Windows\System32\upnp.dll
\Windows\System32\urlmon.dll
\Windows\System32\usbmon.dll
\Windows\System32\usp10.dll
\Windows\System32\UXInit.dll
\Windows\System32\uxtheme.dll
\Windows\System32\wbemcomn.dll
\Windows\system32\wbem\fastprox.dll
\Windows\system32\wbem\repdrvfs.dll
\Windows\system32\wbem\wbemcore.dll
\Windows\system32\wbem\WmiPrvSE.exe
\Windows\system32\wbem\wmiutils.dll
\Windows\System32\wdiasqmmodule.dll
\Windows\System32\wevtapi.dll
\Windows\System32\wevtsvc.dll
\Windows\System32\winmm.dll
\Windows\System32\winsrv.dll
\Windows\System32\winsta.dll
\Windows\System32\wlanapi.dll
\Windows\System32\wlgpclnt.dll
\Windows\System32\wow64.dll
\Windows\System32\wow64cpu.dll
\Windows\System32\ws2_32.dll
\Windows\System32\WSDMon.dll
\Windows\System32\xmllite.dll

Приложение 9. Список файлов ОС Windows 8.1 x 32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\System32\advapi32.dll
\Windows\System32\aelupsvc.dll
\Windows\System32\apphelp.dll
\Windows\System32\audiosrv.dll
\Windows\System32\authui.dll
\Windows\System32\authz.dll
\Windows\System32\bcrypt.dll
\Windows\System32\BFE.DLL
\Windows\System32\cdd.dll
\Windows\System32\cfgmgr32.dll
\Windows\System32\ci.dll
\Windows\System32\crypt32.dll
\Windows\System32\cryptbase.dll
\Windows\System32\cryptsp.dll
\Windows\System32\cryptsvc.dll
\Windows\System32\cscsvc.dll
\Windows\System32\devrtl.dll
\Windows\System32\dhcpcore.dll
\Windows\System32\dhcpcore6.dll
\Windows\System32\dnsrslvr.dll
\Windows\System32\dps.dll
\Windows\System32\dui70.dll
\Windows\System32\duser.dll
\Windows\System32\es.dll
\Windows\System32\esent.dll
\Windows\System32\gdi32.dll
\Windows\System32\gpapi.dll
\Windows\System32\gpsvc.dll
\Windows\System32\lmhsvc.dll
\Windows\System32\mmcss.dll
\Windows\System32\MMDevAPI.dll
\Windows\System32\msctf.dll
\Windows\System32\MsCtfMonitor.dll
\Windows\System32\mssrch.dll
\Windows\System32\msvcrt.dll
\Windows\System32\mswsock.dll
\Windows\System32\msxml6.dll
\Windows\System32\ncobjapi.dll
\Windows\System32\netprofm.dll

\Windows\System32\nlasvc.dll
\Windows\System32\nsi.dll
\Windows\System32\ole32.dll
\Windows\System32\oleaut32.dll
\Windows\System32\PeerDist.dll
\Windows\System32\PlaySndSrv.dll
\Windows\System32\propsys.dll
\Windows\System32\radardt.dll
\Windows\System32\RpcRtRemote.dll
\Windows\System32\rpcss.dll
\Windows\System32\rsaenh.dll
\Windows\System32\samsrv.dll
\Windows\System32\schedsvc.dll
\Windows\System32\sechost.dll
\Windows\System32\setupapi.dll
\Windows\System32\shell32.dll
\Windows\System32\shlwapi.dll
\Windows\System32\srvsvc.dll
\Windows\System32\sxs.dll
\Windows\System32\taskcomp.dll
\Windows\System32\tquery.dll
\Windows\System32\trkwks.dll
\Windows\System32\ubpm.dll
\Windows\System32\umpnpmgr.dll
\Windows\System32\umpo.dll
\Windows\System32\usp10.dll
\Windows\System32\UXInit.dll
\Windows\System32\uxtheme.dll
\Windows\System32\wbemcomn.dll
\Windows\System32\wbem\fastprox.dll
\Windows\System32\wbem\repdrvfs.dll
\Windows\System32\wbem\wbemcore.dll
\Windows\system32\wbem\wmiprvse.exe
\Windows\System32\wbem\wmiutils.dll
\Windows\System32\wdiasqmmodule.dll
\Windows\System32\wevtsvc.dll
\Windows\System32\winmm.dll
\Windows\System32\winsrv.dll
\Windows\System32\winsta.dll
\Windows\System32\wlanapi.dll
\Windows\System32\wlansvc.dll
\Windows\System32\wlgpclnt.dll
\Windows\System32\wpdbusenum.dll

37222406.26.20.40.140.091 90

\Windows\System32\xmllite.dll

Приложение 10. Список файлов ОС Windows 10 x64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\System32\advapi32.dll
\Windows\System32\AudioEng.dll
\Windows\System32\AUDIOKSE.dll
\Windows\System32\audiosrv.dll
\Windows\System32\authui.dll
\Windows\System32\authz.dll
\Windows\System32\basesrv.dll
\Windows\System32\bcrypt.dll
\Windows\System32\bcryptprimitives.dll
\Windows\System32\BFE.DLL
\Windows\System32\cdd.dll
\Windows\System32\cfgmgr32.dll
\Windows\System32\CI.dll
\Windows\System32\comctl32.dll
\Windows\System32\crypt32.dll
\Windows\System32\cryptbase.dll
\Windows\System32\cryptsp.dll
\Windows\System32\cryptsvc.dll
\Windows\System32\cscsvc.dll
\Windows\System32\devobj.dll
\Windows\System32\devrtl.dll
\Windows\System32\dhcpcore.dll
\Windows\System32\dhcpcore6.dll
\Windows\System32\dnsrslvr.dll
\Windows\System32\dps.dll
\Windows\System32\dui70.dll
\Windows\System32\duser.dll
\Windows\System32\dwmcore.dll
\Windows\System32\es.dll
\Windows\System32\esent.dll
\Windows\System32\fdPnp.dll
\Windows\System32\FirewallAPI.dll
\Windows\System32\FntCache.dll
\Windows\System32\fundisc.dll
\Windows\System32\FXSST.dll
\Windows\System32\gpapi.dll
\Windows\System32\gpsvc.dll
\Windows\System32\iertutil.dll
\Windows\System32\inetpp.dll

\Windows\System32\IPHLPAPI.DLL
\Windows\System32\lmhsvc.dll
\Windows\System32\localspl.dll
\Windows\System32\lpk.dll
\Windows\System32\MMDevAPI.dll
\Windows\System32\MPSSVC.dll
\Windows\System32\msctf.dll
\Windows\System32\MsCtfMonitor.dll
\Windows\System32\mssrch.dll
\Windows\System32\msvcrt.dll
\Windows\System32\mswsock.dll
\Windows\System32\msxml6.dll
\Windows\System32\ncobjapi.dll
\Windows\System32\ncsi.dll
\Windows\System32\netcfgx.dll
\Windows\System32\netprofm.dll
\Windows\System32\nlasvc.dll
\Windows\System32\nsi.dll
\Windows\System32\ole32.dll
\Windows\System32\oleaut32.dll
\Windows\System32\PeerDist.dll
\Windows\System32\PlaySndSrv.dll
\Windows\System32\PrintIsolationProxy.dll
\Windows\System32\radardt.dll
\Windows\System32\rpcrt4.dll
\Windows\System32\rpcss.dll
\Windows\System32\rsaenh.dll
\Windows\System32\samsrv.dll
\Windows\System32\sechost.dll
\Windows\System32\setupapi.dll
\Windows\System32\shell32.dll
\Windows\System32\shlwapi.dll
\Windows\System32\SPInf.dll
\Windows\System32\srvsvc.dll
\Windows\System32\ssdpapi.dll
\Windows\System32\ssdpsrv.dll
\Windows\System32\sxs.dll
\Windows\System32\sysmain.dll
\Windows\System32\taskcomp.dll
\Windows\System32\tquery.dll
\Windows\System32\trkwks.dll
\Windows\System32\ubpm.dll
\Windows\System32\umpnpmgr.dll

\Windows\System32\umpo.dll
\Windows\System32\upnp.dll
\Windows\System32\urlmon.dll
\Windows\System32\usbmon.dll
\Windows\System32\usp10.dll
\Windows\System32\UXInit.dll
\Windows\System32\uxtheme.dll
\Windows\System32\wbemcomn.dll
\Windows\system32\wbem\fastprox.dll
\Windows\system32\wbem\repdrvfs.dll
\Windows\system32\wbem\wbemcore.dll
\Windows\system32\wbem\WmiPrvSE.exe
\Windows\system32\wbem\wmiutils.dll
\Windows\System32\wevtapi.dll
\Windows\System32\wevtsvc.dll
\Windows\System32\winmm.dll
\Windows\System32\winsrv.dll
\Windows\System32\winsta.dll
\Windows\System32\wlanapi.dll
\Windows\System32\wlgpclnt.dll
\Windows\System32\wow64.dll
\Windows\System32\wow64cpu.dll
\Windows\System32\ws2_32.dll
\Windows\System32\WSDMon.dll
\Windows\System32\xmllite.dll
\Windows\System32\drivers\mmcss.sys

Приложение 11. Список файлов ОС Windows 10 x32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\System32\advapi32.dll
\Windows\System32\apphelp.dll
\Windows\System32\audiosrv.dll
\Windows\System32\authui.dll
\Windows\System32\authz.dll
\Windows\System32\bcrypt.dll
\Windows\System32\BFE.DLL
\Windows\System32\cdd.dll
\Windows\System32\cfgmgr32.dll
\Windows\System32\ci.dll
\Windows\System32\crypt32.dll
\Windows\System32\cryptbase.dll
\Windows\System32\cryptsp.dll
\Windows\System32\cryptsvc.dll
\Windows\System32\cscsvc.dll
\Windows\System32\devrtl.dll
\Windows\System32\dhcpcore.dll
\Windows\System32\dhcpcore6.dll
\Windows\System32\dnsrslvr.dll
\Windows\System32\dps.dll
\Windows\System32\dui70.dll
\Windows\System32\duser.dll
\Windows\System32\es.dll
\Windows\System32\esent.dll
\Windows\System32\gdi32.dll
\Windows\System32\gpapi.dll
\Windows\System32\gpsvc.dll
\Windows\System32\lmhsvc.dll
\Windows\System32\MMDevAPI.dll
\Windows\System32\msctf.dll
\Windows\System32\MsCtfMonitor.dll
\Windows\System32\mssrch.dll
\Windows\System32\msvcrt.dll
\Windows\System32\mswsock.dll
\Windows\System32\msxml6.dll
\Windows\System32\ncobjapi.dll
\Windows\System32\netprofm.dll
\Windows\System32\nlasvc.dll
\Windows\System32\nsi.dll

\Windows\System32\ole32.dll
\Windows\System32\oleaut32.dll
\Windows\System32\PeerDist.dll
\Windows\System32\PlaySndSrv.dll
\Windows\System32\propsys.dll
\Windows\System32\radardt.dll
\Windows\System32\RpcRtRemote.dll
\Windows\System32\rpcss.dll
\Windows\System32\rsaenh.dll
\Windows\System32\samsrv.dll
\Windows\System32\schedsvc.dll
\Windows\System32\sechost.dll
\Windows\System32\setupapi.dll
\Windows\System32\shell32.dll
\Windows\System32\shlwapi.dll
\Windows\System32\srvsvc.dll
\Windows\System32\sxs.dll
\Windows\System32\taskcomp.dll
\Windows\System32\tquery.dll
\Windows\System32\trkwks.dll
\Windows\System32\ubpm.dll
\Windows\System32\umpnpmgr.dll
\Windows\System32\umpo.dll
\Windows\System32\usp10.dll
\Windows\System32\UXInit.dll
\Windows\System32\uxtheme.dll
\Windows\System32\wbemcomn.dll
\Windows\System32\wbem\fastprox.dll
\Windows\System32\wbem\repdrvfs.dll
\Windows\System32\wbem\wbemcore.dll
\Windows\system32\wbem\wmiprvse.exe
\Windows\System32\wbem\wmiutils.dll
\Windows\System32\wevtsvc.dll
\Windows\System32\winmm.dll
\Windows\System32\winsrv.dll
\Windows\System32\winsta.dll
\Windows\System32\wlanapi.dll
\Windows\System32\wlansvc.dll
\Windows\System32\wlgpclnt.dll
\Windows\System32\wpdbusenum.dll
\Windows\System32\xmllite.dll
\Windows\System32\drivers\mmcss.sys

Приложение 12. Список файлов ОС Windows Server 2003 R2 x32, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\system32\aclui.dll
\Windows\system32\activeds.dll
\Windows\system32\adsldpc.dll
\Windows\system32\advapi32.dll
\Windows\system32\advapi32.dll
\Windows\system32\advpack.dll
\Windows\system32\apphelp.dll
\Windows\system32\authz.dll
\Windows\system32\BOOTVID.dll
\Windows\system32\cabinet.dll
\Windows\system32\cfgmgr32.dll
\Windows\system32\clbcatq.dll
\Windows\system32\comctl32.dll
\Windows\system32\comdlg32.dll
\Windows\system32\credui.dll
\Windows\system32\crypt32.dll
\Windows\system32\crypt32.dll
\Windows\system32\cryptui.dll
\Windows\system32\csrsrv.dll
\Windows\system32\dbgeng.dll
\Windows\system32\dbghelp.dll
\Windows\system32\devmgr.dll
\Windows\system32\dhcpcsvc.dll
\Windows\system32\dnsapi.dll
\Windows\system32\duser.dll
\Windows\system32\efsadu.dll
\Windows\system32\esent.dll
\Windows\system32\Faultrep.dll
\Windows\system32\feclient.dll
\Windows\system32\fltLib.dll
\Windows\system32\gdi32.dll
\Windows\system32\hal.dll
\Windows\system32\hid.dll
\Windows\system32\imagehlp.dll

\Windows\system32\imm32.dll
\Windows\system32\IPHLPAPI.DLL
\Windows\system32\kdcom.dll
\Windows\system32\kernel32.dll
\Windows\system32\linkinfo.dll
\Windows\system32\lpk.dll
\Windows\system32\mfc42u.dll
\Windows\system32\mmcbase.dll
\Windows\system32\mpr.dll
\Windows\system32\mprmsg.dll
\Windows\system32\msasn1.dll
\Windows\system32\msimg32.dll
\Windows\system32\msvcrt.dll
\Windows\system32\msvcrt.dll
\Windows\system32\netapi32.dll
\Windows\system32\newdev.dll
\Windows\system32\ntdll.dll
\Windows\system32\ntdsapi.dll
\Windows\system32\ntshrui.dll
\Windows\system32\odbc32.dll
\Windows\system32\ole32.dll
\Windows\system32\oleacc.dll
\Windows\system32\oleaut32.dll
\Windows\system32\oledlg.dll
\Windows\system32\powrprof.dll
\Windows\system32\printui.dll
\Windows\system32\psapi.dll
\Windows\system32\rasapi32.dll
\Windows\system32\rasman.dll
\Windows\system32\regapi.dll
\Windows\system32\rpcrt4.dll
\Windows\system32\rtutils.dll
\Windows\system32\samlib.dll
\Windows\system32\scecli.dll
\Windows\system32\secur32.dll
\Windows\system32\SensApi.dll
\Windows\system32\setupapi.dll
\Windows\system32\shdocvw.dll
\Windows\system32\shell32.dll

\Windows\system32\shell32.dll
\Windows\system32\shlwapi.dll
\Windows\system32\tapi32.dll
\Windows\system32\urlmon.dll
\Windows\system32\user32.dll
\Windows\system32\userenv.dll
\Windows\system32\uxtheme.dll
\Windows\system32\version.dll
\Windows\system32\w32topl.dll
\Windows\system32\winbrand.dll
\Windows\system32\wininet.dll
\Windows\system32\winmm.dll
\Windows\system32\WinSCard.dll
\Windows\system32\winsta.dll
\Windows\system32\wintrust.dll
\Windows\system32\Wldap32.dll
\Windows\system32\ws2_32.dll
\Windows\system32\wtsapi32.dll
\Windows\system32\xmllite.dll

Приложение 13. Список файлов ОС Windows Server 2003 R2 x64, рекомендуемых для контроля целостности при установке СПО «АККОРД – Win64 K»

\Windows\system32\aclui.dll
\Windows\system32\activeds.dll
\Windows\system32\adsldpc.dll
\Windows\system32\advapi32.dll
\Windows\system32\advapi32.dll
\Windows\system32\advpack.dll
\Windows\system32\apphelp.dll
\Windows\system32\authz.dll
\Windows\system32\BOOTVID.dll
\Windows\system32\cabinet.dll
\Windows\system32\cfgmgr32.dll
\Windows\system32\clbcatq.dll
\Windows\system32\comctl32.dll
\Windows\system32\comdlg32.dll
\Windows\system32\credui.dll
\Windows\system32\crypt32.dll
\Windows\system32\crypt32.dll
\Windows\system32\cryptui.dll
\Windows\system32\csrsrv.dll
\Windows\system32\dbgeng.dll
\Windows\system32\dbghelp.dll
\Windows\system32\devmgr.dll
\Windows\system32\dhcpcsvc.dll
\Windows\system32\dnsapi.dll
\Windows\system32\duser.dll
\Windows\system32\efsadu.dll
\Windows\system32\esent.dll
\Windows\system32\Faultrep.dll
\Windows\system32\feclient.dll
\Windows\system32\fltLib.dll
\Windows\system32\gdi32.dll
\Windows\system32\hal.dll
\Windows\system32\hid.dll
\Windows\system32\imagehlp.dll

\Windows\system32\imm32.dll
\Windows\system32\IPHLPAPI.DLL
\Windows\system32\kdcom.dll
\Windows\system32\kernel32.dll
\Windows\system32\linkinfo.dll
\Windows\system32\lpk.dll
\Windows\system32\mfc42u.dll
\Windows\system32\mmcbase.dll
\Windows\system32\mpr.dll
\Windows\system32\mprmsg.dll
\Windows\system32\msasn1.dll
\Windows\system32\msimg32.dll
\Windows\system32\msvcrt.dll
\Windows\system32\msvcrt.dll
\Windows\system32\netapi32.dll
\Windows\system32\newdev.dll
\Windows\system32\ntdll.dll
\Windows\system32\ntdsapi.dll
\Windows\system32\ntshrui.dll
\Windows\system32\odbc32.dll
\Windows\system32\ole32.dll
\Windows\system32\oleacc.dll
\Windows\system32\oleaut32.dll
\Windows\system32\oledlg.dll
\Windows\system32\powrprof.dll
\Windows\system32\printui.dll
\Windows\system32\psapi.dll
\Windows\system32\puiapi.dll
\Windows\system32\rasapi32.dll
\Windows\system32\rasman.dll
\Windows\system32\regapi.dll
\Windows\system32\rpcrt4.dll
\Windows\system32\rtutils.dll
\Windows\system32\samlib.dll
\Windows\system32\scecli.dll
\Windows\system32\secur32.dll
\Windows\system32\SensApi.dll
\Windows\system32\setupapi.dll
\Windows\system32\shdocvw.dll

\Windows\system32\shell32.dll
\Windows\system32\shell32.dll
\Windows\system32\shlwapi.dll
\Windows\system32\tapi32.dll
\Windows\system32\urlmon.dll
\Windows\system32\user32.dll
\Windows\system32\userenv.dll
\Windows\system32\uxtheme.dll
\Windows\system32\version.dll
\Windows\system32\w32topl.dll
\Windows\system32\winbrand.dll
\Windows\system32\wininet.dll
\Windows\system32\winmm.dll
\Windows\system32\WinSCard.dll
\Windows\system32\winsta.dll
\Windows\system32\wintrust.dll
\Windows\system32\Wldap32.dll
\Windows\system32\wow64.dll
\Windows\system32\wow64cpu.dll
\Windows\system32\wow64win.dll
\Windows\system32\ws2_32.dll
\Windows\system32\wtsapi32.dll
\Windows\system32\xmllite.dll

Приложение 14. Список файлов ОС Windows Server 2012 R2, рекомендуемых для контроля целостности при СПО «АККОРД – Win64 K»

\Windows\system32\aclui.dll
\Windows\system32\activeds.dll
\Windows\system32\adsldpc.dll
\Windows\system32\advapi32.dll
\Windows\system32\advapi32.dll
\Windows\system32\advpack.dll
\Windows\system32\api-ms-win-appmodel-identity-l1-1-0.dll
\Windows\system32\api-ms-win-appmodel-runtime-internal-l1-1-0.dll
\Windows\system32\api-ms-win-appmodel-runtime-l1-1-0.dll
\Windows\system32\api-ms-win-appmodel-runtime-l1-1-1.dll
\Windows\system32\api-ms-win-appmodel-state-l1-1-1.dll
\Windows\system32\api-ms-win-base-bootconfig-l1-1-0.dll
\Windows\system32\api-ms-win-base-util-l1-1-0.dll
\Windows\system32\api-ms-win-core-apiquery-l1-1-0.dll
\Windows\system32\api-ms-win-core-appcompat-l1-1-1.dll
\Windows\system32\api-ms-win-core-appinit-l1-1-0.dll
\Windows\system32\api-ms-win-core-atoms-l1-1-0.dll
\Windows\system32\api-ms-win-core-bem-l1-1-0.dll
\Windows\system32\api-ms-win-core-biplmapi-l1-1-1.dll
\Windows\system32\api-ms-win-core-com-l1-1-0.dll
\Windows\system32\api-ms-win-core-com-l1-1-1.dll
\Windows\system32\api-ms-win-core-comm-l1-1-0.dll
\Windows\system32\api-ms-win-core-com-private-l1-1-0.dll
\Windows\system32\api-ms-win-core-console-l1-1-0.dll
\Windows\system32\api-ms-win-core-console-l2-1-0.dll
\Windows\system32\api-ms-win-core-crt-l1-1-0.dll
\Windows\system32\api-ms-win-core-crt-l2-1-0.dll
\Windows\system32\api-ms-win-core-datetime-l1-1-1.dll
\Windows\system32\api-ms-win-core-debug-l1-1-0.dll
\Windows\system32\api-ms-win-core-debug-l1-1-1.dll
\Windows\system32\api-ms-win-core-delayload-l1-1-1.dll
\Windows\system32\api-ms-win-core-errorhandling-l1-1-0.dll
\Windows\system32\api-ms-win-core-errorhandling-l1-1-1.dll
\Windows\system32\api-ms-win-core-fibers-l1-1-1.dll
\Windows\system32\api-ms-win-core-file-l1-1-0.dll
\Windows\system32\api-ms-win-core-file-l1-2-0.dll
\Windows\system32\api-ms-win-core-file-l1-2-1.dll
\Windows\system32\api-ms-win-core-file-l2-1-0.dll
\Windows\system32\api-ms-win-core-file-l2-1-1.dll

\Windows\system32\api-ms-win-core-handle-l1-1-0.dll
\Windows\system32\api-ms-win-core-heap-l1-1-0.dll
\Windows\system32\api-ms-win-core-heap-l1-2-0.dll
\Windows\system32\api-ms-win-core-heap-obsolete-l1-1-0.dll
\Windows\system32\api-ms-win-core-interlocked-l1-2-0.dll
\Windows\system32\api-ms-win-core-io-l1-1-0.dll
\Windows\system32\api-ms-win-core-io-l1-1-1.dll
\Windows\system32\api-ms-win-core-job-l1-1-0.dll
\Windows\system32\api-ms-win-core-job-l2-1-0.dll
\Windows\system32\api-ms-win-core-kernel32-legacy-l1-1-0.dll
\Windows\system32\api-ms-win-core-kernel32-legacy-l1-1-1.dll
\Windows\system32\api-ms-win-core-libraryloader-l1-1-0.dll
\Windows\system32\api-ms-win-core-libraryloader-l1-2-0.dll
\Windows\system32\api-ms-win-core-localization-l1-2-0.dll
\Windows\system32\api-ms-win-core-localization-l1-2-1.dll
\Windows\system32\api-ms-win-core-localization-l2-1-0.dll
\Windows\system32\api-ms-win-core-localization-obsolete-l1-2-0.dll
\Windows\system32\api-ms-win-core-localization-private-l1-1-0.dll
\Windows\system32\api-ms-win-core-memory-l1-1-0.dll
\Windows\system32\api-ms-win-core-memory-l1-1-2.dll
\Windows\system32\api-ms-win-core-namedpipe-l1-2-0.dll
\Windows\system32\api-ms-win-core-namespace-l1-1-0.dll
\Windows\system32\api-ms-win-core-normalization-l1-1-0.dll
\Windows\system32\api-ms-win-core-path-l1-1-0.dll
\Windows\system32\api-ms-win-core-processenvironment-l1-1-0.dll
\Windows\system32\api-ms-win-core-processenvironment-l1-2-0.dll
\Windows\system32\api-ms-win-core-processsecurity-l1-1-0.dll
\Windows\system32\api-ms-win-core-processthreads-l1-1-0.dll
\Windows\system32\api-ms-win-core-processthreads-l1-1-2.dll
\Windows\system32\api-ms-win-core-processtopology-l1-2-0.dll
\Windows\system32\api-ms-win-core-processtopology-obsolete-l1-1-0.dll
\Windows\system32\api-ms-win-core-profile-l1-1-0.dll
\Windows\system32\api-ms-win-core-psapi-ansi-l1-1-0.dll
\Windows\system32\api-ms-win-core-psapi-l1-1-0.dll
\Windows\system32\api-ms-win-core-psapi-obsolete-l1-1-0.dll
\Windows\system32\api-ms-win-core-psm-appnotify-l1-1-0.dll
\Windows\system32\api-ms-win-core-psm-key-l1-1-0.dll
\Windows\system32\api-ms-win-core-quirks-l1-1-0.dll
\Windows\system32\api-ms-win-core-realtime-l1-1-0.dll
\Windows\system32\api-ms-win-core-registry-l1-1-0.dll
\Windows\system32\api-ms-win-core-registry-l2-1-0.dll
\Windows\system32\api-ms-win-core-registry-private-l1-1-0.dll
\Windows\system32\api-ms-win-core-registryuserspecific-l1-1-0.dll

\Windows\system32\api-ms-win-core-rtlsupport-l1-1-0.dll
\Windows\system32\api-ms-win-core-rtlsupport-l1-2-0.dll
\Windows\system32\api-ms-win-core-shlwapi-legacy-l1-1-0.dll
\Windows\system32\api-ms-win-core-shlwapi-obsolete-l1-1-0.dll
\Windows\system32\api-ms-win-core-sidebyside-l1-1-0.dll
\Windows\system32\api-ms-win-core-stringansi-l1-1-0.dll
\Windows\system32\api-ms-win-core-string-l1-1-0.dll
\Windows\system32\api-ms-win-core-string-l2-1-0.dll
\Windows\system32\api-ms-win-core-string-obsolete-l1-1-0.dll
\Windows\system32\api-ms-win-core-synch-l1-1-0.dll
\Windows\system32\api-ms-win-core-synch-l1-2-0.dll
\Windows\system32\api-ms-win-core-sysinfo-l1-1-0.dll
\Windows\system32\api-ms-win-core-sysinfo-l1-2-0.dll
\Windows\system32\api-ms-win-core-sysinfo-l1-2-1.dll
\Windows\system32\api-ms-win-core-systemtopology-l1-1-0.dll
\Windows\system32\api-ms-win-core-threadpool-l1-2-0.dll
\Windows\system32\api-ms-win-core-threadpool-legacy-l1-1-0.dll
\Windows\system32\api-ms-win-core-threadpool-private-l1-1-0.dll
\Windows\system32\api-ms-win-core-timezone-l1-1-0.dll
\Windows\system32\api-ms-win-core-toolhelp-l1-1-0.dll
\Windows\system32\api-ms-win-core-url-l1-1-0.dll
\Windows\system32\api-ms-win-core-util-l1-1-0.dll
\Windows\system32\api-ms-win-core-versionansi-l1-1-0.dll
\Windows\system32\api-ms-win-core-version-l1-1-0.dll
\Windows\system32\api-ms-win-core-version-private-l1-1-0.dll
\Windows\system32\api-ms-win-core-windowserrorreporting-l1-1-0.dll
\Windows\system32\api-ms-win-core-winrt-error-l1-1-0.dll
\Windows\system32\api-ms-win-core-winrt-error-l1-1-1.dll
\Windows\system32\api-ms-win-core-winrt-errorprivate-l1-1-1.dll
\Windows\system32\api-ms-win-core-winrt-l1-1-0.dll
\Windows\system32\api-ms-win-core-winrt-propertysetprivate-l1-1-0.dll
\Windows\system32\api-ms-win-core-winrt-registration-l1-1-0.dll
\Windows\system32\api-ms-win-core-winrt-robuffer-l1-1-0.dll
\Windows\system32\api-ms-win-core-winrt-string-l1-1-0.dll
\Windows\system32\api-ms-win-core-wow64-l1-1-0.dll
\Windows\system32\api-ms-win-core-xstate-l2-1-0.dll
\Windows\system32\api-ms-win-devices-config-l1-1-1.dll
\Windows\system32\api-ms-win-devices-query-l1-1-1.dll
\Windows\system32\api-ms-win-downlevel-advapi32-l1-1-0.dll
\Windows\system32\api-ms-win-downlevel-advapi32-l2-1-0.dll
\Windows\system32\api-ms-win-downlevel-normaliz-l1-1-0.dll
\Windows\system32\api-ms-win-downlevel-ole32-l1-1-0.dll
\Windows\system32\api-ms-win-downlevel-shlwapi-l1-1-0.dll

\Windows\system32\api-ms-win-downlevel-shlwapi-l2-1-0.dll
\Windows\system32\api-ms-win-downlevel-user32-l1-1-0.dll
\Windows\system32\api-ms-win-downlevel-version-l1-1-0.dll
\Windows\system32\api-ms-win-dx-d3dkmt-l1-1-0.dll
\Windows\system32\api-ms-win-eventing-classicprovider-l1-1-0.dll
\Windows\system32\api-ms-win-eventing-consumer-l1-1-0.dll
\Windows\system32\api-ms-win-eventing-controller-l1-1-0.dll
\Windows\system32\api-ms-win-eventing-legacy-l1-1-0.dll
\Windows\system32\api-ms-win-eventing-obsolete-l1-1-0.dll
\Windows\system32\api-ms-win-eventing-provider-l1-1-0.dll
\Windows\system32\api-ms-win-eventlog-legacy-l1-1-0.dll
\Windows\system32\api-ms-win-gdi-dpiinfo-l1-1-0.dll
\Windows\system32\api-ms-win-mm-joystick-l1-1-0.dll
\Windows\system32\api-ms-win-mm-misc-l1-1-1.dll
\Windows\system32\api-ms-win-mm-misc-l2-1-0.dll
\Windows\system32\api-ms-win-mm-mme-l1-1-0.dll
\Windows\system32\api-ms-win-mm-time-l1-1-0.dll
\Windows\system32\api-ms-win-ntuser-ie-message-l1-1-0.dll
\Windows\system32\api-ms-win-power-base-l1-1-0.dll
\Windows\system32\api-ms-win-power-setting-l1-1-0.dll
\Windows\system32\api-ms-win-rtcore-ntuser-private-l1-1-0.dll
\Windows\system32\api-ms-win-rtcore-ntuser-synch-l1-1-0.dll
\Windows\system32\api-ms-win-rtcore-ntuser-window-l1-1-0.dll
\Windows\system32\api-ms-win-rtcore-ntuser-winevent-l1-1-0.dll
\Windows\system32\api-ms-win-rtcore-ntuser-wmpointer-l1-1-0.dll
\Windows\system32\api-ms-win-security-activedirectoryclient-l1-1-0.dll
\Windows\system32\api-ms-win-security-appcontainer-l1-1-0.dll
\Windows\system32\api-ms-win-security-audit-l1-1-1.dll
\Windows\system32\api-ms-win-security-base-l1-1-0.dll
\Windows\system32\api-ms-win-security-base-l1-2-0.dll
\Windows\system32\api-ms-win-security-base-private-l1-1-1.dll
\Windows\system32\api-ms-win-security-credentials-l1-1-0.dll
\Windows\system32\api-ms-win-security-credentials-l2-1-0.dll
\Windows\system32\api-ms-win-security-grouppolicy-l1-1-0.dll
\Windows\system32\api-ms-win-security-lsalookup-l1-1-1.dll
\Windows\system32\api-ms-win-security-lsalookup-l2-1-0.dll
\Windows\system32\api-ms-win-security-lsalookup-l2-1-1.dll
\Windows\system32\api-ms-win-security-lsapolicy-l1-1-0.dll
\Windows\system32\api-ms-win-security-provider-l1-1-0.dll
\Windows\system32\api-ms-win-security-sddl-l1-1-0.dll
\Windows\system32\api-ms-win-security-sddlparsecond-l1-1-0.dll
\Windows\system32\api-ms-win-service-core-l1-1-1.dll
\Windows\system32\api-ms-win-service-management-l1-1-0.dll

\Windows\system32\api-ms-win-service-management-l2-1-0.dll
\Windows\system32\api-ms-win-service-winsvc-l1-1-0.dll
\Windows\system32\api-ms-win-service-winsvc-l1-2-0.dll
\Windows\system32\api-ms-win-shcore-comhelpers-l1-1-0.dll
\Windows\system32\api-ms-win-shcore-obsolete-l1-1-0.dll
\Windows\system32\api-ms-win-shcore-registry-l1-1-1.dll
\Windows\system32\api-ms-win-shcore-scaling-l1-1-1.dll
\Windows\system32\api-ms-win-shcore-stream-l1-1-0.dll
\Windows\system32\api-ms-win-shcore-stream-winrt-l1-1-0.dll
\Windows\system32\api-ms-win-shcore-sysinfo-l1-1-0.dll
\Windows\system32\api-ms-win-shcore-thread-l1-1-0.dll
\Windows\system32\api-ms-win-shcore-unicodeansi-l1-1-0.dll
\Windows\system32\api-ms-win-shell-shellcom-l1-1-0.dll
\Windows\system32\api-ms-win-shell-shellfolders-l1-1-0.dll
\Windows\system32\apphelp.dll
\Windows\system32\apprepapi.dll
\Windows\system32\AppxAllUserStore.dll
\Windows\system32\authz.dll
\Windows\system32\BCP47Langs.dll
\Windows\system32\bcrypt.dll
\Windows\system32\bcryptprimitives.dll
\Windows\system32\BOOTVID.dll
\Windows\system32\browcli.dll
\Windows\system32\cabinet.dll
\Windows\system32\certca.dll
\Windows\system32\cfgmgr32.dll
\Windows\system32\chartv.dll
\Windows\system32\CI.dll
\Windows\system32\clbcatq.dll
\Windows\system32\combase.dll
\Windows\system32\combase.dll
\Windows\system32\comctl32.dll
\Windows\system32\comdlg32.dll
\Windows\system32\credui.dll
\Windows\system32\crypt32.dll
\Windows\system32\crypt32.dll
\Windows\system32\cryptbase.dll
\Windows\system32\cryptsp.dll
\Windows\system32\cryptui.dll
\Windows\system32\cscapi.dll
\Windows\system32\csrsrv.dll
\Windows\system32\d2d1.dll
\Windows\system32\d3d11.dll

\Windows\system32\davhlpr.dll
\Windows\system32\dbgeng.dll
\Windows\system32\dbghelp.dll
\Windows\system32\dcomp.dll
\Windows\system32\devmgr.dll
\Windows\system32\devobj.dll
\Windows\system32\devrtl.dll
\Windows\system32\dfscli.dll
\Windows\system32\dhcpcsvc.dll
\Windows\system32\dhcpcsvc6.dll
\Windows\system32\difxapi.dll
\Windows\system32\dnsapi.dll
\Windows\system32\dpapi.dll
\Windows\system32\drvstore.dll
\Windows\system32\dsparse.dll
\Windows\system32\dsrole.dll
\Windows\system32\dui70.dll
\Windows\system32\duser.dll
\Windows\system32\dwmapi.dll
\Windows\system32\DWrite.dll
\Windows\system32\dxgi.dll
\Windows\system32\eappcfg.dll
\Windows\system32\efsadu.dll
\Windows\system32\efsutil.dll
\Windows\system32\ELSCore.dll
\Windows\system32\esent.dll
\Windows\system32\ext-ms-win-advapi32-eventingcontroller-l1-1-0.dll
\Windows\system32\ext-ms-win-advapi32-eventlog-l1-1-0.dll
\Windows\system32\ext-ms-win-advapi32-lsa-l1-1-0.dll
\Windows\system32\ext-ms-win-advapi32-msi-l1-1-0.dll
\Windows\SYSTEM32\ext-ms-win-advapi32-ntmarta-l1-1-0.dll
\Windows\system32\ext-ms-win-advapi32-psm-app-l1-1-0.dll
\Windows\system32\ext-ms-win-advapi32-registry-l1-1-0.dll
\Windows\system32\ext-ms-win-advapi32-safer-l1-1-0.dll
\Windows\system32\ext-ms-win-advapi32-shutdown-l1-1-0.dll
\Windows\system32\ext-ms-win-appxdeploymentclient-appxdeploy-l1-1-0.dll
\Windows\system32\ext-ms-win-authz-context-l1-1-0.dll
\Windows\system32\ext-ms-win-authz-remote-l1-1-0.dll
\Windows\system32\ext-ms-win-branding-winbrand-l1-1-0.dll
\Windows\system32\ext-ms-win-cmd-util-l1-1-0.dll
\Windows\system32\ext-ms-win-com-clbcatq-l1-1-0.dll
\Windows\system32\ext-ms-win-com-ole32-l1-1-1.dll
\Windows\system32\ext-ms-win-com-psmregister-l1-1-0.dll

\Windows\system32\ext-ms-win-domainjoin-netjoin-l1-1-0.dll
\Windows\system32\ext-ms-win-firewallapi-webproxy-l1-1-0.dll
\Windows\system32\ext-ms-win-fs-clfs-l1-1-0.dll
\Windows\system32\ext-ms-win-gdi-dc-create-l1-1-1.dll
\Windows\system32\ext-ms-win-gdi-dc-l1-2-0.dll
\Windows\system32\ext-ms-win-gdi-draw-l1-1-1.dll
\Windows\system32\ext-ms-win-gdi-font-l1-1-1.dll
\Windows\system32\ext-ms-win-gdi-metafile-l1-1-1.dll
\Windows\system32\ext-ms-win-gdi-path-l1-1-0.dll
\Windows\system32\ext-ms-win-gdi-render-l1-1-0.dll
\Windows\system32\ext-ms-win-globalization-input-l1-1-0.dll
\Windows\system32\ext-ms-win-gpapi-grouppolicy-l1-1-0.dll
\Windows\system32\ext-ms-win-gui-uxinit-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-appcompat-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-datetime-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-errorhandling-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-file-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-localization-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-package-current-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-package-l1-1-1.dll
\Windows\system32\ext-ms-win-kernel32-quirks-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-registry-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-sidebyside-l1-1-0.dll
\Windows\system32\ext-ms-win-kernel32-windowserrorreporting-l1-1-0.dll
\Windows\system32\ext-ms-win-kernelbase-processthread-l1-1-0.dll
\Windows\system32\ext-ms-win-mpr-multipleproviderrouter-l1-1-0.dll
\Windows\system32\ext-ms-win-mrmcorer-environment-l1-1-0.dll
\Windows\system32\ext-ms-win-MrmCoreR-ResManager-l1-1-0.dll
\Windows\system32\ext-ms-win-ntdsapi-activedirectoryclient-l1-1-0.dll
\Windows\system32\ext-ms-win-ntos-kcminitcfg-l1-1-0.dll
\Windows\system32\ext-ms-win-ntos-ksecurity-l1-1-1.dll
\Windows\system32\ext-ms-win-ntos-ksigningpolicy-l1-1-0.dll
\Windows\system32\ext-ms-win-ntos-ksr-l1-1-0.dll
\Windows\system32\ext-ms-win-ntos-pico-l1-1-0.dll
\Windows\system32\ext-ms-win-ntos-tm-l1-1-0.dll
\Windows\system32\ext-ms-win-ntos-werkernel-l1-1-0.dll
\Windows\system32\ext-ms-win-ntuser-dialogbox-l1-1-1.dll
\Windows\system32\ext-ms-win-ntuser-draw-l1-1-0.dll
\Windows\system32\ext-ms-win-ntuser-gui-l1-1-1.dll
\Windows\system32\ext-ms-win-ntuser-keyboard-l1-1-1.dll
\Windows\system32\ext-ms-win-ntuser-message-l1-1-1.dll
\Windows\system32\ext-ms-win-ntuser-misc-l1-2-0.dll
\Windows\system32\ext-ms-win-ntuser-mouse-l1-1-0.dll

\Windows\system32\ext-ms-win-ntuser-private-l1-1-1.dll
\Windows\system32\ext-ms-win-ntuser-rectangle-ext-l1-1-0.dll
\Windows\system32\ext-ms-win-ntuser-rotationmanager-l1-1-0.dll
\Windows\system32\ext-ms-win-ntuser-string-l1-1-0.dll
\Windows\system32\ext-ms-win-ntuser-synch-l1-1-0.dll
\Windows\system32\ext-ms-win-ntuser-windowclass-l1-1-1.dll
\Windows\system32\ext-ms-win-ntuser-window-l1-1-1.dll
\Windows\system32\ext-ms-win-ntuser-windowstation-l1-1-1.dll
\Windows\system32\ext-ms-win-ole32-bindctx-l1-1-0.dll
\Windows\system32\ext-ms-win-ole32-oleautomation-l1-1-0.dll
\Windows\system32\ext-ms-win-oleacc-l1-1-0.dll
\Windows\system32\ext-ms-win-profile-userenv-l1-1-0.dll
\Windows\system32\ext-ms-win-rtcore-gdi-devcaps-l1-1-0.dll
\Windows\system32\ext-ms-win-rtcore-gdi-object-l1-1-0.dll
\Windows\system32\ext-ms-win-rtcore-gdi-rgn-l1-1-0.dll
\Windows\system32\ext-ms-win-rtcore-ntuser-dc-access-l1-1-0.dll
\Windows\system32\ext-ms-win-rtcore-ntuser-dpi-l1-1-0.dll
\Windows\system32\ext-ms-win-rtcore-ntuser-sysparams-l1-1-0.dll
\Windows\system32\ext-ms-win-security-credui-l1-1-0.dll
\Windows\system32\ext-ms-win-session-userinit-l1-1-0.dll
\Windows\system32\ext-ms-win-session-winlogon-l1-1-0.dll
\Windows\system32\ext-ms-win-session-winsta-l1-1-0.dll
\Windows\system32\ext-ms-win-session-wtsapi32-l1-1-0.dll
\Windows\system32\ext-ms-win-setupApi-cfgmgr32remote-l1-1-0.dll
\Windows\system32\ext-ms-win-setupapi-inf-l1-1-0.dll
\Windows\system32\ext-ms-win-shell32-shellcom-l1-1-0.dll
\Windows\system32\ext-ms-win-shell32-shellfolders-l1-1-0.dll
\Windows\system32\ext-ms-win-sxs-oleautomation-l1-1-0.dll
\Windows\system32\ext-ms-win-winlogon-mincreds-l1-1-0.dll
\Windows\system32\Faultrep.dll
\Windows\system32\feclient.dll
\Windows\system32\FirewallAPI.dll
\Windows\system32\fltLib.dll
\Windows\system32\fms.dll
\Windows\system32\gdi32.dll
\Windows\system32\GdiPlus.dll
\Windows\system32\hal.dll
\Windows\system32\hid.dll
\Windows\system32\iertutil.dll
\Windows\system32\imagehlp.dll
\Windows\system32\imm32.dll
\Windows\system32\IPHLPAPI.DLL
\Windows\system32\kdcom.dll

\Windows\system32\kernel32.dll
\Windows\system32\KernelBase.dll
\Windows\system32\linkinfo.dll
\Windows\system32\logoncli.dll
\Windows\system32\lpk.dll
\Windows\system32\mcupdate_GenuineIntel.dll
\Windows\system32\mfc42u.dll
\Windows\system32\mmcbase.dll
\Windows\system32\MMDevAPI.dll
\Windows\system32\mpr.dll
\Windows\system32\mprmsg.dll
\Windows\system32\MrmCoreR.dll
\Windows\system32\msasn1.dll
\Windows\system32\msctf.dll
\Windows\system32\msiltcfg.dll
\Windows\system32\msimg32.dll
\Windows\system32\msvcrt.dll
\Windows\system32\msvcrt.dll
\Windows\system32\ncrypt.dll
\Windows\system32\netapi32.dll
\Windows\system32\netutils.dll
\Windows\system32\newdev.dll
\Windows\system32\ninput.dll
\Windows\system32\normaliz.dll
\Windows\system32\nsi.dll
\Windows\system32\ntasn1.dll
\Windows\system32\ntdll.dll
\Windows\system32\ntdsapi.dll
\Windows\system32\ntshrui.dll
\Windows\system32\odbc32.dll
\Windows\system32\ole32.dll
\Windows\system32\oleacc.dll
\Windows\system32\oleaut32.dll
\Windows\system32\oledlg.dll
\Windows\system32\pcacli.dll
\Windows\system32\pcwum.dll
\Windows\system32\powrprof.dll
\Windows\system32\printui.dll
\Windows\system32\profapi.dll
\Windows\system32\propsys.dll
\Windows\system32\psapi.dll
\Windows\system32\PSHED.dll
\Windows\system32\puiapi.dll

\Windows\system32\rasapi32.dll
\Windows\system32\rasman.dll
\Windows\system32\regapi.dll
\Windows\system32\rpcrt4.dll
\Windows\system32\RstrtMgr.dll
\Windows\system32\rtutils.dll
\Windows\system32\samcli.dll
\Windows\system32\samlib.dll
\Windows\system32\scecli.dll
\Windows\system32\sechost.dll
\Windows\system32\secur32.dll
\Windows\system32\SensApi.dll
\Windows\system32\setupapi.dll
\Windows\system32\SHCore.dll
\Windows\system32\shdocvw.dll
\Windows\system32\shell32.dll
\Windows\system32\shell32.dll
\Windows\system32\shlwapi.dll
\Windows\system32\slc.dll
\Windows\system32\spfileq.dll
\Windows\system32\SPInf.dll
\Windows\system32\sppc.dll
\Windows\system32\srvcli.dll
\Windows\system32\sspicli.dll
\Windows\system32\sspisrv.dll
\Windows\system32\tapi32.dll
\Windows\system32\tbs.dll
\Windows\system32\twinapi.appcore.dll
\Windows\system32\twinapi.dll
\Windows\system32\urlmon.dll
\Windows\system32\user32.dll
\Windows\system32\userenv.dll
\Windows\system32\UXInit.dll
\Windows\system32\uxtheme.dll
\Windows\system32\vaultcli.dll
\Windows\system32\version.dll
\Windows\system32\virtdisk.dll
\Windows\system32\vpnikeapi.dll
\Windows\system32\w32topl.dll
\Windows\system32\wcmapi.dll
\Windows\system32\webio.dll
\Windows\system32\webservices.dll
\Windows\system32\Websocket.dll

\Windows\system32\wer.dll
\Windows\system32\werui.dll
\Windows\system32\wevtapi.dll
\Windows\system32\winbrand.dll
\Windows\system32\WindowsCodecs.dll
\Windows\system32\winhttp.dll
\Windows\system32\wininet.dll
\Windows\system32\Winlangdb.dll
\Windows\system32\winmm.dll
\Windows\system32\winmmbase.dll
\Windows\system32\winnsi.dll
\Windows\system32\WinSCard.dll
\Windows\system32\winsta.dll
\Windows\system32\wintrust.dll
\Windows\system32\wkscli.dll
\Windows\system32\Wldap32.dll
\Windows\system32\wmiclnt.dll
\Windows\system32\wow64.dll
\Windows\system32\wow64cpu.dll
\Windows\system32\wow64win.dll
\Windows\system32\ws2_32.dll
\Windows\system32\wtsapi32.dll
\Windows\system32\xmllite.dll

Приложение 15. Список файлов ОС Windows Server 2016, рекомендуемых для контроля целостности при СПО «АККОРД – Win64 K»

C:\WINDOWS\SYSTEM32\ABOVELOCKAPPHOST.DLL
C:\WINDOWS\SYSTEM32\ACGINA.DLL
C:\WINDOWS\SYSTEM32\ACPBACKGROUNDMANAGERPOLICY.DLL
C:\WINDOWS\SYSTEM32\ACRUNNT.EXE
C:\WINDOWS\SYSTEM32\ACTIONCENTER.DLL
C:\WINDOWS\SYSTEM32\ACTIVATIONMANAGER.DLL
C:\WINDOWS\SYSTEM32\ACTIVEDS.DLL
C:\WINDOWS\SYSTEM32\ACTXPRXY.DLL
C:\WINDOWS\SYSTEM32\ACUSRM64.DLL
C:\WINDOWS\SYSTEM32\ADHAPI.DLL
C:\WINDOWS\SYSTEM32\ADHSVC.DLL
C:\WINDOWS\SYSTEM32\ADSLDP.DLL
C:\WINDOWS\SYSTEM32\ADSLDPC.DLL
C:\WINDOWS\SYSTEM32\ADTSCHEMA.DLL
C:\WINDOWS\SYSTEM32\ADVAPI32.DLL
C:\WINDOWS\SYSTEM32\ADVAPI32RES.DLL
C:\WINDOWS\SYSTEM32\AEEVTS.DLL
C:\WINDOWS\SYSTEM32\AEPIC.DLL
C:\WINDOWS\SYSTEM32\APPCONTRACTS.DLL
C:\WINDOWS\SYSTEM32\APPHELP.DLL
C:\WINDOWS\SYSTEM32\APPLICATIONFRAME.DLL
C:\WINDOWS\SYSTEM32\APPOINTMENTACTIVATION.DLL
C:\WINDOWS\SYSTEM32\APPVETWCLIENTRES.DLL
C:\WINDOWS\SYSTEM32\APPXALLUSERSTORE.DLL
C:\WINDOWS\SYSTEM32\APPXDEPLOYMENTSERVER.DLL
C:\WINDOWS\SYSTEM32\APPXPACKAGING.DLL
C:\WINDOWS\SYSTEM32\ATL.DLL
C:\WINDOWS\SYSTEM32\ATLTHUNK.DLL
C:\WINDOWS\SYSTEM32\ATMFD.DLL
C:\WINDOWS\SYSTEM32\AUTHBROKER.DLL
C:\WINDOWS\SYSTEM32\AUTHFWGP.DLL
C:\WINDOWS\SYSTEM32\AUTHUI.DLL
C:\WINDOWS\SYSTEM32\AUTHZ.DLL
C:\WINDOWS\SYSTEM32\AUTOCHK.EXE

C:\WINDOWS\SYSTEM32\AZROLES.DLL
C:\WINDOWS\SYSTEM32\BACKGROUNDMEDIAPOLICY.DLL
C:\WINDOWS\SYSTEM32\BASESRV.DLL
C:\WINDOWS\SYSTEM32\BATMETER.DLL
C:\WINDOWS\SYSTEM32\BCD.DLL
C:\WINDOWS\SYSTEM32\BCP47LANGS.DLL
C:\WINDOWS\SYSTEM32\BCRYPT.DLL
C:\WINDOWS\SYSTEM32\BCRYPTPRIMITIVES.DLL
C:\WINDOWS\SYSTEM32\BFE.DLL
C:\WINDOWS\SYSTEM32\BI.DLL
C:\WINDOWS\SYSTEM32\BISRV.DLL
C:\WINDOWS\SYSTEM32\BITSPERF.DLL
C:\WINDOWS\SYSTEM32\BIWINRT.DLL
C:\WINDOWS\SYSTEM32\BLBUIRES.DLL
C:\WINDOWS\SYSTEM32\BLUETOOTHAPIS.DLL
C:\WINDOWS\SYSTEM32\BOOTVID.DLL
C:\WINDOWS\SYSTEM32\BROKERLIB.DLL
C:\WINDOWS\SYSTEM32\BROWCLI.DLL
C:\WINDOWS\SYSTEM32\CABINET.DLL
C:\WINDOWS\SYSTEM32\CAPAUTHZ.DLL
C:\WINDOWS\SYSTEM32\CATSRV.DLL
C:\WINDOWS\SYSTEM32\CATSRVPS.DLL
C:\WINDOWS\SYSTEM32\CATSRVUT.DLL
C:\WINDOWS\SYSTEM32\CBTBACKGROUNDMANAGERPOLICY.DLL
C:\WINDOWS\SYSTEM32\CDP.DLL
C:\WINDOWS\SYSTEM32\CDPRT.DLL
C:\WINDOWS\SYSTEM32\CDPSVC.DLL
C:\WINDOWS\SYSTEM32\CDPUSERSVC.DLL
C:\WINDOWS\SYSTEM32\CERTCA.DLL
C:\WINDOWS\SYSTEM32\CERTENROLL.DLL
C:\WINDOWS\SYSTEM32\CERTPROP.DLL
C:\WINDOWS\SYSTEM32\CI.DLL
C:\WINDOWS\SYSTEM32\CLBCATQ.DLL
C:\WINDOWS\SYSTEM32\CLIPBOARDSERVER.DLL
C:\WINDOWS\SYSTEM32\CLIPC.DLL
C:\WINDOWS\SYSTEM32\CLIPSVC.DLL
C:\WINDOWS\SYSTEM32\CLOUDAP.DLL
C:\WINDOWS\SYSTEM32\CLUSAPI.DLL
C:\WINDOWS\SYSTEM32\CMD.EXE

C:\WINDOWS\SYSTEM32\CMDEXT.DLL
C:\WINDOWS\SYSTEM32\CMINTEGRATOR.DLL
C:\WINDOWS\SYSTEM32\COMBASE.DLL
C:\WINDOWS\SYSTEM32\COMRES.DLL
C:\WINDOWS\SYSTEM32\COMSVCS.DLL
C:\WINDOWS\SYSTEM32\CONFIGURATIONCLIENT.DLL
C:\WINDOWS\SYSTEM32\CONHOST.EXE
C:\WINDOWS\SYSTEM32\CONHOSTV2.DLL
C:\WINDOWS\SYSTEM32\CONTAINER.DLL
C:\WINDOWS\SYSTEM32\COREMESSAGING.DLL
C:\WINDOWS\SYSTEM32\COREUICOMPONENTS.DLL
C:\WINDOWS\SYSTEM32\CREDSSP.DLL
C:\WINDOWS\SYSTEM32\CRYPT32.DLL
C:\WINDOWS\SYSTEM32\CRYPTBASE.DLL
C:\WINDOWS\SYSTEM32\CRYPTCATSVC.DLL
C:\WINDOWS\SYSTEM32\CRYPTDLL.DLL
C:\WINDOWS\SYSTEM32\CRYPTNET.DLL
C:\WINDOWS\SYSTEM32\CRYPTSP.DLL
C:\WINDOWS\SYSTEM32\CRYPTSVC.DLL
C:\WINDOWS\SYSTEM32\CRYPTTPMEKSVC.DLL
C:\WINDOWS\SYSTEM32\CRYPTUI.DLL
C:\WINDOWS\SYSTEM32\CRYPTXML.DLL
C:\WINDOWS\SYSTEM32\CSCAPI.DLL
C:\WINDOWS\SYSTEM32\CSCOBJ.DLL
C:\WINDOWS\SYSTEM32\CSCSVC.DLL
C:\WINDOWS\SYSTEM32\CSCUI.DLL
C:\WINDOWS\SYSTEM32\CSRSRV.DLL
C:\WINDOWS\SYSTEM32\CSRSS.EXE
C:\WINDOWS\SYSTEM32\CSYSTEMEVENTSBROKERCLIENT.DLL
C:\WINDOWS\SYSTEM32\D2D1.DLL
C:\WINDOWS\SYSTEM32\D3D10WARP.DLL
C:\WINDOWS\SYSTEM32\D3D11.DLL
C:\WINDOWS\SYSTEM32\DAB.DLL
C:\WINDOWS\SYSTEM32\DABAPI.DLL
C:\WINDOWS\SYSTEM32\DATAEXCHANGE.DLL
C:\WINDOWS\SYSTEM32\DAXEXEC.DLL
C:\WINDOWS\SYSTEM32\DBGCORE.DLL
C:\WINDOWS\SYSTEM32\DBGHELP.DLL
C:\WINDOWS\SYSTEM32\DCOMP.DLL

C:\WINDOWS\SYSTEM32\DESKTOPSHELLEXT.DLL
C:\WINDOWS\SYSTEM32\DEVDISPITEMPROVIDER.DLL
C:\WINDOWS\SYSTEM32\DEVICEACCESS.DLL
C:\WINDOWS\SYSTEM32\DEVICEASSOCIATION.DLL
C:\WINDOWS\SYSTEM32\DEVICECREDENTIAL.DLL
C:\WINDOWS\SYSTEM32\DEVOBJ.DLL
C:\WINDOWS\SYSTEM32\DEVRTL.DLL
C:\WINDOWS\SYSTEM32\DHCPCORE.DLL
C:\WINDOWS\SYSTEM32\DHCPCORE6.DLL
C:\WINDOWS\SYSTEM32\DHCPCSVC.DLL
C:\WINDOWS\SYSTEM32\DHCPCSVC6.DLL
C:\WINDOWS\SYSTEM32\DIAGTRACK.DLL
C:\WINDOWS\SYSTEM32\DIMSJOB.DLL
C:\WINDOWS\SYSTEM32\DIRECTMANIPULATION.DLL
C:\WINDOWS\SYSTEM32\DLLHOST.EXE
C:\WINDOWS\SYSTEM32\DMCMNUTILS.DLL
C:\WINDOWS\SYSTEM32\DNSAPI.DLL
C:\WINDOWS\SYSTEM32\DNSEXT.DLL
C:\WINDOWS\SYSTEM32\DNSRSLVR.DLL
C:\WINDOWS\SYSTEM32\DPAPI.DLL
C:\WINDOWS\SYSTEM32\DPAPISRV.DLL
C:\WINDOWS\SYSTEM32\DRIVERS\UMDF\SENSORSCX.DLL
C:\WINDOWS\SYSTEM32\DRIVERS\UMDF\SENSORSHID.DLL
C:\WINDOWS\SYSTEM32\DRPROV.DLL
C:\WINDOWS\SYSTEM32\DRVSTORE.DLL
C:\WINDOWS\SYSTEM32\DSCLIENT.DLL
C:\WINDOWS\SYSTEM32\DSREG.DLL
C:\WINDOWS\SYSTEM32\DSROLE.DLL
C:\WINDOWS\SYSTEM32\DSSENH.DLL
C:\WINDOWS\SYSTEM32\DUSER.DLL
C:\WINDOWS\SYSTEM32\DWMAPI.DLL
C:\WINDOWS\SYSTEM32\DWRITE.DLL
C:\WINDOWS\SYSTEM32\DXGI.DLL
C:\WINDOWS\SYSTEM32\DXP.DLL
C:\WINDOWS\SYSTEM32\EDITBUFFERTESTHOOK.DLL
C:\WINDOWS\SYSTEM32\EDPUTIL.DLL
C:\WINDOWS\SYSTEM32\EFSLSAEXT.DLL
C:\WINDOWS\SYSTEM32\EHSTORSHELL.DLL
C:\WINDOWS\SYSTEM32\EMBEDDEDMODESVCAPI.DLL

C:\WINDOWS\SYSTEM32\EQOSSNAP.DLL
C:\WINDOWS\SYSTEM32\ES.DLL
C:\WINDOWS\SYSTEM32\ESENT.DLL
C:\WINDOWS\SYSTEM32\ESENTPRF.DLL
C:\WINDOWS\SYSTEM32\ETHERNETMEDIAMANAGER.DLL
C:\WINDOWS\SYSTEM32\EVENTAGGREGATION.DLL
C:\WINDOWS\SYSTEM32\EXECMODELCLIENT.DLL
C:\WINDOWS\SYSTEM32\EXECMODELPROXY.DLL
C:\WINDOWS\SYSTEM32\EXPLORERFRAME.DLL
C:\WINDOWS\SYSTEM32\FDPNP.DLL
C:\WINDOWS\SYSTEM32\FILEMGMT.DLL
C:\WINDOWS\SYSTEM32\FIREWALLAPI.DLL
C:\WINDOWS\SYSTEM32\FLIGHTSETTINGS.DLL
C:\WINDOWS\SYSTEM32\FLTLIB.DLL
C:\WINDOWS\SYSTEM32\FNTCACHE.DLL
C:\WINDOWS\SYSTEM32\FONTGROUPSOVERRIDE.DLL
C:\WINDOWS\SYSTEM32\FONTSUB.DLL
C:\WINDOWS\SYSTEM32\FRAMEDYNOS.DLL
C:\WINDOWS\SYSTEM32\FUNDISC.DLL
C:\WINDOWS\SYSTEM32\FWBASE.DLL
C:\WINDOWS\SYSTEM32\FWPOLICYIOMGR.DLL
C:\WINDOWS\SYSTEM32\FWPUCLNT.DLL
C:\WINDOWS\SYSTEM32\GAMEUX.DLL
C:\WINDOWS\SYSTEM32\GDI32.DLL
C:\WINDOWS\SYSTEM32\GDI32FULL.DLL
C:\WINDOWS\SYSTEM32\GLOBINPUTHOST.DLL
C:\WINDOWS\SYSTEM32\GMSACLIENT.DLL
C:\WINDOWS\SYSTEM32\GPAPI.DLL
C:\WINDOWS\SYSTEM32\GPSVC.DLL
C:\WINDOWS\SYSTEM32\HAL.DLL
C:\WINDOWS\SYSTEM32\HGCPL.DLL
C:\WINDOWS\SYSTEM32\HID.DLL
C:\WINDOWS\SYSTEM32\HNETCFGCLIENT.DLL
C:\WINDOWS\SYSTEM32\HTTPAPI.DLL
C:\WINDOWS\SYSTEM32\HTTPPRXC.DLL
C:\WINDOWS\SYSTEM32\HTTPPRXM.DLL
C:\WINDOWS\SYSTEM32\HVHOSTSVC.DLL
C:\WINDOWS\SYSTEM32\ICMP.DLL
C:\WINDOWS\SYSTEM32\ICSVC.DLL

C:\WINDOWS\SYSTEM32\IDSTORE.DLL
C:\WINDOWS\SYSTEM32\IEFRAME.DLL
C:\WINDOWS\SYSTEM32\IEPROXY.DLL
C:\WINDOWS\SYSTEM32\IERTUTIL.DLL
C:\WINDOWS\SYSTEM32\IESETUP.DLL
C:\WINDOWS\SYSTEM32\IMAGERES.DLL
C:\WINDOWS\SYSTEM32\IMAPI2.DLL
C:\WINDOWS\SYSTEM32\IMM32.DLL
C:\WINDOWS\SYSTEM32\IMPLATSETUP.DLL
C:\WINDOWS\SYSTEM32\INPUT.DLL
C:\WINDOWS\SYSTEM32\INPUTLOCALEMANAGER.DLL
C:\WINDOWS\SYSTEM32\INPUTSERVICE.DLL
C:\WINDOWS\SYSTEM32\INPUTSWITCH.DLL
C:\WINDOWS\SYSTEM32\IPHLPAPI.DLL
C:\WINDOWS\SYSTEM32\IPHLPSVC.DLL
C:\WINDOWS\SYSTEM32\ISCSICPL.DLL
C:\WINDOWS\SYSTEM32\JOINUTIL.DLL
C:\WINDOWS\SYSTEM32\KBDRU.DLL
C:\WINDOWS\SYSTEM32\KBDUS.DLL
C:\WINDOWS\SYSTEM32\KD.DLL
C:\WINDOWS\SYSTEM32\KEEPALIVEPROVIDER.DLL
C:\WINDOWS\SYSTEM32\KERBCLIENTSHARED.DLL
C:\WINDOWS\SYSTEM32\KERBEROS.DLL
C:\WINDOWS\SYSTEM32\KERNEL.APPCORE.DLL
C:\WINDOWS\SYSTEM32\KERNEL32.DLL
C:\WINDOWS\SYSTEM32\KERNELBASE.DLL
C:\WINDOWS\SYSTEM32\KPSSVC.DLL
C:\WINDOWS\SYSTEM32\KTMW32.DLL
C:\WINDOWS\SYSTEM32\LICENSEMANAGER.DLL
C:\WINDOWS\SYSTEM32\LICENSEMANAGERAPI.DLL
C:\WINDOWS\SYSTEM32\LICENSEMANAGERSVC.DLL
C:\WINDOWS\SYSTEM32\LINKINFO.DLL
C:\WINDOWS\SYSTEM32\LMHSVC.DLL
C:\WINDOWS\SYSTEM32\LOADPERF.DLL
C:\WINDOWS\SYSTEM32\LOCALSPL.DLL
C:\WINDOWS\SYSTEM32\LOGONCLI.DLL
C:\WINDOWS\SYSTEM32\LSASRV.DLL
C:\WINDOWS\SYSTEM32\LSASS.EXE
C:\WINDOWS\SYSTEM32\LSM.DLL

C:\WINDOWS\SYSTEM32\LSMPROXY.DLL
C:\WINDOWS\SYSTEM32\MCUPDATE_GENUINEINTEL.DLL
C:\WINDOWS\SYSTEM32\MFCSUBS.DLL
C:\WINDOWS\SYSTEM32\MFPLAT.DLL
C:\WINDOWS\SYSTEM32\MFSENSORGROUP.DLL
C:\WINDOWS\SYSTEM32\MI.DLL
C:\WINDOWS\SYSTEM32\MICROSOFT-WINDOWS-KERNEL-PNP-EVENTS.DLL
C:\WINDOWS\SYSTEM32\MICROSOFT-WINDOWS-KERNEL-POWER-EVENTS.DLL
C:\WINDOWS\SYSTEM32\MICROSOFT-WINDOWS-KERNEL-PROCESSOR-POWER-EVENTS.DLL
C:\WINDOWS\SYSTEM32\MICROSOFT-WINDOWS-SYSTEM-EVENTS.DLL
C:\WINDOWS\SYSTEM32\MICROSOFTACCOUNTCLOUDAP.DLL
C:\WINDOWS\SYSTEM32\MIGUIRESOURCE.DLL
C:\WINDOWS\SYSTEM32\MINTDH.DLL
C:\WINDOWS\SYSTEM32\MIUTILS.DLL
C:\WINDOWS\SYSTEM32\MMDEVAPI.DLL
C:\WINDOWS\SYSTEM32\MOBSYNC.EXE
C:\WINDOWS\SYSTEM32\MODERNEXECSERVER.DLL
C:\WINDOWS\SYSTEM32\MPR.DLL
C:\WINDOWS\SYSTEM32\MPRDDM.DLL
C:\WINDOWS\SYSTEM32\MPREXT.DLL
C:\WINDOWS\SYSTEM32\MPSSVC.DLL
C:\WINDOWS\SYSTEM32\MRMCORER.DLL
C:\WINDOWS\SYSTEM32\MSASN1.DLL
C:\WINDOWS\SYSTEM32\MSAUSEREXT.DLL
C:\WINDOWS\SYSTEM32\MSCOREE.DLL
C:\WINDOWS\SYSTEM32\MSCTFMONITOR.DLL
C:\WINDOWS\SYSTEM32\MSDTC.EXE
C:\WINDOWS\SYSTEM32\MSDTCLOG.DLL
C:\WINDOWS\SYSTEM32\MSDTCPRX.DLL
C:\WINDOWS\SYSTEM32\MSDTCTM.DLL
C:\WINDOWS\SYSTEM32\MSDTCUIU.DLL
C:\WINDOWS\SYSTEM32\MSDTCVSP1RES.DLL
C:\WINDOWS\SYSTEM32\MSFTEDIT.DLL
C:\WINDOWS\SYSTEM32\MSHTML.DLL
C:\WINDOWS\SYSTEM32\MSIMG32.DLL
C:\WINDOWS\SYSTEM32\MSKEYPROTECT.DLL
C:\WINDOWS\SYSTEM32\MSPRIVS.DLL
C:\WINDOWS\SYSTEM32\MSSCNTRS.DLL
C:\WINDOWS\SYSTEM32\MSTASK.DLL

C:\WINDOWS\SYSTEM32\MSUTB.DLL
C:\WINDOWS\SYSTEM32\MSV1_0.DLL
C:\WINDOWS\SYSTEM32\MSVCP110_WIN.DLL
C:\WINDOWS\SYSTEM32\MSVCP_WIN.DLL
C:\WINDOWS\SYSTEM32\MSVCR120_CLR0400.DLL
C:\WINDOWS\SYSTEM32\MSVCRT.DLL
C:\WINDOWS\SYSTEM32\MSWB7.DLL
C:\WINDOWS\SYSTEM32\MSWSOCK.DLL
C:\WINDOWS\SYSTEM32\MSXML3.DLL
C:\WINDOWS\SYSTEM32\MSXML3R.DLL
C:\WINDOWS\SYSTEM32\MSXML6.DLL
C:\WINDOWS\SYSTEM32\MSXML6R.DLL
C:\WINDOWS\SYSTEM32\MTFSERVER.DLL
C:\WINDOWS\SYSTEM32\MTXCLU.DLL
C:\WINDOWS\SYSTEM32\MTXOCI.DLL
C:\WINDOWS\SYSTEM32\MUSNOTIFICATION.EXE
C:\WINDOWS\SYSTEM32\MYCOMPUT.DLL
C:\WINDOWS\SYSTEM32\NAPINSP.DLL
C:\WINDOWS\SYSTEM32\NCBSERVICE.DLL
C:\WINDOWS\SYSTEM32\NCI.DLL
C:\WINDOWS\SYSTEM32\NCOBJAPI.DLL
C:\WINDOWS\SYSTEM32\NCRYPT.DLL
C:\WINDOWS\SYSTEM32\NCRYPTPROV.DLL
C:\WINDOWS\SYSTEM32\NCRYPTSSLP.DLL
C:\WINDOWS\SYSTEM32\NCSI.DLL
C:\WINDOWS\SYSTEM32\NEGOEXTS.DLL
C:\WINDOWS\SYSTEM32\NETAPI32.DLL
C:\WINDOWS\SYSTEM32\NETFXPERF.DLL
C:\WINDOWS\SYSTEM32\NETJOIN.DLL
C:\WINDOWS\SYSTEM32\NETLOGON.DLL
C:\WINDOWS\SYSTEM32\NETMSG.DLL
C:\WINDOWS\SYSTEM32\NETPROFM.DLL
C:\WINDOWS\SYSTEM32\NETPROFMSVC.DLL
C:\WINDOWS\SYSTEM32\NETPROVFW.DLL
C:\WINDOWS\SYSTEM32\NETSETUPAPI.DLL
C:\WINDOWS\SYSTEM32\NETSETUPENGINE.DLL
C:\WINDOWS\SYSTEM32\NETSETUPSHIM.DLL
C:\WINDOWS\SYSTEM32\NETSETUPSVC.DLL
C:\WINDOWS\SYSTEM32\NETUTILS.DLL

C:\WINDOWS\SYSTEM32\NETWORKUXBROKER.DLL
C:\WINDOWS\SYSTEM32\NGCCTNR.DLL
C:\WINDOWS\SYSTEM32\NGCCTNRGIDSHANDLER.DLL
C:\WINDOWS\SYSTEM32\NGCCTNRSVC.DLL
C:\WINDOWS\SYSTEM32\NGCSVC.DLL
C:\WINDOWS\SYSTEM32\NINPUT.DLL
C:\WINDOWS\SYSTEM32\NLAAPI.DLL
C:\WINDOWS\SYSTEM32\NLASVC.DLL
C:\WINDOWS\SYSTEM32\NOTIFICATIONCONTROLLER.DLL
C:\WINDOWS\SYSTEM32\NOTIFICATIONCONTROLLERPS.DLL
C:\WINDOWS\SYSTEM32\NOTIFICATIONOBJFACTORY.DLL
C:\WINDOWS\SYSTEM32\NOTIFICATIONPLATFORMCOMPONENT.DLL
C:\WINDOWS\SYSTEM32\NPMPROXY.DLL
C:\WINDOWS\SYSTEM32\NPSM.DLL
C:\WINDOWS\SYSTEM32\NRPSRV.DLL
C:\WINDOWS\SYSTEM32\NSISVC.DLL
C:\WINDOWS\SYSTEM32\NTASN1.DLL
C:\WINDOWS\SYSTEM32\NTDLL.DLL
C:\WINDOWS\SYSTEM32\NTLANMAN.DLL
C:\WINDOWS\SYSTEM32\NTLMSHARED.DLL
C:\WINDOWS\SYSTEM32\NTMARTA.DLL
C:\WINDOWS\SYSTEM32\NTSHRUI.DLL
C:\WINDOWS\SYSTEM32\ODBC32.DLL
C:\WINDOWS\SYSTEM32\ODBCINT.DLL
C:\WINDOWS\SYSTEM32\OLE32.DLL
C:\WINDOWS\SYSTEM32\OLEACC.DLL
C:\WINDOWS\SYSTEM32\OLEACCRC.DLL
C:\WINDOWS\SYSTEM32\OLEAUT32.DLL
C:\WINDOWS\SYSTEM32\ONDEMANDCONNROUTEHELPER.DLL
C:\WINDOWS\SYSTEM32\ONECORECOMMONPROXYSTUB.DLL
C:\WINDOWS\SYSTEM32\ONECOREUAPCOMMONPROXYSTUB.DLL
C:\WINDOWS\SYSTEM32\OPCSERVICES.DLL
C:\WINDOWS\SYSTEM32\OSCIAPI.DLL
C:\WINDOWS\SYSTEM32\PAUTOENR.DLL
C:\WINDOWS\SYSTEM32\PCACLI.DLL
C:\WINDOWS\SYSTEM32\PCAEVTS.DLL
C:\WINDOWS\SYSTEM32\PCASVC.DLL
C:\WINDOWS\SYSTEM32\PCPKSP.DLL
C:\WINDOWS\SYSTEM32\PCPTPM12.DLL

C:\WINDOWS\SYSTEM32\PCWUM.DLL
C:\WINDOWS\SYSTEM32\PDH.DLL
C:\WINDOWS\SYSTEM32\PEERDISTSH.DLL
C:\WINDOWS\SYSTEM32\PERFCTRS.DLL
C:\WINDOWS\SYSTEM32\PERFDISK.DLL
C:\WINDOWS\SYSTEM32\PERFNET.DLL
C:\WINDOWS\SYSTEM32\PERFOS.DLL
C:\WINDOWS\SYSTEM32\PERFPROC.DLL
C:\WINDOWS\SYSTEM32\PERFTS.DLL
C:\WINDOWS\SYSTEM32\PERSONAX.DLL
C:\WINDOWS\SYSTEM32\PHOTOMETADATAHANDLER.DLL
C:\WINDOWS\SYSTEM32\PKU2U.DLL
C:\WINDOWS\SYSTEM32\PMCSNAP.DLL
C:\WINDOWS\SYSTEM32\PNIDUI.DLL
C:\WINDOWS\SYSTEM32\POLICYMANAGER.DLL
C:\WINDOWS\SYSTEM32\PORTABLEDEVICEAPI.DLL
C:\WINDOWS\SYSTEM32\PORTABLEDEVICECONNECTAPI.DLL
C:\WINDOWS\SYSTEM32\PORTABLEDEVICETYPES.DLL
C:\WINDOWS\SYSTEM32\PRINTISOLATIONPROXY.DLL
C:\WINDOWS\SYSTEM32\PRM0019.DLL
C:\WINDOWS\SYSTEM32\PRNFLDR.DLL
C:\WINDOWS\SYSTEM32\PROFEXT.DLL
C:\WINDOWS\SYSTEM32\PROFSVC.DLL
C:\WINDOWS\SYSTEM32\PROFSVCEXT.DLL
C:\WINDOWS\SYSTEM32\PROPSYS.DLL
C:\WINDOWS\SYSTEM32\PROVTHRD.DLL
C:\WINDOWS\SYSTEM32\PROXIMITYCOMMON.DLL
C:\WINDOWS\SYSTEM32\PROXIMITYCOMMONPAL.DLL
C:\WINDOWS\SYSTEM32\PROXIMITYSERVICE.DLL
C:\WINDOWS\SYSTEM32\PROXIMITYSERVICEPAL.DLL
C:\WINDOWS\SYSTEM32\PSHED.DLL
C:\WINDOWS\SYSTEM32\PSMSERVICEEXTHOST.DLL
C:\WINDOWS\SYSTEM32\PSMSRV.DLL
C:\WINDOWS\SYSTEM32\PWRSHPLUGIN.DLL
C:\WINDOWS\SYSTEM32\QUICKACTIONSDATAMODEL.DLL
C:\WINDOWS\SYSTEM32\RASADHLP.DLL
C:\WINDOWS\SYSTEM32\RASCTRS.DLL
C:\WINDOWS\SYSTEM32\RASMAN.DLL
C:\WINDOWS\SYSTEM32\RASSFM.DLL

C:\WINDOWS\SYSTEM32\RDPCORETS.DLL
C:\WINDOWS\SYSTEM32\REAGENT.DLL
C:\WINDOWS\SYSTEM32\REG.EXE
C:\WINDOWS\SYSTEM32\REGAPI.DLL
C:\WINDOWS\SYSTEM32\REGSVC.DLL
C:\WINDOWS\SYSTEM32\RESOURCEPOLICYCLIENT.DLL
C:\WINDOWS\SYSTEM32\RESOURCEPOLICYSERVER.DLL
C:\WINDOWS\SYSTEM32\RESUTILS.DLL
C:\WINDOWS\SYSTEM32\RFXVMT.DLL
C:\WINDOWS\SYSTEM32\RMCLIENT.DLL
C:\WINDOWS\SYSTEM32\ROTMGR.DLL
C:\WINDOWS\SYSTEM32\RPCEPMAP.DLL
C:\WINDOWS\SYSTEM32\RPCRT4.DLL
C:\WINDOWS\SYSTEM32\RPCRTREMOTE.DLL
C:\WINDOWS\SYSTEM32\RPCSS.DLL
C:\WINDOWS\SYSTEM32\RSAENH.DLL
C:\WINDOWS\SYSTEM32\RSTRTMGR.DLL
C:\WINDOWS\SYSTEM32\RTMEDIAFRAME.DLL
C:\WINDOWS\SYSTEM32\RTUTILS.DLL
C:\WINDOWS\SYSTEM32\RTWORKQ.DLL
C:\WINDOWS\SYSTEM32\RUNTIMEBROKER.EXE
C:\WINDOWS\SYSTEM32\SAMCLI.DLL
C:\WINDOWS\SYSTEM32\SAMLIB.DLL
C:\WINDOWS\SYSTEM32\SAMSRV.DLL
C:\WINDOWS\SYSTEM32\SBSERVICETRIGGER.DLL
C:\WINDOWS\SYSTEM32\SCARDBI.DLL
C:\WINDOWS\SYSTEM32\SCARDSVR.DLL
C:\WINDOWS\SYSTEM32\SCDEVICEENUM.DLL
C:\WINDOWS\SYSTEM32\SCECLI.DLL
C:\WINDOWS\SYSTEM32\SCESRV.DLL
C:\WINDOWS\SYSTEM32\SCHANNEL.DLL
C:\WINDOWS\SYSTEM32\SCHEDCLI.DLL
C:\WINDOWS\SYSTEM32\SCHEDSVC.DLL
C:\WINDOWS\SYSTEM32\SDCLIENT.DLL
C:\WINDOWS\SYSTEM32\SEBBACKGROUNDMANAGERPOLICY.DLL
C:\WINDOWS\SYSTEM32\SECHOST.DLL
C:\WINDOWS\SYSTEM32\SECUR32.DLL
C:\WINDOWS\SYSTEM32\SECURETIMEAGGREGATOR.DLL
C:\WINDOWS\SYSTEM32\SECURITY.DLL

C:\WINDOWS\SYSTEM32\SENS.DLL
C:\WINDOWS\SYSTEM32\SENSORSAPI.DLL
C:\WINDOWS\SYSTEM32\SENSORSERVICE.DLL
C:\WINDOWS\SYSTEM32\SENSORSNATIVEAPI.DLL
C:\WINDOWS\SYSTEM32\SENSORSNATIVEAPI.V2.DLL
C:\WINDOWS\SYSTEM32\SENSORSUTILSV2.DLL
C:\WINDOWS\SYSTEM32\SENSRSVC.DLL
C:\WINDOWS\SYSTEM32\SERVERMANAGER.EXE
C:\WINDOWS\SYSTEM32\SERVERMANAGERLAUNCHER.EXE
C:\WINDOWS\SYSTEM32\SERVICES.EXE
C:\WINDOWS\SYSTEM32\SESSENV.DLL
C:\WINDOWS\SYSTEM32\SETTINGMONITOR.DLL
C:\WINDOWS\SYSTEM32\SETTINGSYNC.DLL
C:\WINDOWS\SYSTEM32\SETTINGSYNCCORE.DLL
C:\WINDOWS\SYSTEM32\SETTINGSYNCPOLICY.DLL
C:\WINDOWS\SYSTEM32\SFC_OS.DLL
C:\WINDOWS\SYSTEM32\SHACCTPROFILE.DLL
C:\WINDOWS\SYSTEM32\SHAREDSTARTMODEL.DLL
C:\WINDOWS\SYSTEM32\SHAREHOST.DLL
C:\WINDOWS\SYSTEM32\SHDOCVW.DLL
C:\WINDOWS\SYSTEM32\SHELL32.DLL
C:\WINDOWS\SYSTEM32\SHFOLDER.DLL
C:\WINDOWS\SYSTEM32\SHLWAPI.DLL
C:\WINDOWS\SYSTEM32\SHPSETUP.DLL
C:\WINDOWS\SYSTEM32\SHSVCS.DLL
C:\WINDOWS\SYSTEM32\SIHOST.EXE
C:\WINDOWS\SYSTEM32\SLC.DLL
C:\WINDOWS\SYSTEM32\SLUI.EXE
C:\WINDOWS\SYSTEM32\SLWGA.DLL
C:\WINDOWS\SYSTEM32\SMARTCARDBACKGROUNDPOLICY.DLL
C:\WINDOWS\SYSTEM32\SMSS.EXE
C:\WINDOWS\SYSTEM32\SNDVOLSSO.DLL
C:\WINDOWS\SYSTEM32\SNMPAPI.DLL
C:\WINDOWS\SYSTEM32\SPEECH_ONECORE\COMMON\SAPI_ONECORE.DLL
C:\WINDOWS\SYSTEM32\SPINF.DLL
C:\WINDOWS\SYSTEM32\SPOOLSS.DLL
C:\WINDOWS\SYSTEM32\SPOOLSV.EXE
C:\WINDOWS\SYSTEM32\SPOOL\PRTPROCS\X64\TPWINPRN.DLL
C:\WINDOWS\SYSTEM32\SPOOL\PRTPROCS\X64\WINPRINT.DLL

C:\WINDOWS\SYSTEM32\SPPC.DLL
C:\WINDOWS\SYSTEM32\SPPCEXT.DLL
C:\WINDOWS\SYSTEM32\SPPCOMAPI.DLL
C:\WINDOWS\SYSTEM32\SPPEXTCOMOBJ.EXE
C:\WINDOWS\SYSTEM32\SPPOBJS.DLL
C:\WINDOWS\SYSTEM32\SPPSVC.EXE
C:\WINDOWS\SYSTEM32\SPPWINOB.DLL
C:\WINDOWS\SYSTEM32\SQMAPI.DLL
C:\WINDOWS\SYSTEM32\SRCHADMIN.DLL
C:\WINDOWS\SYSTEM32\SRVCLI.DLL
C:\WINDOWS\SYSTEM32\SRVSVC.DLL
C:\WINDOWS\SYSTEM32\SSCORE.DLL
C:\WINDOWS\SYSTEM32\SSCOREEXT.DLL
C:\WINDOWS\SYSTEM32\SSDPAPI.DLL
C:\WINDOWS\SYSTEM32\SSPICLI.DLL
C:\WINDOWS\SYSTEM32\SSPISRV.DLL
C:\WINDOWS\SYSTEM32\SSTPSVC.DLL
C:\WINDOWS\SYSTEM32\STATEREPOSITORY.CORE.DLL
C:\WINDOWS\SYSTEM32\STOBJECT.DLL
C:\WINDOWS\SYSTEM32\STRUCTUREDQUERY.DLL
C:\WINDOWS\SYSTEM32\SVCHOST.EXE
C:\WINDOWS\SYSTEM32\SVRMGRNC.DLL
C:\WINDOWS\SYSTEM32\SXS.DLL
C:\WINDOWS\SYSTEM32\SXSSRV.DLL
C:\WINDOWS\SYSTEM32\SYNCCENTER.DLL
C:\WINDOWS\SYSTEM32\SYNCINFRASTRUCTURE.DLL
C:\WINDOWS\SYSTEM32\SYNCREG.DLL
C:\WINDOWS\SYSTEM32\SYSNTFY.DLL
C:\WINDOWS\SYSTEM32\SYSTEMEVENTSBROKERCLIENT.DLL
C:\WINDOWS\SYSTEM32\SYSTEMEVENTSBROKERSERVER.DLL
C:\WINDOWS\SYSTEM32\TAPIPERF.DLL
C:\WINDOWS\SYSTEM32\TASKBARCPL.DLL
C:\WINDOWS\SYSTEM32\TASKCOMP.DLL
C:\WINDOWS\SYSTEM32\TASKHOSTW.EXE
C:\WINDOWS\SYSTEM32\TASKSCHD.DLL
C:\WINDOWS\SYSTEM32\TBS.DLL
C:\WINDOWS\SYSTEM32\TCPIPCFG.DLL
C:\WINDOWS\SYSTEM32\TCPMON.DLL
C:\WINDOWS\SYSTEM32\TDH.DLL

C:\WINDOWS\SYSTEM32\TERMSRV.DLL
C:\WINDOWS\SYSTEM32\TEXTINPUTFRAMEWORK.DLL
C:\WINDOWS\SYSTEM32\THEMESERVICE.DLL
C:\WINDOWS\SYSTEM32\THEMEUI.DLL
C:\WINDOWS\SYSTEM32\THREADPOOLWINRT.DLL
C:\WINDOWS\SYSTEM32\THUMBCACHE.DLL
C:\WINDOWS\SYSTEM32\TILEOBJSERVER.DLL
C:\WINDOWS\SYSTEM32\TIMEBROKERCLIENT.DLL
C:\WINDOWS\SYSTEM32\TIMEBROKERSERVER.DLL
C:\WINDOWS\SYSTEM32\TLSCSP.DLL
C:\WINDOWS\SYSTEM32\TMATT64.DLL
C:\WINDOWS\SYSTEM32\TMDRV64.DLL
C:\WINDOWS\SYSTEM32\TOKENBINDING.DLL
C:\WINDOWS\SYSTEM32\TOKENBROKER.DLL
C:\WINDOWS\SYSTEM32\TPMCOREPROVISIONING.DLL
C:\WINDOWS\SYSTEM32\TPMTASKS.DLL
C:\WINDOWS\SYSTEM32\TPRDPW32.DLL
C:\WINDOWS\SYSTEM32\TPVMMON.DLL
C:\WINDOWS\SYSTEM32\TPVMW32.DLL
C:\WINDOWS\SYSTEM32\TQUERY.DLL
C:\WINDOWS\SYSTEM32\TRKWKS.DLL
C:\WINDOWS\SYSTEM32\TSPKG.DLL
C:\WINDOWS\SYSTEM32\TSSDJET.DLL
C:\WINDOWS\SYSTEM32\TWINAPI.APPCORE.DLL
C:\WINDOWS\SYSTEM32\TWINAPI.DLL
C:\WINDOWS\SYSTEM32\TWINUI.APPCORE.DLL
C:\WINDOWS\SYSTEM32\TWINUI.DLL
C:\WINDOWS\SYSTEM32\TWINUI.PCSHELL.DLL
C:\WINDOWS\SYSTEM32\TXFLOG.DLL
C:\WINDOWS\SYSTEM32\TZRES.DLL
C:\WINDOWS\SYSTEM32\UALAPI.DLL
C:\WINDOWS\SYSTEM32\UBPM.DLL
C:\WINDOWS\SYSTEM32\UCRTBASE.DLL
C:\WINDOWS\SYSTEM32\UIANIMATION.DLL
C:\WINDOWS\SYSTEM32\UIAUTOMATIONCORE.DLL
C:\WINDOWS\SYSTEM32\UMB.DLL
C:\WINDOWS\SYSTEM32\UMCRES.DLL
C:\WINDOWS\SYSTEM32\UMPNPMGR.DLL
C:\WINDOWS\SYSTEM32\UMPO-OVERRIDES-BASE.DLL

C:\WINDOWS\SYSTEM32\UMPO-OVERRIDES-XPC.DLL
C:\WINDOWS\SYSTEM32\UMPO.DLL
C:\WINDOWS\SYSTEM32\UMPOEXT.DLL
C:\WINDOWS\SYSTEM32\UMRDP.DLL
C:\WINDOWS\SYSTEM32\UPDATEHANDLERS.DLL
C:\WINDOWS\SYSTEM32\UPDATEPOLICY.DLL
C:\WINDOWS\SYSTEM32\URLMON.DLL
C:\WINDOWS\SYSTEM32\USBMON.DLL
C:\WINDOWS\SYSTEM32\USBPERF.DLL
C:\WINDOWS\SYSTEM32\USER32.DLL
C:\WINDOWS\SYSTEM32\USERENV.DLL
C:\WINDOWS\SYSTEM32\USERINIT.EXE
C:\WINDOWS\SYSTEM32\USERINITEXT.DLL
C:\WINDOWS\SYSTEM32\USERMGR.DLL
C:\WINDOWS\SYSTEM32\USERMGRCLI.DLL
C:\WINDOWS\SYSTEM32\USERMGRPROXY.DLL
C:\WINDOWS\SYSTEM32\USOAPI.DLL
C:\WINDOWS\SYSTEM32\USOCORE.DLL
C:\WINDOWS\SYSTEM32\UTILDLL.DLL
C:\WINDOWS\SYSTEM32\UXTHEME.DLL
C:\WINDOWS\SYSTEM32\VAULTCLI.DLL
C:\WINDOWS\SYSTEM32\VCTM64.DLL
C:\WINDOWS\SYSTEM32\VEEVENTDISPATCHER.DLL
C:\WINDOWS\SYSTEM32\VERSION.DLL
C:\WINDOWS\SYSTEM32\VIRTDISK.DLL
C:\WINDOWS\SYSTEM32\VM3DUM64.DLL
C:\WINDOWS\SYSTEM32\VM3DUM64_10.DLL
C:\WINDOWS\SYSTEM32\VMBUSPIPE.DLL
C:\WINDOWS\SYSTEM32\VMHGFS.DLL
C:\WINDOWS\SYSTEM32\VMICTIMEPROVIDER.DLL
C:\WINDOWS\SYSTEM32\VSOCKLIB.DLL
C:\WINDOWS\SYSTEM32\VSSAPI.DLL
C:\WINDOWS\SYSTEM32\VSSTRACE.DLL
C:\WINDOWS\SYSTEM32\VSSVC.EXE
C:\WINDOWS\SYSTEM32\VSS_PS.DLL
C:\WINDOWS\SYSTEM32\W32TIME.DLL
C:\WINDOWS\SYSTEM32\WBEMCOMN.DLL
C:\WINDOWS\SYSTEM32\WBEM\CIMWIN32.DLL
C:\WINDOWS\SYSTEM32\WBEM\ESSCLI.DLL

C:\WINDOWS\SYSTEM32\WBEM\FASTPROX.DLL
C:\WINDOWS\SYSTEM32\WBEM\NTEVT.DLL
C:\WINDOWS\SYSTEM32\WBEM\REPDRVFS.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMCORE.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMESS.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMPROX.DLL
C:\WINDOWS\SYSTEM32\WBEM\WBEMSVC.DLL
C:\WINDOWS\SYSTEM32\WBEM\WINMGMTR.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIAPRPL.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIAPSRV.EXE
C:\WINDOWS\SYSTEM32\WBEM\WMIPERFCLASS.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPERFINST.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPROV.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSD.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIPRVSE.EXE
C:\WINDOWS\SYSTEM32\WBEM\WMISVC.DLL
C:\WINDOWS\SYSTEM32\WBEM\WMIUTILS.DLL
C:\WINDOWS\SYSTEM32\WBIOSRVC.DLL
C:\WINDOWS\SYSTEM32\WCMCSP.DLL
C:\WINDOWS\SYSTEM32\WCMSVC.DLL
C:\WINDOWS\SYSTEM32\WDC.DLL
C:\WINDOWS\SYSTEM32\WDIGEST.DLL
C:\WINDOWS\SYSTEM32\WDSCORE.DLL
C:\WINDOWS\SYSTEM32\WEBIO.DLL
C:\WINDOWS\SYSTEM32\WEBSERVICES.DLL
C:\WINDOWS\SYSTEM32\WER.DLL
C:\WINDOWS\SYSTEM32\WEVTAPI.DLL
C:\WINDOWS\SYSTEM32\WEVTFWD.DLL
C:\WINDOWS\SYSTEM32\WEVTSVC.DLL
C:\WINDOWS\SYSTEM32\WFAPIGP.DLL
C:\WINDOWS\SYSTEM32\WIN32SPL.DLL
C:\WINDOWS\SYSTEM32\WIN32U.DLL
C:\WINDOWS\SYSTEM32\WINBIO.DLL
C:\WINDOWS\SYSTEM32\WINBIOEXT.DLL
C:\WINDOWS\SYSTEM32\WINBIOPLUGINS\FACERECOGNITIONENGINEADAPTER.DLL
C:\WINDOWS\SYSTEM32\WINBIOPLUGINS\FACERECOGNITIONSENSORADAPTER.DLL
C:\WINDOWS\SYSTEM32\WINBIOPLUGINS\NUIVOICEWBSADAPTERS.DLL
C:\WINDOWS\SYSTEM32\WINBIOPLUGINS\WINBIOSTORAGEADAPTER.DLL
C:\WINDOWS\SYSTEM32\WINBRAND.DLL

C:\WINDOWS\SYSTEM32\WINCORLIB.DLL
C:\WINDOWS\SYSTEM32\WINDOWMANAGEMENT.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.APPLICATIONMODEL.BACKGROUND.SYSTEMEVENTSBROKER.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.APPLICATIONMODEL.BACKGROUND.TIMEBROKER.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.APPLICATIONMODEL.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.CORTANA.DESKTOP.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.CORTANA.PAL.DESKTOP.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.CORTANA.PROXYSTUB.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.DEVICES.ENUMERATION.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.DEVICES.RADIOS.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.GLOBALIZATION.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.GLOBALIZATION.FONTGROUPS.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.GRAPHICS.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.IMMERSIVESHELL.SERVICEPROVIDER.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.INTERNAL.SHELL.BROKER.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.MEDIA.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.NETWORKING.BACKGROUNDTRANSFER.BACKGROUNDMANAGERPOLICY.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.NETWORKING.CONNECTIVITY.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.NETWORKING.SOCKETS.PUSHENABLEDAPPLICATION.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.SECURITY.AUTHENTICATION.ONLINEID.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.SECURITY.AUTHENTICATION.WEB.CORE.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.SHELL.SERVICEHOSTBUILDER.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.STATEREPOSITORY.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.STATEREPOSITORYBROKER.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.STORAGE.APPLICATIONDATA.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.STORAGE.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.STORAGE.SEARCH.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.SYSTEM.LAUNCHER.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.UI.CORE.TEXTINPUT.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.UI.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.UI.IMMERSIVE.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.UI.SHELL.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.UI.XAML.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.UI.XAML.RESOURCES.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.WEB.DLL
C:\WINDOWS\SYSTEM32\WINDOWS.WEB.HTTP.DLL
C:\WINDOWS\SYSTEM32\WINDOWSCODECS.DLL

C:\WINDOWS\SYSTEM32\WINDOWSPERFORMANCERECORDERCONTROL.DLL
C:\WINDOWS\SYSTEM32\WINDOWSPOWERSHELL\V1.0\PSEVENTS.DLL
C:\WINDOWS\SYSTEM32\WINHTTP.DLL
C:\WINDOWS\SYSTEM32\WININET.DLL
C:\WINDOWS\SYSTEM32\WININIT.EXE
C:\WINDOWS\SYSTEM32\WININITEXT.DLL
C:\WINDOWS\SYSTEM32\WINLOGON.EXE
C:\WINDOWS\SYSTEM32\WINMM.DLL
C:\WINDOWS\SYSTEM32\WINMMBASE.DLL
C:\WINDOWS\SYSTEM32\WINNLSRES.DLL
C:\WINDOWS\SYSTEM32\WINNSI.DLL
C:\WINDOWS\SYSTEM32\WINRNR.DLL
C:\WINDOWS\SYSTEM32\WINSCARD.DLL
C:\WINDOWS\SYSTEM32\WINSQLITE3.DLL
C:\WINDOWS\SYSTEM32\WINSRV.DLL
C:\WINDOWS\SYSTEM32\WINSTA.DLL
C:\WINDOWS\SYSTEM32\WINTYPES.DLL
C:\WINDOWS\SYSTEM32\WKSCLI.DLL
C:\WINDOWS\SYSTEM32\WKSSVC.DLL
C:\WINDOWS\SYSTEM32\WLDP.DLL
C:\WINDOWS\SYSTEM32\WLIDPROV.DLL
C:\WINDOWS\SYSTEM32\WLIDRES.DLL
C:\WINDOWS\SYSTEM32\WLS0WNDH.DLL
C:\WINDOWS\SYSTEM32\WMICLNT.DLL
C:\WINDOWS\SYSTEM32\WMIDCOM.DLL
C:\WINDOWS\SYSTEM32\WMP.DLL
C:\WINDOWS\SYSTEM32\WMPLOC.DLL
C:\WINDOWS\SYSTEM32\WMSGAPI.DLL
C:\WINDOWS\SYSTEM32\WOFUTIL.DLL
C:\WINDOWS\SYSTEM32\WOW64CPU.DLL
C:\WINDOWS\SYSTEM32\WPDBUSENUM.DLL
C:\WINDOWS\SYSTEM32\WPDSHSERVICEOBJ.DLL
C:\WINDOWS\SYSTEM32\WPNAPPS.DLL
C:\WINDOWS\SYSTEM32\WPNCORE.DLL
C:\WINDOWS\SYSTEM32\WPNPRV.DLL
C:\WINDOWS\SYSTEM32\WPNSERVICE.DLL
C:\WINDOWS\SYSTEM32\WPPORTINGLIBRARY.DLL
C:\WINDOWS\SYSTEM32\WPPRECORDERUM.DLL
C:\WINDOWS\SYSTEM32\WPTASKSCHEDULER.DLL

C:\WINDOWS\SYSTEM32\WSDAPI.DLL
C:\WINDOWS\SYSTEM32\WSDMON.DLL
C:\WINDOWS\SYSTEM32\WSECEDIT.DLL
C:\WINDOWS\SYSTEM32\WSHHYPERV.DLL
C:\WINDOWS\SYSTEM32\WSHIP6.DLL
C:\WINDOWS\SYSTEM32\WSHQOS.DLL
C:\WINDOWS\SYSTEM32\WSHTCPIP.DLL
C:\WINDOWS\SYSTEM32\WSMRES.DLL
C:\WINDOWS\SYSTEM32\WSMSELPL.DLL
C:\WINDOWS\SYSTEM32\WSMSVC.DLL
C:\WINDOWS\SYSTEM32\WSMWMIPL.DLL
C:\WINDOWS\SYSTEM32\WSNMP32.DLL
C:\WINDOWS\SYSTEM32\WSOCK32.DLL
C:\WINDOWS\SYSTEM32\WTSAPI32.DLL
C:\WINDOWS\SYSTEM32\WUAPI.DLL
C:\WINDOWS\SYSTEM32\WUAUENG.DLL
C:\WINDOWS\SYSTEM32\WUDFHOST.EXE
C:\WINDOWS\SYSTEM32\WUDFPLATFORM.DLL
C:\WINDOWS\SYSTEM32\WUDFSVC.DLL
C:\WINDOWS\SYSTEM32\WUDFX02000.DLL
C:\WINDOWS\SYSTEM32\WUPS.DLL
C:\WINDOWS\SYSTEM32\WUPS2.DLL
C:\WINDOWS\SYSTEM32\WUUHEXT.DLL
C:\WINDOWS\SYSTEM32\XMLLITE.DLL
C:\WINDOWS\SYSTEM32\XOLEHLP.DLL
C:\WINDOWS\SYSWOW64\ACRUNTI.EXE
C:\WINDOWS\SYSWOW64\ACUSRMOD.DLL
C:\WINDOWS\SYSWOW64\DWMAPI.DLL
C:\WINDOWS\SYSWOW64\EDPUTIL.DLL
C:\WINDOWS\SYSWOW64\GDI32.DLL
C:\WINDOWS\SYSWOW64\IERTUTIL.DLL
C:\WINDOWS\SYSWOW64\IMM32.DLL
C:\WINDOWS\SYSWOW64\KERNEL32.DLL
C:\WINDOWS\SYSWOW64\NTDLL.DLL
C:\WINDOWS\SYSWOW64\ODBCINT.DLL
C:\WINDOWS\SYSWOW64\OLEAUT32.DLL
C:\WINDOWS\SYSWOW64\PROPSYS.DLL
C:\WINDOWS\SYSWOW64\RUNONCE.EXE
C:\WINDOWS\SYSWOW64\TMATTACH.DLL

C:\WINDOWS\SYSWOW64\TMDRV32.DLL
C:\WINDOWS\SYSWOW64\URLMON.DLL
C:\WINDOWS\SYSWOW64\USER32.DLL
C:\WINDOWS\SYSWOW64\UXTHEME.DLL
C:\WINDOWS\SYSWOW64\VCTMDRV.DLL
C:\WINDOWS\SYSWOW64\WINSTA.DLL
C:\WINDOWS\SYSWOW64\WMPLOC.DLL
C:\WINDOWS\SYSWOW64\WTSAPI32.DLL

Лист регистрации изменений

№	Содержание изменения (обновления)	Дата	Примечание
1			
2			
3			
4			
5			
6			