К вопросу о защите профессиональной и коммерческой тайны при их обработке в информационных системах

Справка ТБ

Барановский Олег Константинович. И.о. заместителя директора по науке Государственного предприятия «НИИ ТЗИ». Образование высшее, радиофизик, в 1998 закончил Белорусский государственный университет. Имеет академическую степень магистра естественных наук, кандидат физико-математических наук. Опыт работы в области защиты информации с 1998 года по настоящее время.

Закон Республики Беларусь от 10 ноября 2008 г. N 455-З «Об информации, информатизации и защите информации» гласит, что обработка информации, распространение и (или) предоставление которой ограничено (далее — охраняемая информация), допускается в информационных системах (ИС) с применением системы защиты информации (СЗИ), аттестованной в установленном порядке.

К охраняемой информации среди прочих относят информацию о частной жизни физического лица и персональные данные, коммерческую и профессиональную тайну.

Какими нормативными правовыми актами следует руководствоваться и каким образом выполнить их требования при создании СЗИ?

Основным вопросом для владельцев ИС остается способ организации информационного обмена между находящимися в разных зданиях сегментами ИС, с другими ИС, а также с удаленными пользователями.

Для взаимодействия с ИС, обрабатывающими охраняемую информацию, принято использовать выделенные каналы передачи данных. В соответствии с постановлением Совета Министров Республики Беларусь от 26 мая 2009 г. N 675 «О некоторых вопросах защиты информации» подключение ИС, обрабатывающих охраняемую информацию, к сетям общего пользования, в том числе к глобальной сети Интернет, запрещается.

Тем не менее, для обеспечения передачи охраняемой информации с использованием сетей общего пользования рекомендуется применять выделенные компьютеры. Данные компьютеры не имеют подключения к локальной сети передачи данных, на них запрещается обрабатывать охраняемую информацию в открытом виде, передача данных должна осуществляться в зашифрованном виде, перенос которых осуществляется с применением съемных носителей.

В соответствии с приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 3 марта 2011 г. N 18 «Об утверждении положения о порядке применения средств криптографической защиты информации в системах защиты информации» для реализации криптографических операций (зашифрование / расшифрование, удостоверение документов с применением электронной цифровой подписи) необходимо применять только программно-аппаратные (программно-технические) или технические (аппаратные) средства криптографической защиты информации (СКЗИ). Данные СКЗИ должны быть установлены на отдельном выделенном компьютере. Выделенный компьютер для СКЗИ не должен иметь подключения ни к локальной сети, ни к сетям общего пользования. Для современных информационных технологий, характеризующихся ростом скоростей передачи и объемов обработки данных, данный подход часто неэффективен.

В связи с этим, согласно выше указанному приказу, в целях обеспечения технологических процессов функционирования информационных систем, допускается подключать средства вычислительной техники с установленными СКЗИ к сетям общего пользования с применением средств защиты информации, имеющих сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы, обеспечивающих исключение возможности несанкционированного получения информации для служебного пользования. При этом, используя данную возможность, следует помнить, что понятия «информация для служебного пользования» и «информация, распространение и (или) предоставление которой ограничено» не тождественны, последнее понятие охватывает более широкий круг информации.

Можно предположить, что в скором времени в процедуры сертификации будет введен механизм, в результате которого сертификаты соответствия будут выдаваться с указанием наивысшего ограничительного грифа информации, которую можно обрабатывать в информационной системе с применением сертифицируемого средства защиты информации. Соответственно, владельцам будет проще реализовать безопасное подключение ИС, обрабатывающих охраняемую информацию, к сетям общего пользования.

Применение сертифицированных средств защиты информации для создания СЗИ является еще одним вопросом, акцентирующим внимание как владельцев ИС, так и организации, оказывающие услуги по защите информации

Следует помнить, что создание СЗИ ИС основывается на реализации взаимосвязи правовых, организационных и технических мер. Выявленные уязвимости конкретной ИС актуальным угрозам могут быть закрыты как техническими, так и организационными мерами. Учитывая человеческий фактор, бизнесу с высокими рисками предпочтительно применять средства технической защиты информации в целях снижения рисков информационной безопасности. Однако сегодня рынок республики характеризуется явно недостаточной для удовлетворения потребностей пользователей линейкой средств защиты информации, имеющих сертификат соответствия, выданный в На-

циональной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы. Выход может быть найден путем комбинирования организационных мер в совокупности с применением функционала средств защиты информации (если в нормативных правовых актах явно не указаны условия применения и тип сертифицированных средств защиты информации). Так, в настоящее время на рынке отсутствуют сертифицированные средства защиты информации, осуществляющие архивирование и резервное копирование данных. Как правило, владельцы ИС подкрепляют использование данных продуктов введением локальных инструкций, регламентирующих своевременное создание резервных копий и восстановление данных в случаях инцидентов информационной безопасности. В отдельных случаях, реализация требований интеграции имеющихся на рынке сертифицированных средств защиты в проектируемую или модернизируемую СЗИ требует чрезвычайно высоких затрат.

Другим препятствием перед разработчиком СЗИ на пути принятия решения о выборе сертифицированного средства защиты с требуемыми параметрами является недостаток информации о реализуемых данным средством функциях. Хорошо, если сертификация прошла на соответствие требованиям государственных стандартов, а не отдельных пунктов технических условий или задания по безопасности, которые необходимо дополнительно запрашивать для принятия решения.

Однако, в скором времени ситуация должна измениться в связи с вступлением в силу в июле текущего года новой редакции Закона Республики Беларусь от 05.01.2004 N 269-3 (ред. от 31.12.2010) «Об оценке соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации».

Так как подтверждение соответствия проводится на соответствие техническим нормативным правовым актам в области технического нормирования и стандартизации, то согласно статье 2 к таким актам теперь «…относятся технические регламенты и государственные стандарты Республики Беларусь». Остается надеяться, что вскоре будет введено достаточное количество государственных стандартов, удовлетворяющих как поставщиков и разработчиков средств защиты, так и их пользователей (потребителей). ■

Контроль защищенности информационных систем

Справка ТБ

Мазилкин Максим Анатольевич. Заместитель начальника отдела безопасности информационных вычислительных систем

Государственного предприятия "НИИ ТЗИ". Образование высшее, инженер электронной техники, в 1993 году закончил Минское высшее военное инженерное училище. Начинал работу в Главном штабе Министерства обороны Республики Беларусь с должности инженера 1-го отдела 202 ЦАСУ. Работал в должности ведущего специалиста, начальника ЦТО (ЗАО "Белорусская страховая компания"); инженера, ведущего специалиста, ведущего инженера (ООО "Белтим"); главного инженера проектов (ЗАО "НПП Белсофт"); ведущего инженера (СОДО "Белсофтсистемы"); старшего научного сотрудника ЦИиАИО, заместителя начальника отдела (Государственное предприятие "НИИ ТЗИ"). Опыт разработки систем защиты информации с 1999 года.

Контроль состояния защищенности относится к категории так называемых превентивных защитных механизмов. Его главное назначение — своевременно "заметить" слабость (уязвимость) в защищаемой системе, тем самым предотвратить возможные атаки с ее использованием.

Основным фактором, определяющим защищенность ИС от угроз безопасности, является наличие в них уязвимостей защиты. Уязвимости защиты могут быть обусловлены как ошибками в конфигурации компонентов ИС, так и другими причинами, к числу которых относятся ошибки и программные закладки в коде программного обеспечения, отсутствие механизмов безопасности, их неправильное использование либо их неадекватность существующим рискам, а также уязвимости, обусловленные человеческим фактором. Наличие уязвимостей в системе защиты ИС в конечном счете приводит к успешному осуществлению атак, использующих эти уязвимости.

Поиск уязвимостей можно осуществлять вручную или с помощью автоматизированных инструментов — сканеров безопасности.

Сетевые сканеры являются, пожалуй, наиболее доступными и широко используемыми средствами анализа защищенности. Основной принцип их функционирования заключается в эмуляции действий потенциального злоумышленника по осуществлению атак. Поиск уязвимостей путем имитации возможных атак является одним из наиболее эффективных способов анализа защищенности ИС, который дополняет результаты анализа конфигурации по шаблонам, выполняемого локально с использованием списков проверки. Сканер безопасности является необходимым инструментом в арсенале любого администратора либо аудитора безопасности ИС.

Сканеры безопасности предназначены для поиска уязвимостей узлов (от маршрутизаторов до рабочих станций и серверов) ИС с помощью средств тестирования

и сбора информации о конфигурации и функционировании ИС и средств, эмулирующих действия злоумышленника по проникновению к ресурсам системы, по требованию администратора (пользователя) ИС, или в запланированный промежуток времени, или после определенных событий с использованием встроенных или добавленных (вновь разработанных) сценариев проверок и предоставлением отчетов по окончании проверок с отражением информации об обнаруженных уязвимых местах проверяемых узлов с пояснениями (или без них) по каждому типу уязвимостей и приведением рекомендуемых действий (или без них) по их коррекции с оценкой риска уязвимостей.

В настоящее время наибольшее распространение получили сетевые сканеры безопасности, выполняющие проверки дистанционно, по сети. Проверки, выполняемые сетевыми сканерами безопасно-

Таблица 1 — Сравнение основных характеристик сканеров безопасности

Функциональные характеристики	Применяемость				
		зарубежные образцы		отечественные образцы	
	Сканер "Контролер"	Nessus v 3.2.0	IIS Internet Scanner	Застава-Инспектор Версия 1.0	XSpider — версия 7.7
Режим работы:					
а) сбор и анализ состояний узлов ИС по запросу администратора (эксперта);	+	+	+	+	+
б) сбор и анализ состояний узлов ИС по заданному расписанию.	+	-	+	+	+
Применяемость на фазах жизненного цикла ИС:					
а) проектирование;	-	-	-	-	-
б) реализация;	+	+	+	+	+
в) тестирование;	+	+	+	+	+
г) внедрение;	+	+	+	+	+
д) эксплуатация;	+	+	+	+	+
е) обслуживание.	+	+	+	+	+
Подсистема сканирования и контроля:					
а) сканирование сети;	+	+	+	+	+
б) проверка на уязвимости;	+	+	+	+	+
в) имитация атак.	+	-	-	-	-
Подсистема оповещения:					
а) администратора (эксперта) о найденных уязвимостях;	+	+	+	+	+
б) администратора (эксперта) об обнаруженных атаках.	+	-	-	-	-
Подсистема формирования отчетов.	+	+	+	+	+
Подсистема оценки, анализа и управления:					
а) оценка рисков уязвимостей;	+	+	+	+	+
б) оценка уровня угроз;	+	-	-	-	-
в) оценка показателей защищенности от воздействия атак;	+	-	-	-	-
г) оценка показателей устойчивости к воздействию атак;	+	-	-	-	-
д) оценка показателей противодействия воздействию атак;	+	-	-	-	-
е) анализ рисков;	+	-	-	-	-
ж) управление рисками;	+	-	-	-	-
и) выдача рекомендуемых действий по уменьшению рисков уязвимостей;	+	+	+	+	+
к) оценка эффективности защиты от воздействия атак.	+	-	-	-	-
Подсистема обновления:					
а) базы угроз и уязвимостей;	+	+	+	+	+
б) базы сценариев проверки на уязвимости;	+	+	-	-	+
в) базы сценариев реакций на атаки.	+	-	-	-	-
Подсистема выбора сценария:					
а) проверки на уязвимости;	+	+	+	+	+
б) реакции для каждого типа атак.	+	-	-	-	-
Стоимость изделия	2500 — 5000$ (с оборудованием)	1200$ (стоимость подписки на год)	187761,6$ (на 10 тыс. узлов)	Нет данных	30000$ (на 10 тыс. узлов)

Примечание — Условные обозначения, принятые в таблице:
– знак "+" — функция реализована;
– знак "-" — функция не реализована.

сти, направлены, прежде всего, на сетевые службы. Но сегодня значительная часть сетевых сканеров безопасности, используя различные способы подключения к исследуемым узлам (SSH, WMI, Remote Registry, SMB/NetBIOS), может осуществлять поиск уязвимостей операционных систем, а также некоторых приложений, установленных на сканируемом узле.

Сканеры безопасности могут быть использованы для решения следующих задач:

– инвентаризация ресурсов ИС: узлов, сетевых служб, приложений. Инвентаризационное сканирование предоставляет обобщенную (базовую) информацию об ИС. Параллельно решается задача обнаружения несанкционированно подключенных устройств;

– тестирование ИС на устойчивость к взлому: такое тестирование может осуществляться как изнутри ИС, так и снаружи. В последнем случае это часто называют анализом защищенности периметра. В процессе проведения такого исследования могут быть использованы и другие инструменты, но сканеры безопасности, как правило, используются всегда;

– аудит безопасности ИС или отдельных ее областей на соответствие заданным требованиям. Осуществляется периодически с целью, например, проверки правильности и своевременности установки обновлений.

Первая и третья задачи чаще всего выполняются силами самой организации. Для решения второй задачи, как правило, привлекаются внешние ресурсы. Соответственно, первая и третья задачи решаются чаще, тестирование ИС на устойчивость к взлому осуществляется реже.

Сканеры безопасности могут быть использованы как в крупных, территориально-распределенных, так и в небольших ИС. Например, в крупной ИС сетевой сканер безопасности может помочь в решении задачи инвентаризации ресурсов ИС, в небольшой — помочь оценить защищенность ее периметра. Потребителями систем анализа защищенности могут быть администраторы безопасности сетей, сотрудники организаций, оказывающих услуги по оценке защищенности ИС, а также организации, занимающиеся разработкой и оценкой систем защиты. В любом случае, перед потребителями возникает проблема выбора "подходящего инструмента" и оценки того, насколько выбранный сканер безопасности подходит для решения поставленной перед ним задачи.

Данные сравнения основных характеристик сканеров безопасности

Для сравнения основных характеристик различных сканеров безопасности были выбраны следующие изделия: Nessus v 3.2.0 (Tenable Network Securuty, США), IIS Internet Scanner (IBM, США), Застава-Инспектор версия 1.0 (ОАО "Элвис-плюс", Россия), XSpider версия 7.7 (Positive Technologies, Россия), сканер "Контролер" (Государственное предприятие "НИИ ТЗИ", Беларусь).

Данные сравнения приведены в таблице 1.

Существующие сканеры безопасности направлены прежде всего на выявление уязвимостей в программном обеспечении и не предназначены для полноценной оценки защищенности от воздействия атак.

Принимая во внимание, что в Республике Беларусь широко используются импортные продукты и системы ИТ, в том числе сетевые операционные системы серии Windows, Unix, Linux, можно констатировать, что исследование эффективности защиты ИС к воздействию атак при помощи сканеров безопасности является актуальной задачей. ■

Современные средства хранения криптографических ключей

Справка ТБ

Головач Алексей Алексеевич. Ведущий инженер Государственного предприятия "НИИ ТЗИ". Образование высшее, радиофизик, в 1999 году закончил Белорусский Государственный Университет. Начинал работу в ИТК НАНБ с должности стажера-исследователя, младший научный сотрудник, аспирант; "РСП-Электроникс": инженер, специалист по маркетингу; ЗАО "Мультичип": специалист по продажам; Государственное предприятие "НИИ ТЗИ": инженер 1 категории, ведущий инженер. Опыт разработки аппаратно-программных средств защиты информации с 2007 года.

В современных условиях полноценную защиту информации возможно обеспечить только с применением криптографических методов защиты информации.

В большинстве криптографических алгоритмов защита, в конечном счете, основывается на некотором секретном ключе. Основная проблема заключается в организации хранения секретного ключа, поскольку если злоумышленнику удается завладеть этим секретным ключом, защищаемая информация автоматически оказывается в его руках.

Одним из существующих методов хранения секретного ключа является способ разделить его между группой людей, каждый из которых будет владеть частью секретного ключа. Когда необходимо, секретный ключ может быть воссоздан на основе частей. Часть секретного ключа сама по себе не несет никакой секретной информации.

В настоящее время теория разделения секрета нашла много примене-

ний. К их числу относятся протоколы электронного голосования, групповая электронная подпись, помехоустойчивое кодирование, безопасное управление ключами корневых удостоверяющих центров (УЦ), решение задач обеспечения сетевой безопасности при создании инфраструктуры открытых ключей, а также организация защищенного хранения резервной копии криптографических ключей.

Примеры применения устройства с разделением секретов

1. Для подписания документов или сертификатов открытых ключей электронно-цифровой подписью используется пара ключей: открытый ключ, секретный ключ. Секретный ключ известен только владельцу и служит для подписания документов, открытый ключ известен всем и служит для удостоверения подлинности того, кто подписал документ.

Для генерации пары ключей (секретного и открытого ключей) в УЦ применяются специальные программно-аппаратные криптографические устройства (далее устройства), которые обеспечивают такие функции как генерация пары ключей, защита секретных ключей, выполнение криптографической обработки данных.

Секретный ключ УЦ храниться внутри самого устройства и защита данного ключа при его использовании осуществляется за счет выполнения всех криптографических преобразований внутри самого устройства, без передачи его внешним приложениям, использующим криптографические сервисы. Эта особенность повышает защищенность системы и секретный ключ от компрометации или утери.

Для таких устройств необходимо осуществлять такие меры защиты, как:

– защита от несанкционированного доступа к устройству и его настройкам;

– защита от потери ключевой информации при отказе устройства путем восстановления секретных ключей.

Рассмотрим использование флэш-носителя с разделением секретов для реализации вышеуказанных мер защиты на примере двух администраторов: администратора устройства, администратора безопасности УЦ.

В процессе инициализации устройства флэш-носитель с разделением секретов генерирует общий секрет, разделяет его на частичные секреты, производит запись частичных секретов на два внешних стандартных флэш-накопителя. Один флэш-накопитель хранится у администратора устройства, другой — у администратора безопасности УЦ.

При таком подходе нарушителю необходимо получить доступ к нескольким флэш-накопителям, что намного труднее, чем в случае с одним носителем информации.

Для запуска устройства необходимо предъявить общий секрет. Поэтому администратор безопасности УЦ и администратор устройства последовательно подсоединяют к флэш-носителю с разделением секретов, который подключен к устройству через USB интерфейс, свои флэш-накопители, содержащие частичные секреты. После считывания частичных секретов с флэш-накопителей администраторов флэш-носитель с разделением секретов собирает общий секрет и предъявляет его устройству. Устройство сравнивает предъявленный секрет с тем, который храниться в самом устройстве. Если они совпали, тогда происходит запуск устройства. Самостоятельно, каждый из администраторов не сможет получить доступ к устройству. Только согласованные действия двух администраторов позволяют осуществить доступ к устройству.

2. Флэш-носитель с разделением секретов может применяться для организации резервного хранения ключевой информации в различных организациях. На сегодняшний день в организациях криптографические средства защиты информации широко применяются сотрудниками для защиты служебной информации на ПЭВМ. И при этом организацию хранения криптографических ключей осуществляет сам сотрудник. Потеря криптографического ключа в таком случае приводит к потере служебной информации. При организации хранения криптографического ключа сотрудника администратором у последнего появляется возможность НСД к служебной информации сотрудника. Поэтому одним из решений организации резервного хранения ключевой информации является разделение этой информации на частичные секреты с помощью флэш-носителя с разделением секретов. В организации назначаются лица, каждый из которых отвечают за хранение выданного ему частичного секрета.

3. Помимо защиты от НСД к объектам (устройствам, документам на ПЭВМ), защиты от потери ключевой информации флэш-носитель с разделением секретов может применяться в других приложениях, применяющих алгоритмы разделения секрета.

Данные сравнения основных технических характеристик USB флэш-накопителей с функциями защиты информации

Рассмотрим характеристики существующих на рынке USB флэш-накопителей с функциями защиты информации на примере таких устройств, как USB флэш-накопитель IronKey (IronKey,USA), DataTraveler BlackBox Secure USB Flash Drive (Kingston, USA), Kanguru Defender AES (Kanguru Solutions, USA), Криптофлэш (ФГУП "ПНИЭИ", Россия), Шипка 1.7 (ОКБ САПР, Россия), специализированный носитель (Государственное предприятие "НИИ ТЗИ", рисунок 1).

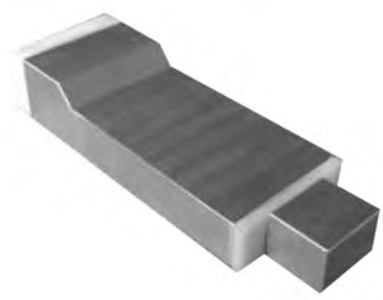

Рисунок 1 — Специализированный носитель

Обзор выполняемых функций рассматриваемых USB флэш-накопителей приведен в таблице 1.

Проведем анализ изложенных сравнительных характеристик USB флэш-накопителей с функциями защиты информации. Все рассмотренные USB флэш-накопители обеспечивают криптографическую защиту информации, хранимой во флэш-памяти самого накопителя. Криптографический ключ, на котором происходит зашифровывание информации, храниться внутри USB флэш-накопителей. Защита криптографического ключа обеспечивается средствами USB флэш-накопителей.

Во флэш-накопителе IronKey используется специализированный микроконтроллер, который обеспечивает защиту ключевой информации в его внутренней памяти. Отличительной особенностью данного микроконтроллера является защита ключевой информации от НСД даже при отключенном электропитании

всего накопителя. Встроенными средствами микроконтроллера обеспечивается уничтожение ключевой информации при попытке физического доступа к внутренней защищенной памяти микропроцессора. Данный флэш-накопитель соответствует стандарту FIPS 140-2 уровень 3, что означает противодействие атаке даже на физическом уровне.

Другой производитель Kingston приводит данные о том, что DataTraveler BlackBox Secure USB Flash Drive соответствует стандарту FIPS 140-2 уровень 2. Это означает, что данный флэш-накопитель не обладает средствами противодействия атаке, но позволяет определить, что к информация был осуществлен несанкционированный доступ. Другие зарубежные производители не приводят информации о методах защиты криптографических ключей.

На основе вышесказанного видно, что уровень защиты информации флэш-накопителя определяется защитой криптографических ключей, которая обеспечивается аппаратными средствами самого флэш-накопителя. Для обеспечения высокого уровня защиты информации в USB флэш-накопителе необходимо применение специальной элементной базы с крипто-инженерной защитой, или применение других методов защиты информации. На сегодняшний день в Республике Беларусь не существует сертифицированных современных скоростных микроконтроллеров, которые могли бы гарантировать требуемый уровень защиты информации.

стандартные USB флэш-накопители. Каждый в отдельности USB флэш-накопитель, содержащий частичный секрет не представляет особой ценности, поскольку не позволяет получить информацию об общем секрете (рисунок 2).

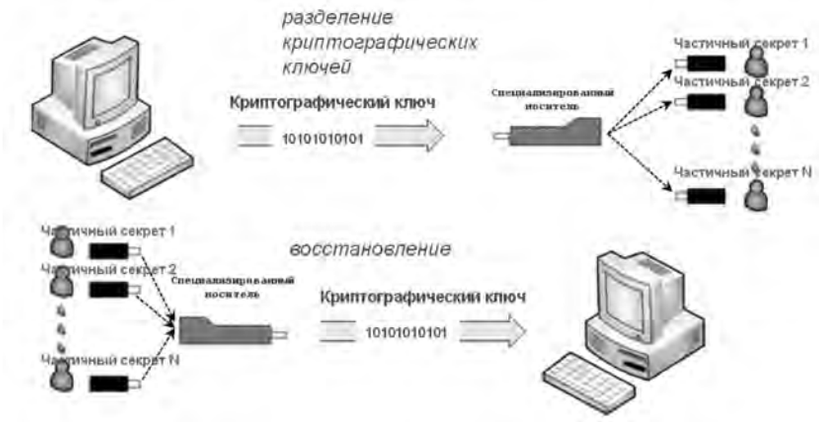

Рисунок 2 — Организация хранения криптографических ключей

Использование алгоритмов разделения секретов в составе специализированного носителя Государственного предприятия "НИИ ТЗИ" позволяет обеспечить высокий уровень защиты криптографических ключей, поскольку происходит разделение ключа (общего секрета) на частичные и сохранение их на внешние, по отношению к специализированному носителю,

Применение алгоритмов разделения секрета позволяет использовать современную импортную элементную базу в специализированном носителе без снижения уровня защиты криптографических ключей, а так же позволяет не хранить в самом специализированном носителе криптографические ключи, а только ключевую информацию (значения функции хэширования). ■

Таблица 1

Функция	IronKey	DataTraveler BlackBox Secure USB Flash Drive	Kanguru Defender AES	Криптоф-лэш	Шипка 1.7	Специализированный носитель
Хранение ключевой информации во флэш-памяти накопителя	+	+	+	+	+	+
Криптографическая защита информации	+	+	+	+	+	+ на стандартных USB флэш-накопителях
Защита криптографических ключей	метод крипто-инженерной защиты	-	-	-	-	метод разделения секрета
Информационный обмен с ПЭВМ по интерфейсу USB 2.0	+	+	+	+	+	+
Генерация ключей	-	-	-	+	+	+
Поддерживаемые алгоритмы	AES SHA RSA*	AES	AES	ГОСТ 28147-89, ОСТ Р 34.10-2001 (ЭЦП)	ГОСТ 28147-89, ГОСТ Р 34.11-94, ГОСТ Р 34.10-2001 (ЭЦП), ГОСТ Р 34.10-94; DES/ DESX/ Triple DES/ RC2/AES/ SHA-1/ MD5	ГОСТ 28147-89, СТБ 34.101.31-2011, алгоритмы разделения секрета
Поддерживаемая операционная система	Windows XP/ Vista/2000 SP4, Linux ядро 2.6, MAC OSX	Windows 2000 (SP3, SP4)/XP (SP1, SP2)/Vista (32-bit only)	Windows 2000/XP/ Vista (32-bit only), Windows Server 2003, Mac OS 8.6 и выше, Linux 2.4.1 и выше*	Windows 9x/ 2000/ XP	Windows 2000/ XP/2003/Vista	Windows XP/2000, Linux ядро 2.6 и выше.

* — используется только при шифровании информационного обмена между накопителем и сервером