Аккорд-АМДЗ

Надежность в ненадежном мире

ОКБ САПР
2022

Терминология

Доверенная загрузка (ДЗ) – это загрузка

- доверенной операционной системы
- из доверенного источника
- по доверенному каналу
- с сохранением заданного порядка операций загрузки;

Терминология

СДЗ – средство доверенной загрузки (может быть реализовано как аппаратно (СДЗ уровня платы расширения), так и программно (СДЗ уровня BIOS)). Сертифицируется ФСТЭК России.

АПМДЗ – аппаратно-программный модуль доверенной загрузки. АПМДЗ сертифицируется ФСБ России.

Некоторые СДЗ являются АПМДЗ, некоторые – нет, и наоборот.
Является ли то или иное средство СДЗ или АПМДЗ – определяется его сертификатами.

Терминология

АМДЗ (зарегистрированный товарный знак, принадлежащий ОКБ САПР) – аппаратный модуль доверенной загрузки.

Аккорд-АМДЗ является СДЗ согласно требованиям ФСТЭК России и АПМДЗ согласно требованиям ФСБ России.

Резидентный компонент безопасности

Комплекс «Аккорд-АМДЗ» реализует концепцию резидентного компонента безопасности (РКБ):

- автономного
- примитивного
- перенастраиваемого
- устройства с защищенной памятью.

Контроль загрузки компьютера со стороны такого устройства, стартующего в самом начале работы BIOS, позволяет на время старта изменить архитектуру компьютера, блокировав его архитектурную уязвимость.

Блокировка архитектурной уязвимости

Современные компьютеры – универсальны, то есть могут выполнить любую задачу, в том числе, и вредоносную.

В этом заключается их архитектурная уязвимость (АУ).

Во время старта компьютеру не нужно выполнять любые задачи, а нужно только строго определенные. Значит, необходимо лишить его универсальности.

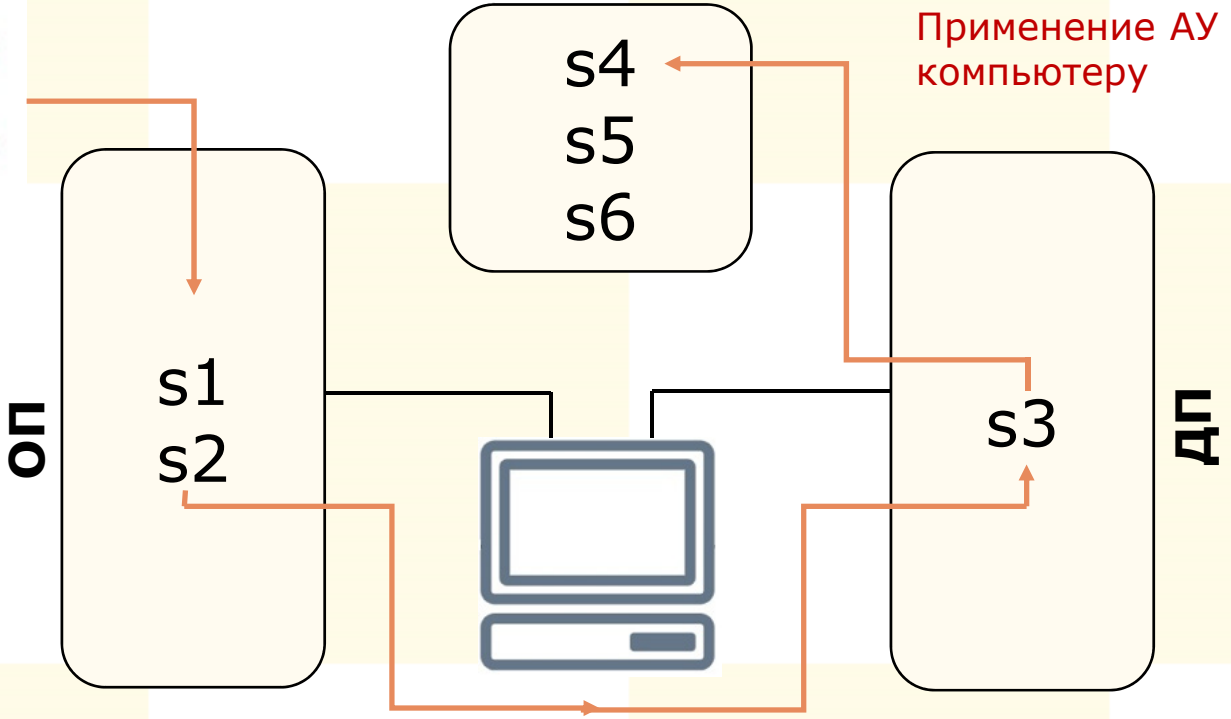
Это и есть задача РКБ.

Блокировка архитектурной уязвимости

«Аккорд-АМДЗ» блокирует архитектурную уязвимость компьютера за счет:

- ✓ контроля целостности BIOS, MBR, аппаратуры и дисков до загрузки ОС;
- ✓ контроля целостности файлов данных и реестра;
- ✓ контроля процессов.

Выполнение атаки на перехват управления

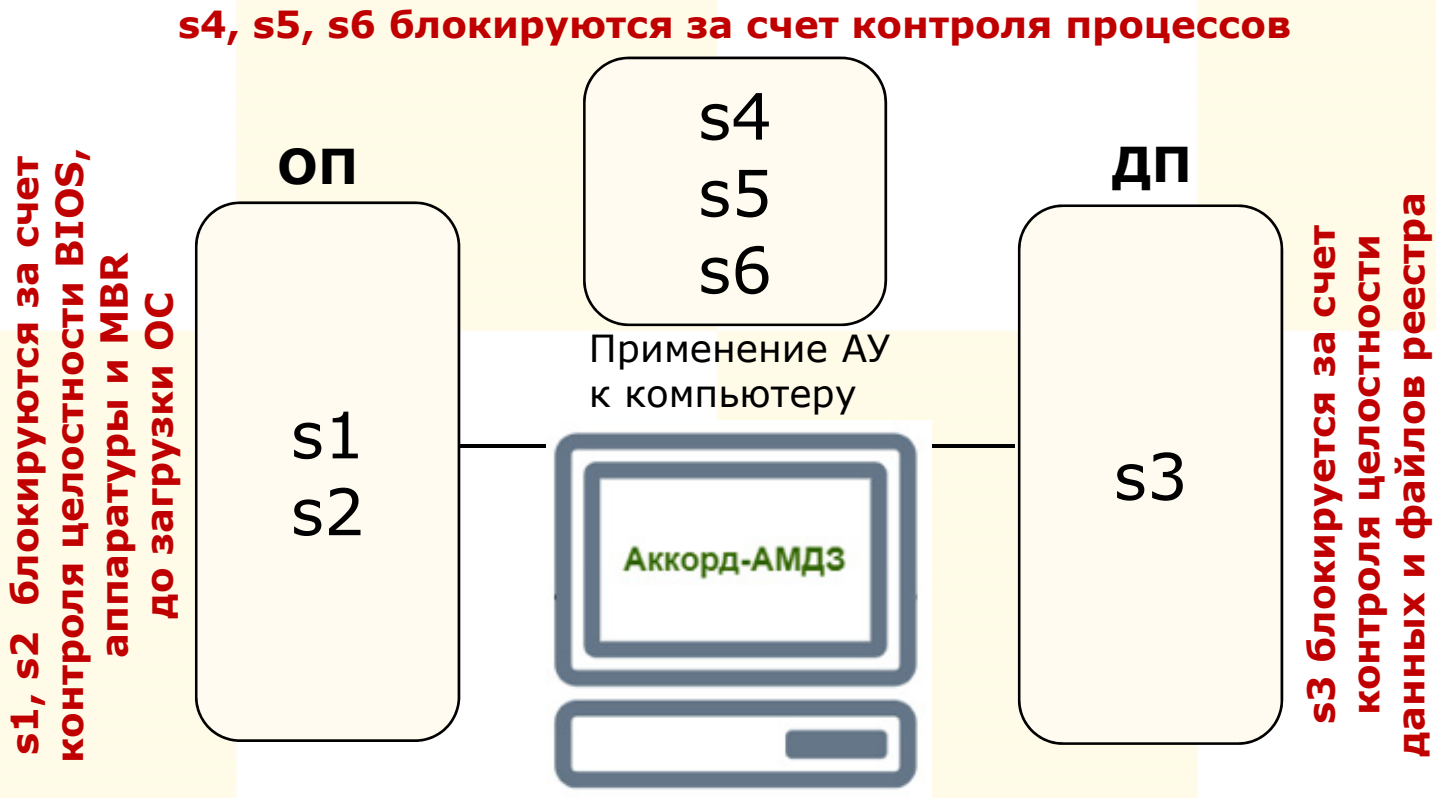


Обозначения:

АУ – архитектурная уязвимость;
s1-s6 – этапы проведения атаки;
ОП – оперативная память;
ДП – долговременная память.

Блокировка атаки на перехват управления

«Аккорд-АМДЗ» создает доверенную среду для работы программных средств, обеспечивающих защиту компьютера на шагах s1 – s6.



Функции «Аккорд-АМДЗ»

- ✓ блокировка загрузки ОС с внешних носителей информации;
- ✓ проверка целостности технических и программных средств ПК с использованием алгоритма пошагового контроля целостности;
- ✓ идентификация/аутентификация пользователя.

«Аккорд-АМДЗ» поддерживает

Файловые системы:

FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, ReiserFS, FreeBSD UFS/UFS2, Solaris UFS, QNX4, MINIX.

ОС:

те, что используют перечисленные ФС, в частности, **ОС семейств MS DOS, Windows, QNX, OS/2, UNIX, LINUX, BSD** и др.

Состав «Аккорд-АМДЗ»

- ✓ специализированный контроллер с предустановленной на этапе изготовления резидентной операционной средой;
- ✓ функциональное программное обеспечение (ФПО), работающее в резидентной операционной среде.

Резидентная операционная среда и ФПО – это единое резидентное ПО (firmware), размещающееся в энергонезависимой флэш-памяти контроллера.

Аппаратные платформы

- ✓ **PCI-express** – контроллеры Аккорд-GX;
- ✓ **Mini PCI-express** – Аккорд-GXM;
- ✓ **Mini PCI-express half card** – контроллер Аккорд-GXMH;
- ✓ **M.2 с ключами A и/или E** (интерфейс PCI-express) – Аккорд-GXM.2.

В компании ОКБ САПР постоянно выполняется разработка новых аппаратных платформ.

Выполнение требований регуляторов

«Аккорд-АМДЗ» имеет **сертификаты** ФСТЭК России и ФСБ России.

Базовые меры 17-21 Приказов ФСТЭК России:

ИАФ: 1, 2, 3, 4, 5, 6;

УПД: 1, 2, 4, 5, 6, 9, 10, 11, 15, 17;

ОПС: 1;

ЗНИ: 2, 5, 8;

РСБ: 1, 2, 3, 4, 5, 7;

АНЗ: 1, 2, 3, 4, 5;

ОЦЛ: 1, 3, 6;

ОДТ: 3, 4, 5;

Выполнение требований регуляторов

Базовые меры 17-21 Приказов ФСТЭК России:

ЗСВ: 1, 2, 3, 6, 7, 8;

ЗИС: 1, 5, 15, 21, 30;

ИНЦ: 2;

Выполнение требований регуляторов

Дополнительные (не включенные в базовый набор) меры Приказов 17-21 ФСТЭК России:

ИАФ: 7;

УПД: 7, 12;

ОПС: 4;

ЗНИ: 4, 6, 7;

РСБ: 8;

ОЦЛ: 2, 5, 8;

ЗСВ: 5;

ЗИС: 6, 19, 29.

Выполнение требований регуляторов

Базовые меры 31 Приказа ФСТЭК России:
ИАФ: 1, 2, 3, 4, 5, 7;
УПД: 1, 2, 3, 4, 5, 6, 9, 10, 11;
ОПС: 1;
ЗНИ: 2, 5, 6, 7, 8;
АУД: 2, 4, 6, 7, 8, 9;
ОЦЛ: 1, 3, 4, 5;
ОДТ: 3, 4, 5;
ЗИС: 1, 13, 21, 33, 38, 39;
ИНЦ: 1, 2;
ОПО: 4;
ДНС: 4, 5;

Выполнение требований регуляторов

Дополнительные (не включенные в базовый набор) меры 31 Приказа ФСТЭК России:

УПД: 7, 12;

ОПС: 3;

ЗНИ: 4;

ОЦЛ: 2;

ЗИС: 12, 22, 37.

Спасибо за внимание!

Если у вас возникли вопросы, то **напишите нам**.

Наш сайт в интернете:
www.okbsapr.ru