Код безопасности

Рынок средств защиты информации от несанкционированного доступа (СЗИ от НСД)

Декабрь, 2015 г.

Содержание

Введение

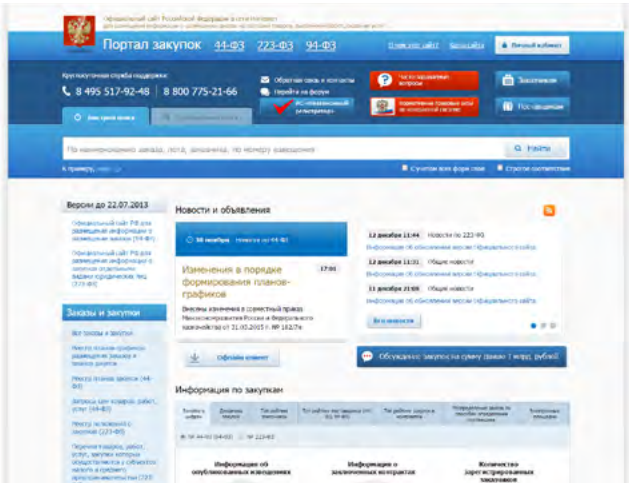
Рынок средств защиты информации от несанкционированного доступа формировался с 1992 года, после выхода руководящих документов ФСТЭК России (ранее – Гостехкомиссия России) по защите автоматизированных систем от НСД.

Применение СЗИ от НСД для защиты рабочих станций и серверов объясняется необходимостью исполнения законодательных требований по защите персональных данных (ФЗ-152 «О персональных данных»), защите государственных информационных систем (приказ ФСТЭК России №17), требований по защите конфиденциальной информации, государственной тайны и ряда других нормативных документов.

Данный обзор подготовлен с целью ознакомления с рынком СЗИ от НСД – определения основных игроков и анализа тенденций развития решений по защите информации от несанкционированного доступа.

Методика анализа

При подготовке данного обзора использовались данные с официального сайта госзакупок (http://www.zakupki.gov.ru/).

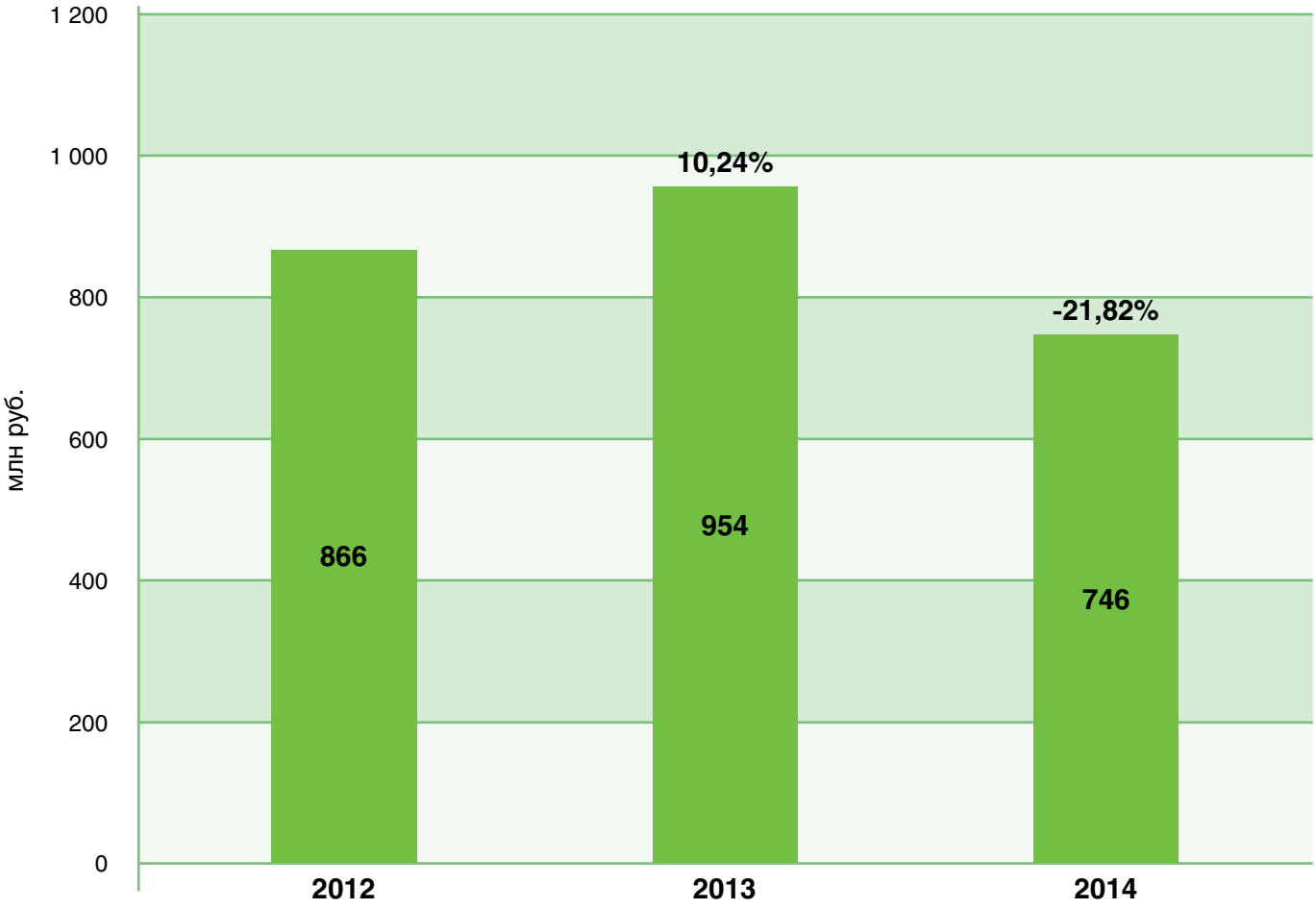


Необходимость применения СЗИ от НСД определяется рядом требований к информационным системам в организациях государственного сектора, как следствие – более 80% рынка составляют закупки госкомпаний.

Детальный анализ опубликованных на сайте госзакупок контрактов на поставку СЗИ от НСД позволил получить исчерпывающую информацию об объеме рынка и долях основных игроков за период с 2012 по 2014 год.

Оценка и динамика рынка

Исследование, основанное на анализе данных официального сайта госзакупок, позволяет сделать выводы об объеме рынка средств защиты информации от несанкционированного доступа. В 2012 году объем рынка составил 866 млн руб., в 2013 вырос примерно на 10% и составил почти 1 млрд руб. (954 млн руб.), а в 2014 году снизился на 22% по отношению к 2014 году и составил 746 млн руб.



Данную ситуацию можно объяснить снижением уровня продаж персональных компьютеров в РФ в 2014 году. По подсчетам аналитиков IDC, объем рынка ПК в натуральном выражении в 2014 году сократился на 22,7%, а объем рынка СЗИ от НСД практически напрямую зависит от количества проданных компьютеров.

Стоит отметить, что, по мнению экспертов, в целом рынок ИБ по-прежнему показывает положительную динамику, в 2014 году рост рынка, по мнению TAdviser, составил 8%.

Основные игроки

Средства защиты информации от несанкционированного доступа (СЗИ от НСД) можно условно разделить на программные продукты и программно-аппаратные комплексы (модули доверенной загрузки).

Под доверенной загрузкой принято понимать реализацию загрузки операционной системы с определенного носителя (например, внутреннего жесткого диска защищаемого компьютера). Загрузка с других носителей должна блокироваться. Причем загрузка ОС происходит только после выполнения идентификации и аутентификации пользователя, а также проверки целостности программного и аппаратного обеспечения компьютера. Тем самым обеспечивается защита компьютера от НСД на важнейшей фазе его функционирования – этапе загрузки операционной системы.

Программные средства защиты информации от несанкционированного доступа сочетают в себе ряд механизмов для безопасной работы пользователей за компьютером: разграничение доступа, контроль файлов и приложений, механизмы контроля утечек и ряд других. Управление доступом к файлам, папкам и приложениям может производиться дискреционными методами или с использованием меток конфиденциальности (так называемое мандатное разграничение доступа). СЗИ от НСД помимо инструментов защиты обеспечивают оперативный мониторинг событий ИБ и оповещение офицеров безопасности. Для расследования инцидентов безопасности в СЗИ предусмотрено ведение журналов с отображением событий НСД.

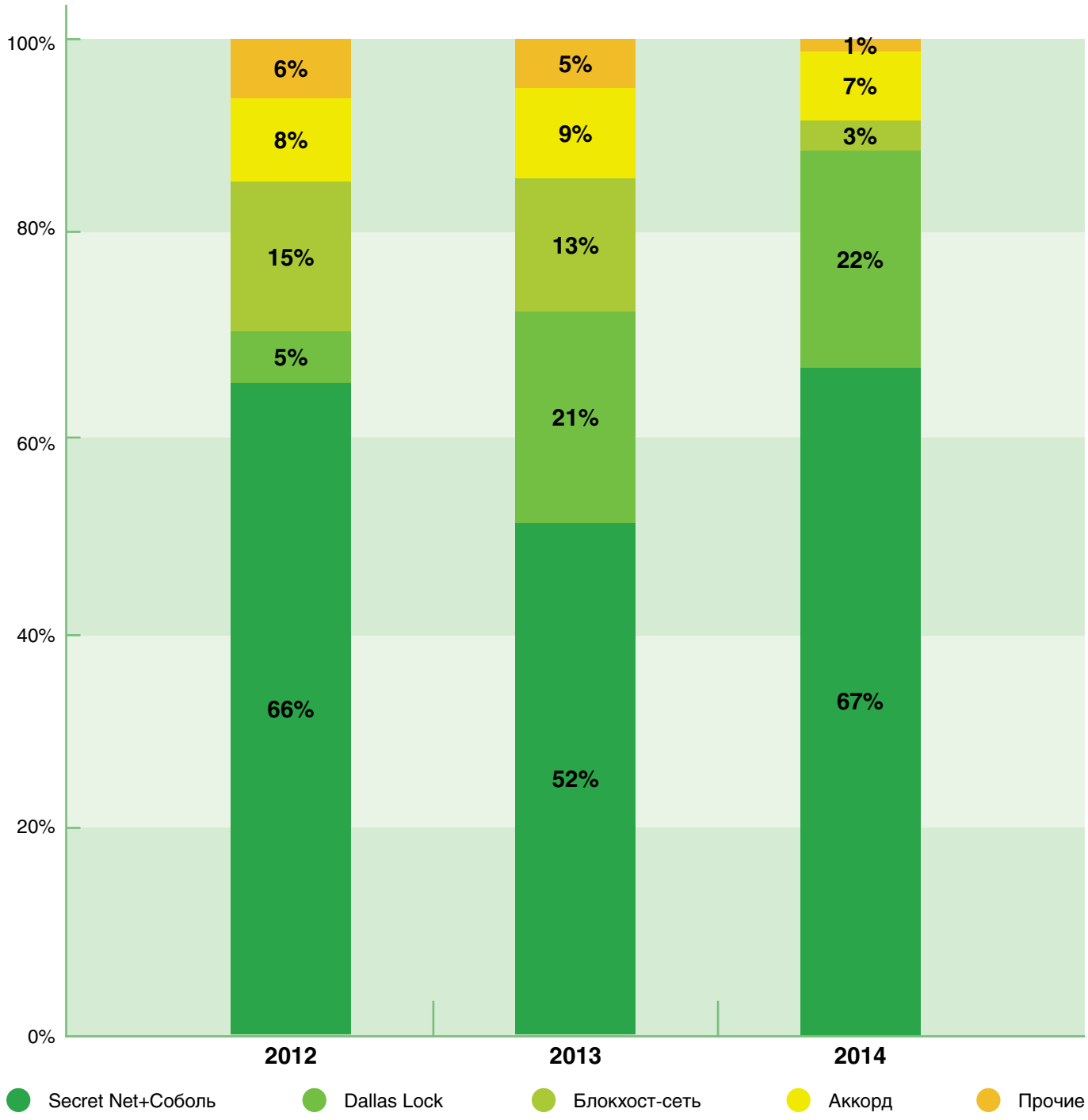
Программные СЗИ от НСД часто реализуются в двух вариантах: для защиты конфиденциальной информации (АС до класса 1Г) и защиты государственной тайны (АС до класса 1В или 1Б). Отличие таких средств защиты обычно состоит в методах управления правами доступа, маркировке выводимых на печать документов и теневом копировании конфиденциальной информации при ее выводе на подключаемые устройства.

Особенностью применения АПМДЗ и программных СЗИ от НСД является их совместное использование. Разработчики во многих случаях реализуют механизмы защиты от НСД в двух разных продуктах, которые могут иметь механизмы совместного управления и создания отчетов. Поэтому заказчики часто приобретают решения одного и того же производителя.

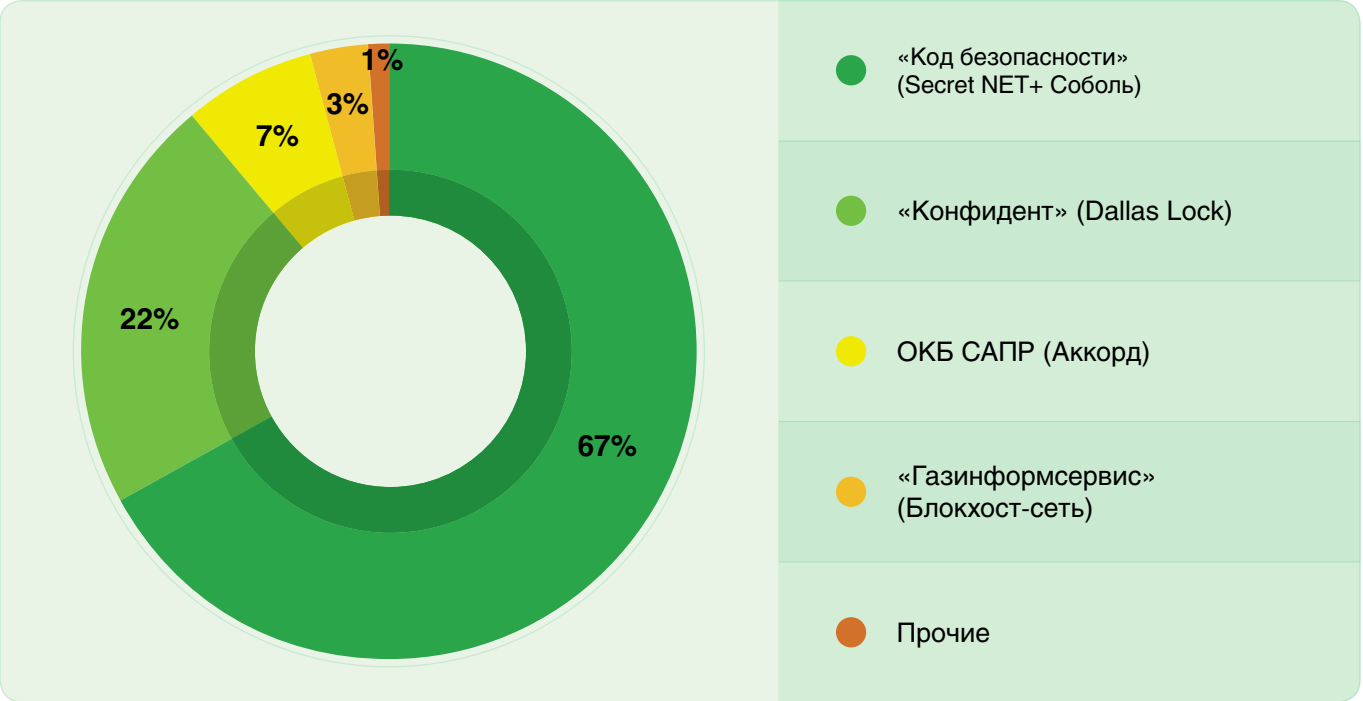
Игроки рынка СЗИ от НСД

Продукт	Вендор	Исполнение
Secret Net	Код Безопасности	Программный
Соболь	Код Безопасности	Программно-аппаратный
Аккорд	ОКБ САПР	Программно -аппаратный
Аккорд-АМДЗ	ОКБ САПР	Программно-аппаратный
Dallas Lock	Конфидент	Программный
Блокхост-сеть К	Газинформсервис	Программный
Блокхост-АМДЗ	Газинформсервис	Программно-аппаратный
Блокхост-МДЗ	Газинформсервис	Программно-аппаратный
СЗИ Аура	СПИИРАН	Программный
Diamond ACS	TSS	Программный
КСЗИ «Панцирь-С», КСЗИ «Панцирь-К»	НПП Информационные технологии в бизнесе	Программный
Страж NT	НПЦ Модуль	Программный
Криптон-замок	Анкад	Программно-аппаратный
Тринити-АПМДЗ	Setec	Программно-аппаратный
Максим-М1	НПО РусБИТех	Программно-аппаратный
М-654 «Форпост-экспресс»	Концерт Системпром	Программно-аппаратный
Щит-ЭЦП	Концерт Системпром	Программно-аппаратный
МДЗ-Эшелон	НПО Эшелон	Программно-аппаратный
ALTELL TRUST	Альтэль	Программно-аппаратный
Витязь	Kraftway	Программно-аппаратный
Цезарь	Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В.В.Соломатина (ВНИИНС)	Программно-аппаратный
Центурион	ЦНИИ экономики, информатики и систем управления (ЦНИИ ЭИСУ)	Программно-аппаратный

Структура рынка по продуктам 2012-2014



Структура рынка по поставщикам 2012-2014



СЗИ от НСД Secret Net и модуль доверенной загрузки ПАК «Соболь» разрабатываются одним вендором – «Код Безопасности», поэтому на диаграмме отображены данные по суммарному объему продаж.

Выводы:

Российский рынок СЗИ от НСД слабо сегментирован. Так, вышеупомянутые продукты «Кода Безопасности» даже в относительно неудачный для них 2013 год занимают более 50% доли рынка. А в прошлом 2014 году российскому разработчику удалось даже несколько улучшить свои показатели по отношению к 2012 году и завоевать 67% всей выручки на данном рынке.

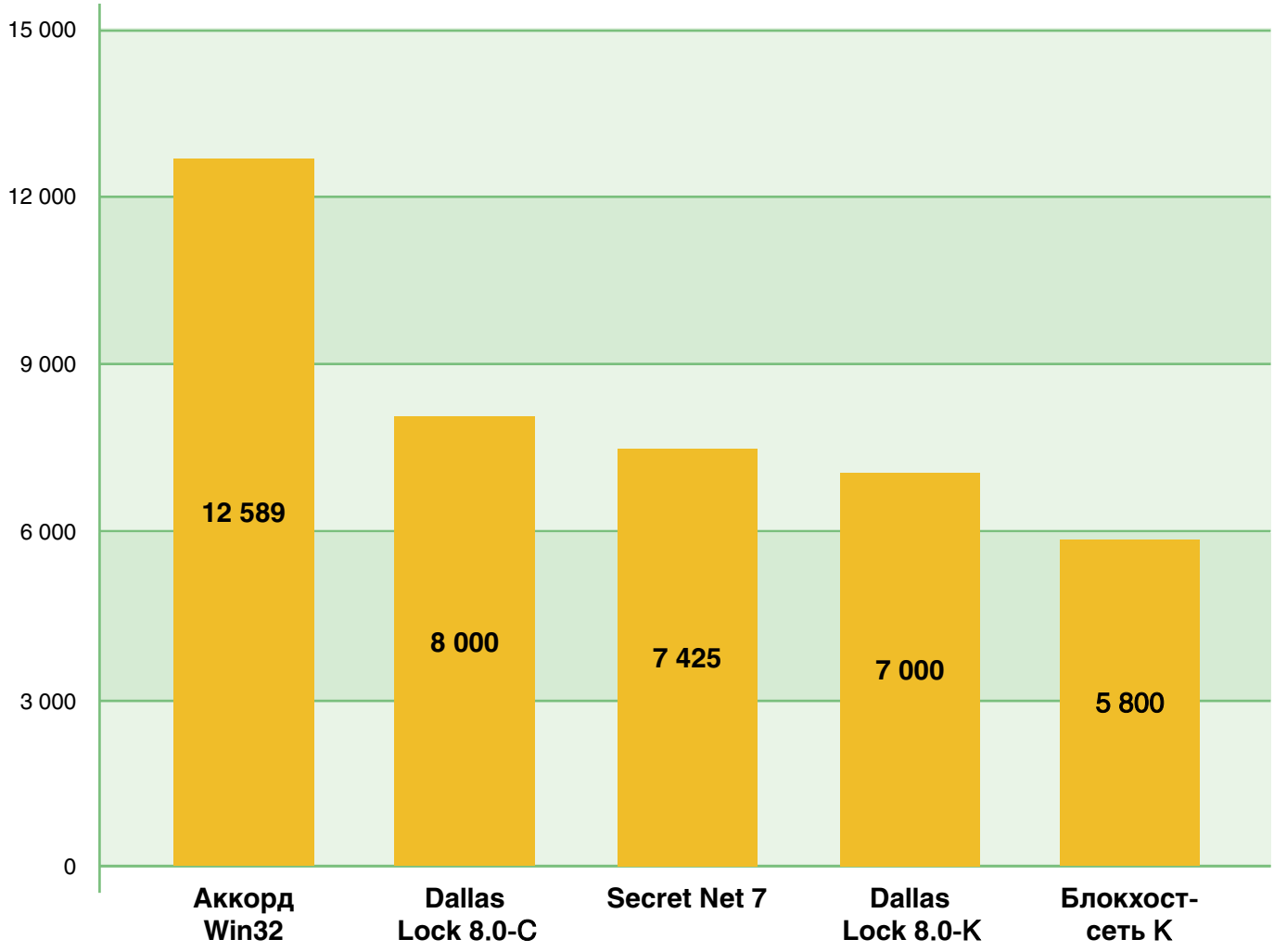
Вторым по значимости игроком по итогам прошедших трех лет стал Dallas Lock разработки компании «Конфидент», продемонстрировав стремительный рост – с 5% в 2012 году до 21% в 2013-м – и упрочив свои позиции на 1% в 2014 году.

Доля рынка СЗИ «Блокхост-сеть К» резко снизилась в 2014 году. Успехи компании в 2012–2013 годах обусловлены заключением многомиллионных контрактов с Федеральной налоговой службой.

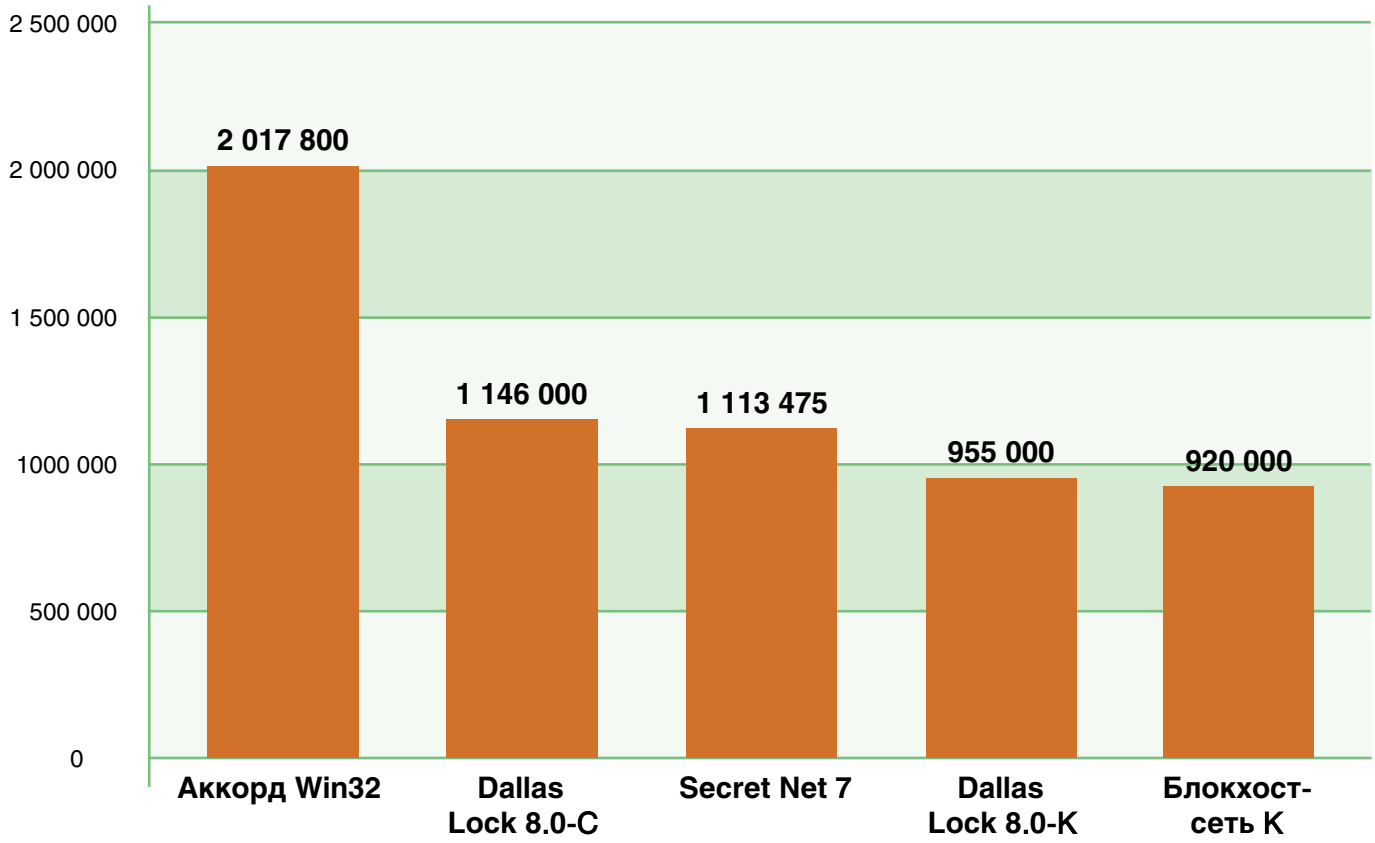
Ценовое сравнение программных СЗИ от НСД[1]

Продукт/его стоимость (руб.)	Аккорд Win 32	Блокхост-сеть К	Dallas Lock 8.0-K	Dallas Lock 8.0-C	Secret Net 7
Цена комплекта за 1 рабочее место (автономный вариант)	12 589	5 800	7 000	8 000	7425
Цена комплекта с централизованным управлением на 200 рабочих мест	2 017 800	920 000	955 000	1 146 000	1 113 475

Цена комплекта за 1 рабочее место (автономный вариант)



Цена комплекта с централизованным управлением на 200 рабочих мест



Сравнение функциональных возможностей СЗИ от НСД

	Secret Net 7.4	Dallas Lock 8.0-K (C)	Аккорд-Win32/ Win64 (ПАК)
Разработчик	ООО «Код Безопасности»	ООО «Конфидент»	ОКБ САПР
Сертификат ФСТЭК России	3СВТ, 2НДВ, защита АС до 1Б	5СВТ, 4НДВ, защита АС до 1Г (3СВТ, 2НДВ, защита АС до 1Б)	3СВТ, 2НДВ, защита АС до 1Б
Другие сертификаты	Минобороны России: 3НСД, 2НДВ		
Варианты установки СЗИ	Автономный, сетевой	Автономный, сетевой	Автономный, сетевой

	Secret Net 7.4	Dallas Lock 8.0-K (C)	Аккорд-Win32/ Win64 (ПАК)
Windows XP/Vista/7	+	+	+
Windows Server 2003/2008	+	+	+
Windows 8/8.1	+	+	+/-
Windows Server 2012/2012 R2	+	+	+
База данных	MS SQL или Oracle	Встроенная	Встроенная
Возможность централизованной установки СЗИ на рабочие станции	+	+	-
Удаленная установка СЗИ на рабочие станции	+	+	-
Наличие встроенных драйверов аппаратных идентификаторов	+	- (+)	+
Поддержка централизованного управления аппаратными средствами доверенной загрузки	+ (ПАК «Соболь»)	-	-
Программная реализация доверенной загрузки	+	- (+)	-
Идентификация и аутентификация пользователей при входе в систему	+	+	+
Возможность блокировки сессии пользователя по периоду неактивности	+	-	+
Сквозная аутентификация по аппаратным идентификаторам со средством доверенной загрузки	+	-	+
Поддерживаемые аппаратные идентификаторы	eToken JaCarta Rutoken iButton iKey ESMART	eToken JaCarta Rutoken iButton	eToken iButton ШИПКА

	Secret Net 7.4	Dallas Lock 8.0-K (C)	Аккорд-Win32/ Win64 (ПАК)
Возможность блокировки станции при нарушении целостности	+	+	+
Возможность восстановления объектов при нарушении целостности	+	+	-
Контроль неизменности аппаратной конфигурации компьютера	+	-	+
Контроль неизменности (целостности) разрешенных к запуску модулей перед их запуском	+	-	-
Блокировка запуска при нарушении целостности контролируемых модулей	+	-	-
Теневое копирование информации, выводимой на внешние носители	+	+	-
Назначение категорий конфиденциальности на устройства	+	- (+)	-
Сохранение данных в теневой копии перед выполнением операций с устройствами	+	-	-
USB	+	+	+
PCMCIA	+	+	+
IEEE 1394 (FireWire)	+	+	+
Контроль появления программно-конфигурируемых дисков	+	-	+
Контроль на уровне групп устройств (шины)	+	+	+

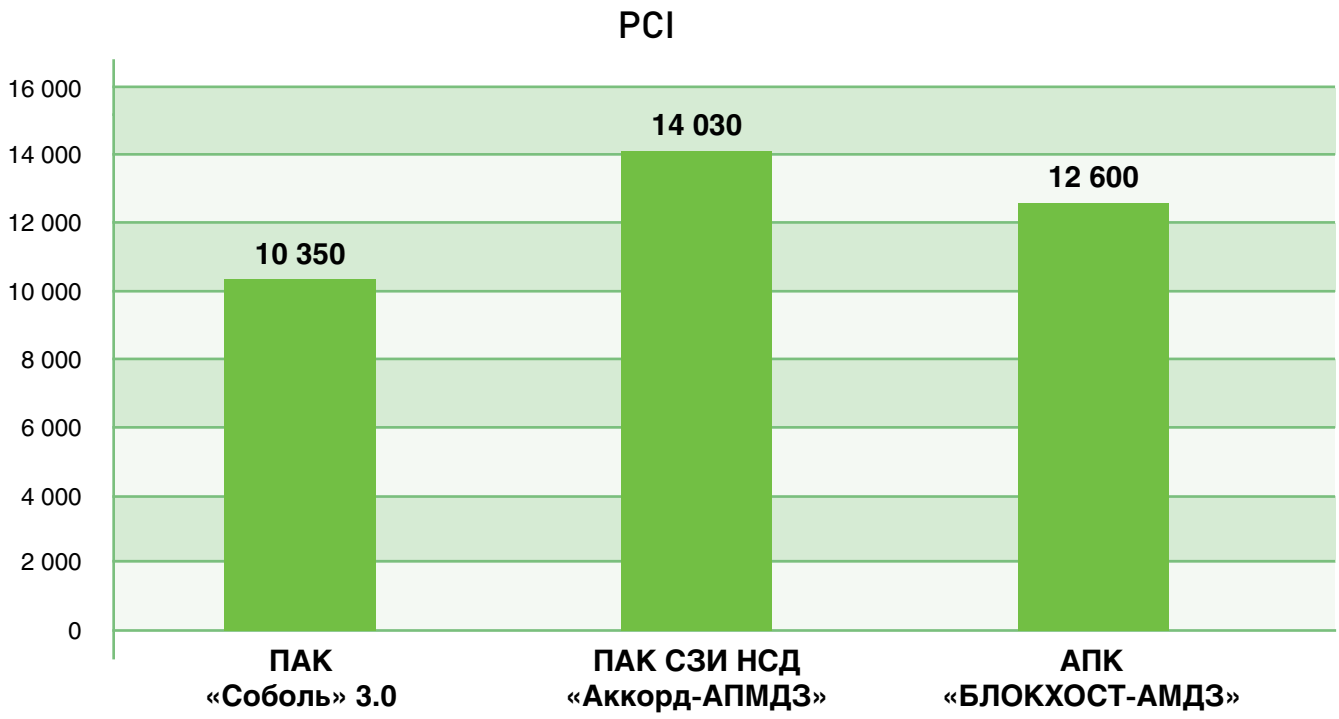
	Secret Net 7.4	Dallas Lock 8.0-K (С)	Аккорд-Win32/ Win64 (ПАК)
Контроль доступа к физическим дискам	+	+	+
Контроль появления новых сетевых интерфейсов	+	-	-
Возможность ограничить работу сетевого интерфейса заданными уровнями конфиденциальности сессий	+	- (+)	-
Возможность дискреционного разграничения доступа к принтерам	+	+	+
Печать из обычных приложений	+	+	+
Возможность ограничения категорий конфиденциальности документов, выводимых на принтер	+	- (+)	-
Ограничение пользователей, допущенных к печати конфиденциальной информации	+	+	+
Получение теневой копии напечатанных документов	+	- (+)	-
Маркировка документов при выводе на печать	+	+	+
Доступ к файлам и папкам	+	- (+)	+
Доступ к устройствам	+	- (+)	+
Доступ к принтерам	+	- (+)	-
Доступ к сетевым интерфейсам	+	- (+)	-
Контроль потоков конфиденциальной информации	+	- (+)	+

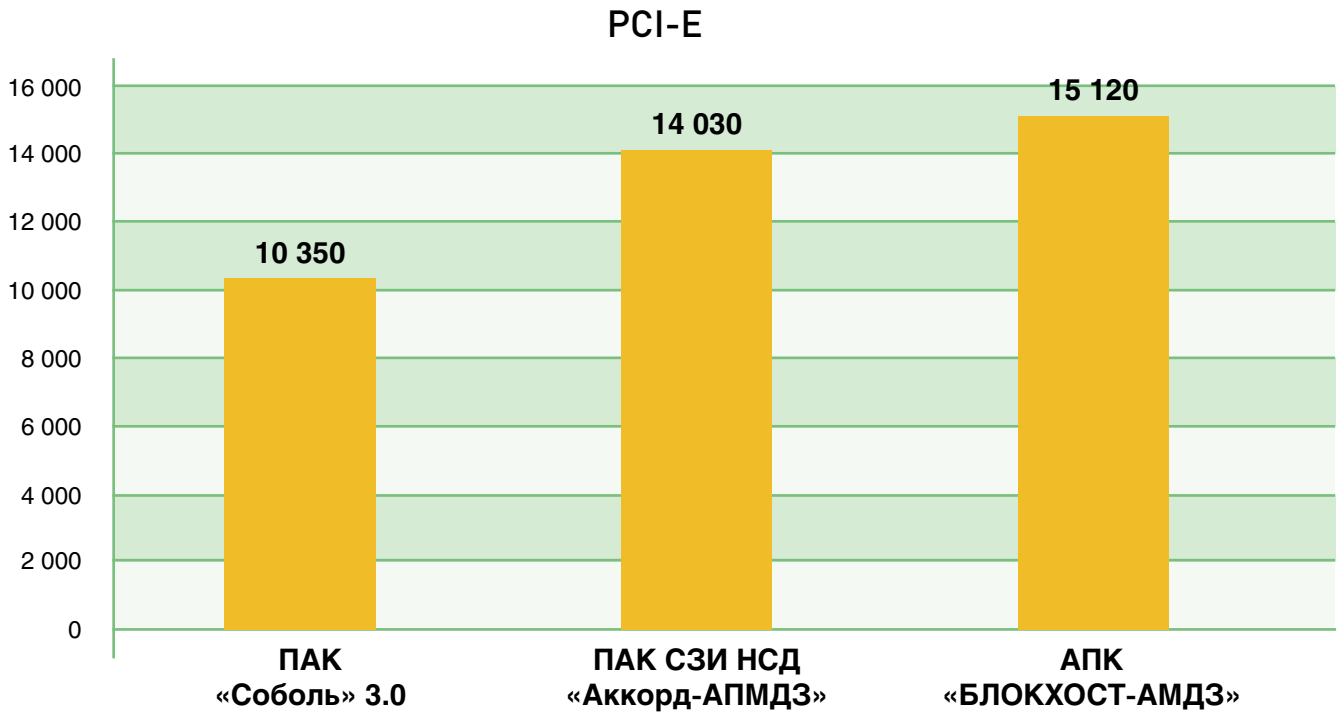
	Secret Net 7.4	Dallas Lock 8.0-K (C)	Аккорд-Win32/ Win64 (ПАК)
Контроль вывода конфиденциальной информации на внешние носители	+	- (+)	+
Затирание данных на локальных дисках и сменных носителях	+	+	+
Настройка количества проходов затирания информации	+	- (+)	+
Автоматическая зачистка удаляемых файлов	+	+	-
Возможность локального управления СЗИ	+	+	+
Локальное оповещение пользователя о событиях НСД	+	+	+
Централизованное управление СЗИ	+	+	+ (Аккорд-РАУ)
Интеграция управления пользователями с Active Directory	+	+	-
Возможность управления политиками на уровне организационных подразделений (OU) AD	+	+	-
Экспорт/импорт типовых настроек для ускорения развертывания	+	+	+
Удаленный контроль состояния рабочей станции	+	+	+
Возможность автоматического оповещения о событии НСД по электронной почте	+	+	-

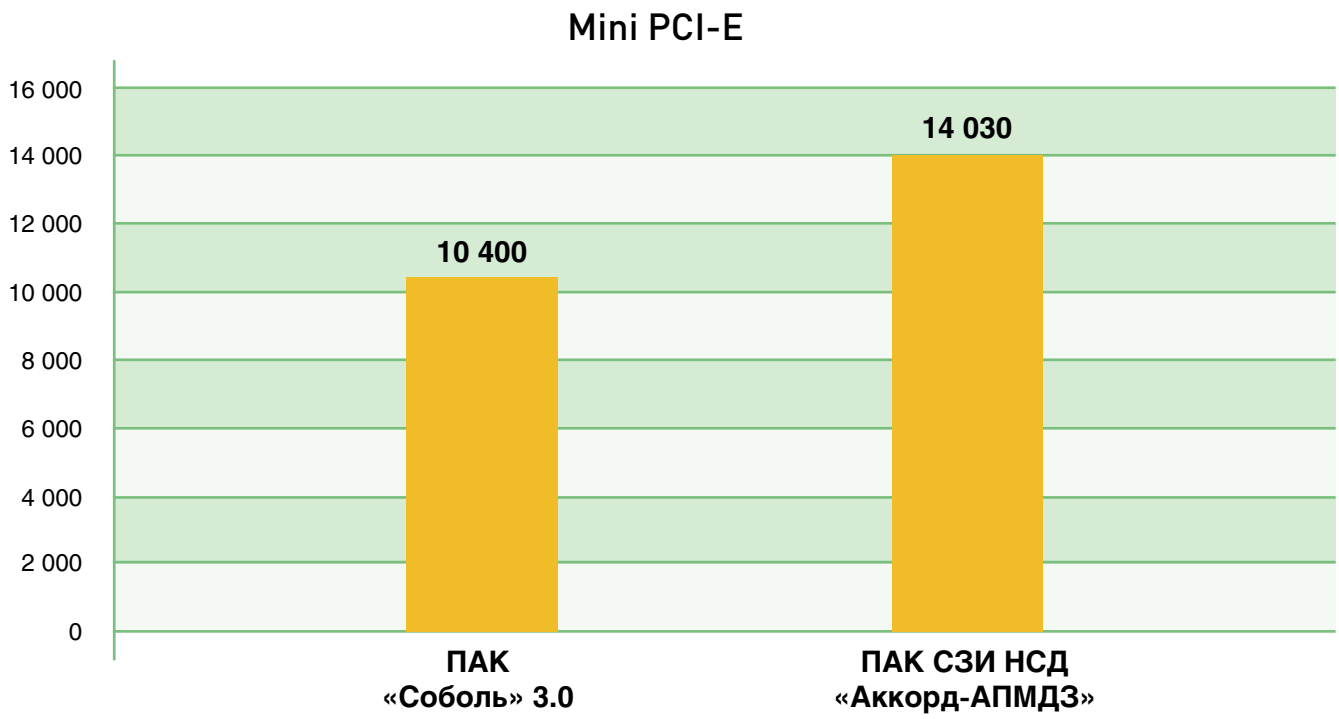
	Secret Net 7.4	Dallas Lock 8.0-K (C)	Аккорд-Win32/ Win64 (ПАК)
Инвентаризация ПО, установленного на рабочей станции	+	+	-
Получение отчета по всем настройкам СЗИ на рабочей станции	+	+	-
Централизованный сбор журналов СЗИ с рабочих станций	+	+	+ (Аккорд-РАУ)
Автоматическое архивирование журналов	+	+	-
Возможность формирования произвольных выборок по журналам	+	+	+
Возможность фильтрации информации при просмотре журналов	+	+	+
Возможность поиска информации при просмотре журналов	+	+	+
Работа с архивами журналов без необходимости их восстановления (загрузки) в СУБД	+	+	-

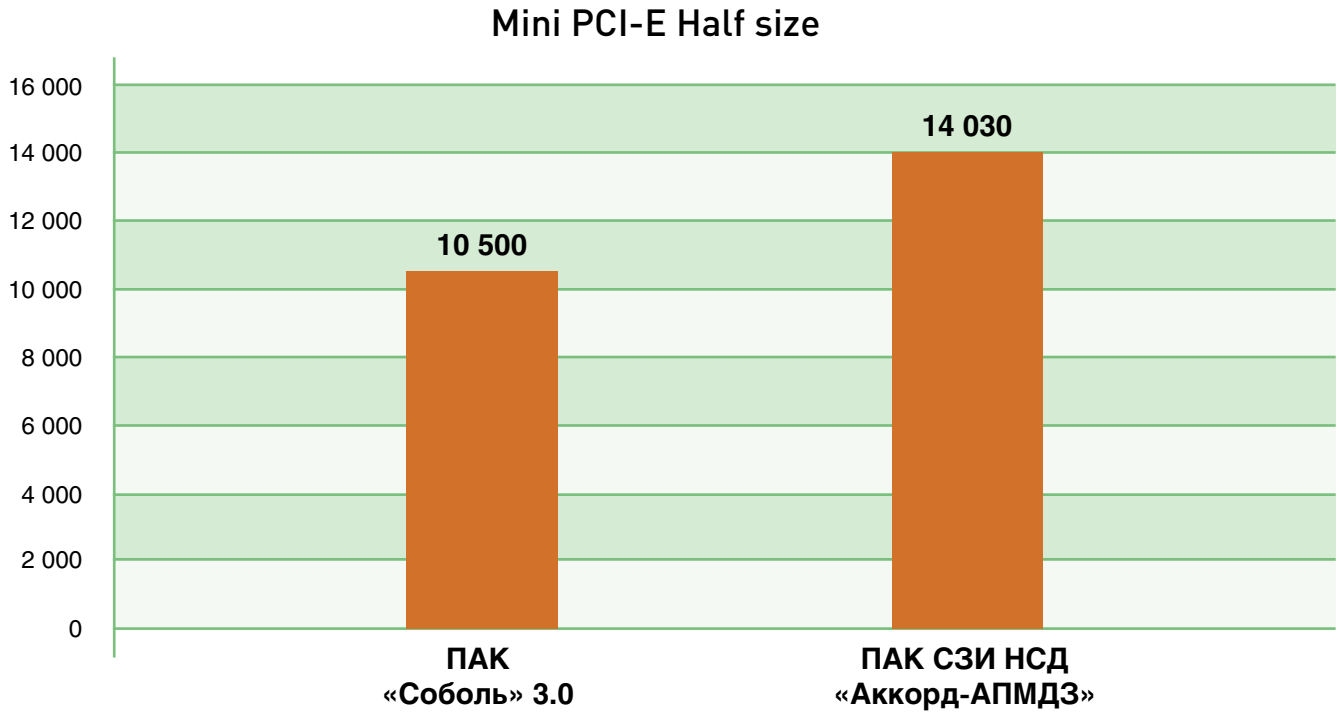
Ценовое сравнение АПМДЗ[2]

	ПАК «Соболь» 3.0	ПАК СЗИ НСД «Аккорд-АПМДЗ»	АПК «БЛОКХОСТ-АМДЗ»
PCI	10 350	14 030	12 600
PCI-E	10 350	14 030	15 120
Mini PCI-E	10 400	14 030	—
Mini PCI-E Half	10 500	14 030	—


PCI
16 000
14 000
12 000
10 000
8 000
6 000
4 000
2 000
0
10 350
14 030
12 600
ПАК «Соболь» 3.0
ПАК СЗИ НСД «Аккорд-АПМДЗ»
АПК «БЛОКХОСТ-АМДЗ»


PCI-E
16 000
14 000
12 000
10 000
8 000
6 000
4 000
2 000
0
10 350
14 030
15 120
ПАК «Соболь» 3.0
ПАК СЗИ НСД «Аккорд-АПМДЗ»
АПК «БЛОКХОСТ-АМДЗ»


Mini PCI-E
16 000
14 000
12 000
10 000
8 000
6 000
4 000
2 000
0
10 400
14 030
ПАК «Соболь» 3.0
ПАК СЗИ НСД «Аккорд-АПМДЗ»


Mini PCI-E Half size
16 000
14 000
12 000
10 000
8 000
6 000
4 000
2 000
0
10 500
14 030
ПАК «Соболь» 3.0
ПАК СЗИ НСД «Аккорд-АПМДЗ»

Сравнение возможностей аппаратно-программных модулей доверенной загрузки (АПМДЗ)

	ПАК «Соболь» 3.0	ПАК СЗИ НСД «Аккорд-АПМДЗ»	АПК «БЛОКХОСТ-АМДЗ»
Производитель	ООО «Код Безопасности»	ОКБ САПР	ООО «Газинформсервис»
Сертификат ФСБ России	АПМДЗ класса 1Б и возможность использования для защиты информации, содержащей сведения, составляющие государственную тайну	АПМДЗ класса 3Б и возможность использования для защиты информации, содержащей сведения, составляющие государственную тайну	-
Сертификат ФСТЭК России	СДЗ уровня платы расширения 2, в АС до класса 1Б	НДВ 2 и АС до 1Б	НДВ 2 и АС до 1Б
Сертификат Минобороны России	+	+	-
Поддерживаемые платы	PCI PCI Express Mini PCI Express Mini PCI Express Half	PCI PCI-X PCI Express Mini PCI Express Mini PCI -E Half card АМДЗ на шине USB (контроллер «Инаф»)	PCI PCI Express
Идентификаторы	iButton, eToken PRO, eToken PRO (Java), смарт-карта eToken PRO через USB-считыватель Athene ASEDrive IIIe USB V2, iKey 2032, Rutoken/ Rutoken RF	iButton, TM-идентификаторы DS 1992–1996 с объемом памяти до 64 Кбит, ПСКЗИ «Шипка» модификаций 1.5, 1.6 и 2.0, Touch memory DS-199x, смарт-карты (Acos3 и Acos5), JaCarta (Аккорд-GX, Аккорд-GXM и Аккорд-GXMH), радиокарты	iButton, eToken, SafeNet eToken, ESMART Token, ESMART Token SC, JaCarta PRO, Rutoken-ЭЦП, USB-накопители
Блокировка загрузки ОС с внешних носителей	+	+	+

	ПАК «Соболь» 3.0	ПАК СЗИ НСД «Аккорд-АПМДЗ»	АПК «БЛОКХОСТ-АМДЗ»
Контроль целостности программной среды	+	+	+
Контроль целостности системного реестра Windows	+	+	+
Поддерживаемые операционные системы			
ОС MS Windows	Windows XP/Vista/7/8/8.1. Windows Server 2003/2003 R2/2008/2008 R2/2012/2012 R2	MS DOS. Windows 3.x, Windows 95/98, Windows NT/2000/XP/Vista. OS/2	Windows 2000/XP/2003/Vista/7/2008/8/8.1/2012. Windows Server 2012/2012R
GNU/Linux	FreeBSD 6.2/6.3/7.2/8.2 МСВС 3.0 x86. Альт Линукс СПТ 6.0.0 x86/x64. Astra Linux Special Edition “Смоленск” 1.3 x64. Astra Linux Common Edition “Орел” 1.9 x64. CentOS 6.2 x64, 6.5 x86/x64. Debian 6.0.3/7.6 x86/x64. Mandriva ROSA Desktop 2011.0 x86/x64. Red Hat Enterprise Linux 6.0 x86/x64, 7.0 x64. Ubuntu 14.04 LTS Desktop/Server x86/x64.	UNIX. BSD	ОС семейств Linux/Unix, поддерживающих стандарт Linux Standard Base (LSB) версий 3.x/4.x. Debian 6.0/7.1. FreeBSD 8.0/9.1. ОС МСВС 3.0/5.0
Поддерживаемые файловые системы	FAT12, FAT16, FAT32, NTFS, UFS, UFS2, EXT2, EXT3, EXT4	FAT12, FAT16, FAT32, NTFS, HPFS, FreeBSD EXT2FS, EXT3FS, Sol86FS, QNXFS, MINIX, VMFS	EXT2/EXT3/EXT4, MS-DOS, FAT, NTFS, UFS, UFS2
Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией	+ VMware vSphere ESXi	+ VMware vSphere ESXi	+ VMware vSphere ESXi

	ПАК «Соболь» 3.0	ПАК СЗИ НСД «Аккорд-АПМДЗ»	АПК «БЛОКХОСТ-АМДЗ»
Сторожевой таймер	+	+	-
Регистрация попыток доступа к ПК	+	+	+
Датчик случайных чисел (ДСЧ)	+ Аппаратный ДСЧ, соответствующий требованиям ФСБ России	+ Аппаратный ДСЧ устанавливается во всех контроллерах	+ Аппаратный и программный (количество аппаратных ДСЧ 2 – основной и резервный)
Программная инициализация комплекса	+	-	-
Контроль конфигурации	+ Позволяет контролировать неизменность конфигурации компьютера – PCI-устройств, ACPI, SMBIOS и оперативной памяти	+ После регистрации в СЗИ «Аккорд» хотя бы одного пользователя контроль аппаратуры производится при каждой загрузке компьютера после идентификации/ аутентификации пользователя	+/- Возможность аппаратного управления внешними устройствами (FDD, CD, DVD), до 6 устройств
Поддержка высокоскоростного режима USB 2.0/3.0	+	-	-
Поддержка UEFI	- При наличии на компьютере UEFI работает в Legacy	-	+ Поддержка загрузки на ПЭВМ с Legacy BIOS и EFI/UEFI. Поддержка загрузки ОС с MBR и GPT-разделов
Ведение журнала безопасности	+	+	+

Требования к СЗИ от НСД и модулям доверенной загрузки (АПМДЗ) определены руководящими документами ФСТЭК России. Как следствие – защитные механизмы во всех СЗИ имеют схожую реализацию, различия в основном заключ ются в механизмах управления и количестве поддерживаемых плат (для АПМДЗ).

Тенденции рынка

Ввиду отсутствия возможностей увеличения продаж за счет естественного роста рынка персональных компьютеров российские производители вынуждены добавлять в продукты новый функционал.

Новые механизмы защиты уже появились в продуктах компании «Код Безопасности»: Secret Net Studio позиционируется как продукт для защиты от внешних и внутренних угроз, где функционал СЗИ от НСД является лишь составной частью. Компанией ТСС в решение Diamond ACS помимо традиционных функций защиты от НСД добавлены механизмы защиты от вирусов и руткитов.

Таким образом, в ближайшее время ожидается изменение традиционного рынка СЗИ от НСД. Продукты вендоров охватывают соседние сегменты, включая межсетевые экраны и антивирусы, и как следствие – могут в составе комплексного решения повлиять в целом на ландшафт рынка защиты рабочих станций и серверов.

---

[1] Цены на июль 2015 г.
[2] Цены на июль 2015 г.

Код Безопасности

«Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

Продукты «Кода Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, среды виртуализации, облачных сред, мобильных устройств, а также коммерческой и государственной тайны. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

Тел.: +7 (495) 982 30 20

buy@securitycode.ru

www.securitycode.ru