

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра «Информационная
безопасность систем и технологий»

Специальность 100503 –

Информационная безопасность
автоматизированных систем

Специализация -

Защищенные автоматизированные
системы управления

ДИПЛОМНАЯ РАБОТА

на тему

МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ КОНФИДЕНЦИАЛЬНОЙ
ИНФОРМАЦИИ, ОБРАБАТЫВАЕМОЙ СРЕДСТВАМИ
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ С УНИФИЦИРОВАННЫМ
РАСШИРЯЕМЫМ ИНТЕРФЕЙСОМ ВСТРОЕННОГО ПРОГРАММНОГО
ОБЕСПЕЧЕНИЯ «UEFI»

Студент

 Лубнина Мария Юрьевна

Руководитель

 Клейменов А.А.

Нормоконтролёр

 Иванов А.П.

Рецензент зам. начальника отделения АО «ПНИЭИ»

 Сомкин С.А.

Работа допущена к защите (протокол заседания кафедры от 20.06.2016 № 14)

Заведующий кафедрой

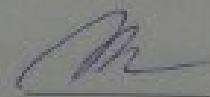
 С.Л. Зефирюв

Работа защищена с отметкой

хорошо (протокол заседания ГЭК

от 23.06.16, № 4)

Секретарь ГЭК

 А.П. Иванов

Пенза 2016

РЕФЕРАТ

Отчёт 73 с. , 7 рис. , 6 табл. , 9 источников

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, UEFI, СВТ, УГРОЗА БЕЗОПАСНОСТИ, ИСТОЧНИКИ УГРОЗ, УЯЗВИМОСТИ, МОДЕЛЬ УГРОЗ, РЕКОМЕНДАЦИИ.

Объектом исследования работы является средство вычислительной техники на базе UEFI обрабатывающее конфиденциальную информацию в частных организациях и компаниях.

Цель работы - разработка модели угроз целостности, доступности, конфиденциальности информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI» и формирование рекомендаций по обработке конфиденциальной информации средствами вычислительной техники с UEFI.

В процессе работы проводился анализ актуальности исследования UEFI, его описание и определение основных характеристик, идентификация и обзор уязвимостей UEFI в области обеспечения доступности, целостности и конфиденциальности информации, анализ уязвимостей, разработана модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники в соответствии с приведенными:

- идентификацией источников угроз информационной безопасности;
- моделью нарушителя безопасности;
- идентификацией угроз информационной безопасности;
- способов реализации угроз безопасности;
- характеристикой средств вычислительной техники с UEFI.

В результате проделанной работы была реализована из приведенного списка угроза нарушения доступности и разработаны рекомендации по обработке конфиденциальной информации средствами вычислительной

техники с UEFI с учетом разработанной модели угроз безопасности конфиденциальной информации.

СОДЕРЖАНИЕ

Введение	7
1 Анализ актуальности исследований UEFI, описание и основные характеристики UEFI	9
1.1 Описание и основные характеристики UEFI	9
1.2 Анализ актуальности исследований UEFI	10
1.3 Идентификация и обзор уязвимостей UEFI в области обеспечения доступности, целостности и конфиденциальности информации	14
1.3.1 Идентификация уязвимостей UEFI в области информационной безопасности.....	14
1.3.1.1 Уязвимости, затрагивающие хранилище основной прошивки UEFI.....	15
1.3.1.2 Уязвимости SMM.....	18
1.3.1.3 Уязвимости в реализации ACPI S3	20
1.3.1.4 Уязвимости NVRAM	23
1.3.1.5 Уязвимости SecureBoot.....	26
1.3.2 Анализ уязвимостей UEFI.....	29
1.3.2.1 Идентификация и определение ценности элементов UEFI подверженных атакам	29
1.3.2.2 Определение величин ущерба от нарушения свойств ИБ элементов UEFI подверженных атакам.....	30
2 Модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI»	35

2.1 Идентификация источников угроз информационной безопасности	35
2.2 Модель нарушителя безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с UEFI	36
2.3 Идентификация угроз информационной безопасности.....	43
2.3.1 Угрозы доступности информации, обрабатываемой средствами вычислительной техники с UEFI.....	44
2.3.2 Угрозы целостности информации, обрабатываемой средствами вычислительной техники с UEFI.....	49
2.3.3 Угрозы конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI.....	52
2.4 Анализ успешных реализаций угроз целостности, доступности и конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI.....	53
2.5 Характеристики средств вычислительной техники с UEFI	59
3 Реализация угрозы отказа в обслуживании СВТ с UEFI.....	63
4 Разработка рекомендаций по обработке конфиденциальной информации средствами вычислительной техники с UEFI.....	65
Заключение	66
Список использованных источников	67
Приложение А	70
Приложение Б.....	71
Приложение В	71
Приложение Г	72
Приложение Д	73

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем отчете применяют следующие термины с соответствующими определениями:

Угроза – потенциальная причина инцидента, способного нанести ущерб системе или организации;

Уязвимость – слабость одного или нескольких активов, которая может быть использована одной или несколькими угрозами;

В настоящем отчете применяют следующие обозначения и сокращения:

UEFI – унифицированный расширяемый интерфейс встроенного программного обеспечения;

BIOS – базовая система ввода-вывода;

GPT – стандарт формата размещения таблиц разделов на физическом жестком диске;

Firmware – встроенное программное обеспечение;

CBT – средство вычислительной техники;

CSM – модуль поддержки совместимости;

DoS – хакерская атака на вычислительную систему с целью довести её до отказа в обслуживании;

SMM – режим исполнения кода у x86/amd64-совместимых процессоров;

NVRAM – разновидность запоминающих устройств с произвольным доступом, которые способны хранить данные при отсутствии электрического питания;

НСД – несанкционированный доступ.

ВВЕДЕНИЕ

Информационная составляющая с каждым днем все больше и больше влияет на важные аспекты жизнедеятельности человека. И именно этот факт впоследствии привел к увеличению требований к средствам вычислительной техники обрабатывающих конфиденциальную информацию, где в свою очередь основополагающей частью является информационная безопасность.

Вполне закономерно, что в настоящее время одной из важнейших составляющих функционирования организации становится информационная безопасность и защита информации, которая считается важным ресурсом наравне с материальными активами организации, поскольку именно от безопасности информации зависят все информационные ресурсы.

Настоящая дипломная работа посвящена изучению проблем с информационной безопасностью средств вычислительной техники на базе UEFI в частных организациях и компаниях, обрабатывающих конфиденциальную информацию и персональные данные.

Защита информации в средствах вычислительной техники достигается путем принятия совокупности организационных и технических мер защиты информации, направленных на блокирование или нейтрализацию угроз безопасности информации, реализация которых может привести к негативным последствиям, на локализацию и минимизацию последствий от возможной реализации угроз безопасности информации, восстановление нормального режима функционирования средств вычислительной техники в случае реализации угроз безопасности информации.

В данной дипломной работе проводится анализ актуальности исследований UEFI в области информационной безопасности, идентификация уязвимостей СВТ, их анализ, а также разработка модели угроз безопасности, и как результат, разработка рекомендаций по обработке

конфиденциальной информации средствами вычислительной техники с UEFI с учетом нормативных документов ФСТЭК, проведенного анализа источников угроз, угроз и способов их реализации.

Разработанные модель угроз и рекомендации предназначены для операторов, организующих и (или) осуществляющих обработку конфиденциальной информации средствами вычислительной техники с UEFI, а также для заказчиков и разработчиков информационных систем и подсистем, включающих в себя данные средства.

1 Анализ актуальности исследований UEFI, описание и основные характеристики UEFI

1.1 Описание и основные характеристики UEFI

Английская аббревиатура UEFI звучит следующим образом - Unified Extensible Firmware Interface. В переводе на русский язык получаем следующее определение – унифицированный расширяемый интерфейс встроенного программного обеспечения. Его разработки начались еще с начала 2000-х годов, а занималась ими компания Intel, и предназначались для серверного процессора Itanium. Так что же послужило заняться разработкой UEFI? Тот факт, что Itanium было принципиально новейшим оборудованием, и абсолютно ни одна версия BIOS не работала с ним, а любые доработки тут помочь не могли, привел к принятию решения о разработке нового встроенного интерфейса. Первым шагом на пути формирования системы стал EFI, а применила данную разработку компания Apple, установив EFI на все выпускаемые персональные компьютеры и ноутбуки. К аббревиатуре EFI была добавлена еще одна буква U, а за этой буквой слово Unified, унифицированный, единый, что свидетельствует о том, что разработкой интерфейса uefi bios занимается сразу несколько компаний, а конечным результатом является единый интерфейс. К числу компаний разрабатывающих интерфейс относятся Dell, HP, IBM, и Phoenix Insyde, а также Microsoft, поскольку именно она является основным разработчиком операционных систем. В приложении А на рисунке А.1 – интерфейс UEFI.

UEFI – это интерфейс между операционной системой и микропрограммами, управляющими низкоуровневыми функциями оборудования. Основной, а главное фундаментальной задачей UEFI, является непосредственная замена устаревшего интерфейса встроенного программного обеспечения, а также стандартизация интерфейса взаимодействующего программного обеспечения с СВТ.

Основные характеристики UEFI:

- поддержка GUID Partition Table (GPT), замена MBR. GPT - стандарт формата размещения таблиц разделов на физическом жестком диске. Таблица разделов GUID является новой архитектурой диска. Использует 64-битные идентификаторы для разделов. Количество разделов не ограничено.
- модульность UEFI. Модульная архитектура UEFI позволяет значительно расширить функционал системы, интегрировать необходимые модули в соответствии с пожеланиями заказчика — к примеру, удаленная авторизация пользователей, биометрическая.
- встроенный загрузчик. Загрузчик (boot loader) - первичная программа, которую запускает UEFI. Загрузчик отвечает за загрузку операционной системы с желаемыми параметрами ядра и initial RAM disk перед тем, как начать процесс загрузки. Кроме того, существует возможность добавлять в загрузочное меню UEFI собственные пункты.
- поддержка сервисов. UEFI имеет два типа сервисов: boot services и runtime services. Первый тип работает только до загрузки ОС и обеспечивает взаимодействие с графическими и текстовыми терминалами, шинами, блочными устройствами и т.д. Тип runtime services может использовать ОС. Один из примеров runtime services — variable service, который хранит значения в NVRAM. ОС Linux использует variable service для хранения кеш дампов, которые можно извлечь после перезагрузки компьютера.

1.2 Анализ актуальности исследований UEFI

Достаточно констатировать тот факт, что на протяжении двух последних лет, на рынке компьютеров практически невозможно приобрести персональный компьютер, в состав которого бы не входил UEFI. А это значит, что исследование UEFI с точки зрения информационной безопасности является актуальным.

В 2014 году состояние безопасности UEFI можно было отметить на достаточно низком уровне, но уже, спустя почти два года, стал очевидным тот факт, что развитие и надежность UEFI значительно укрепились, даже не смотря на тот факт, что производители персональных компьютеров до недавних пор не уделяли должного внимания безопасности. Так вот, для того чтобы рассмотреть актуальность исследований UEFI с точки зрения информационной безопасности, необходимо определить, какими уязвимостями UEFI располагает по сей день.

Основные причины исследования UEFI.

Актуальность исследования данного интерфейса связано с рядом определенных причин. К примеру, информация по безопасности UEFI на русском языке в сети интернет представлена в очень ограниченном диапазоне, по факту она практически отсутствует, существуют лишь редкие переводы англоязычных разработчиков, которые, в свою очередь, судя по переводу статей мало знакомы с информационной безопасностью. Такое упущение необходимо остановить, поскольку русскоязычным специалистам необходима данная информация.

Кроме того, на сегодняшний момент, не существует методики или требований по сертификации и аттестации СВТ с UEFI. Поэтому исследование UEFI на наличие уязвимостей является актуальной проблемой.

Для определения защиты и слабых мест UEFI имеет смысл рассмотреть модель угроз. В приложении Б на рисунке Б.1 - начало работы UEFI.

Первое, что следует отметить так это то, что не существует абсолютной защиты, проще говоря, нет абсолютно неуязвимой системы защиты. Всегда существует вероятность чрезвычайного происшествия, антропогенного или природного характера. В любом случае, подобного рода уязвимости не будут затронуты в данной ситуации. Нарушитель – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является

нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах. Для нарушителя (атакующего) обозначим несколько уровней доступа для того, чтобы наглядно определить насколько доступная реализация UEFI способна ему противостоять.

Нарушитель с первым уровнем доступа, располагающий физическим доступом к системе, может загружать любые операционные системы, менять настройки UEFI, внедрять собственный код UEFI вместо установленного на программаторе, изменять положение джамперов на материнской плате, осуществлять замыкание выводов на микросхемах и т.д.

Нарушитель со вторым уровнем доступа также располагает физическим доступом к системе, за исключением отсутствия программатора у него.

Нарушитель с третьим уровнем доступа имеет в своем распоряжении удаленный доступ к системе. Управление осуществляется в режиме администратора.

В остальных случаях, злоумышленник способный изменять чипы, входящие в состав микросхем, UEFI остановить не способна. Такие нарушители рассмотрению подлежать не будут. Для дальнейшего рассмотрения актуальности исследования UEFI определим основные направления атак, а также их последствия в порядке убывания по их значимости.

Атака на хранилище основной прошивки (в большинстве современных системах – это одна или две микросхемы NOR-flash, с интерфейсом SPI). На чем основывается эта атака: злоумышленник, внедряет свой код в прошивку, производит удаление части имеющегося кода, а далее выполняет свои задуманные планы. Последствия же данной атаки на хранилище основной прошивки находятся в диапазоне от малого, а именно получения полного

контроля над программным обеспечением, аппаратным обеспечением и операционной системы, до большего, DoS атаки. Физический нарушитель способен осуществить DoS атаку в любой ситуации (вплоть до прямого физического вмешательства в микросхемы).

Атака на код в SMM. Суть данной атаки заключается в получении доступа к особо привилегированному режиму процессора, исходя из чего, вся физическая память и многое другое находится в доступе для выполнения чтения и записи. Последствия же, как и в первом случае, находятся в диапазоне от малого, именно доступа к хранилищу программного обеспечения, а также особенности последствий таких же, как при атаке на хранилище данных, до большего, способность обхода механизмов операционной системы, а также гипервизора.

Атака на хранилище прошивки PCI-устройств. Данная атака заключается во внедрении злоумышленником своего кода в прошивку в любое PCI-устройство (Option ROM). В качестве примера, могут быть использованы сетевая карта или контроллер Thunderbolt. UEFI выполняет установленный код и атака реализована. Диапазон последствий варьируется от малого - как в предыдущей атаке на хранилище данных, до большего обхода операционной системы, только с одним различием, во времени загрузки, поскольку многие аспекты уже заблокированы или настроены.

Атака на скрытые настройки UEFI. Суть проста и заключается она в получении возможности изменения настроек UEFI, как доступных, так и скрытых. Последствиями могут являться в малом, это отключение видимых защитных настроек UEFI, а в большем DoS атака. В NVRAM можно прописать абсолютно любой код, что впоследствии приведет к непредсказуемым последствиям.

Атака с помощью SecureBoot. Задачей данной атаки являться получение возможности загружать любую необходимую операционную

систему, в том числе и UEFI Shell. Последствия атаки варьируются от загрузки UEFI Shell, до замены стандартного загрузчика операционной системы, на измененный, расположившись тем самым в операционной системе, до тех пор, пока пользователем не будет установлен факт измены настроек SecureBoot.

Именно наличие уязвимых мест в унифицированном расширяемом интерфейсе встроенного программного обеспечения UEFI говорит о необходимости его исследования в области информационной безопасности. Для проведения более точного анализа необходима идентификация уязвимостей UEFI в области информационной безопасности, что и будет проведено в следующем пункте настоящего отчета, а также построение модели угроз информационной безопасности к СВТ.

1.3 Идентификация и обзор уязвимостей UEFI в области обеспечения доступности, целостности и конфиденциальности информации

1.3.1 Идентификация уязвимостей UEFI в области информационной безопасности

Перечень идентифицированных уязвимостей информационной безопасности СВТ с UEFI приведен в таблице 1.

Таблица 1 – Перечень уязвимостей информационной безопасности

Основные области уязвимостей информационной безопасности				
Хранилище основной прошивки	Уязвимости SMM	Уязвимости в реализации ACPI S3	Уязвимости NVRAM	Уязвимости SecureBoot
Уязвимость проверки прошивки перед выполнением кода	Уязвимость внешнего кода SMRAM	Уязвимость в области памяти AcpiNVS	Уязвимость RO-микросхемы, PR-регистров	Уязвимость CSM

Продолжение таблицы 1

Основные области уязвимостей информационной безопасности				
Хранилище основной прошивки:	Уязвимости SMM:	Уязвимости в реализации ACPI S3:	Уязвимости NVRAM:	Уязвимости SecureBoot:
Уязвимость микросхемы с Flash Descriptor	Уязвимость наличия в чипсете собственного контролера DMA	Уязвимость с платформой Intel, AMD	Уязвимость UEFI-загрузчика	Уязвимость удаления главного ключа
Уязвимость PR регистров	Уязвимость использования указателя буфера	Уязвимость регистра BootScript	Уязвимость наличия утилиты Linux efibootmgr	Уязвимость при флаге RT
Уязвимость Guard режима		Уязвимость обеспечения доверия прошивки		Уязвимость с повреждением NVRAM
Уязвимость BLE BIOS_WE по отношению к race condition				Уязвимость с помощью PCI-устройств
				Уязвимость с преобразованием загрузчика
				Уязвимость при загрузке с внешнего носителя

В соответствии с таблицей 1 и техническим заданием был проведен анализ идентифицированных уязвимостей.

1.3.1.1 Уязвимости, затрагивающие хранилище основной прошивки UEFI

Проверка прошивки, либо части прошивки перед выполнением кода.

Intel BootGuard и AMD Hardware – Validated Boot. В этом разделе речь пойдет об этих двух технологиях, которые позволяют UEFI быть защищенным на всех атакуемых трех уровнях. Основными задачами данных технологий выступает проверка целостности определенной части прошивки, подписанной электронно-цифровой подписью изготовителя материнской

платы, а ведь сам ключ встроен в чипсет платы. Успешная проверка способствует старту прошивки, в иных случаях все зависит от индивидуальных настроек. Тем самым, Intel BootGuard и AMD Hardware-Validated Boot являются прикорневым аппаратным гарантом доверия для следующих стадий загрузки, прошивка в свою очередь выстраивает цепочку, где чипсет осуществляет проверку bootstrap-кода, потом тот в свою очередь том PEI, а последующий том DXE. В том DXE по цепочке подключается SecureBoot и уже осуществляет проверку подписи загрузчика операционной системы. Абсолютно любая модификация защищенных с помощью этих технологий частей прошивки приводит к DoS атаке. С другой стороны, данная защита свидетельствует о невозможности изменения прошивки даже пользователем, наделенным соответствующими правами управления системой, а также сложность в ремонте материнской платы в случае отказа работоспособности чипсета. Верификация прошивки с помощью этих технологий позволяет существенно снизить атаки на данную уязвимость, а значит, нарушитель первого уровня не опасен. Благодаря этим технологиям уязвимость минимизирована, но только в случае отсутствия прямого доступа нарушителя.

Flash Descriptor.

До UEFI в материнских платах был предусмотрен джампер, который защищал микросхему с BIOS от вредоносного кода прошивки. Все, что содержалось в BIOS Setup, было расположено в CMOS SRAM (статической памяти с произвольным доступом). Intel, пришел к выводу, что CMOS не обладает достаточным объемом памяти, и микросхему нужно сделать емкой и быстрой, собственно и все настройки прописывать именно туда. Результат – скопление всего и в одном месте: UEFI, часть кода сетевой карты GbE, основная часть чипсета ME и многое другое. А главное, каждый из трех владельцев микросхемы, CPU, ME и GbE, смогли писать в нее в любой

момент и не только при обновлении. Для упорядочивания этой ситуации Intel добавил в микросхему Flash Descriptor, который прописывает права доступа владельцев к региону. Для того чтобы отделить нововведения владельцев, предлагалось установить сразу две микросхемы SPI, первая для Descriptor, ME и GbE , вторая под остаток UEFI, после чего #WP второго чипа на аппаратном уровне защищает его от записи. Недостатки – дороговизна, наличие 2-х чипов, в связи с чем, данную плату найти практически невозможно; наличие физического доступа обязательно, поскольку вывод #WP на GPIO (низкоуровневом интерфейсе ввода-вывода прямого управления) изначально нарушает безопасность; порча микросхемы RW возможна. Итог – уязвимость на минимальном уровне использования атакой.

Чипсет.

Защита с помощью четырех регистров PR, для обеспечения безопасности чтения\записи физической памяти. Недостатки – грамотная реализация защиты, с условием сброса значений регистров при перезагрузке и их восстановлении; установка lock на конфигурацию регистров, в противном случае вредоносное программное обеспечение сбрасывает их; отсутствие остановки защиты, то есть обновление прошивки из операционной системы без предварительной перезагрузки невозможно; NVRAM и RW-области защитить таким образом невозможно. Защита с PR регистрами, на данный момент, реализована недостаточно.

Intel BIOS Guard режим.

Intel BIOS Guard был разработан BIOS в целях:

- минимизации кода записанного в SMM , где абсолютно любая уязвимость дает полный доступ к прошивке;
- защиты от ошибок в коде в реализации самого исполнителя;
- в зависимости от управления переменной NVRAM.

При решении имеющихся недостатков добавлением нового режима защиты добавились новые: осложнилось понимание и обращение, а именно скрипты на DSL, подписи, обновление компонентов и т.д.; невозможность прошивки образа с помощью программатора, а для восстановления потребуются собрать прошивку буквально из кусков, что само по себе сложно в исполнении. Атаки на Intel BIOS Guard в настоящее время не распространены, но для минимизации уязвимости, лучше всего провести дополнительный аудит SMM.

BLE и BIOS_WE биты.

Данные биты позволяют чипсету подать команду на запись, они доступны любому коду, в связи с чем, происходит генерация SMI, BIOS регистрирует обработчик SMI. В общем виде данная защита основывается на добавлении BIOS обработчика, и генерация SMI. В конечном итоге, для осуществления атаки необходим лишь SmiLock, для отключения источника SMI и выполнения задуманных планов. И все бы было безопасно, но как выяснилось, что многоядерные процессоры BLE BIOS_WE, являются уязвимостью по отношению к race condition. А это свидетельствует о его неработоспособности защиты, так как сама атака занимает малое количество времени и практически всегда успешно завершается. Не смотря, на тот факт, что не все компьютеры обладают BLE BIOS_WE, большинство из них имеет лишь BLE бит, что подтверждает наличие уязвимости.

1.3.1.2 Уязвимости SMM

Первоначально SMM был предназначен для использования для независимой от операционной системы автоматического управления питанием и системными устройствами, поскольку обучить такому самой операционную систему было сложнее, нежели добавление режима исполнения в процессоре. Для перехода в режим SMM, необходимо прерывание SM, которое генерируется с помощью:

- аппаратной реализации, а именно выдача высокого уровня на SMI#;
- системой, в виде результата событий;
- программной реализации, при отправке байта в CPU IO-регистр с заданным регистром.

Код из вне SMRAM.

Ранее данная уязвимость таковой и не считалось, а все потому, что в случае, когда обработчик SMI вызывает код, который не находится в SMRAM, то нарушитель, наделенный правами записи и в физическую память может заменить вызываемый код своим, то есть выполнить его в SMM. Данная уязвимость была распространена повсеместно на многих компьютерах, чей возраст превышал июль 2015 года. Иными словами обработчики SMI в этих компьютерах уязвимы. Но для защиты от вызываемого внешнего кода, который находится вне SMRAM, Intel добавляет MSR_SMM_FEATURE_CONTROL. Обычному пользователю следует защититься с помощью мониторинга, то есть не допускать исполнения неизвестного кода от суперпользователя, что, к большому сожалению, на современных операционных системах практически невозможно.

Уязвимость контроллера DMA.

Эта уязвимость затронула собственный чипсет SMM. Современные чипсеты имеют контролер DMA. Он необходим для разгрузки центрального процессора от различных задач пересылки данных из одной памяти в другую, как это происходит с DRAM, а также DRAM и памятью PCI-устройств. При всем этом произвести подобную передачу может как операционная система, так и PCI-устройство, при наличии собственного DMA контролера. Нарушитель, владеющий правами администратора, приводит в действие DMA с управляемой им областью памяти и областью SMRAM, что приводит к полному доступу к ней. В качестве защиты выступает регистр TSEGMB, в

нем повторяется информация о расположении TSEG, и бит Lock, который в свою очередь дает отказ на изменение содержимого. В случае отсутствия данной установки в прошивку компьютера уязвимость может быть использована.

Уязвимость указателя буфера.

И вновь уязвимыми остаются обработчики SMI, использующие в роли параметра размер и указатель буфера, осуществляя в него запись. Нарушитель способен передать эти параметры таким образом, чтобы они повлияли на буфер, а тот в свою очередь вышел за границы RAM-SMRAM. Поскольку обработчик SMI имеет доступ к SMRAM, то будет переписана определенная часть данных впереди SMRAM. Данная атака не пользуется популярностью, в связи с большими временными затратами на отладку, хотя вполне может быть реализована. Новые версии поддерживают алгоритм обработчиков SMI, принимающих указатели на буфер, валидируют его перед самым использованием. В старых версиях такого нет, поэтому данная уязвимость имеет место быть, только вот вероятность ее использования мала.

1.3.1.3 Уязвимости в реализации ACPI S3

Стоит отметить тот факт, что данная уязвимость указала на целый ряд проблем в области безопасности UEFI, которые ранее таковыми не считались. ACPI S3 – режим ожидания, или всем известный как режим сна подразумевает под собой целый ряд так называемых состояний. S0 (все устройства находятся в рабочем состоянии). S1 (ядра процессора осуществили команду HLT, кэш и RAM обновляются, питание с линий S0-only отключено, регистры центрального управляющего процессора, чипсета, устройств в этом состоянии не сбрасываются). S2-S3 (в этом состоянии содержание памяти остается надежным и осуществляет обновление, процессор и часть чипсета отключены совсем, с потерей содержимого

регистров, после включения процессор выполняет код с ResetVector'a, а именно, происходит восстановление контекста для процессора и чипсета). S4 (информация памяти сброшена на диск, система отключила все устройства и питание, отличие от S5 – наличие FastBoot). S5 (система отключена, при наличии подключения питания при возобновлении работы). S3 является очень важной характеристикой любого персонального компьютера, поскольку от работоспособности сохранения и восстановления контекста при включении зависит многое. S3 BootScript – разработка Intel, суть которой заключается в следующем: после инициализации базовых устройств (процессора, кэш, оперативной памяти) определяется текущий режим загрузки.

Уязвимость в области памяти AspiNVS.

Именно в этой области памяти и хранится S3 BootScript, и как было выявлено, она уязвима от изменения. Операционная система относит данную область к служебной, и не изменяет ее, а вот нарушитель, обладающий правами администратора имеет такую возможность. Основная часть защитных механизмов, которая обеспечивает защиту от внедрения кода в микросхему SPI, от НСД в SMM, настраивается через регистры процессора и чипсета, а для успешного преодоления данных механизмов необходимо найти BootScript в памяти, далее регистр, поменяв в нем значения, чтобы S3 Resume защита не была включена. Для минимизации уязвимости, Intel внедряет SmmLockBox. Суть атаки – после составления скрипта, он скопирован полностью в SMRAM, причем оригинальный BootScript не удален. Восстановление из S3 вызывается обработчиком SMI, который проверяет наличие совпадения оригинального BootScript с копией в SMRAM, а в случае отсутствия данного совпадения — либо переписывает измененный BootScript копией, либо перезагружает компьютер. При наличии

всех проблем с прошивкой, система, которая новее 2015 года, не подвержена атаке на S3 BootScript.

Уязвимость с платформой Intel, AMD.

BootScript был помещен в DISPATCH, стало известно, что есть от производителей Intel и AMD ряд модулей PEI, которые в свою очередь:

- дублировались в память, находясь вблизи BootScript;
- командой вызова служил DISPATCH, при этом вызывались они многократно;
- объем затронутой памяти в SMRAM, копии исчерпали весь лимит.

Удаление модулей влекло за собой нарушения работы S3. Альтернативным вариантом исправления данного исправления была процедура переноса их в неупакованную область DXE-тома, исправив команды DISPATCH, таким образом, чтобы он вызывался напрямую с микросхемы SPI. Скорость выполнения данной процедуры значительно увеличилась, но проблему все же удалось избежать, но до сих пор, систем с подобной уязвимостью очень много.

Уязвимость регистра BootScript.

Зачастую, разработчики DXE-драйверов забывают написать добавление важного регистра в BootScript, а уже после S3 в этом регистре окажется его исходное значение. Известная уязвимость в прошивках ноутбуков Apple, где разработчики забыли добавить в S3 BootScript запись в PR-регистры, а после S3 защита микросхемы SPI от прошивки снималась автоматически.

Уязвимость обеспечения доверия прошивки.

С появлением S3 BootScript была обнаружена скрытая проблема, которая на протяжении долгого времени серьезного резонанса не получила, а случилось это только сейчас. Дело в том, что безопасность прошивки, а именно доверие к системам, имеющим влияние операционной системы,

отсутствовало как таковая. Устройства необходимо было сбросить и провести инициализацию вручную, очистить память и ни в коем случае не использовать ничего из нее, а также свои сервисы Runtime, после ReadyToBoot, компонентам прошивки пользоваться запрещено. Иными словами, неосторожность использования приведет к образованию BIOS с чужим кодом, и вполне легальным драйверам в SMRAM уже нет места. В связи с чем, изготовители платформ принимали попытки решения проблемы в аппаратной реализации: внедрение validated boot; хранение S3 BootScript в Security Coprocessor'e; разработка собственного крипточипа и т.д. Intel, в свою очередь, добавляет в Skylake технологию SGX, необходимую для изоляции отдельных частей кода и данных от остальных частей системы, в своем роде аналог SMM. Несмотря на точность воспроизведения, не обошлось и без минусов. Первое, сложность в программировании. Второе, это наличие данной технологии у Intel и только на Skylake. Что касается безопасности операционной системы – абсолютно идентичный уровень недоверия к самой прошивке, и, наличие технологии STM необходимо.

1.3.1.4 Уязвимости NVRAM

NVRAM – представляет собой набор переменных, каждая переменная имеет имя, атрибуты, данные и GUID. Сами переменные делятся по типу на: обычные, которые хранятся в RAM, а при перезагрузке своих значений не сохраняют; NV переменные, которые хранятся в выделенной области SPI микросхемы, а при перезагрузке считываются именно с нее; переменные HR, которые, так же как и NV переменные, хранятся на микросхеме SPI, но отдельно от них, используются операционной системой с UEFI, для того, чтобы оповещать прошивку об обнаруженных ошибках. Кроме того, переменные делятся по уровню доступа. Переменные BS, они недоступны в начале загрузки операционной системы. Переменные RT, эти переменные

доступные всегда, а с внедрением технологии SecureBoot, к RT переменным добавились еще два подвида:

- AW переменные, для записи которых требуется аутентификация;
- переменные TA, то же самое, только еще с временной меткой для защиты от replay-атак.

Для того чтобы определить тип переменной необходимы ее атрибуты: тип переменной + уровень доступа + подуровень. Переменная хранится в микросхеме SPI, доступная на запись и чтение, в момент загрузки, так и из операционной системы.

Уязвимость RO-микросхемы, PR-регистров.

NV переменные, а именно для их хранения используется SPI, а это значит, что при работе NVRAM необходимо осуществить запись в нее во время работы операционной системы, что соответственно ставит под угрозу безопасность в случае с RO-микросхемы и PR-регистров. Не смотря на это, большинство изготовителей до сих пор используют PR-регистры, устанавливая их таким образом, чтобы NVRAM оказался в незащищенной от записи области, и при этом забывают о том, что для данной области требуется отдельная защита в виде SMM-драйвера для NVRAM и установка бита SMM_BWP/SpiRomProtect. Отсутствие данной защиты приводит к полному доступу ко всем NV переменным в независимости от атрибутов и, в том числе, к переменным требующим аутентификацию SecureBoot, что приводит эту технологию в неработоспособный вид, а также Setup, что влечет за собой отключение частей системы, а после самой перезагрузки получению полному доступу всей микросхемы SPI, и конечно же DoS атаке. Уязвимых к такой атаке систем огромное количество, взять хотя бы практически все виды ноутбуков компании Acer.

Уязвимость UEFI-загрузчика.

Загрузчик, который обладает возможностью выполнения произвольного кода до появления ExitBS события, приводит к тому, что начальные стадии загрузки имеют весь доступ к переменным BS, также как и к Setup. В случае если изготовитель платформы не предусмотрел запрет записи в данную переменную после того, как временное окно вызова BIOS Setup завершилось, то сам загрузчик способен выполнить чтение и изменение содержимого переменной Setup. Защита от данной уязвимости такова, что с ключами по умолчанию предлагается доверять Microsoft, а тем, кто пользуется открытыми операционными системами, в чьей прошивке ключи не только MS, но и Canonical, защититься от атаки практически нечем.

Уязвимость наличия утилиты Linux efibootmgr.

При обновлении ядра утилите efibootmgr удастся добавить переменную в BootXXXX, кроме того удалить после чего несколько соседних переменных, а в некоторых случаях и все. А это напрямую приводит к тому, что UEFI, Phoenix либо Insyde останавливаются, поскольку фаза BDS завершилась, и выполнять загрузку уже невозможно. После чего, возможность выйти из сложившегося положения, к примеру, BIOS Setup, оказался среди BootXXXX. У пользователя было два пути, или использовать подсистему Crisis Recovery, или воспользоваться услугами сервиса. В последнее время, с подобной проблемой сталкиваются не редко.

При наличии достаточно серьезных уязвимостей NVRAM лучшей защитой от всех возникающих проблем является удаление NV, а именно перенос всех находящихся в SPI микросхеме переменных в RAM, а также установить защиту на запись в их области на запись с использованием PR-регистров сразу после BIOS Setup.

1.3.1.5 Уязвимости SecureBoot

Программная технология SecureBoot, благодаря которой UEFI проверяет наличие подлинности исполняемых ей внешних компонентов, таких как загрузчики, драйверы, и UEFI OptionROM. Данные компоненты обязательно подписаны электронно-цифровой подписью, которая подлежит проверке во время загрузки, а в случае отсутствия подписи, повреждения, отсутствия в списке разрешенных (db) или наличия в списке запрещенных (dbx), загрузка соответствующего компонента не осуществляется. Стандартом электронно-цифровой подписи считается алгоритм, комбинации из RSA2048 и SHA256, которые используются на всех системах.

Иерархия ключей SecureBoot.

ПК - KEK - db\ dbx.

Вершиной является ПК – это главный ключ, который устанавливает доверие между пользователем платформы и ее прошивкой. В состав входит открытый ключ Pkpub и закрытый ключ Pkpriv, расположен в NVRAM в виде само подписанного сертификата. В зависимости от требуемого уровня безопасности, ПК генерируется различными способами: собственным ключом для каждого отдельного персонального компьютера; общим ключом для каждой модели материнской платы; общим ключом линейки материнский плат; общим ключом для всех плат производителя.

Первоначально ПК генерирует производитель платформы. ПК необходим для управления хранилищем ключей KEK. Пользователь, обладающий KEKpriv, является авторизованным пользователем. Ключи KEK устанавливают доверие меду изготовителем исполняемого компонента и самой прошивкой. Эти ключи необходимы для управления хранилищами db, в них находятся сертификаты разрешенных к запуску компонентов, и dbx, где хранятся сертификаты, запрещенные к запуску. Иерархия ключей SecureBoot приведена в приложении В.

CSM уязвимость.

SecureBoot не поддерживается при наличии CSM, иными словами компьютеры, которые используют старые операционные системы, не способные выполнять загрузку без CSM. В таком случае, SecureBoot лишен всех защитных механизмов. К примеру, в Windows 7 отсутствует поддержка GOP, а без нее загрузка операционной системы в отсутствие CSM или не работает вовсе, или в произвольном виде, что делает Windows 7 несовместимым по отношению к SecureBoot, даже в том случае, если пользователь сам подпишет для нее загрузчик.

Уязвимость SecureBoot удалением главного ключа.

При наличии доступа к записи хранилища NVRAM у злоумышленника, то он может просто удалить его, что повлечет за собой отключение SecureBoot, а тот в свою очередь перейдет в режим установления новых ключей.

Уязвимость SecureBoot при CurrentMode и ExecutionPolicy.

В случае если управляющая переменная SecureBoot, записанная в Setup имеет флаг RT, то злоумышленник отключает систему SecureBoot, установив в Setup ноль в нужном смещении, которое можно найти при помощи анализа IFR дампа. Системы с подобной уязвимостью имеются до сих пор. Во втором случае, отключается не SecureBoot, а осуществляется запрет на дальнейшую загрузку при отсутствии подлинности электронно-цифровой подписи или ее отсутствия. Такая атака, встречается реже, но реализуется менее открыто, поскольку сам SecureBoot работоспособен.

Уязвимость с повреждением NVRAM.

Для того чтобы обойти SecureBoot достаточно подпортить NVRAM, переполнив хранилище. В случае если драйвер NVRAM находится в плохом состоянии, не исключена DoS атака.

Уязвимость SecureBoot с помощью PCI-устройств.

Запуск UEFI OptionROM из PCI-устройств при работающем SecureBoot не должен происходить, если соответствующий OROM не прошел верификацию, но на практике большое количество систем доверяет PCI-устройствам беспрекословно и загружает все без дополнительной проверки. Системы без SecureBoot подвержены такой атаке безоговорочно. Именно поэтому вынос PCIЕ на внешние разъемы по типу: Thunderbolt, PCMCIA, ExpressCard и т.п. — прямая угроза безопасности платформы, даже не смотря на то, что любое PCI-устройство может инициировать DMA с любым регионом физической памяти, за исключением SMRAM, и только в том случае, если изготовитель платформы не забыл установить защиту.

Уязвимость SecureBoot с преобразованием загрузчика.

UEFI-загрузчик, или любой исполняемый файл UEFI может быть в формате PE (формат исполняемых файлов, объектного кода и динамических библиотек, используемый в 32 и 64битных версиях операционной системы Microsoft Windows) , или в формате TE, который, в принципе, тот же PE, только с уменьшенными заголовками, уменьшающие количество затронутого места в памяти. Формат TE, очень редко используется для компонентов прошивки, кроме PEI-модулей, поскольку только в первой половине PEI, до инициализации RAM, есть смысл в экономии 240h байт на заголовке, и потому, эталонная реализация проверки электронно-цифровой подписи не проверяла ее у образов в формате TE совсем. А вследствие комбинации двух ошибок проверка такого образа всегда заканчивалась успешно. Перевод PE в TE считается типичным, SecureBoot можно было обойти лишь изменением файла с загрузчиком, поэтому проблема была признана серьезной и быстро была принята к исправлению. Тем не менее, на данный момент имеется достаточное количество старых систем с этой проблемой.

Уязвимость SecureBoot при загрузке с внешнего носителя.

SecureBoot не может защитить от подмены загрузчика, и физически присутствующий злоумышленник способен загрузить систему со своего личного носителя. От подобного инцидента существуют попытки защиты паролем на BIOS и меню выбора загрузочного устройства, но разработчики из MS позволили выбрать его и из Windows, в связи с чем, достаточно просто нажать Shift, выбрав действие «перезагрузка» на экране входа в систему, а после же, выбрать нужное устройство загрузки.

1.3.2 Анализ уязвимостей UEFI

Для проведения полного анализа идентифицированных уязвимостей необходимо определение элементов UEFI подверженных уязвимостям в части обеспечения доступности, целостности и конфиденциальности информации. Приложение В - архитектура UEFI.

1.3.2.1 Идентификация и определение ценности элементов UEFI подверженных атакам

Были идентифицированы элементы UEFI подверженные атакам в области информационной безопасности. Затем для каждого из элементов были определены значимые свойства ИБ.

Документированный перечень элементов UEFI подверженных атакам представлен в таблице 2.

Таблица 2 – Перечень элементов UEFI и их значимых свойств.

Элементы UEFI	Значимые свойства информационной безопасности		
	Конфиденциальность	Целостность	Доступность
Хранилище основной прошивки UEFI:	+	+	+
Технологии Intel BootGuard и AMD Hardware – Validated Boot	-	+	+
Flash Descriptor	-	+	+
Чипсет	+	-	+

Продолжение таблицы 2

Элементы UEFI	Значимые свойства информационной безопасности		
	Конфиденциальность	Целостность	Доступность
Intel BIOS Guard режим	-	+	+
BLE и BIOS_WE биты	-	+	+
SMM:	+	+	+
SMRAM	-	+	+
Контроллер DMA	-	+	+
Указатель буфера	-	+	+
ACPI S3:	+	+	+
Память AspiNVS	+	+	+
Платформы Intel, AMD	-	+	+
Регистр BootScript	-	+	+
Обеспечение доверия прошивки	+	+	-
NVRAM:	+	+	+
RO-микросхемы и PR-регистры	+	-	+
UEFI-загрузчик	+	+	+
Linux efibootmgr	-	+	+
SecureBoot:	+	+	+
CSM	+	-	+
Главный ключ	+	-	+
CurrentMode и ExecutionPolicy	+	-	+
PCI-устройства	-	+	+
Преобразование загрузчика	+	+	+
Внешний носитель	+	-	-

1.3.2.2 Определение величин ущерба от нарушения свойств ИБ элементов UEFI подверженных атакам

Далее было проведено оценивание величин ущерба от нарушения свойств ИБ элементов по следующим направлениям:

- степень влияния на непрерывность деятельности организации;
- объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для элементов UEFI и ликвидации последствий нарушения ИБ;

- объем дополнительных людских ресурсов, необходимых для восстановления свойств ИБ для элементов UEFI и ликвидации последствий нарушения ИБ;
- объем дополнительных временных затрат, необходимых для восстановления свойств ИБ для элементов UEFI и ликвидации последствий нарушения ИБ;
- степень нарушения законодательных требований и(или) договорных обязательств организации.

На основании результатов оценивания величины нарушений ИБ для каждого элемента UEFI с зависимым информационным ресурсом была определена обобщенная качественная оценка величины нарушения ИБ. Результаты оценивания представлены в таблице 3.

Качественная характеристика:

М – малая,

С – средняя,

В – высокая.

Таблица 3 – Оценка величины нарушений ИБ для элементов UEFI

Элементы UEFI	Свойства безопасности	Величины нарушения ИБ по направлениям оценивания					Обобщенная величина нарушения ИБ	Ценности элементов UEFI	Информационный ресурс
		1	2	3	4	5			
Технологии Intel BootGuard и AMD Hardware – Validated Boot	Конфиденциальность	М	С	М	С	С	С	С	Информация о системе
	Целостность	В	С	М	С	С	С		
	Доступность	С	С	М	С	С	С		
Flash Descriptor Validated Boot	Конфиденциальность	С	С	М	С	С	С	С	Информация о системе
	Целостность	В	С	М	М	С	С		
	Доступность	В	С	М	С	В	С		
Чипсет	Конфиденциальность	М	С	М	С	С	С	С	Информация об активах
	Целостность	В	С	В	М	В	В		
	Доступность	С	С	М	М	С	С		
Intel BIOS Guard режим	Конфиденциальность	М	С	М	С	С	С	С	Информация о системе
	Целостность	В	С	М	С	С	С		
	Доступность	С	С	М	С	В	С		
BLE и BIOS_WE биты	Конфиденциальность	С	С	М	С	С	С	С	Информация о системе
	Целостность	В	С	М	М	С	С		
	Доступность	С	М	М	М	С	М		
SMRAM	Конфиденциальность	С	С	С	С	М	С	С	Информация о системе
	Целостность	В	М	М	М	С	М		
	Доступность	С	М	М	С	В	С		
Контроллер DMA	Конфиденциальность	С	С	М	С	М	С	С	Информация об активах
	Целостность	В	С	М	С	С	С		
	Доступность	С	С	М	М	С	С		
Указатель буфера	Конфиденциальность	С	С	М	С	М	С	М	Информация о системе
	Целостность	В	М	М	С	М	М		
	Доступность	С	М	М	С	М	М		

Продолжение таблицы 3

Элементы UEFI	Свойства безопасности	Величины нарушения ИБ по направлениям оценивания					Обобщенная величина нарушения ИБ	Ценности элементов UEFI	Информационный ресурс
		1	2	3	4	5			
Память AspiNVS	Конфиденциальность	В	С	М	С	М	С	М	Информация о системе
	Целостность	В	С	М	М	С	М		
	Доступность	С	М	М	М	С	М		
Платформы Intel, AMD	Конфиденциальность	С	С	М	С	М	С	М	Информация об активах
	Целостность	В	М	М	М	С	М		
	Доступность	С	М	М	М	С	М		
Регистр BootScript	Конфиденциальность	С	С	М	С	М	С	С	Информация об активах
	Целостность	В	М	М	С	В	С		
	Доступность	С	С	М	С	С	С		
Обеспечение доверия прошивки	Конфиденциальность	В	С	М	С	М	С	С	Информация об активах
	Целостность	В	С	М	С	В	В		
	Доступность	С	М	М	С	В	С		
RO-микросхемы и PR-регистры	Конфиденциальность	С	С	М	М	С	С	С	Информация об активах
	Целостность	В	М	М	М	С	С		
	Доступность	С	М	М	С	С	С		
UEFI-загрузчик	Конфиденциальность	С	С	М	С	С	С	В	Информация о системе
	Целостность	В	М	В	С	В	В		
	Доступность	С	В	В	С	В	В		
Linux efibootmgr	Конфиденциальность	В	В	М	В	М	В	В	Информация об активах
	Целостность	В	М	В	М	В	В		
	Доступность	С	М	М	М	С	М		
CSM	Конфиденциальность	С	С	М	М	М	М	М	Информация об активах
	Целостность	В	М	М	М	В	М		
	Доступность	С	М	М	М	С	М		
Главный ключ	Конфиденциальность	В	С	М	С	С	С	С	Информация об активах
	Целостность	В	М	М	С	С	С		
	Доступность	С	С	М	С	С	С		

Продолжение таблицы 3

CurrentMode и ExecutionPolicy	Конфиденциальность	В	С	В	В	В	В	В	Информация об активах
	Целостность	В	М	М	С	В	С		
	Доступность	В	В	В	С	С	В		
PCI-устройства	Конфиденциальность	В	С	М	М	С	С	С	Информация об активах
	Целостность	В	М	М	С	С	С		
	Доступность	С	М	М	С	С	С		
Преобразование загрузчика	Конфиденциальность	В	С	В	С	В	В	В	Информация об активах
	Целостность	В	С	М	С	С	С		
	Доступность	В	С	В	В	В	В		
Внешний носитель	Конфиденциальность	В	С	С	С	С	С	С	Информация об активах
	Целостность	В	С	М	М	С	С		
	Доступность	В	В	В	М	С	В		

2 Модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI»

Разработанная модель угроз целостности, доступности, конфиденциальности информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI» включает в себя: перечень источников угроз, модель нарушителя безопасности конфиденциальной информации, перечень угроз безопасности по конфиденциальности, целостности и доступности, способы реализации угроз и оценку реализации угроз.

2.1 Идентификация источников угроз информационной безопасности

Для идентификации дальнейшего перечня источников угроз необходимо воспользоваться определением. Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

Источники угрозы безопасности конфиденциальной информации подразделяются на нарушителей, программно-аппаратные закладки, вредоносные программы.

Нарушители безопасности конфиденциальной информации подробно будут рассмотрены в следующем пункте пояснительной записки.

Программно-аппаратные закладки – относящиеся к аппаратным средствам компьютера, расположены в BIOS, подразделяются на конструктивно встроенные закладки и автономные.

Аппаратные закладки.

Конструктивно встроенные закладки возникают в процессе проектирования и разработки аппаратного обеспечения, используемого в информационной системе и способны проявлять себя в виде не

декларированных возможностей различных частей вычислительной системы. В отличие от конструктивно встроенных закладок, автономные являются законченными устройствами, которые выполняют определенные функции перехвата, передачи и накопления информации. Стоит учесть тот факт, что аппаратные закладки представляют собой некую часть технических средств, внедренная или подключенная к информационной системе и обеспечивающая при необходимых условиях несанкционированного доступа или реализацию деструктивных действий, то в них, располагаются микрокоманды, необходимые для взаимодействия закладок с программно-техническими средствами информационной системы обрабатывающей конфиденциальную информацию.

Программные закладки.

Программные закладки подразделяются на программно-аппаратные закладки, загрузочные закладки, драйверные закладки, прикладные закладки, исполняемые закладки, закладки-имитаторы, замаскированные закладки.

Вредоносные программы.

Вредоносная программа - компьютерная программа либо переносной код, предназначенный для выполнения угроз безопасности информации, расположенной в компьютерной системе, или другого воздействия, препятствующего естественному функционированию компьютерной системы. Подразделяются на компьютерные вирусы, троянские программы, шпионское программное обеспечение, сетевые черви, руткиты.

2.2 Модель нарушителя безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с UEFI

Анализируя возможности, которыми вполне способен воспользоваться нарушитель безопасности конфиденциальной информации, составлена его модель.

Характеристика нарушителей.

Если рассматривать нарушителя со стороны наличия возможности постоянного либо единовременного доступа в объект информатизации, где размещены элементы информационной системы персональных данных, то все физические лица могут характеризоваться в соответствии с критериями:

- первая категория - это лица, которые не имеют прав доступа к объекту информатизации информационной системы обрабатывающей конфиденциальную информацию;

- вторая категория – это лица, которые обладают правом доступа к объекту информатизации информационной системы обрабатывающей конфиденциальную информацию.

Нарушители, также классифицируются на:

- внутренних нарушителей, способных осуществлять атаки, находясь при этом в объекте информатизации информационной системы персональных данных;

- внешних нарушителей, способных осуществлять атаки, находясь за пределами объекта информатизации информационной системы персональных данных.

К внешним нарушителям помимо лиц первой категории могут так же относиться лица второй категории, которые находятся за пределами контролируемой зоны. По отношению к информационной системе персональных данных из первой категории лиц могут также относиться:

- лица преступных организаций;
- иные лица, которые пытаются получить доступ к конфиденциальной информации в преднамеренном порядке;
- бывшие сотрудники организации.

Перечень действий осуществляющих внешним нарушителем.

Внешний нарушитель способен осуществлять перехват конфиденциальной информации обрабатываемой техническими средствами с помощью их утечки по техническим каналам утечки информации, а также применяя носимые, возимые и портативные автоматические средства разведки.

Внешний нарушитель способен оказывать разрушающие воздействия с элементами информационной структуры информационной системы персональных данных, а также конфиденциальной системы организации, которые в процессе осуществления собственной работоспособности (улучшение, сопровождение, ремонтные работы, утилизация) находятся за пределами контролируемой зоны.

Внешний нарушитель способен осуществлять несанкционированный доступ к информации с помощью программных воздействий, а именно внедрения вредоносного программного кода, алгоритмических закладок.

Внешний нарушитель способен осуществлять перехват информации, поступающей по сетям связи общего пользования либо каналам связи, которые незащищены от несанкционированного доступа к информации с помощью организационно-технических мер.

Внешний нарушитель способен осуществлять атаки на информационную систему персональных данных и конфиденциальную информацию организации благодаря осуществлению реализаций угроз с удаленного доступа.

Анализируя внутреннего нарушителя, то есть лиц второй категории, можно классифицировать их в соответствии по способу и полномочиями осуществления доступа к информационным ресурсам информационной системы персональных данных, а также конфиденциальной информации организации.

Первая группа. В состав первой группы входят служащие предприятия организации, которые не зарегистрированы пользователями и не были допущены к информационным ресурсам конфиденциальной информации организации, но имеют согласованный с руководством доступ в контролируемую зону. К данной группе нарушителей могут относиться сотрудники сторонних организаций имеющих непосредственное отношение к объекту информатизации (обслуживающий персонал: уборка помещений, сантехнические работы, энергообеспечение организации, служба охраны). Данные сотрудники, способствующие естественному выполнению бизнес-процессов.

Возможности первой группы нарушителей:

- вести мониторинг пользователей имеющих отношение к конфиденциальной информации организации;
- использование программно-аппаратных закладок, осуществлять перехват передаваемой информации по техническим каналам, подключившись к техническим средствам обработки конфиденциальной информации.

Вторая группа. В состав второй группы входят допущенные сотрудники к конфиденциальной информации, полномочиями которых является ограниченный доступ к конфиденциальной информации с установленного рабочего места. К данной группе относятся лица, обладающие правом доступа к локальным информационным ресурсам конфиденциальной информации организации для осуществления должностных обязательств и установленных требований.

Возможности второй группы нарушителей:

- располагает всеми возможностями нарушителей первой категории доступа;

- частично располагать знаниями о зарегистрированных пользователях для осуществления доступа;

- располагать атрибутами доступа к системе (логин, пароль), необходимыми для доступа к конфиденциальной информации организации;

- располагать атрибутами доступа к системе (логин, пароль), необходимыми для доступа к конфиденциальной информации организации;

- располагать информацией имеющей к ней доступ.

Третья группа. В состав третьей группы входят зарегистрированные пользователи подсистем объекта информатизации обрабатываемого конфиденциальную информацию и персональные данные, с помощью удаленного доступа к конфиденциальной информации по локальной либо распределительной сети организации.

Возможности третьей группы нарушителей:

- располагать всеми возможностями нарушителей второй категории;

- обладать сведениями о топологии сети информационной системы организации и имеющихся технических средствах, необходимых для обработки конфиденциальной информации организации;

- располагать прямым доступом к отдельным техническим средствам информационной системы организации.

Четвертая группа. В состав четвертой группы входят зарегистрированные пользователи информационной системы обрабатывающей конфиденциальную информацию организации наделенные правами администратора безопасности определенного сегмента информационной системы.

Возможности четвертой группы нарушителей:

- располагать всей информацией о системном и прикладном программном обеспечении, затрагивающем информационную систему организации;

- располагать всей информацией о технических средствах обрабатывающих конфиденциальную информацию на объекте информатизации, доступного сегмента информационной системы;
- располагать доступом к СЗИ, кроме того к другим элементам сегмента информационной системы;
- располагать правами конфигурации и администрирования настройками некоторых элементов технических средств сегмента информационной системы.

Пятая группа. В состав пятой группы входят зарегистрированные пользователи с правами системного администрирования информационной системы обрабатывающей конфиденциальную информацию, выполняющие конфигурацию и управление программным обеспечением, а также оборудованием, в том числе отвечающим за безопасность объекта информатизации. В данном случае, это средства, отвечающие за мониторинг, регистрацию, архивацию, защиту от несанкционированного доступа к конфиденциальной информации и персональным данным.

Возможности пятой группы нарушителей:

- располагать всей информацией о системном, прикладном и специальном программном обеспечении, используемом в информационной системе организации;
- располагать всей информацией о технических средствах , а также конфигурации информационной системы организации;
- располагать доступом ко всем техническим средствам информационной системы организации;
- располагать правами конфигурации и администрирования по настройке информационной системы организации.

Шестая группа. В состав шестой группы входят зарегистрированные пользователи информационной системы с правами администрирования

безопасности информационной системы, предназначенный для соблюдения правил разграничения доступа, генерации основных элементов, смену паролей, криптозащиту информации. Пользователь, наделенный правами администратора безопасности, осуществляет мониторинг тех же средств защиты объекта информатизации, что и системный администратор.

Возможности шестой группы нарушителей:

- располагать всей информацией об информационной системе организации;
- располагать доступом ко всем техническим средствам информационной системы организации, а также средствам защиты информации, протоколирования, части основных элементов информационной системы;
- не располагает правами доступа к конфигурации технических средств сети, только контрольных.

Седьмая группа. В состав седьмой группы входят программисты, разработчики сторонних организаций, которые могут являться поставщиком программного обеспечения и лица, отвечающие за техническое обслуживание на объекте информатизации организации.

Возможности седьмой группы нарушителей:

- располагать информацией об программном обеспечении информационной системы обрабатывающей конфиденциальную информацию, а также о алгоритмах ее реализации;
- располагать возможностью внесения ошибок, программных закладок, внедрения вредоносного программного кода в программное обеспечение информационной системы еще на стадии разработки, обслуживания и внедрения;

- располагать всеми фрагментами информации о технических средствах обрабатывающих и защищающих конфиденциальную информацию на объекте информатизации.

Восьмая группа. В состав седьмой группы входят персонал, осуществляющий обслуживание технических средств объекта информатизации, кроме того поставщики и лица уполномоченные для ремонта технических средств.

Возможности восьмой группы нарушителей:

- располагать возможностями внедрения закладок в технические средства объекта информатизации еще на стадиях разработки, обслуживания и сопровождения;

- располагать элементами информации о топологии объекта информатизации, серверах, технических средствах защиты в информационной системе, автоматизированных рабочих местах и оборудовании коммуникации.

Подводя итог анализа модели нарушителя, для разработки требований к средствам вычислительной техники, обрабатывающих конфиденциальную информацию необходимо учитывать все виды рассмотренных групп.

2.3 Идентификация угроз информационной безопасности

На данном этапе работы была проведена идентификация угроз ИБ организации. Были приведены источники угроз (кто и что является причиной угрозы), установлены цели угроз (то есть, на какие элементы UEFI может оказать влияние угроза) и типы потерь (то есть, на нарушение каких свойств ИБ угроза может быть направлена).

Перечни идентифицированных угроз, источников угроз, объектов воздействия угроз и последствия реализации угроз информационной безопасности СВТ с UEFI приведены в таблицах 4, 5, 6.

2.3.1 Угрозы доступности информации, обрабатываемой средствами вычислительной техники с UEFI

Список угроз доступности информации, обрабатываемой средствами вычислительной техники с UEFI, приведен в таблице 4.

Таблица 4 - Угрозы доступности информации, обрабатываемой средствами вычислительной техники с UEFI

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
1	Внедрение вредоносного кода в UEFI.	Угроза заключается в возможности заставить UEFI выполнять вредоносный код при каждом запуске компьютера, внедрив его в UEFI путём замены микросхемы UEFI или обновления программного обеспечения UEFI на версию, уже содержащую вредоносный код. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения UEFI и заменой чипсета UEFI.	Внутренний нарушитель с высоким потенциалом	Flash Descriptor, SMRAM.	Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера
2	Несанкционированное выключение, либо обход механизма защиты от записи.	Угроза заключается в возможности внедрения в UEFI вредоносного программного кода после ошибочного или злонамеренного выключения пользователем механизма защиты UEFI от записи, а также в возможности установки неподписанного обновления в обход механизма защиты от записи в UEFI. Данная угроза обусловлена слабостями мер по разграничению доступа к управлению механизмом защиты UEFI от записи, а также уязвимостями механизма обновления UEFI, приводящими к переполнению буфера.	Внутренний нарушитель с низким потенциалом	Чипсет, Платформы Intel, AMD	Реализация данной угрозы возможна в одном из следующих условий: - при выключенном механизме защиты UEFI от записи; - успешной эксплуатации нарушителем уязвимости механизма обновления UEFI, приводящей к переполнению буфера.

Продолжение таблицы 4

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
4	Восстановление предыдущей уязвимой версии UEFI.	Угроза заключается в возможности осуществления вынужденного перехода на использование UEFI, содержащей уязвимости. Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения UEFI.	Внутренний нарушитель с низким потенциалом.	Указатель буфера, Платформы Intel, AMD.	При использовании технологии обновления UEFI возможно возникновение следующей ситуации (условия, характеризующие ситуацию указаны в хронологическом порядке): - на компьютере установлена некоторая версия UEFI, для которой на момент её работы не известны уязвимости; - в силу некоторых обстоятельств UEFI проходит процедуру обновления, сохраняя при этом предыдущую версию UEFI на случай «отката» системы.

Продолжение таблицы 4

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
5	Нарушение изоляции среды исполнения UEFI.	Угроза заключается в возможности изменения параметров и (или) логики работы программного обеспечения UEFI путём программного воздействия из операционной системы компьютера или путём несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к UEFI, его функциям администрирования и обновления, со стороны операционной системы или каналов связи.	Внутренний нарушитель с низким потенциалом.	Обеспечение доверия прошивки, Регистр BootScript.	Реализация данной угрозы возможна: - со стороны операционной системы – при условии наличия UEFI функционала обновления и (или) управления ПО UEFI из операционной системы; - со стороны сети – при наличии у дискредитируемого серверного сервис-процессора достаточных привилегий для управления всей системой, включая модификацию серверов системы, и дискредитируемого сервера.
6	Использование слабых криптографических алгоритмов UEFI.	Угроза заключается в сложности проверки реальных параметров алгоритмов, реализованных в криптографических средствах UEFI, при том доверие к криптографической защите будет ограничено доверием к производителю. Данная угроза обусловлена сложностью использования собственных криптографических алгоритмов в программном обеспечении UEFI.	Внешний нарушитель с высоким потенциалом.	Чипсет, Intel BIOS Guard режим.	Возможность реализации данной угрозы снижает достоверность оценки реального уровня защищённости системы

Продолжение таблицы 4

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
7	Изменение режимов работы аппаратных элементов компьютера.	Угроза заключается в возможности подмены нарушителем загружаемой операционной системы путём несанкционированного изменения в UEFI пути доступа к загрузчику операционной системы, и обусловлена слабостями технологий разграничения доступа к управлению UEFI.	Внутренний нарушитель с низким потенциалом	BLE и BIOS_WE биты, Контроллер DMA.	Реализация данной угрозы возможна при условии доступности нарушителю следующего параметра настройки UEFI – указания источника загрузки операционной системы.
8	Сбой процесса обновления UEFI.	Угроза заключается в возможности выведения из строя компьютера из-за внесения критических ошибок в программное обеспечение UEFI в результате нарушения процесса его обновления, и обусловлена слабостями технологий контроля за обновлением ПО UEFI.	Внутренний нарушитель со средним потенциалом	SMRAM	Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера как при установке корректной/совместимой версии, так и при установке повреждённой/несовместимой версии обновления.
9	Подбор пароля UEFI.	Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам UEFI путём входа в консоль UEFI по паролю, подобранному программно или «вручную». Данная угроза обусловлена слабостями механизма аутентификации, реализуемого в консолях UEFI.	Внутренний нарушитель с низким потенциалом.	Главный ключ, PCI-устройства	Реализация данной угрозы возможна если: - нарушитель может осуществить физический доступ к СБТ и имеет возможность его перезагрузить; - нарушитель обладает специальным программным средством перебора паролей UEFI и привилегиями системы.

2.3.2 Угрозы целостности информации, обрабатываемой средствами вычислительной техники с UEFI

Список угроз целостности информации, обрабатываемой средствами вычислительной техники с UEFI, приведен в таблице 5.

Таблица 5 - Список угроз целостности информации, обрабатываемой средствами вычислительной техники с UEFI

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
1	Деструктивное использование декларированного функционала UEFI	Угроза заключается в возможности неправомерного использования декларированного функционала UEFI для нарушения целостности информации, хранимой на внешних носителях информации и в оперативном запоминающем устройстве компьютера. Данная угроза обусловлена уязвимостями программного обеспечения UEFI, предназначенного для тестирования и обслуживания компьютера (средств проверки целостности памяти, программного обеспечения управления RAID-контроллером и т.п.).	Внутренний нарушитель с низким потенциалом	Преобразование загрузчика, Главный ключ.	Реализации данной угрозы может способствовать возможность обновления некоторых UEFI без прохождения аутентификации.

Продолжение таблицы 5

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
2	Установка уязвимых версий обновления программного обеспечения.	Угроза заключается в возможности внесения уязвимостей в программное обеспечение UEFI в ходе его обновления, которые могут быть использованы в дальнейшем для приведения компьютера в состояние «отказ в обслуживании», несанкционированного изменения конфигурации UEFI или выполнения вредоносного кода при каждом запуске компьютера. Данная угроза обусловлена слабостями мер контроля отсутствия уязвимостей в только что вышедших версиях обновления программного обеспечения UEFI.	Внутренний нарушитель со средним потенциалом.	CSM, RO-микросхемы и PR-регистры.	Реализация данной угрозы возможна в ходе проведения ремонта и обслуживания компьютера.
4	Аппаратный сброс пароля UEFI	Угроза заключается в возможности сброса паролей, установленных в UEFI без прохождения процедуры авторизации в системе путём обесточивания микросхемы UEFI (съёма аккумулятора) или установки перемычки в штатном месте на системной плате (переключение «джампера»), и обусловлена уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в UEFI.	Внутренний нарушитель с низким потенциалом.	CSM.	Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера.

Продолжение таблицы 5

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
5	Использование поддельных цифровых подписей UEFI.	Угроза заключается в возможности установки уязвимой версии обновления UEFI или версии, содержащей вредоносное программное обеспечение, но имеющей цифровую подпись. Данная угроза обусловлена слабостями мер за контролем по благонадёжности центров выдачи цифровых подписей.	Внешний нарушитель со средним потенциалом.	CSM, Главный ключ.	Реализация данной угрозы возможна при условии выдачи неблагонадёжным центром сертификации цифровой подписи на версию обновления UEFI, содержащую уязвимости, или на версию, содержащую вредоносное программное обеспечение (т.е. при осуществлении таким центром подлога), а также подмены нарушителем доверенного источника обновлений.
6	Подмена резервной копии программного обеспечения UEFI	Угроза заключается в возможности опосредованного внедрения нарушителем в UEFI дискредитируемого компьютера вредоносного кода, путём создания необходимости выполнения процедуры восстановления предыдущей версии программного обеспечения UEFI, предварительно подменённой нарушителем. Данная угроза обусловлена недостаточностью мер разграничения доступа и контроля целостности резервных копий программного обеспечения UEFI.	Внутренний нарушитель с низким потенциалом	Контроллер DMA.	Реализация данной угрозы возможна при: - нарушитель успешно подменил резервную копию программного обеспечения UEFI; возникла необходимость восстановления предыдущей версии программного обеспечения UEFI (данное условие может произойти как случайно, так и быть спровоцировано нарушителем).

2.3.3 Угрозы конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI

Список угроз конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI, приведен в таблице 6.

Таблица 6 - Список угроз конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI

№	Наименование	Описание угрозы	Источник угрозы	Объект воздействия	Способы реализации угрозы
1	Несанкционированное использование привилегированных функций UEFI.	Угроза заключается в возможности использования нарушителем потенциально опасных возможностей UEFI. Данная угроза обусловлена наличием в UEFI потенциально опасного функционала.	Внутренний нарушитель с низким потенциалом.	UEFI-загрузчик, Linux efibootmgr.	Реализация данной угрозы возможна при условии наличия у нарушителя физического доступа к системному блоку компьютера.
2	Отсутствие возможности управления правами пользователей UEFI.	Угроза заключается в возможности неправомерного использования пользователями декларированного функционала UEFI, ориентированного на администраторов. Данная угроза обусловлена слабостями технологий разграничения доступа (распределения прав) к функционалу UEFI между различными пользователями и администраторами.	Внутренний нарушитель с низким потенциалом.	SecureBoot, CSM, Главный ключ, NVRAM, PCI-устройства, Внешние носители.	Реализация данной угрозы возможна при условии физического доступа к терминалу и, при необходимости, к системному блоку компьютера.

2.4 Анализ успешных реализаций угроз целостности, доступности и конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI

Угроза внедрения вредоносного кода (угроза нарушения доступности). Угроза заключается в способности заставить UEFI выполнять вредоносный код при автоматическом запуске компьютера, установив его в UEFI с помощью замены микросхемы SPI либо обновления программного обеспечения UEFI на иную версию, которая уже содержит вредоносный код. Угроза связана со слабостями технологий контроля за обновлением программного обеспечения UEFI, а также заменой чипсета UEFI. Реализация угрозы внедрения вредоносного кода возможна в ходе проведения ремонтных работ и обслуживания компьютера. CMOS SRAM (статическая память с произвольным доступом). В результате уязвимости CMOS SRAM образуется скопление всего в одном месте: UEFI, часть кода сетевой карты GbE, основная часть чипсета ME и многое другое. Для упорядочивания этой ситуации Intel добавил в микросхему Flash Descriptor, который прописывает права доступа владельцев к региону. Для того чтобы отделить нововведения владельцев, предлагалось установить сразу две микросхемы SPI, первая для Descriptor, ME и GbE, вторая под остаток UEFI, после чего #WP второго чипа на аппаратном уровне защищает его от записи. Реализация угрозы возможна: в случае отсутствия наличия двух чипов, которые необходимы для микросхемы Flash Descriptor; при наличии физического доступа у нарушителя увеличивает риск реализации данной угрозы, поскольку вывод #WP на GPIO (низкоуровневом интерфейсе ввода-вывода прямого управления) изначально нарушает безопасность; злоумышленная порча микросхемы RW является возможностью реализации данной угрозы доступности конфиденциальной информации.

Угроза несанкционированного выключения, либо обхода механизма защиты от записи (угроза нарушения доступности). Угроза связана со слабостями мер по разграничению доступа к управлению механизмом

защиты UEFI от записи, а также уязвимостями механизма обновления UEFI, приводящими к переполнению буфера.

Способы реализации угрозы возможны исходя из следующих условий:

- при отсутствии механизма защиты UEFI от записи;
- успешной эксплуатации нарушителем уязвимости механизма обновления UEFI, которая приведет к переполнению буфера.

UEFI реализация. Нарушитель, изменяя размер и указатель буфера, осуществляет в него запись. Злоумышленник, с помощью внедрения либо вредоносного программного кода, либо программных закладок способен передать данные параметры таким образом, чтобы они повлияли на буфер, а тот в свою очередь вышел за границы RAM-SMRAM. Поскольку обработчик SMI имеет доступ к SMRAM, то будет переписана определенная часть данных впереди SMRAM. Тем самым, буфер переполняется, приводя к обходу механизма защиты от записи, следовательно, данная угроза успешно реализована.

Угроза загрузки нештатной операционной системы (угроза нарушения доступности). Угроза обусловлена возможностью подмены нарушителем загружаемой операционной системы с помощью несанкционированного переконфигурирования пути доступа к загрузчику операционной системы в UEFI. Угроза загрузки операционной системы возможна при условии доступности нарушителю параметра настройки UEFI – указания источника загрузки операционной системы. Загрузчик, который обладает возможностью выполнения произвольного кода до появления ExitBS события, приводит к тому, что начальные стадии загрузки имеют весь доступ к переменным BS, также как и к Setup. В случае если изготовитель платформы не предусмотрел запрет записи в данную переменную после того, как временное окно вызова BIOS Setup завершилось, то сам загрузчик способен выполнить чтение и изменение содержимого переменной Setup. Данная угроза может быть

устранена на этапе установки платформы изготовителя, который предусмотрел настоящую уязвимость загрузчика. В других случаях, нарушитель с физическим доступом с помощью параметра указателя буфера меняет значение в настройках UEFI, тем самым производя загрузку иной операционной системы и, тем самым, успешно реализует данную угрозу.

Восстановление предыдущей уязвимой версии UEFI (угроза нарушения доступности). Данная угроза обусловлена слабостями технологий контроля за обновлением программного обеспечения UEFI.

При использовании технологии обновления UEFI возможно возникновение следующей ситуации:

- на компьютере уже установлена некоторая версия UEFI, для которой на момент её работы не были известны ее уязвимости;
- в силу определенных обстоятельств, UEFI (несанкционированные действия нарушителя, системные ошибки) проходит процедуру обновления, сохраняя в процессе предыдущую версию UEFI на случай возобновления системы.

Угроза восстановления предыдущей уязвимой версии, как и предыдущая угроза загрузки нештатной операционной системы, может быть реализована при наличии загрузчика, который обладает возможностью выполнения произвольного кода до появления ExitBS события. Также, отсутствие знаний о слабостях установленной версии UEFI приведет к реализации данной угрозы нарушителем с как с физическим доступом, так и с удаленным доступом к системе.

Нарушение изоляции среды исполнения UEFI (угроза доступности). Угроза обусловлена возможностью изменения параметров и (или) логики работы программного обеспечения UEFI вследствие программного воздействия из операционной системы компьютера или путём

несанкционированного доступа к каналу сетевого взаимодействия серверного сервис-процессора. Данная угроза обусловлена слабостями технологий разграничения доступа к UEFI, его функциям администрирования и обновления, со стороны операционной системы, а также каналов связи.

Реализация данной угрозы обусловлена безопасностью прошивки, а именно доверием к системам, имеющим влияние операционной системы. Устройства необходимо сбросить и провести инициализацию вручную, очистить память и не использовать ничего из нее, а также свои сервисы Runtime, после ReadyToBoot, компонентам прошивки пользоваться запрещено. Тем самым, неосторожность использования приведет к образованию UEFI с чужим кодом, и вполне легальным драйверам в SMRAM уже нет места. Иными словами, неосторожное обращение с устройствами, влечет за собой реализацию угрозы нарушения изоляции среды исполнения UEFI.

Угроза изменения режимов работы аппаратных элементов компьютера (угроза доступности). Угроза связана со слабостями технологий разграничения доступа по управлению UEFI. Реализация угрозы осуществляется при условии, что нарушитель обладает следующим параметром настройки UEFI – указание источника загрузки операционной системы. Загрузчик (boot loader) - первичная программа, которую запускает UEFI. Загрузчик отвечает за загрузку операционной системы с желаемыми параметрами ядра и initial RAM disk перед тем, как начать процесс загрузки. Кроме того, существует возможность добавлять в загрузочное меню UEFI собственные пункты. UEFI-загрузчик, или любой исполняемый файл UEFI может быть в формате PE (формат исполняемых файлов, объектного кода и динамических библиотек, используемый в 32- и 64-битных версиях операционной системы Microsoft Windows) , или в формате TE, который, в принципе, тот же PE, только с уменьшенными заголовками, уменьшающие

количество затронутого места в памяти. Перевод PE в TE считается типичным, SecureBoot можно было обойти лишь изменением файла с загрузчиком, поэтому проблема была признана серьезной и быстро была принята к исправлению. К сожалению, на данный момент системы, не обладающие подобной технологией, все еще встречаются. И применение подобных вычислительных машин является прямой реализацией подобной угрозы.

Сбой процесса обновления UEFI (угроза доступности). Данная угроза обусловлена возможностью выведения из рабочего состояния компьютера из-за внесения критических ошибок в программное обеспечение UEFI в результате сбоя процесса его обновления. Угроза связана со слабостями технологий контроля за обновлением программного обеспечения UEFI. AcpiNVS. Именно в этой области памяти и хранится S3 BootScript. Основная часть защитных механизмов, которая обеспечивает защиту от внедрения кода в микросхему SPI, от НСД в SMM, настраивается через регистры процессора и чипсета, а для успешного преодоления данных механизмов необходимо найти BootScript в памяти, далее регистр, поменяв в нем значения, чтобы S3 Resume защита не была включена. Для минимизации уязвимости, Intel внедрил SmmLockBox. Суть атаки на AcpiNVS – после составления скрипта, он будет скопирован в SMRAM, при том, что оригинальный BootScript не удален. Восстановление из S3 вызывается обработчиком SMI, который в свою очередь проверяет наличие совпадения оригинального BootScript с копией в SMRAM, а в случае отсутствия данного совпадения — либо переписывает измененный BootScript копией, либо перезагружает компьютер. Реализация данной угрозы возможна в том случае, если система старше 2015 года выпуска и обладает всеми проблемами с прошивкой с S3 BootScript.

Подбор пароля UEFI (угроза доступности). Угроза связана со слабостями механизма аутентификации, реализуемого в консолях UEFI.

Реализация угрозы возможна при следующих условиях, если:

- нарушитель, обладает физическим доступом к компьютеру и может осуществлять перезагрузку системы;
- нарушитель, обладает специальными программными средствами перебора паролей UEFI и привилегиями в системе по установке и запуску подобных средств.

При наличии доступа к записи хранилища NVRAM у нарушителя, то он может просто удалить ключ, что повлечет за собой отключение SecureBoot, а тот в свою очередь перейдет в режим установления новых ключей. Подобная реализация угрозы возможна в случае прямого и сетевого доступа нарушителя к системе. Злоумышленник, удаляет ключ и подбирает новый пароль, что влечет за собой нарушение доступности информации, хранимой на данном компьютере.

Установка уязвимых версий обновления программного обеспечения (угроза нарушения целостности). Угроза обусловлена в возможности внесения уязвимостей в программное обеспечение UEFI в процессе его обновления, которые могут быть задействованы в дальнейшем для вывода компьютера в состояние отказа в обслуживании, либо выполнения вредоносного кода автоматическом запуске компьютера. Реализация данной угрозы возможна с использованием ACPI S3 – режимом ожидания, или всем известным как режим сна. S3 является очень важной характеристикой любого персонального компьютера, поскольку от работоспособности сохранения и восстановления контекста при включении зависит многое. В случае, внесения уязвимостей, либо внедрения вредоносного программного обеспечения в составные элементы ACPI S3, то реализация данной угрозы является успешной.

Программный сброс пароля UEFI, аппаратный сброс пароля UEFI (нарушение целостности). Угроза связана со слабостями мер разграничения доступа в операционной системе к функции сброса пароля UEFI (программный сброс). Угроза связана с уязвимостями некоторых системных (материнских) плат – наличием механизмов аппаратного сброса паролей, установленных в UEFI (аппаратный сброс).

CSM. SecureBoot не поддерживается при наличии CSM, иными словами компьютеры, которые используют старые операционные системы, не способные выполнять загрузку без CSM. В таком случае, SecureBoot лишен всех защитных механизмов. К примеру, в Windows 7 отсутствует поддержка GOP, а без нее загрузка операционной системы в отсутствие CSM или не работает вовсе, или в произвольном виде. Данный факт делает Windows 7 несовместимым по отношению к SecureBoot. Даже в том случае, если пользователь сам подпишет для нее загрузчик, тем самым угроза аппаратного сброса успешно реализована.

BLE и BIOS_WE биты. Данные биты позволяют чипсету подать команду на запись, они доступны любому коду, в связи с чем, происходит генерация SMI, BIOS регистрирует обработчик SMI. В общем виде данная защита основывается на добавлении BIOS обработчика, и генерация SMI. В конечном итоге, для осуществления атаки необходим лишь SMI_Lock, для отключения источника SMI и выполнения задуманных планов, тем самым угроза программного сброса успешно реализована.

2.5 Характеристики средств вычислительной техники с UEFI

Основными критериями оценки средств вычислительной техники являются эксплуатационно-технические характеристики, к примеру объем памяти устройства, быстродействие точность вычисления и т.д. Приведена краткая характеристика основных критериев оценки средств вычислительной

техники. Угроза заключается в возможности осуществления нарушителем несанкционированного доступа к настройкам UEFI после перезагрузки компьютера путём ввода «пустого» пароля.

Объем памяти электронно-вычислительной машины. Как правило, определяется максимальным возможным количеством хранимой информации, расположенной в электронно-вычислительной машине. Объем памяти запоминающего устройства измеряется в байтах. Память средства вычислительной техники делится на внутреннюю и внешнюю. Внутренняя память, оперативная, по объему допустимой информации может отличаться в зависимости от класса машины определённая системой адресации электронно-вычислительной машины. Объем внешней памяти, из-за съёмных конструкций накопителей и блочных структур находится в неограниченном диапазоне.

Точность вычислений электронно-вычислительной машины. Варьируется в зависимости от количества разрядов, необходимых для представления одного числа. На сегодняшний день электронно-вычислительные машины оснащены 32 разрядными и 64 разрядными микропроцессорами, что в свою очередь достаточно для поддержания высокой точности расчетов в расширениях с высокими показателями требований. Но, в случае, если данного количества разрядов не достаточно количество, возможно использование двойную или тройную разрядную сеть.

Быстродействие электронно-вычислительной машины. Характеризуется количеством элементарных операций, которые выполняет центральный процессор в секунду и, также, по организации ее памяти, поскольку затраченное время на поиск необходимых данных в памяти, существенно оказывает влияние на быстродействие (элементарная операция – любая простая операция по типу пересылки, сложения, сравнения и т.д.). Область применения электронно-вычислительной машины оказывает

влияние на величину быстродействия. Решение более сложных задач требует объединения нескольких электронно-вычислительных машин в единый комплекс с необходимой совокупностью быстродействия. В вопросе о быстродействии часто используют понятие производительности. В первом случае быстродействие обусловлено системой элементов в электронно-вычислительной машине, то уже во втором случае производительность связано с архитектурой и конкретными задачами, которыми необходимо решить. Быстродействие не является постоянной величиной для электронно-вычислительной машины, отсюда разделение на критерии: пиковое быстродействие, обусловленное тактовой частотой процессора не учитывая обращения к оперативной памяти; номинальное быстродействие, обусловленное системными издержками на организацию вычислительного процесса; эксплуатационное быстродействие, обусловленное характером задач, а именно составом операций или их разности.

Надежность электронно-вычислительных машин. Данная способность компьютера наделяет его возможностью сохранять свои свойства при установленных условиях его эксплуатации за определенный период времени.

Критерии надежности:

- вероятность безотказной работы за условный временный период при установленных условиях эксплуатации;
- наработка электронно-вычислительной машины на отказ;
- время, затраченное на восстановление машины (средняя величина).

Для сложных систем, объединенных, по типу «вычислительный комплекс» отказ не является необходимым, поскольку выход из строя отдельных элементов системы может привести лишь к уменьшению эффективности работоспособности, но не ко всей потере функционирования системы.

Для разработки рекомендаций по обработке конфиденциальной информации средствами вычислительной техники с UEFI необходимо следующее программно-аппаратное обеспечение:

- СВТ с установленным UEFI;
- ОС MS Windows 7 (и выше).

Структура средства вычислительной техники с UEFI приведена в приложении Д на рисунке Д.1.

3 Реализация угрозы отказа в обслуживании CBT с UEFI

В соответствии с техническим заданием выпускной квалификационной работы проведена реализация угрозы внедрения вредоносного программного обеспечения, которая впоследствии повлекла за собой блокировку CBT.

Описание успешной реализации угрозы отказа в обслуживании CBT.

При реализации данной угрозы задействована уязвимость SecureBoot, реализованная с помощью OptionROM. Программная технология SecureBoot, благодаря которой UEFI проверяет наличие подлинности исполняемых ей внешних компонентов, таких как загрузчики, драйверы, и UEFI OptionROM. Запуск UEFI OptionROM из PCI-устройств при работающем SecureBoot не должен происходить, если соответствующий OptionROM не прошел верификацию, но на практике большое количество систем доверяет PCI-устройствам беспрекословно и загружает все без дополнительной проверки. Системы без SecureBoot подвержены такой атаке безоговорочно. Именно поэтому вынос PCI-E на внешние разъемы по типу: Thunderbolt, PCMCIA, ExpressCard и т.п. — прямая угроза безопасности платформы, даже не смотря на то, что любое PCI-устройство может инициировать DMA с любым регионом физической памяти, за исключением SMRAM, и только в том случае, если изготовитель платформы не забыл установить защиту.

В плату ПЭВМ была встроена микросхема PCI (плата расширения), с вредоносным программным обеспечением. Нарушитель внедряет микросхему в плату ПЭВМ, тем самым приводя в исполнение вредоносный код. При последующем включении компьютера было получено следующее сообщение.

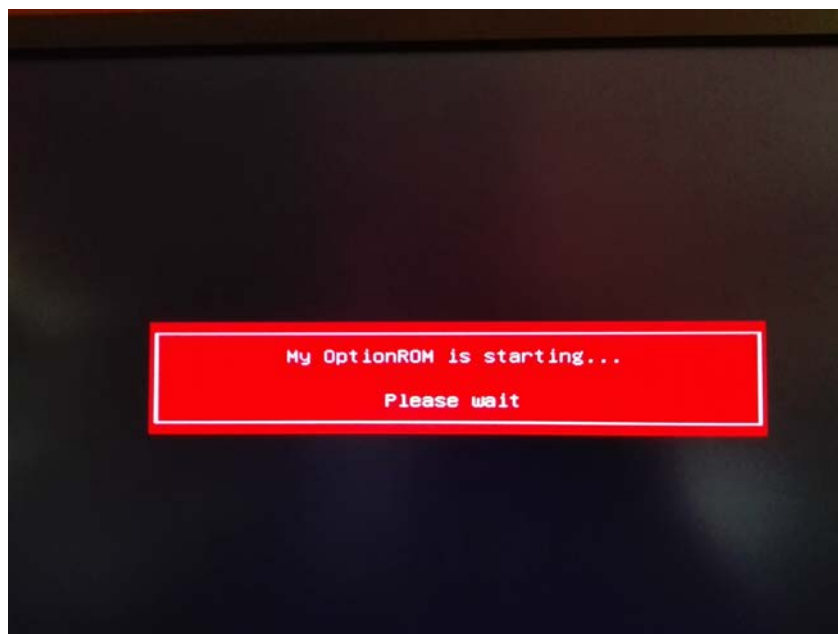


Рисунок 1 – Ожидание запуска CBT

После ожидания загрузки OptionROM система выдает следующее сообщение об ошибке.

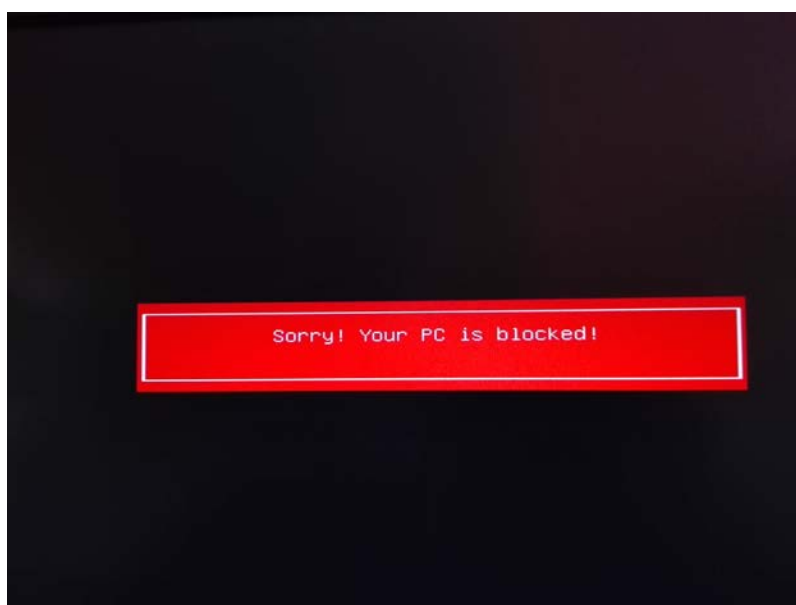


Рисунок 2 – Сообщение об ошибке

Полученный результат является доказательством успешной реализации угрозы внедрения вредоносного кода. В приложении Г на рисунке Г.1 приведена схема реализации угрозы.

4 Разработка рекомендаций по обработке конфиденциальной информации средствами вычислительной техники с UEFI

В соответствии с идентифицированными уязвимостями UEFI и разработанной моделью угроз безопасности необходимо соответствие СВТ с UEFI с заданными требованиями по защите конфиденциальной информации.

Необходимые требования.

Для проведения необходимых работ по обработке конфиденциальной информации необходимо проведение организационно-технических мер по устранению уязвимостей, приведенных в пункте 1.3 пояснительной записки.

Также, проведение организационно-технических мер по минимизации риска возникновения угроз информационной безопасности в областях доступности, конфиденциальности, целостности представленной в пункте 2.3 пояснительной записки.

Учитывая приведенную модель угроз безопасности в пункте 2.2 пояснительной записке, а также перечень источников угроз проведенного в пункте 2.1 пояснительной записки, необходимо проведение организационно-технических мер по защите конфиденциальной информации.

В соответствии с установленными характеристиками средств вычислительной техники с UEFI для конкретной организации, необходимо проведение организационно-технических мер по защите конфиденциальной информации.

Разработанные модель угроз и рекомендации будут предназначаться для операторов, организующих и осуществляющих обработку конфиденциальной информации средствами вычислительной техники с UEFI, а также для заказчиков и разработчиков информационных систем и подсистем, включающих в себя данные средства. При соблюдении всех установленных рекомендаций риск возникновения угроз безопасности минимизирован.

ЗАКЛЮЧЕНИЕ

В процессе работы проводился анализ актуальности исследования UEFI, его описание и определение основных характеристик, идентификация и обзор уязвимостей UEFI в области обеспечения доступности, целостности и конфиденциальности информации, анализ уязвимостей, разработана модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники в соответствии с приведенными:

- идентификацией источников угроз информационной безопасности;
- моделью нарушителя безопасности;
- идентификацией угроз информационной безопасности;
- способов реализации угроз безопасности;
- характеристикой средств вычислительной техники с UEFI.

В результате проделанной работы была реализована из приведенного списка угроза нарушения доступности и разработаны рекомендации по обработке конфиденциальной информации средствами вычислительной техники с UEFI с учетом разработанной модели угроз безопасности конфиденциальной информации.

Все выполненные пункты соответствуют техническому заданию, следовательно, выпускная квалификационная работа выполнена в полном объеме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 UEFI, как новый шаг развития BIOS [Электронный ресурс]: Режим доступа:

http://knowledge.allbest.ru/programming/2c0a65625a2bc78b4d43b89421216c37_0.html , свободный

2 Немного про UEFI и SecureBoot [Электронный ресурс]: Режим доступа: <https://habrahabr.ru/post/185492/>, свободный

«Extensible Firmware Interface» [Электронный ресурс]: Режим доступа: <http://ru.wikipedia.org> , свободный

3 Особенности установки на платы с UEFI. Русскоязычная документация [Электронный ресурс]: Режим доступа:

http://help.ubuntu.ru/wiki/%D1%80%D1%83%D0%BA%D0%BE%D0%B2%D0%BE%D0%B4%D1%81%D1%82%D0%B2%D0%BE_%D0%BF%D0%BE_ubuntu_desktop_14_04/%D0%BE%D1%81%D0%BE%D0%B1%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D1%83%D1%81%D1%82%D0%B0%D0%BD%D0%BE%D0%B2%D0%BA%D0%B8_%D0%BD%D0%B0_%D0%BF%D0%BB%D0%B0%D1%82%D1%8B_%D1%81_uefi, свободный

4 Банк данных угроз безопасности информации [Электронный ресурс]: Режим доступа: <http://www.bdu.fstec.ru/threat> , свободный

5 Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка).

ФСТЭК России, 2008 год [Электронный ресурс]: Режим доступа:

<http://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god> , свободный

6 О безопасности UEFI, часть четвертая [Электронный ресурс]: Режим доступа: <http://savepearlharbor.com/?p=266196> , свободный

7 О безопасности UEFI, части нулевая и первая [Электронный ресурс]:
Режим доступа: <https://habrahabr.ru/post/266935/> , свободный

8 Немного про UEFI и Secure Boot [Электронный ресурс]: Режим
доступа: <https://habrahabr.ru/post/185492/> , свободный

9 Модификация UEFI BIOS, часть первая: знакомство с
UEFITool [Электронный ресурс]: Режим доступа:
<https://habrahabr.ru/post/211574/> , свободный

ПРИЛОЖЕНИЕ А



Рисунок А.1 - Интерфейс UEFI

ПРИЛОЖЕНИЕ Б

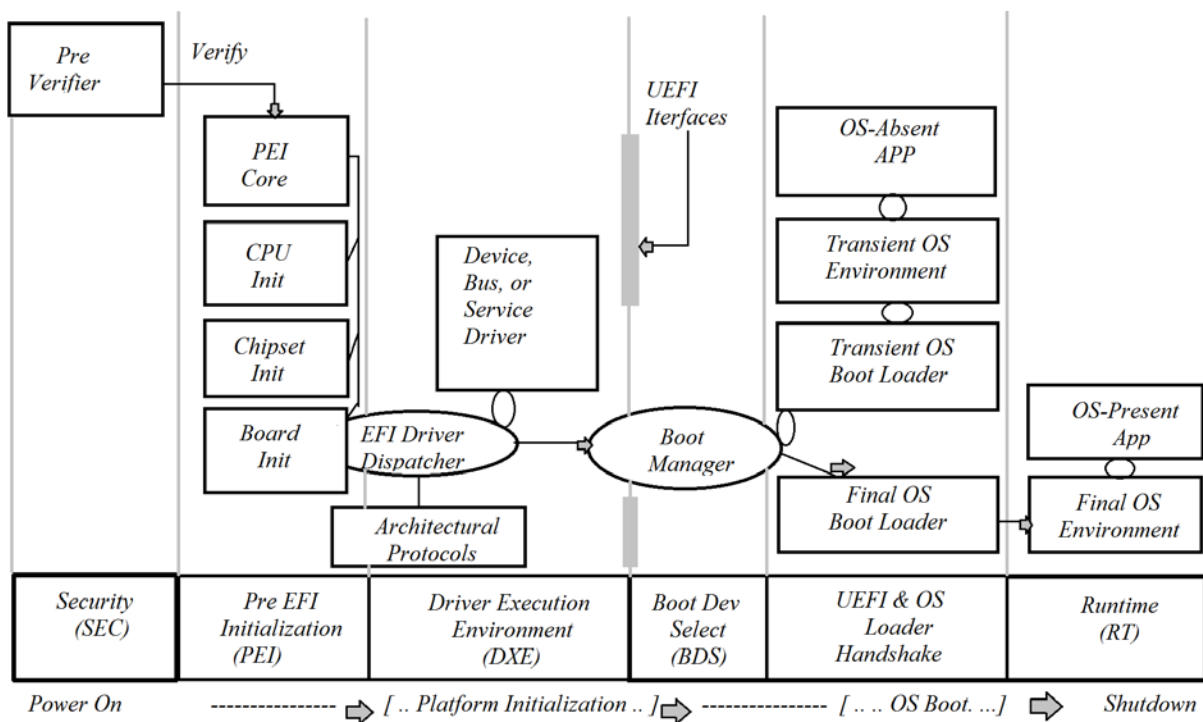


Рисунок Б.1 – Начало работы UEFI

ПРИЛОЖЕНИЕ В

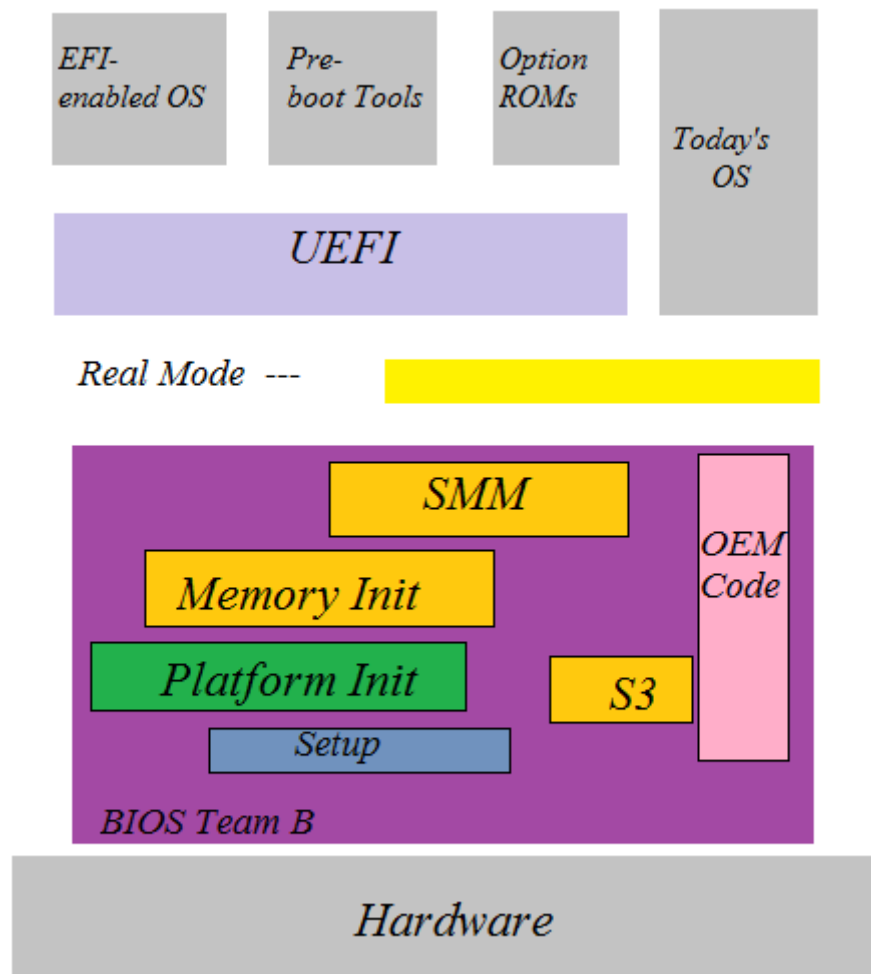


Рисунок В.1 - Архитектура UEFI

ПРИЛОЖЕНИЕ Г

Схема реализации угрозы безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с UEFI

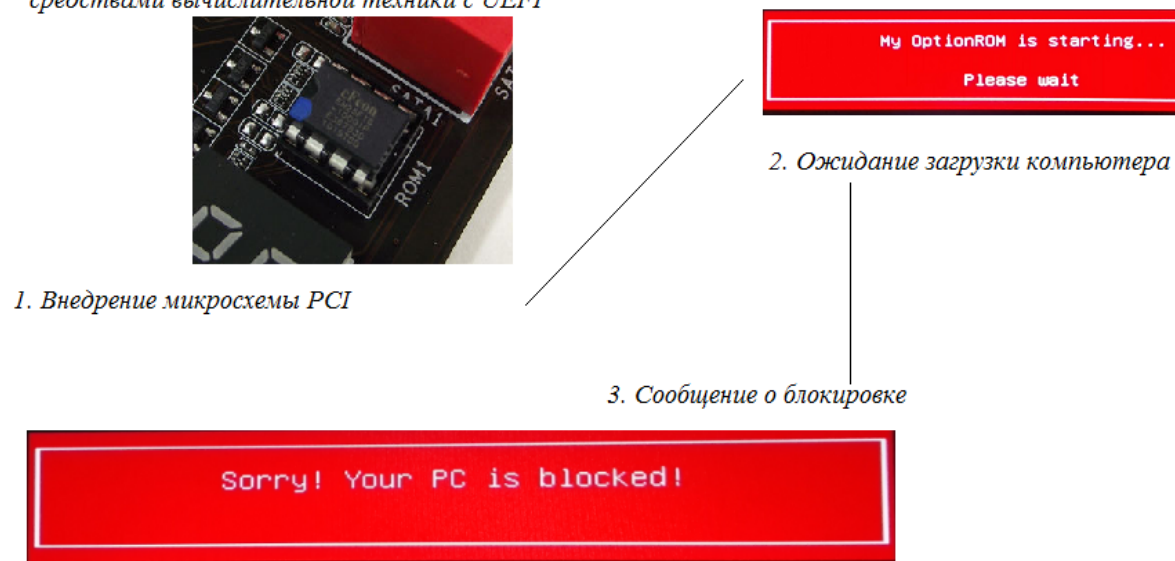


Рисунок Г.1 - Схема реализации угрозы

ПРИЛОЖЕНИЕ Д

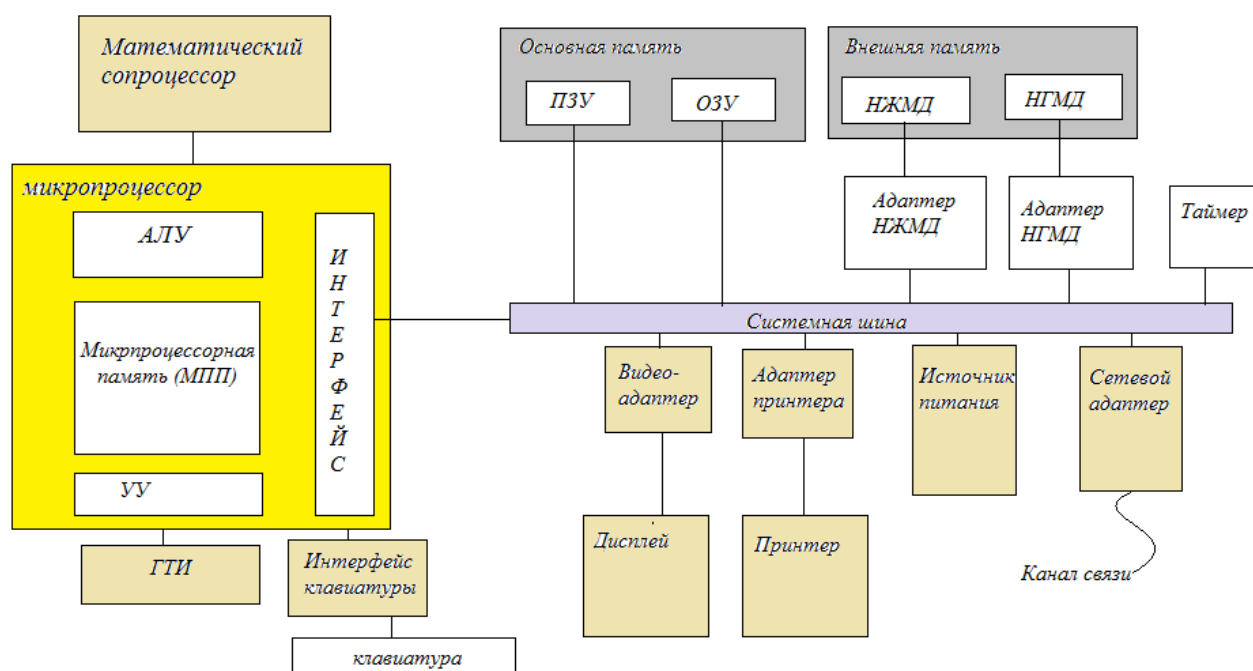


Рисунок Д.1 - Структура средства вычислительной техники с UEFI

МИНОБРАЗОВАНИЯ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего профессионального образования

«НЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

УДК 004.056.53

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Выпускающая кафедра:
Информационная безопасность систем
и технологий

Учебная группа ГНИИ

УТВЕРЖДАЮ

Зав. кафедрой ИБСТ

к.т.н., доцент С.А. Зефирова

27.04 2016 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ

РАБОТУ

студентки группы ГНИИ Дубининой Марии Юрьевны

Специальность 100503 Информационная безопасность

автоматизированных систем

Тема дипломного проекта: Модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI».

Руководитель ВКР

и. о. начальника сектора
АО «ЦНИИЭИ»



Клейменов Алексей Александрович

Нормоконтролер

к.т.н., доцент



Иванов А.П.

1 Цели и задачи ВКР

Цели работы:

- разработка модели угроз целостности, доступности, конфиденциальности информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI»;
- разработка рекомендаций по обработке конфиденциальной информации средствами вычислительной техники с UEFI.

Разработанные модель угроз и рекомендации предназначены для операторов, организующих и (или) осуществляющих обработку конфиденциальной информации средствами вычислительной техники с UEFI, а также для заказчиков и разработчиков информационных систем и комплексов, включающих в себя данные средства.

2 Тактико-технические требования к выполнению ВКР

Технические требования:

- модель угроз должна включать в себя:
 - характеристику средств вычислительной техники с UEFI;
 - перечень источников угроз;
 - список угроз целостности информации, обрабатываемой средствами вычислительной техники с UEFI;
 - список угроз доступности информации, обрабатываемой средствами вычислительной техники с UEFI;
 - список угроз конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI;
 - способы реализации угроз целостности, доступности и конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI;
 - оценку последствий реализации угроз целостности, доступности и конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI;



- модель нарушителя безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с UEFI;

- должны быть разработаны рекомендации к средствам вычислительной техники с UEFI с учетом разработанной модели угроз;

- при выполнении ВКР на практике должна быть реализована одна угроза из списка в разработанной модели угроз.

В ВКР должны быть рассмотрены следующие вопросы:

- анализ актуальности исследований UEFI, описание и основные характеристики UEFI;

- анализ уязвимостей UEFI в части обеспечения доступности, целостности и конфиденциальности информации;

- анализ успешных реализаций угроз целостности, доступности и конфиденциальности информации, обрабатываемой средствами вычислительной техники с UEFI;

- анализ требований к средствам вычислительной техники, обрабатывающих конфиденциальную информацию, с учетом нормативных документов ФСТЭК и законодательства РФ.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- интерфейс UEFI – 1 л., ф. А1 (плакат);

- архитектура UEFI – 1 л., ф. А1 (плакат);

- структура средства вычислительной техники с UEFI – 1 л., ф. А1 (плакат);

- UEFI начало работы – 1 л., ф. А1 (плакат);

- уязвимости UEFI – 1 л., ф. А1 (плакат);

- угрозы безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с UEFI – 1 л., ф. А1 (плакат);



– схема реализации угрозы безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с UEFI – 1 л., ф. А1 (плакат);

– рекомендации по обработке конфиденциальной информации средствами вычислительной техники с UEFI – 1 л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № 194 от «25» 04 2016 г.

Дата выдачи задания «15» февраля 2016 г.

Время дипломного проектирования с 18.04.2016 г. по 10.07.2016 г.

Задание к исполнению принял «15» февраля 2016 г.

Исполнитель ВКР  – Лубнина М.Ю.



Ректору Пензенского
государственного университета
А. Д. Гулякову
студентки 5 курса ФПИТЭ
очной формы обучения
Дубининой Марии Юрьевны

Заявление

Я, Дубинина Мария Юрьевна, студент 5 курса очной формы обучения специальности 10.05.03 – «Информационная безопасность автоматизированных систем», прошу провести проверку с использованием системы «Антиплагиат» дипломной работы на тему: «Модель угрозы безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI», выполненной мной самостоятельно, на содержание элементов плагиата.

Все прямые цитирования из печатных и электронных источников, а также из опубликованных ранее научных квалификационных работ, кандидатских и докторских диссертаций имеют соответствующие ссылки.

Я ознакомлен с действующим Стандартом университета «Выпускная квалификационная работа обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета и программам магистратуры», согласно которому обнаружение плагиата является основанием для недопуска ВКР к защите и отчисления из университета.

 М.Ю. Дубинина

ВКР представлена на проверку

Руководитель ВКР  А.А. Косычев

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI» студента 5 курса М.Ю. Лубниной специальности 10.05.03 – «Информационная безопасность автоматизированных систем».

Руководитель ВКР и. о. начальника сектора АО «ПНИЭИ» Клейменов Алексей Александрович.

Отчет о проверке № 1

ФИО: Лубнина Мария Петровна
дата выгрузки: 02.06.2016 23:29:43
периодичность до: [настройка](#) / ID: 1267396
отчет предоставлен сервисом «Антиплагиат»
на сайте [http://www.antiplagiat.ru](#)

Информация о документе

ID документа: 33
Имя исходного файла: ВКР_Лубнина МО_11785.pdf
Размер текста: 1090 кб
Тип документа: по умолчанию
Синонимы в тексте: 0/419
Слов в тексте: 11775
Число предложений: 497

Информация об отчете

Дата: Отчет от 02.06.2016 23:28:47 - Повторный текстовый отчет
Комментарий от пользователя:
Средняя оригинальность: 97,5%
Заимствования: 2,5%
Цитирование: 0%



Оригинальность: 97,5%
Заимствования: 2,5%
Цитирование: 0%

08.06.2016 г.

Секретарь ГЭК

А.А.Клейменов

А.П.Иванов

ОТЗЫВ

На выпускную квалификационную работу студентки

Пензенского государственного университета

Лубининой Марии Юрьевны

(фамилия, имя и отчество)

Тема работы: Модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI»

Целью квалификационной работы Лубининой М.Ю. является разработка модели угроз целостности, доступности, конфиденциальности информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI» и формирование рекомендаций по обработке конфиденциальной информации средствами вычислительной техники с UEFI.

Во время выполнения задания автором работы был изучен большой объем теоретического и практического материала о UEFI для дальнейшего построения модели угроз безопасности конфиденциальной информации. На основе проведенного анализа была разработана модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с UEFI, учитывающая:

- источники угроз информационной безопасности;
- модель нарушителя безопасности;
- угрозы информационной безопасности;
- способы реализации угроз безопасности.

В процессе выполнения работы была реализована угроза нарушения доступности и разработаны рекомендации по обработке конфиденциальной информации средствами вычислительной техники с UEFI. Разработанная

модель достаточно подробно определяет наличие уязвимостей средств вычислительной техники с UEFI, а также угрозы информационной безопасности и способы их реализации.

Необходимо отметить, что такая работа требует большой работоспособности, терпения и упорства, которые Лубнина М.Ю. проявила в полной мере. Ранее Лубнина М.Ю. зарекомендовала себя как ответственный и исполнительный студент.

Работа по всем приведенным пунктам технического задания выполнена в полном объеме. Пояснительная записка и плакаты содержат необходимые сведения о проделанной работе.

Считано, что дипломная работа была выполнена в полном соответствии с техническим заданием и заслуживает оценки «хорошо», а дипломник Лубнина М.Ю. достойна присвоения квалификации специалиста по информационной безопасности специальности 10.05.03 - «Информационная безопасность автоматизированных систем».

Руководитель ВКР,
и. о. начальника сектора
АО «ПНИЭИ»



 /А.А. Клейменов/

Рецензия на дипломную работу

Лубниной Марии Юрьевны

(фамилия, имя и отчество)

Тема работы: Модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI»

Дипломная работа Лубниной М.Ю. посвящена разработке модели угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI».

В процессе работы был приведен анализ актуальности исследования UEFI, а также его описание и определение основных характеристик. Проведены идентификация и обзор уязвимостей UEFI в области обеспечения доступности, целостности и конфиденциальности информации, и анализ уязвимостей средств вычислительной техники, а также проведены идентификация и обзор уязвимостей UEFI в области обеспечения доступности, целостности и конфиденциальности информации, анализ уязвимостей средств вычислительной техники. В результате была разработана модель угроз безопасности конфиденциальной информации, обрабатываемой средствами вычислительной техники с унифицированным расширяемым интерфейсом встроенного программного обеспечения «UEFI» и разработаны рекомендации по обработке конфиденциальной информации средствами вычислительной техники с UEFI.

Все пункты технического задания дипломной работы выполнены в полном объеме. В ходе работы студентом продемонстрированы хороший уровень теоретических и практических знаний.

Недостатком дипломной работы является малый объем рекомендаций к средствам вычислительной техники с UEFI для организаций обрабатывающих конфиденциальную информацию.

Учитывая тот факт, что все пункты технического задания были выполнены, считаю, что выпускная квалификационная работа может быть допущена к защите ГАК, а Лубнина М.Ю. достойна присвоения квалификации специалист по информационной безопасности по специальности «Информационная безопасность автоматизированных систем». С учетом актуальности выпускной квалификационной работы, достоверности результатов выпускной квалификационной работы, обобщенная оценка выпускной квалификационной работы составляет 9 баллов.



Заместитель начальника отделения АО «ПНИЭИ»

 /Сомкин С.А.