Код безопасности
ГК «Информзащита»

Средство защиты информации

SECRET NET 6

Руководство администратора

Аппаратные средства

RU.88338853.501410.007 91 8

Почтовый адрес:	**127018, г. Москва, ул. Сущёвский Вал, дом 47, стр. 2, помещение №1**
Телефон:	**(495) 980-23-45**
Факс:	**(495) 980-23-45**
e-mail:	**info@securitycode.ru**
Web:	**http://www.securitycode.ru**

Версия: 6.5 Последнее обновление: 14-09-10

Оглавление

Список сокращений

ДСЧ	Датчик случайных чисел
КС	Контрольная сумма
КЦ	Контроль целостности
НСД	Несанкционированный доступ
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СИА	Средство идентификации и аутентификации
ЦУ	Централизованное управление

Введение

Данное руководство предназначено для администраторов изделия "Средство защиты информации Secret Net 6" RU.88338853.501410.007 (далее — система Secret Net 6, Secret Net 6). В руководстве содержатся сведения, необходимые администраторам для установки, настройки и эксплуатации средств аппаратной поддержки Secret Net 6.

Условные обозначения

В руководстве для выделения некоторых элементов текста (примечаний и ссылок) используется ряд условных обозначений.

Внутренние ссылки обычно содержат указание на номер страницы с нужными сведениями. Ссылки на другие документы или источники информации размещаются в тексте примечаний или на полях.

Важная и дополнительная информация оформлена в виде примечаний. Степень важности содержащихся в них сведений отображают пиктограммы на полях.

- Так обозначается дополнительная информация, которая может содержать примеры, ссылки на другие документы или другие части этого руководства.
- Такой пиктограммой выделяется важная информация, которую необходимо принять во внимание.
- Эта пиктограмма сопровождает информацию предостерегающего характера.

Исключения. Некоторые примечания могут и не сопровождаться пиктограммами. А на полях, помимо пиктограмм примечаний, могут быть приведены и другие графические элементы, например, изображения кнопок, действия с которыми упомянуты в тексте расположенного рядом абзаца.

Другие источники информации

Сайт в Интернете. Если у вас есть доступ в Интернет, вы можете посетить сайт компании "Код Безопасности" (http://www.securitycode.ru/) или связаться с представителями компании по электронной почте (support@securitycode.ru и hotline@infosec.ru).

Учебные курсы. Освоить аппаратные и программные продукты компании "Код Безопасности" можно на курсах Учебного центра "Информзащита". Перечень курсов и условия обучения представлены на сайте http://www.itsecurity.ru/. Связаться с представителем учебного центра можно по электронной почте (edu@infosec.ru).

Глава 1
Аппаратная поддержка Secret Net 6

Система Secret Net 6 предназначена для защиты информации в локальных вычислительных сетях, рабочие станции и серверы которых работают под управлением 32- и 64-разрядных ОС MS Windows 2000/XP/2003/Vista/2008/7. Система Secret Net 6 дополняет стандартные механизмы защиты операционных систем функциями защиты от НСД к информационным ресурсам компьютеров.

В Secret Net 6 поддерживается работа со следующими аппаратными средствами:

- Комплексы семейства "Соболь":
  - Программно-аппаратный комплекс "Соболь". Версия 3.0 (далее — комплекс "Соболь 3.0");
  - Программно-аппаратный комплекс "Соболь". Версия 2.1 (далее — комплекс "Соболь 2.1").
- Изделие Secret Net Touch Memory Card PCI 2.
- Изделие Secret Net Card.
- USB-ключи eToken PRO, iKey 2032, Rutoken v.1, Rutoken S, Rutoken RF S.
- Внешние средства хранения данных (дискеты, ZIP-устройства, магнитооптические диски, USB-диски и др.).

Применение конкретного типа устройства или их комбинации зависит от различных факторов (требований заказчика, конфигурации защищаемого компьютера, вариантов использования Secret Net 6 и др.). Средства аппаратной поддержки Secret Net 6 могут обеспечивать:

- защиту от НСД к информационным ресурсам компьютеров посредством реализации механизма идентификации и аутентификации, блокировки несанкционированной загрузки ОС со съемных носителей и т. д.;
- контроль и регистрацию (КЦ программной среды компьютера, регистрация событий, имеющих отношение к безопасности системы);
- хранение конфиденциальной информации (криптографических ключей, паролей доступа, сертификатов и других важных данных).

Средства идентификации и аутентификации

В системах защиты информации одним из основных способов защиты компьютеров от НСД является реализация процедуры идентификации и аутентификации. Идентификация заключается в распознавании субъекта доступа по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности) осуществляется в процессе аутентификации. В настоящее время в системах защиты компьютеров от НСД широко используются аппаратные СИА.

В состав СИА входят идентификатор, считывающее устройство (считыватели, контактные устройства, адаптеры, платы доверенной загрузки, разъемы материнской платы и др.) и соответствующее программное обеспечение. Идентификатор предназначен для хранения уникальных идентификационных признаков. Кроме того, он может хранить и обрабатывать разнообразные конфиденциальные данные. Считывающее устройство обеспечивает обмен данными между идентификатором и защищаемым компьютером.

Современные СИА принято классифицировать по следующим особенностям:

- по способу считывания идентификационных признаков;
- по виду используемых идентификационных признаков.

По способу считывания СИА подразделяются на контактные, бесконтактные (дистанционные) и комбинированные.

Контактное считывание идентификационных признаков подразумевает непосредственный контакт идентификатора и считывающего устройства. Считывание данных происходит при проведении идентификатора через считыватель или в результате их простого соприкосновения.

Бесконтактный (дистанционный) способ считывания не требует четкого позиционирования идентификатора и считывающего устройства. Чтение данных происходит при поднесении идентификатора на определенное расстояние к считывателю.

Комбинированный способ подразумевает сочетание нескольких различных способов считывания.

По виду используемых идентификационных признаков СИА могут быть электронными, биометрическими и комбинированными.

В электронных СИА идентификационные признаки представляются в виде цифрового кода, хранящегося в памяти идентификатора. Устройства такого типа разрабатываются на базе идентификаторов iButton, USB-ключей и смарт-карт (контактных и бесконтактных).

В биометрических устройствах идентификационными признаками являются индивидуальные физические признаки человека, называемые биометрическими характеристиками. Например, отпечатки пальцев, форма кисти руки, узор радужной оболочки глаза, рисунок сетчатки глаза, черты лица, параметры голоса и др. В комбинированных СИА для идентификации применяются одновременно несколько идентификационных признаков.

В современных системах защиты информации наиболее широко используются электронные СИА в силу их высокой надежности, удобства считывания идентификационных признаков и относительно низкой стоимости.

В Secret Net 6 поддерживается применение электронных СИА на базе идентификаторов iButton и USB-ключей eToken PRO, iKey 2032, Rutoken v.1, Rutoken S, Rutoken RF S.

СИА на базе iButton

В настоящее время компания Maxim Integrated Products выпускает более 20 моделей идентификаторов iButton. Для защиты компьютеров от НСД в основном используются идентификаторы семейства DS199X (см. Табл. 1 на стр. 7), которые различаются внутренней структурой, функциональными возможностями и, соответственно, ценой.

В Secret Net 6 поддерживается функционирование СИА на базе идентификаторов DS1990 — DS1996.

Идентификаторы iButton представляют собой микросхему (чип), вмонтированную в герметичный корпус из нержавеющей стали. Корпус iButton отдаленно напоминает батарейку для наручных часов и имеет диаметр 17,35 мм при высоте 5,89 мм (корпус F5) или 3,1 мм (корпус F3). Корпус защищает микросхему от различных внешних воздействий и обеспечивает высокую живучесть прибора в условиях агрессивных сред, пыли, влаги, внешних электромагнитных полей, механических ударов и т. п.

Рис. 1. Идентификаторы iButton

В структуре iButton можно выделить следующие основные части: постоянное запоминающее устройство ROM, энергонезависимое (nonvolatile — NV) оперативное запоминающее устройство NV RAM, сверхоперативное запоминающее устройство (scratchpad memory — SM), часы реального времени (для DS1994), а также элемент питания — встроенную миниатюрную литиевую батарейку. Изделие DS1990 содержит только ROM.

В ROM хранится 64-разрядный код, состоящий из 48-разрядного уникального серийного номера (идентификационного признака), 8-разрядного кода типа

идентификатора и 8-разрядной контрольной суммы. Память SM является буферной и выполняет функции блокнотной памяти. Память NV RAM идентификатора DS1991 является закрытой, доступ к ее блокам защищается паролями. Память NV RAM идентификаторов DS1992 — DS1996 является открытой.

Табл. 1. Идентификаторы iButton

Тип изделия	Корпус	Емкость ROM, бит	Емкость SM, бит	Емкость NV RAM, бит	Примечание
DS1990	F3, F5	64	–	–	
DS1991	F5	64	512	1152 (3 блока x 384 бит)	3 блока NV RAM защищаются паролями
DS1992	F5	64	256	1K (4 страницы x 256 бит)	Незащищенная NV RAM
DS1993	F5	64	256	4K (16 страниц x 256 бит)	Незащищенная NV RAM
DS1994	F5	64	256	4K (16 страниц x 256 бит)	Незащищенная NV RAM Часы реального времени
DS1995	F5	64	256	16K (64 страницы x 256 бит)	Незащищенная NV RAM
DS1996	F5	64	256	64K (256 страниц x 256 бит)	Незащищенная NV RAM

Обмен информацией, хранящейся в идентификаторе, с компьютером происходит в соответствии с протоколом 1-Wire с помощью разнообразных считывающих устройств (PCI-адаптеров, адаптеров последовательного и параллельного портов). Информация записывается в идентификатор и считывается из него путем прикосновения корпуса iButton к считывающему устройству. Время контакта — не менее 5 мс, гарантированное количество контактов составляет несколько миллионов. Интерфейс 1-Wire обеспечивает обмен информацией со скоростью 16 Кбит/с или 142 Кбит/с (ускоренный режим).

В Secret Net 6 считывающее устройство iButton (в дальнейшем — считыватель iButton) подключается к внешнему (или внутреннему) разъему плат комплексов "Соболь" и к внешнему разъему плат изделий Secret Net Touch Memory Card PCI 2, Secret Net Card.

Достоинствами СИА на базе идентификаторов iButton являются:

- долговечность (время хранения информации в памяти идентификатора составляет не менее 10 лет);
- высокая степень механической и электромагнитной защищенности;
- малые размеры, удобство хранения;
- относительно невысокая стоимость.

СИА на базе USB-ключей

Средства идентификации и аутентификации на базе USB-ключей предназначаются для работы непосредственно с USB-портом компьютера и не требуют аппаратного считывающего устройства. Подключение к USB-порту осуществляется непосредственно или с помощью соединительного кабеля. Идентификаторы конструктивно изготавливаются в виде брелоков, которые выпускаются в цветных корпусах, имеют световые индикаторы работы и легко размещаются на связке с ключами. Каждый USB-ключ имеет прошиваемый при изготовлении уникальный 32/64-разрядный серийный номер.

Рис. 2. USB-ключ eToken PRO

В состав USB-ключей могут входить:

- процессор — управление и обработка данных;
- криптографический процессор — реализация алгоритмов ГОСТ 28147-89, DES, 3DES, RSA, DSA, MD5, SHA-1 и других криптографических преобразований;
- USB-контроллер — обеспечение интерфейса с USB-портом компьютера;
- RAM — хранение изменяемых данных;
- многократно программируемая постоянная память EEPROM — хранение ключей шифрования, паролей, сертификатов и других важных данных;
- ROM — хранение команд и констант.

На российском рынке компьютерной безопасности наибольшей популярностью пользуются следующие USB-ключи:

- eToken — разработка компании Aladdin Knowledge Systems;
- iKey — разработка компании SafeNet;
- Rutoken — совместная разработка российских компаний "Актив" и "АНКАД".

В Secret Net 6 поддерживается работа СИА на базе USB-ключей eToken PRO, iKey 2032, Rutoken v.1, Rutoken S, Rutoken RF S.

В USB-ключе eToken PRO закрытая информация хранится в защищенной памяти емкостью 32/64 Кбайт. Каждый идентификатор имеет уникальный серийный 32-разрядный номер. В eToken PRO аппаратно реализованы криптографические алгоритмы RSA с ключами длиной 1024 бит и 2048 бит, DES/56, 3DES/168, SHA-1, MAC, iMAC.

Емкость памяти USB-ключа iKey 2032 составляет 32 Кбайт. Разрядность серийного номера равна 64. Помимо отмеченных выше криптоалгоритмов в iKey 2032 также реализованы MD5, RC2, RC4, RC5.

Главным отличием USB-ключей Rutoken от зарубежных аналогов является аппаратная реализация российского алгоритма шифрования ГОСТ 29147-89. В Rutoken RF S встроена радиочастотная метка, позволяющая дополнительно реализовать бесконтактный способ считывания идентификационных признаков.

Достоинствами СИА на базе USB-ключей являются:

- малые размеры, удобство хранения идентификатора;
- отсутствие аппаратного считывателя;
- простота подсоединения идентификатора к USB-порту.

К недостаткам USB-ключей можно отнести их относительно высокую стоимость.

Устройства аппаратной поддержки Secret Net 6

Аппаратные СИА обеспечивают реализацию одной из основных функций Secret Net 6 — контроль входа пользователей в систему. В зависимости от решаемых Secret Net 6 задач СИА могут функционировать совместно с комплексами семейства "Соболь" и изделиями Secret Net Touch Memory Card PCI 2, Secret Net Card.

Идентификация и аутентификация пользователей с помощью устройств аппаратной поддержки в Secret Net 6 может осуществляться как во время непосредственного входа пользователя на рабочий компьютер, так и во время его входа с удаленного компьютера. Особенности настройки параметров ОС Windows для реализации удаленного доступа рассматриваются в приложении "Использование терминального доступа" документа [3].

Программно-аппаратные комплексы семейства "Соболь"

Комплексы семейства "Соболь" ("Соболь 3.0", "Соболь 2.1") предназначены для предотвращения НСД посторонних лиц к ресурсам защищаемого компьютера.

Комплексы реализуют следующие основные функции:

- идентификация и аутентификация пользователей при их входе в систему с помощью персональных электронных идентификаторов:
  - iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S — "Соболь 3.0";
  - iButton — "Соболь 2.1";
- контроль целостности файлов и физических секторов жесткого диска компьютера до загрузки операционной системы;
- контроль работоспособности основных компонентов комплекса — энергонезависимой памяти, идентификаторов, датчика случайных чисел;
- защита от несанкционированной загрузки операционной системы со съемных носителей информации — дискет, оптических дисков, ZIP-устройств, магнитооптических дисков, USB-устройств и др.;
- функционирование механизма сторожевого таймера;
- регистрация событий, связанных с безопасностью системы.

В комплект поставки комплексов семейства "Соболь" входят:

- компакт-диск с ПО и эксплуатационной документацией;
- плата для шины:
  - стандарта PCI — в комплексах "Соболь 3.0/2.1" (см. Рис. 3 на стр. 10);
  - стандарта PCI Express (PCI-E) — в комплексе "Соболь 3.0" (см. Рис. 4 на стр. 10);
- идентификаторы (количество и тип идентификаторов согласовывается с заказчиком и определяется договором о поставке изделия):
  - iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S — для "Соболь 3.0";
  - iButton — для "Соболь 2.1";
- контактное устройство для идентификатора iButton (считыватель iButton);
- соединительный кабель для механизма сторожевого таймера.

Основными компонентами плат комплексов являются:

- микросхема флэш-памяти с кодом расширения BIOS;
- программируемая логическая интегральная схема XILINX с двумя микросхемами постоянной памяти, содержимое которых загружается в XILINX;
- две микросхемы энергонезависимой памяти EEPROM;
- два канала аппаратных ДСЧ;
- два твердотельных оптоэлектронных реле аппаратной блокировки устройств.

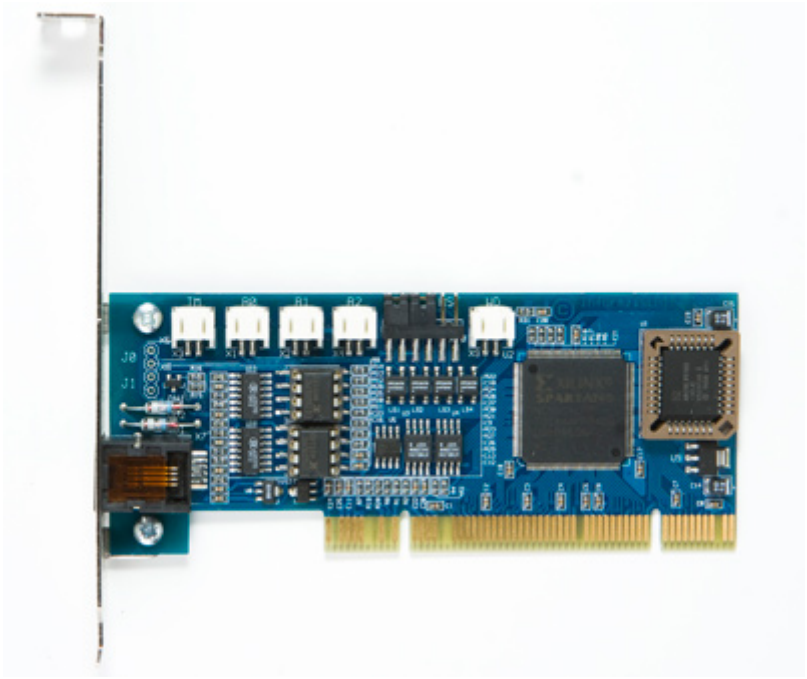


Рис. 3. Плата комплекса "Соболь 2.1 / 3.0" для шины PCI

Рис. 4. Плата комплекса "Соболь 3.0"для шины PCI-E

Комплексы позволяют хранить информацию о 32 учетных записях пользователей, не считая администратора. Идентификация пользователей осуществляется с помощью СИА на базе iButton, eToken PRO, iKey 2032, Rutoken S, Rutoken RF S . Контактное устройство для iButton может подключаться как к внутреннему разъему платы, так и к внешнему. Скорость обмена данными между идентификатором iButton и платой комплекса составляет 16 Кбит/с. Аутентификация пользователя осуществляется по паролю длиной до 16 символов и персональному идентификатору.

Блокировка несанкционированной загрузки ОС со съемных носителей (дискет, оптических дисков, ZIP-устройств, магнитооптических дисков, USB-устройств и др.) осуществляется программным способом путем блокирования доступа к указанным устройствам при запуске компьютера. После успешной загрузки ОС доступ к этим носителям восстанавливается.

Контроль целостности программной среды компьютера заключается в проверке изменения файлов и секторов жесткого диска. Для этого вычисляются некоторые текущие контрольные значения проверяемых объектов и сравниваются с

эталонными значениями, заранее рассчитанными для каждого из этих объектов. Контроль целостности программной среды может выполняться для файловых объектов любых операционных систем, использующих файловые системы NTFS, FAT 16, FAT 32.

Сведения и специальные рекомендации, необходимые администратору для установки и эксплуатации комплексов "Соболь 2.1" и "Соболь 3.0", приводятся в документах [10] и [12] соответственно.

Secret Net Card и Secret Net Touch Memory Card PCI 2

Изделия Secret Net Card и Secret Net Touch Memory Card PCI 2 (далее — SN Card и SN TM Card PCI 2 соответственно) разработаны на базе комплекса "Соболь". В Secret Net 6 изделия SN Card и SN TM Card PCI 2 используются как средства аппаратной поддержки, реализующие:

- аппаратную поддержку реализуемой Secret Net 6 процедуры идентификации и аутентификации пользователей с помощью персональных идентификаторов iButton;
- блокировку несанкционированной загрузки ОС со съемных носителей (дискет, оптических дисков, ZIP-устройств, магнитооптических дисков, USB-устройств и др.);
- механизм сторожевого таймера — автоматическую перезагрузку компьютера при условии, что после включения его питания и по истечении определенного времени управление не было передано расширению BIOS платы изделия.

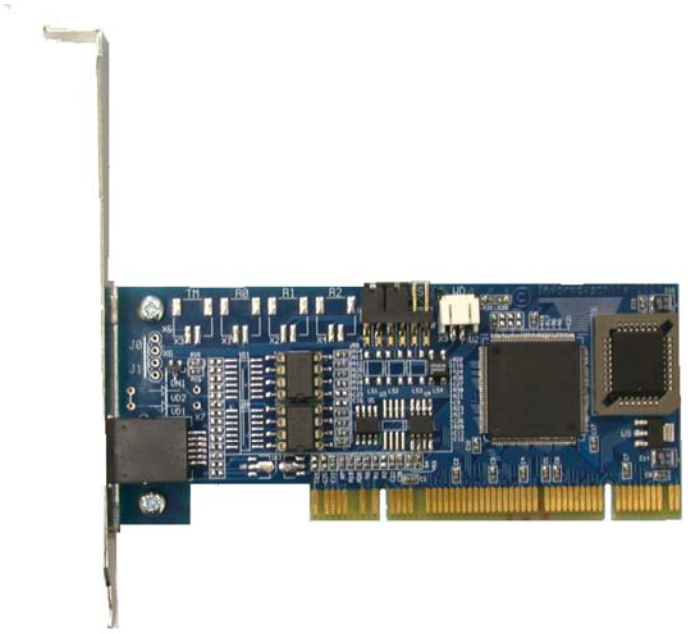


Рис. 5. Плата SN Card и SN TM Card PCI 2 для шины PCI

В комплект поставки SN Card и SN TM Card PCI 2 входят:

- плата для шины:
  - стандарта PCI — в SN TM Card PCI 2 и SN Card (см. Рис. 5 на стр. 11);
  - стандарта PCI-E — в SN Card;
- идентификаторы iButton (количество и тип идентификаторов согласовывается с заказчиком и определяется договором о поставке изделия);
- контактное устройство для идентификатора iButton;
- соединительный кабель для механизма сторожевого таймера.

Основными узлами платы изделия являются:

- микросхема флэш-памяти с кодом расширения BIOS;

- программируемая логическая интегральная схема XILINX с двумя микросхемами постоянной памяти, содержимое которых загружается в XILINX;
- две микросхемы энергонезависимой памяти EEPROM.

Блокировка несанкционированной загрузки ОС со съемных носителей (дискет, оптических дисков, ZIP-устройств, магнитооптических дисков, USB-устройств и др.) осуществляется программным способом путем запрета доступа к указанным устройствам при запуске компьютера. После успешной загрузки ОС доступ к этим устройствам восстанавливается.

Варианты применения устройств аппаратной поддержки

В Secret Net 6 имеется возможность использования четырех вариантов аппаратной поддержки. Применение конкретного варианта определяется требованиями заказчика и аппаратно-программными возможностями защищаемых компьютеров.

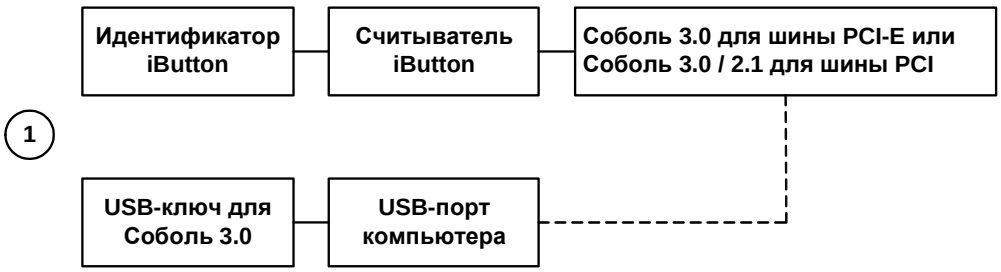
В Табл. 2 представлены варианты применения аппаратных средств в зависимости от решаемых Secret Net 6 задач ("Да" — поддержка работы изделия, "Нет" — отсутствие поддержки).

Табл. 2. Варианты аппаратной поддержки Secret Net 6

Задачи, решаемые с помощью средств аппаратной поддержки	Номера вариантов использования аппаратных средств		
	1	2 , 3	4
Идентификация и аутентификация пользователей до загрузки ОС	Да	Нет	Нет
Идентификация и аутентификация во время входа пользователя после загрузки ОС	Да	Да	Да
Идентификация и аутентификация во время входа пользователя с удаленного компьютера	Да	Да	Да
Запрет загрузки ОС со съемных носителей	Да	Да	Нет
Контроль целостности программной среды компьютера до загрузки ОС	Да	Нет	Нет
Снятие временной блокировки компьютера	Да	Да	Да
Хранение в идентификаторе пароля и криптографического ключа	Да[1]	Да[2]	Да

В Secret Net 6 для хранения криптографических ключей поддерживается применение внешних средств хранения данных (дискет, ZIP-устройств, магнитооптических дисков, USB-дисков и др.).

Ниже в виде схем представлены пронумерованные в Табл. 2 варианты. В каждой схеме структурно показаны соединения аппаратных средств и устройств ввода/вывода компьютера.

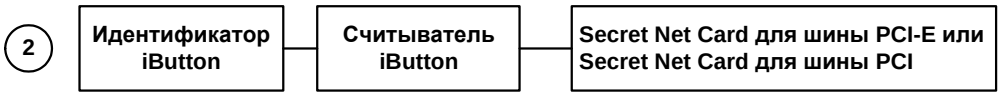


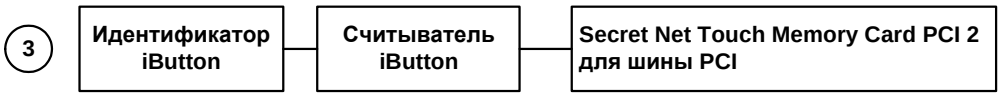
[1] Используются идентификаторы iButton DS1993, DS1994, DS1995, DS1996, USB-ключи eToken PRO, iKey 2032, Rutoken v.1, Rutoken S, Rutoken RF S.

[2] Используются идентификаторы iButton DS1992, DS1993, DS1994, DS1995, DS1996.

Для использования в Secret Net 6 комплексов семейства "Соболь" (вариант 1) с USB-ключами требуется свободный USB-порт (для комплекса "Соболь 3.0") и необходимо наличие на материнской плате защищаемого компьютера свободного разъема системной шины:

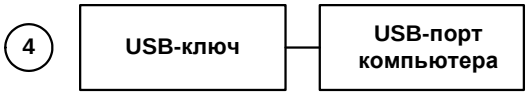
- либо стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В — для платы "Соболь 3.0/2.1";
- либо стандарта PCI-E версии 1.0a и выше — для платы "Соболь 3.0".





Для использования SN Card и SN TM Card PCI 2 (варианты 2 и 3) необходимо наличие на материнской плате защищаемого компьютера свободного разъема системной шины:

- либо стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В — для плат SN Card и SN TM Card PCI 2;
- либо стандарта PCI-E версии 1.0a и выше — для платы SN Card.



Для использования USB-ключей в варианте 4 требуется свободный USB-порт защищаемого компьютера.

Глава 2
Установка аппаратных средств

Комплексы семейства "Соболь"

Общие сведения об интеграции Secret Net 6 и комплексов "Соболь"

Комплексы семейства "Соболь" обеспечивают защиту от НСД к информационным ресурсам автономных компьютеров, сетевых рабочих станций и серверов, на которые устанавливается система Secret Net 6. Комплексы семейства "Соболь" могут функционировать как автономно, так и совместно с Secret Net 6.

В автономном режиме работы комплексы "Соболь" реализуют свои основные функции до старта операционной системы независимо от Secret Net 6. Любым внешним программам при этом запрещается доступ к энергонезависимой памяти комплекса. Управление пользователями, журналом регистрации событий, настройка общих параметров осуществляются средствами администрирования комплекса без ограничений.

В режиме совместного использования (интеграции) внешним программам, входящим в состав Secret Net 6, разрешается доступ к энергонезависимой памяти комплекса. В этом случае значительная часть функций управления комплексом осуществляется с помощью средств администрирования Secret Net 6.

В режиме интеграции системы Secret Net 6 и комплекса "Соболь" идентификатор iButton DS1992 не используется. Рекомендуется использовать идентификаторы DS1995, DS1996 или USB-ключи, поддерживаемые ПАК "Соболь".

В Secret Net 6 администратору предоставляется возможность осуществления локального и централизованного управления параметрами средства защиты (соответственно — так называемые **автономный** и **сетевой** режимы функционирования Secret Net 6).

Для обеспечения защиты данных в процессе централизованного управления комплексами "Соболь" в Secret Net 6 реализован ряд криптографических преобразований на основе ГОСТ 28147-89, ГОСТ Р34.10-2001. В Табл. 3 представлен перечень используемых ключей шифрования и их назначение.

Табл. 3. Ключи шифрования, используемые в механизме централизованного управления комплексами "Соболь"

Наименование ключа	Назначение	Место хранения
Симметричный ключ ЦУ	Шифрование хранимых в AD аутентификаторов[3] пользователей. Расчет имитовставки для списка доступных пользователю компьютеров	Персональный идентификатор администратора
Закрытый ключ ЦУ	Расчет сессионного ключа компьютера при выполнении операций администрирования	Персональный идентификатор администратора
Открытый ключ ЦУ	Расчет сессионного ключа компьютера при выполнении операций синхронизации	Локальная база данных управляемого компьютера
Закрытый ключ компьютера	Расчет сессионного ключа компьютера при выполнении операций синхронизации	Локальная база данных управляемого компьютера
Открытый ключ компьютера	Расчет сессионного ключа компьютера при выполнении операций администрирования	Active Directory

[3] Аутентификатор — структура данных, хранящаяся в Active Directory, которая совместно с паролем пользователя используется в процедуре его аутентификации.

Наименование ключа	Назначение	Место хранения
Сессионный ключ компьютера	Шифрование информации в AD, предназначенной для защищаемого компьютера	Не хранится (вычисляется в процессе работы)
Ключ преобразования паролей комплексов "Соболь"	Шифрование информации в закрытой памяти платы комплексов "Соболь". Шифрование информации, хранящейся в локальной базе данных защищаемого компьютера	Закрытая память платы комплексов "Соболь"

Подробные сведения об установке Secret Net 6 приводятся в документе [2]. Процедуры установки и удаления комплексов семейства "Соболь", их настройки и эксплуатации подробно излагаются в документах [10] и [12]. Настройка в Secret Net 6 механизмов контроля входа с использованием комплексов рассматривается в документе [3]. Ниже основное внимание уделено особенностям установки комплексов семейства "Соболь" на защищаемые компьютеры и настройке режима совместного использования комплексов с Secret Net 6.

Установка комплексов "Соболь"

Установку комплексов семейства "Соболь" на защищаемый компьютер рекомендуется производить до установки программного обеспечения Secret Net 6.

Комплексы устанавливаются на компьютеры, функционирующие под управлением 32- и 64-разрядных ОС MS Windows 2000/XP/2003/Vista/2008/7.

Компьютер, в который устанавливается плата комплекса, должен удовлетворять следующим требованиям:

- наличие свободного разъема шины:
  - либо стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В;
  - либо стандарта PCI-E версии 1.0a и выше;
- наличие на материнской плате разъема Reset, подачу сигналов на который невозможно отключить из BIOS Setup или каким-либо другим образом.

Для компьютеров с установленными комплексами семейства "Соболь" должны быть предусмотрены меры, обеспечивающие контроль физического доступа к системным блокам компьютеров.

Подробные сведения о процедурах установки комплексов содержатся в документах [10] и [12].

Во время установки комплекса "Соболь" на защищаемый компьютер в среде ОС Windows 2003/Vista/2008/7 на экране может появиться диалоговое окно "Предупреждение безопасности — установка драйвера" с сообщением, что устанавливаемый драйвер не подписан с применением технологии Authenticode. Для продолжения установки нажмите кнопку "Да".

Для установки комплекса:

1. Установите программное обеспечение комплекса.

Программное обеспечение комплекса необходимо устанавливать до установки в компьютер платы комплекса.

2. Подготовьте плату комплекса к инициализации:
   - снимите перемычку, установленную на разъеме **J0** платы (см. Рис. 6, Рис. 7);
   - выключите компьютер, вскройте корпус системного блока;
   - для использования механизма сторожевого таймера:
     - отключите штекер стандартного кабеля кнопки "Reset" от разъема Reset, расположенного на материнской плате;
     - подключите штекер стандартного кабеля кнопки "Reset" к разъему **RST** платы комплекса "Соболь"(см. Рис. 6, Рис. 7);

- подключите штекер кабеля механизма сторожевого таймера, входящего в комплект поставки, к разъему платы **WD**. Затем подключите другой штекер этого кабеля к разъему Reset, расположенному на материнской плате;

- выберите свободный слот системной шины PCI-E/PCI и аккуратно вставьте в него плату;
- при необходимости подключите считыватель iButton к внешнему или к внутреннему разъему **TM** платы (см. Рис. 6, Рис. 7);
- закройте корпус системного блока.

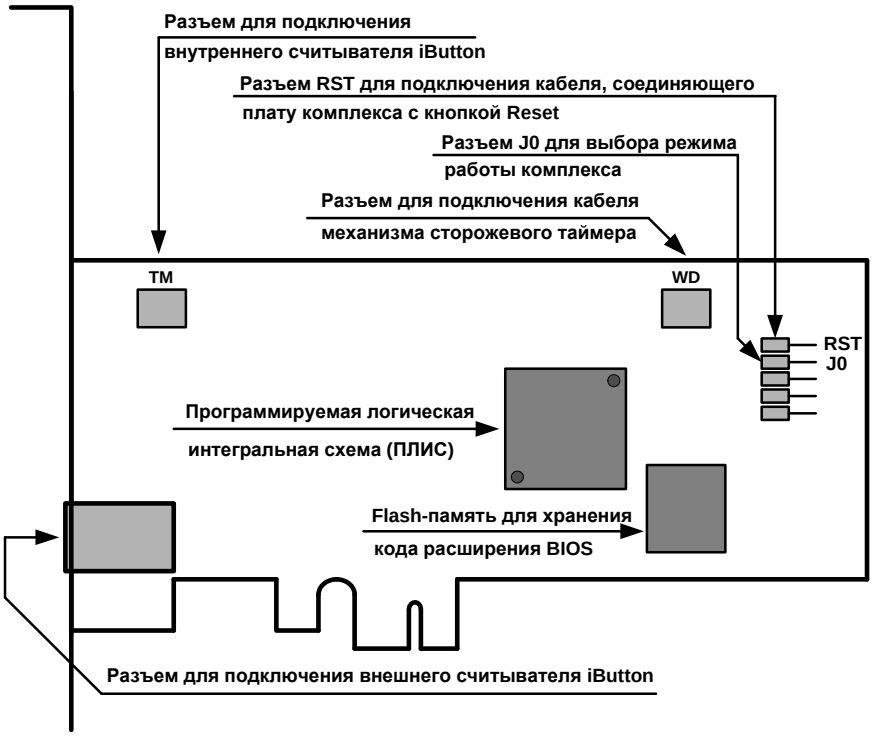


Рис. 6. Расположение разъемов на плате "Соболь 3.0" для шины PCI-E

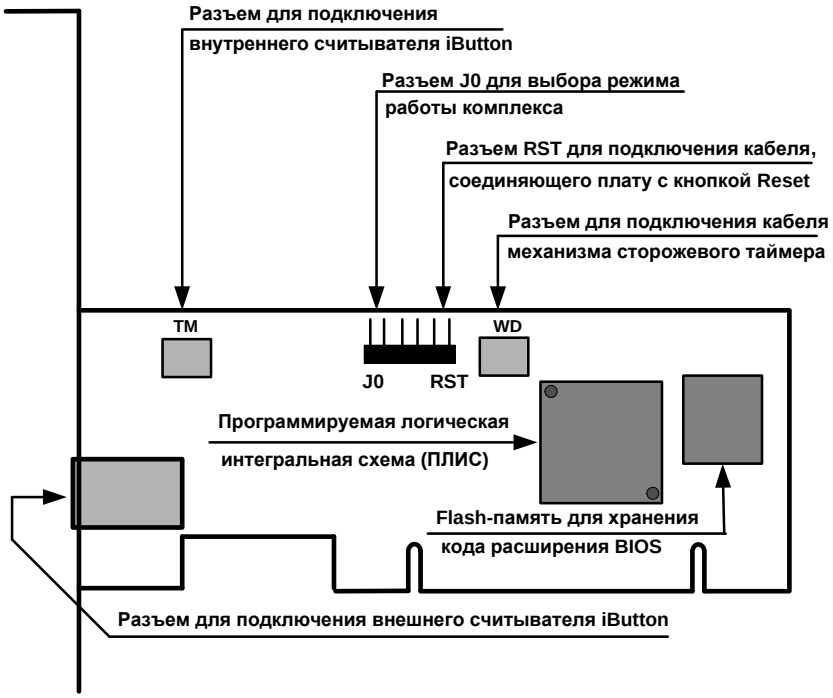


Рис. 7. Расположение разъемов на плате "Соболь 3.0/2.1" для шины PCI

3. Выполните инициализацию комплекса:

Внимание! При инициализации комплексов на компьютерах домена:

- используйте при регистрации администратора один и тот же идентификатор администратора (или его копию). При этом на первом компьютере регистрация администратора выполняется в режиме первичной регистрации, а на всех остальных — в режиме повторной регистрации;
- для комплексов "Соболь 3.0/2.1" установите одинаковое значение параметра "Версия криптографической схемы".

- включите питание компьютера;
- в появившемся на экране меню "Режим инициализации" активируйте команду "Инициализация платы";

Если после включения питания компьютера управление не было передано модулю расширения BIOS комплекса, то необходимо в BIOS Setup разрешить загрузку операционной системы с модулей расширения BIOS сетевых плат.

- в появившемся на экране меню "Общие параметры системы" настройте параметры комплекса (см. документы [10] и [12]);
- выполните регистрацию администратора (см. документы [10] и [12]);
- при необходимости выполните расчет эталонных значений контрольных сумм для объектов, заданных шаблонами контроля целостности;
- выключите питание компьютера.

4. Подготовьте комплекс к эксплуатации:
   - вскройте корпус системного блока;
   - при наличии подключенного к плате комплекса "Соболь" считывателя iButton отсоедините считыватель от платы:
     - при использовании внешнего считывателя отключите его штекер от разъема платы, расположенного на задней панели системного блока;
     - при использовании внутреннего считывателя отключите его штекер от разъема **TM**;
   - аккуратно извлеките плату комплекса из разъема шины PCI-E/PCI;
   - установите перемычку на разъем **J0** платы (см. Рис. 6, Рис. 7);
   - аккуратно вставьте плату в разъем системной шины PCI-E/PCI и закрепите планку крепления платы крепежным винтом;
   - при необходимости подключите к плате считыватель iButton:
     - при использовании внешнего считывателя подключите его штекер к разъему платы, расположенному на задней панели системного блока;
     - при использовании внутреннего считывателя подключите его штекер к разъему **TM**.
   - закройте корпус системного блока.

Интеграция комплексов "Соболь" с Secret Net 6 в сетевом режиме

В сетевом режиме функционирования Secret Net 6 реализуются:

- централизованное управление входом доменных пользователей и локальное управление входом локальных пользователей Secret Net 6 в комплекс "Соболь" с помощью персональных идентификаторов, инициализированных и присвоенных пользователям в Secret Net 6;
- централизованное управление доступом доменных пользователей к компьютерам домена, защищаемым комплексами "Соболь";
- централизованное и локальное управление работой механизма контроля целостности комплекса "Соболь";
- автоматическая передача записей журнала событий комплекса "Соболь" в журнал Secret Net (см. Табл. 4) с возможностью дальнейшего централизованного сбора всех журналов в базу данных.

Табл. 4. События, регистрируемые комплексом "Соболь" и Secret Net

События комплекса "Соболь"	События системы Secret Net 6
Вход пользователя	Соболь: вход пользователя
Вход администратора	
Не рассчитаны контрольные суммы	Соболь: не рассчитаны контрольные суммы
Переход в автономный режим	Соболь: изменение режима работы
Переход в сетевой режим	
Удаление системного журнала	Соболь: очистка журнала
Ошибка КС внешнего запроса	Соболь: ошибка синхронизации параметров
Ошибка внешнего запроса	
Перерасчет контрольных сумм	Соболь: перерасчет контрольных сумм
Автоматический перерасчет КС	
Смена аутентификатора администратора	Соболь: смена аутентификатора
Смена аутентификатора пользователя	
Идентификатор не зарегистрирован	Соболь: запрет входа пользователя
Неправильный пароль	
Превышено число попыток входа	
Пользователь блокирован	
Ошибка при контроле целостности	Соболь: нарушена целостность ресурса
Обработаны внешние запросы	Соболь: синхронизация параметров
Добавлен новый пользователь	
Пользователь удален	
Запрос Все пользователи удалены	
Запрос Добавление пользователя	
Запрос Удаление пользователя	
Администратор сменил свой пароль	Соболь: смена пароля
Администратор сменил пароль пользователя	
Пользователь сменил свой пароль	
Ошибка КС в памяти идентификатора	Соболь: ошибка КС в памяти идентификатора
Изменены параметры загрузочного диска	Соболь: изменены параметры загрузочного диска

Подробные сведения о настройке в Secret Net 6 механизмов контроля входа с использованием персональных идентификаторов приводятся в документе [3].

Управление работой механизма контроля целостности комплекса "Соболь" заключается в формировании для комплекса средствами администрирования Secret Net 6 задания на контроль целостности файлов жесткого диска. Порядок настройки механизма КЦ комплекса "Соболь" с помощью Secret Net 6 приводится в документе [3].

Передача записей журнала регистрации событий комплекса "Соболь" в журнал Secret Net и их преобразование осуществляются автоматически при загрузке подсистемы аппаратной поддержки Secret Net 6. Подробное описание событий, регистрируемых комплексом "Соболь" и системой Secret Net 6, приводится в документе [5].

Общий порядок настройки режима интеграции комплексов "Соболь" и Secret Net 6

Для включения режима интеграции Secret Net 6 и комплекса "Соболь" необходимо перевести каждое из этих средств в режим интеграции. Для отключения этого режима необходимо отключить режим интеграции в Secret Net 6 (см. стр. 22) и перевести "Соболь" в автономный режим (см. документы [10] и [12]).

Для включения и настройки в рамках домена режима интеграции комплексов "Соболь" и Secret Net 6 в сетевом режиме функционирования выполните следующие действия:

1 **Рабочее место администратора безопасности (контроллер домена).** Установите комплекс "Соболь" (см. стр. 15). Переведите установленный комплекс "Соболь" из автономного режима в режим совместного использования (см. документы [10] и [12]).

2 **Рабочее место администратора безопасности (контроллер домена).** Установите ПО системы Secret Net 6.

Подробные сведения об установке Secret Net 6 приводятся в документе [2].

3 **Рабочее место администратора безопасности (контроллер домена).** Сгенерируйте ключи централизованного управления комплексами "Соболь" (см. ниже).

4 **Рабочее место администратора безопасности (контроллер домена).** Подключите комплекс "Соболь" к Secret Net 6 (см. стр. 20).

5 **Рабочее место администратора безопасности (контроллер домена).** Настройте параметры пользователей с целью организации их доступа к компьютерам домена (назначение идентификаторов, паролей, формирование списка разрешенных компьютеров).

Подробные сведения о настройке параметров пользователей приводятся в документе [3].

6 **Компьютеры домена.** На других защищаемых компьютерах домена последовательно выполните следующие операции:

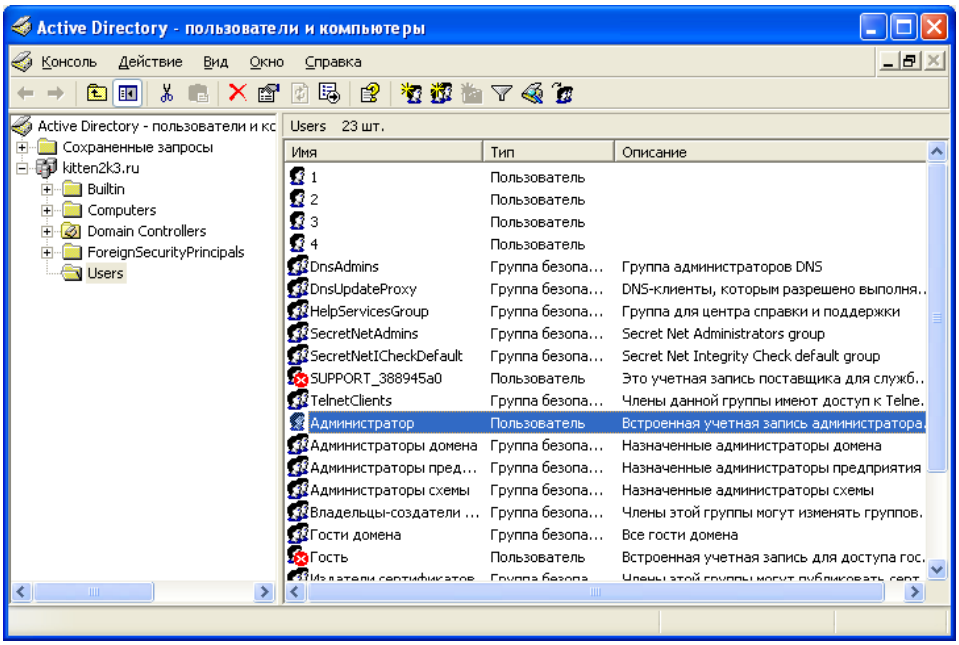
- установите комплекс "Соболь" (см. стр. 15);
- переведите установленный комплекс "Соболь" из автономного режима в режим совместного использования (см. документы [10] и [12]);
- установите ПО системы Secret Net 6 (см. документ [2]);
- подключите комплекс "Соболь" к Secret Net 6 (см. стр. 20).

Генерация ключей централизованного управления

Для генерации ключей:

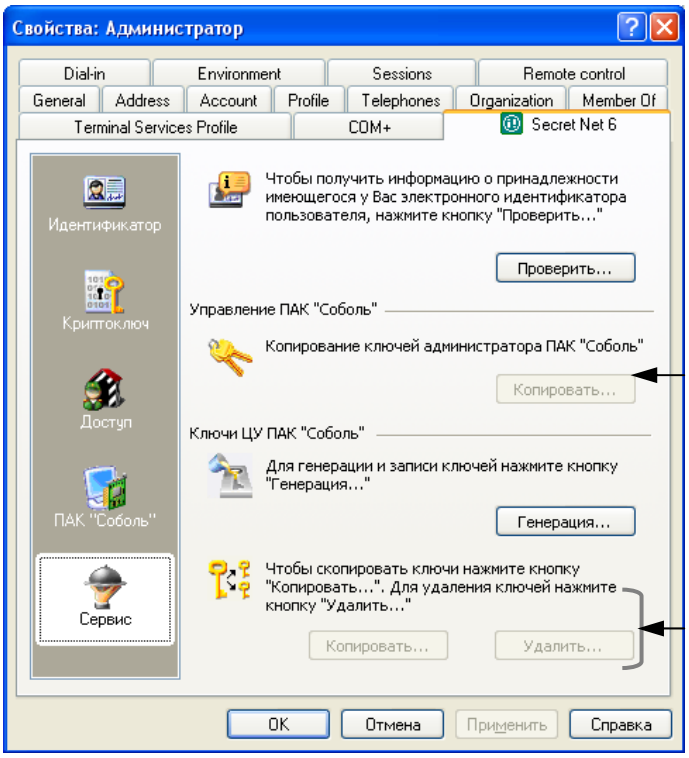
1. Нажмите кнопку "Пуск", найдите в главном меню Windows и активируйте команду "Все Программы | Администрирование | Active Directory – пользователи и компьютеры".

   На экране появится оснастка "Active Directory – пользователи и компьютеры":



2. Вызовите контекстное меню пользователя и активируйте команду "Свойства". В появившемся диалоговом окне выберите вкладку "Secret Net 6".

Диалог примет следующий вид:

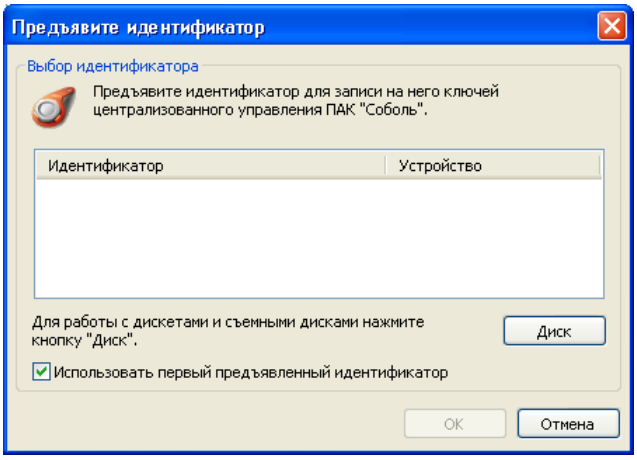


Кнопка становится доступной после подключения комплекса "Соболь" и загрузки ключей в оснастке "AD – пользователи и компьютеры"

Кнопки становятся доступными после завершения генерации и записи ключей

3. На вкладке "Secret Net 6" нажмите кнопку "Генерация".

   На экране появится диалог с предложением предъявить ключевой носитель (идентификатор) для записи на него ключей ЦУ комплексами "Соболь":



4. Предъявите ключевой носитель, предназначенный для хранения ключей ЦУ комплексами "Соболь". По окончании процедуры генерации и записи ключей нажмите кнопку "ОК".

Не допустите потери ключей ЦУ. В случае их утраты необходимо заново создать структуру централизованного управления комплексами "Соболь".

Подключение комплекса "Соболь" к Secret Net 6

Для подключения комплекса:

1. Выполните стандартную процедуру входа в систему пользователя с правами администратора Secret Net 6.
2. Вызовите на экран "Панель управления" и активируйте в ней элемент "Управление СЗИ Secret Net 6".

   На экране появится окно "Управление СЗИ Secret Net 6".
3. Выберите вкладку "Управление ПАК "Соболь".

Диалог примет следующий вид:

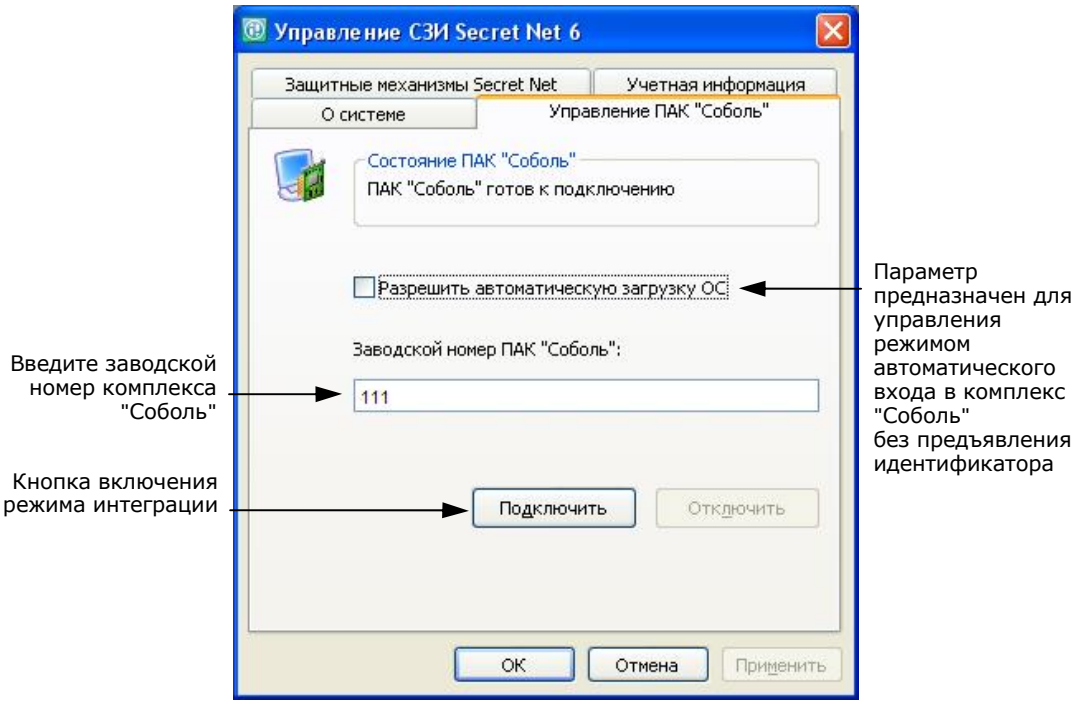


Рис. 8. Вкладка "Управление ПАК "Соболь" (режим подключения)

4. Выполните следующие действия:

- для отображения в отчете "Ресурсы АРМ" (см. документ [3]) заводского номера изделия введите этот номер в поле "Заводской номер ПАК "Соболь" и нажмите кнопку "Применить";

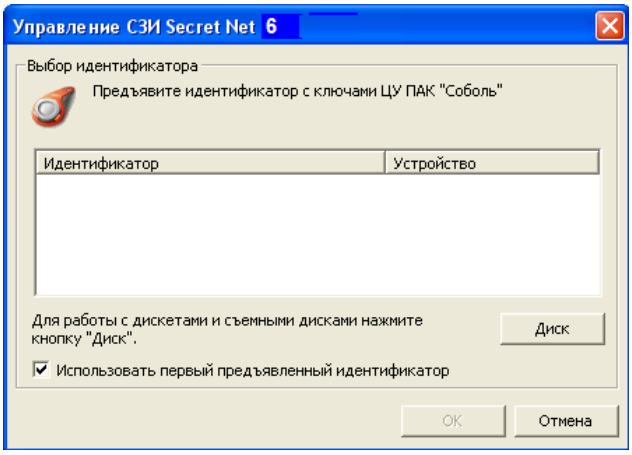
Заводской номер комплекса "Соболь" указан в паспорте изделия и на обратной стороне его платы.

- если требуется организовать автоматический вход в комплекс "Соболь" без предъявления персонального идентификатора, то установите отметку в поле "Разрешить автоматическую загрузку ОС";

Режим автоматического входа в комплекс "Соболь" начнет действовать после перезагрузки операционной системы компьютера. Время ожидания автоматического входа в комплекс составляет 30 секунд.

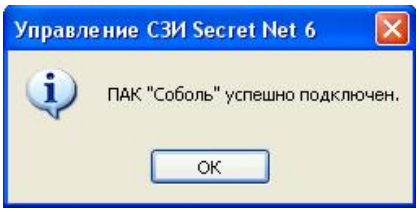
- для подключения комплекса "Соболь" нажмите кнопку "Подключить".

На экране появится диалог с предложением предъявить ключевой носитель (идентификатор) с ключами ЦУ комплексами "Соболь":



5. Предъявите носитель с ключами ЦУ комплексами "Соболь".

Система Secret Net 6 немедленно перейдет в режим интеграции с комплексом "Соболь". На экране появится информационное окно с сообщением об успешном подключении комплекса:



6. Нажмите кнопку "OK" в информационном окне.

   Вкладка "Управление ПАК "Соболь" примет следующий вид:

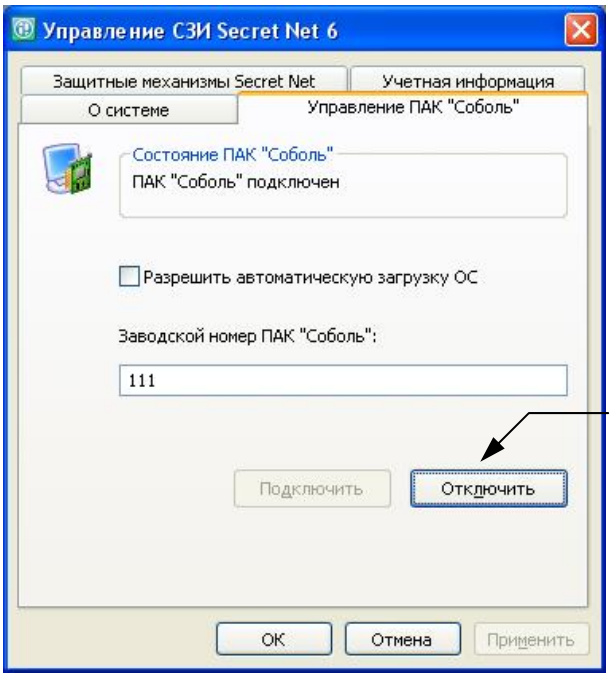


Рис. 9. Вкладка "Управление ПАК "Соболь" (режим отключения)

7. Нажмите кнопку "OK" в окне "Управление СЗИ Secret Net 6".

Отключение режима интеграции Secret Net 6 и "Соболь"

Для отключения режима интеграции:

1. Вызовите на экран "Панель управления" и активируйте в ней элемент "Управление СЗИ Secret Net 6".

   На экране появится окно "Управление СЗИ Secret Net 6".

2. Выберите вкладку "Управление ПАК "Соболь".

   Диалог примет вид, представленный на Рис. 9.

3. На вкладке "Управление ПАК "Соболь" нажмите кнопку "Отключить".

   Система Secret Net 6 немедленно выйдет из режима интеграции с комплексом "Соболь". Кнопки управления режимом интеграции станут недоступными.

Внимание! Повторное включение в Secret Net 6 режима интеграции с комплексом "Соболь" возможно только после перезагрузки компьютера.

4. Если не планируется дальнейшее использование режима интеграции, то при загрузке компьютера войдите с правами администратора в комплекс "Соболь" и переведите изделие в автономный режим работы (см. документы [10] и [12]).

Интеграция комплексов "Соболь" с Secret Net 6 в автономном режиме

В автономном режиме функционирования Secret Net 6 реализуются:

- локальное управление входом доменных и локальных пользователей Secret Net 6 в комплекс "Соболь" с помощью персональных идентификаторов, инициализированных и присвоенных пользователям в Secret Net 6;
- локальное управление работой механизма контроля целостности комплекса "Соболь";
- автоматическая передача записей журнала событий комплекса "Соболь" в журнал Secret Net.

Подробные сведения о настройке в Secret Net 6 механизмов контроля входа с использованием персональных идентификаторов приводятся в документе [3].

Управление работой механизма КЦ комплекса "Соболь" заключается в формировании для комплекса средствами администрирования Secret Net 6 задания на КЦ файлов жесткого диска. Порядок настройки механизма КЦ комплекса "Соболь" с помощью Secret Net 6 приводится в документе [3].

Передача записей журнала регистрации событий комплекса "Соболь" в журнал Secret Net и их преобразование (см. Табл. 4 на стр. 18) осуществляется автоматически на этапе загрузки подсистемы аппаратной поддержки Secret Net 6. Подробное описание событий, регистрируемых комплексом "Соболь" и системой Secret Net 6, приводится в документе [5].

Общий порядок настройки режима интеграции комплексов "Соболь" и Secret Net 6

Для включения режима интеграции системы Secret Net 6 и комплекса "Соболь" необходимо перевести каждое из этих средств в режим интеграции. Для отключения этого режима необходимо отключить режим интеграции в Secret Net 6 (см. стр. 24) и перевести "Соболь" в автономный режим (см. документы [10] и [12]).

Для включения и настройки режима интеграции комплексов "Соболь" и Secret Net 6 в автономном режиме на каждом защищаемом компьютере последовательно выполните следующие действия:

1. Установите комплекс "Соболь" (см. стр. 15). Переведите установленный комплекс "Соболь" из автономного режима в режим совместного использования (см. документы [10] и [12]).
2. Установите ПО системы Secret Net 6. Подробные сведения об установке программного обеспечения Secret Net 6 приводятся в документе [2].
3. Подключите комплекс "Соболь" к Secret Net 6 (см. ниже).
4. Настройте параметры пользователей и их персональных идентификаторов. Подробные сведения о настройке параметров приводятся в документе [3].

Подключение комплекса "Соболь" к Secret Net 6

Для подключения комплекса Соболь":

1. Выполните стандартную процедуру входа в систему пользователя с правами администратора компьютера.
2. Вызовите на экран "Панель управления" и активируйте в ней элемент "Управление СЗИ Secret Net 6".

   На экране появится окно "Управление СЗИ Secret Net 6".
3. Выберите вкладку "Управление ПАК "Соболь".

   Диалог примет вид, представленный на Рис. 8 на стр. 21.

4. Выполните следующие действия:
   - для отображения в отчете "Ресурсы АРМ" (см. документ [3]) заводского номера изделия введите этот номер в поле "Заводской номер ПАК "Соболь" и нажмите кнопку "Применить";

Заводской номер комплекса "Соболь" указан в паспорте изделия и на обратной стороне его платы.

   - если требуется организовать автоматический вход в комплекс "Соболь" без предъявления персонального идентификатора, то установите отметку в поле "Разрешить автоматическую загрузку ОС";

Режим автоматического входа в комплекс "Соболь" начнет действовать после перезагрузки операционной системы компьютера. Время ожидания автоматического входа в комплекс составляет 30 секунд.

   - для подключения комплекса "Соболь" нажмите кнопку "Подключить".

   Система Secret Net 6 немедленно перейдет в режим интеграции с комплексом "Соболь". На экране появится информационное окно с сообщением об успешном подключении комплекса.

5. Нажмите кнопку "ОК" в информационном окне.

   Вкладка "Управление ПАК "Соболь" примет вид, представленный на Рис. 9.

6. Нажмите кнопку "ОК" в окне "Управление СЗИ Secret Net 6".

Отключение режима интеграции Secret Net 6 и "Соболь"

Для отключения режима интеграции:

1. Вызовите на экран "Панель управления" и активируйте в ней элемент "Управление СЗИ Secret Net 6".

   На экране появится окно "Управление СЗИ Secret Net 6".

2. Выберите вкладку "Управление ПАК "Соболь".

   Диалог примет вид, представленный на Рис. 9.

3. На вкладке "Управление ПАК "Соболь" нажмите кнопку "Отключить".

   Система Secret Net 6 немедленно выйдет из режима интеграции с комплексом "Соболь". Кнопки управления режимом интеграции станут недоступными.

Внимание! Повторное включение в Secret Net 6 режима интеграции с комплексом "Соболь" возможно только после перезагрузки компьютера.

4. Если не планируется дальнейшее использование режима интеграции, то при загрузке компьютера войдите с правами администратора в комплекс "Соболь" и переведите изделие в автономный режим работы (см. документы [10] и [12]).

Secret Net Card и Secret Net Touch Memory Card PCI 2

Установку SN Card и SN TM Card PCI 2 на защищаемый компьютер следует выполнять после установки драйвера изделия, входящего в состав программного обеспечения Secret Net 6 (подробные сведения об установке ПО Secret Net 6 приводятся в документе [2]). На компьютере под управлением ОС Windows 2000/XP/2003 драйвер изделия устанавливается по умолчанию при установке клиентского ПО Secret Net 6. На ОС Windows Vista и выше перед установкой драйвера выводится запрос системы с предоставлением возможности отказа от установки драйвера. В дальнейшем, чтобы установить драйвер вручную, достаточно запустить файл "Драйвер платы Secret Net Touch Memory Card.msi" из соответствующего каталога на установочном компакт-диске:

- \Setup\SnTmCard\Win32\ — для 32-разрядных версий ОС Windows;
- \Setup\SnTmCard\x64\ — для 64-разрядных версий ОС Windows.

Процедура автоматической установки/обновления клиентского ПО Secret Net 6 на компьютерах системы не предусматривает установку или обновление драйвера изделия. Драйвер, оставшийся от предыдущей версии Secret Net, не удаляется из системы программой установки и не будет работать корректно с новой версией системы. Поэтому после завершения автоматической установки или обновления необходимо выполнить установку драйвера вручную на нужных компьютерах.

Изделия SN Card и SN TM Card PCI 2 используются в вариантах 2 и 3 — с СИА на базе iButton (см. стр. 12).

Изделия SN Card и SN TM Card PCI 2 устанавливаются на компьютеры, функционирующие под управлением 32- и 64-разрядных ОС MS Windows 2000/XP/2003/Vista/2008/7.

Компьютер, в который устанавливается плата SN Card или SN TM Card PCI 2, должен удовлетворять следующим требованиям:

- наличие свободного разъема системной шины:
  - либо стандарта PCI версий 2.0, 2.1, 2.2, 2.3 с напряжением питания 5 В или 3,3 В — для плат SN TM Card PCI 2 и SN Card;
  - либо стандарта PCI-E версии 1.0a и выше — для платы SN Card;
- наличие на материнской плате разъема Reset, подачу сигналов на который невозможно отключить из BIOS Setup или каким-либо другим образом.

Если на начальных этапах загрузки компьютера управление не передается модулю расширения BIOS изделия, то необходимо в BIOS Setup разрешить загрузку операционной системы с модулей расширения BIOS сетевых плат. Для проверки работоспособности расширения BIOS изделия достаточно при перезагрузке компьютера выполнить попытку загрузки ОС с дискеты или CD-ROM. Если загрузка ОС с этих сменных носителей невозможна — расширение BIOS изделия функционирует нормально.

Для компьютеров с установленными изделиями SN Card или SN TM Card PCI 2 должны быть предусмотрены меры, обеспечивающие контроль физического доступа к системным блокам компьютеров.

Для установки Secret Net Card/SN TM Card PCI 2 :

1. Подготовьте SN Card/SN TM Card PCI 2 к инициализации:
   - выключите питание компьютера, вскройте корпус системного блока;
   - снимите перемычку, установленную на разъеме **J0** платы (см. Рис. 10, Рис. 11 на стр. 26);
   - для использования механизма сторожевого таймера:
     - отключите штекер стандартного кабеля кнопки "Reset" от разъема Reset, расположенного на материнской плате;
     - подключите штекер стандартного кабеля кнопки "Reset" к разъему **RST** платы комплекса "Соболь" (см. Рис. 10, Рис. 11);
     - подключите штекер кабеля механизма сторожевого таймера, входящего в комплект поставки, к разъему платы **WD**. Затем подключите другой штекер этого кабеля к разъему Reset, расположенному на материнской плате;
   - выберите свободный слот системной шины PCI-E/PCI, вставьте в него плату, закрепите планку крепления платы крепежным винтом;
   - закройте корпус системного блока и включите питание компьютера.

Начнется процедура инициализации. После завершения инициализации подготовьте изделие к эксплуатации.

2. Подготовьте SN Card/SN TM Card PCI 2 к эксплуатации:
   - вскройте корпус системного блока и извлеките плату из разъема шины PCI/PCI-E;
   - установите перемычку на разъем **J0** платы (см. Рис. 6, Рис. 7);
   - вставьте плату в разъем системной шины PCI-E/PCI и закрепите планку крепления платы крепежным винтом;
   - подключите контактное устройство для идентификатора iButton к разъему платы, расположенному на задней панели системного блока;
   - закройте корпус системного блока.

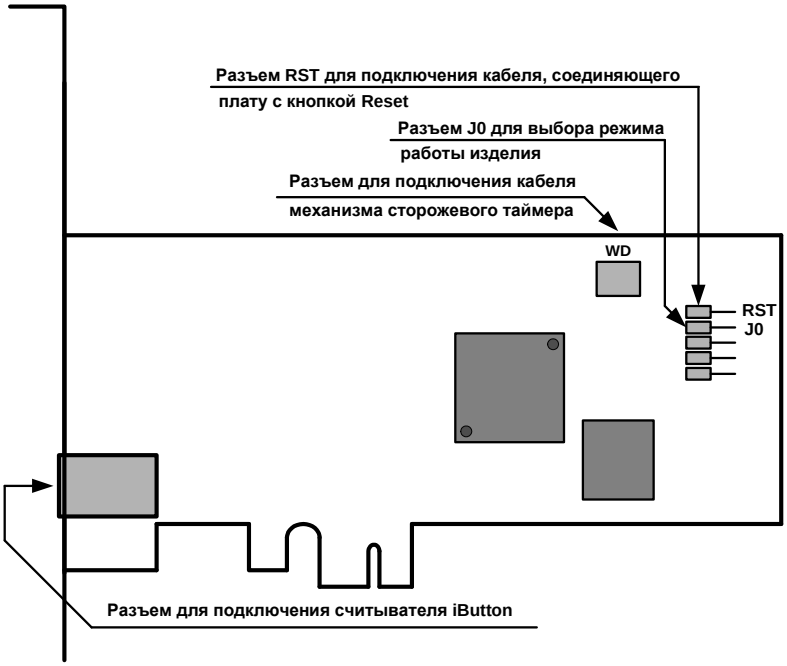


Рис. 10. Расположение разъемов на плате SN Card для шины PCI-E

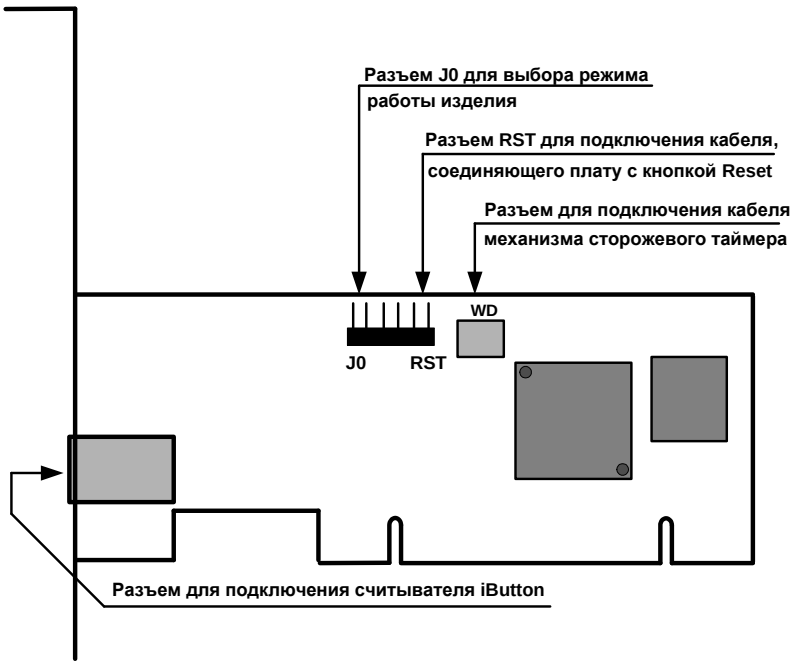


Рис. 11. Расположение разъемов на плате SN Card/SN TM Card PCI 2 для шины PCI

Установка программного обеспечения СИА на базе USB-ключей

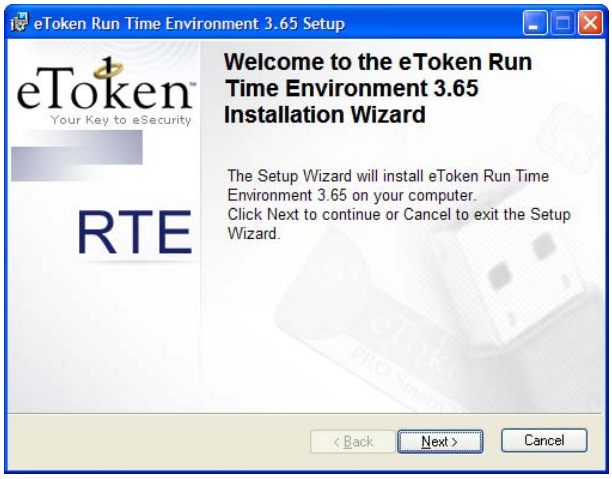
eToken PRO

Для использования в Secret Net 6 СИА на базе eToken PRO в среде ОС Windows 2000 выполните установку ПО eToken RTE версии 3.65 или 3.66, в среде ОС Windows XP/2003/Vista/2008/7 — eToken PKI Client версии 5.1.

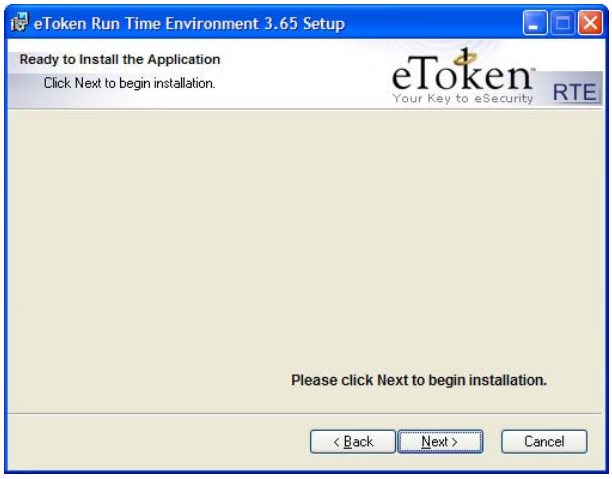
Для установки ПО eToken RTE 3.65:

Установка ПО eToken RTE версии 3.65 и 3.66 выполняется одинаково.

1. Запустите на исполнение файл программы установки.
   На экране появится следующее диалоговое окно:



2. Нажмите кнопку "Next >".
   На экране появится диалоговое окно с текстом лицензионного соглашения.
3. Выберите пункт "I accept the license agreement" и нажмите кнопку "Next >".
   На экране появится следующее диалоговое окно:



4. Нажмите кнопку "Next >".

Программа выполнит процедуру установки, по окончании которой на экране появится следующее диалоговое окно:

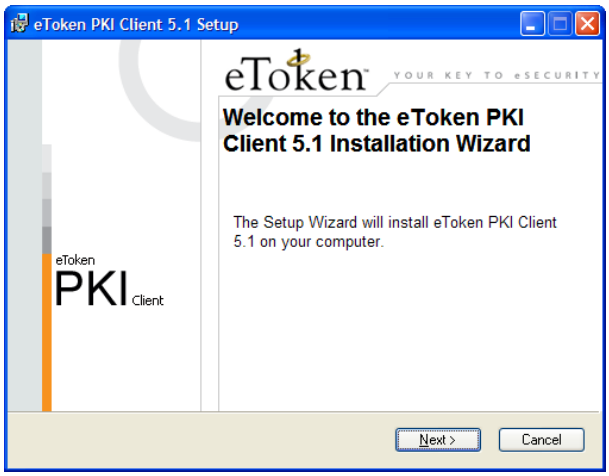
5. Нажмите кнопку "Finish".

После завершения установки ПО eToken RTE на защищаемый компьютер перезагрузите его операционную систему.

Для установки ПО eToken PKI Client 5.1:

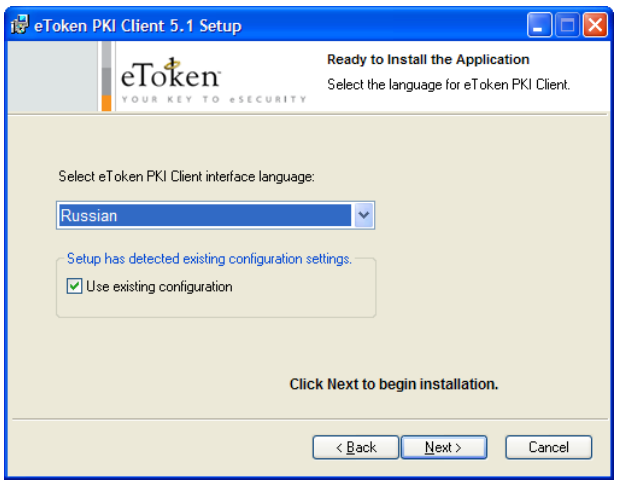
1. Запустите на исполнение файл программы установки.

   На экране появится следующее диалоговое окно:



2. Нажмите кнопку "Next >".

   На экране появится окно выбора языка интерфейса ПО eToken PKI Client:

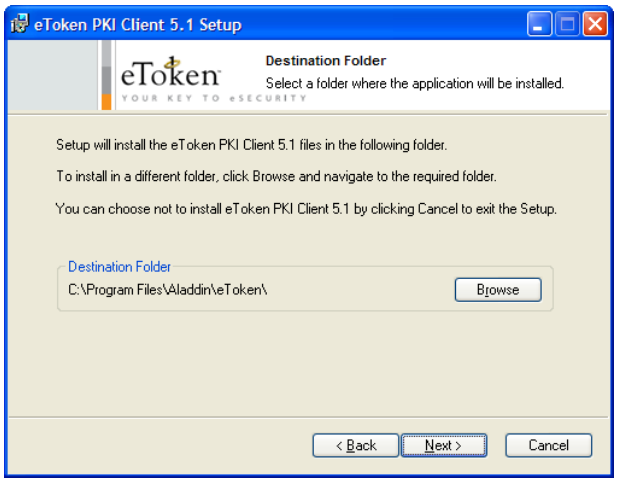


3. При необходимости выберите русский язык и нажмите кнопку "Next >".

   На экране появится диалоговое окно с текстом лицензионного соглашения.

4. Выберите пункт "I accept the license agreement" и нажмите кнопку "Next >".

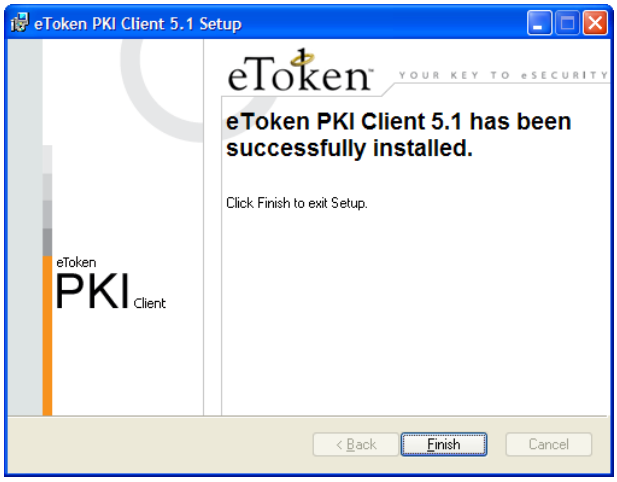
   На экране появится диалоговое окно выбора места размещения ПО eToken PKI Client:



5. Если вас устроит стандартный вариант места размещения ПО, то нажмите кнопку "Next >".

Для изменения стандартного пути размещения ПО воспользуйтесь кнопкой "Browse".

Программа выполнит процедуру установки, по окончании которой на экране появится следующее окно:



6. Нажмите кнопку "Finish".

После завершения установки ПО eToken PKI Client на защищаемый компьютер перезагрузите его операционную систему.

iKey 2032

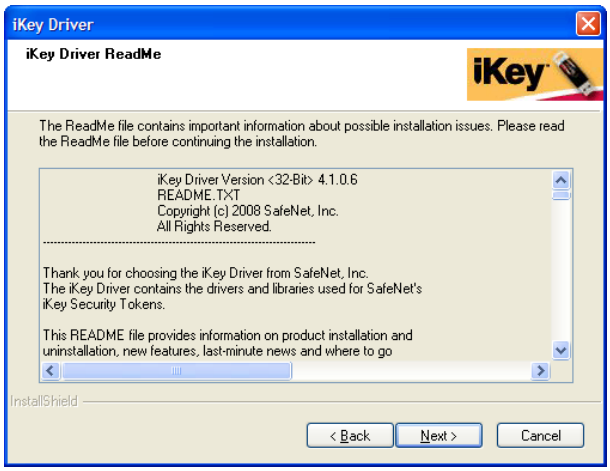
Для установки программного обеспечения:

1. Запустите на исполнение файл программы установки.

   Программа выполнит подготовку к установке. После завершения подготовительных действий на экране появится стартовый диалог программы установки.

2. Нажмите кнопку "Next >".

   На экране появится диалоговое окно с информацией об устанавливаемой версии драйвера USB-ключа.



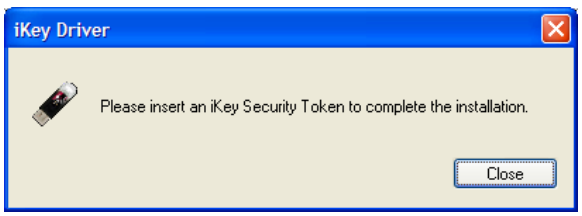
3. Ознакомьтесь с информацией, содержащейся в информационном окне, и нажмите кнопку "Next >" для продолжения установки.

   На экране появится диалог с текстом лицензионного соглашения.

4. Ознакомьтесь с условиями лицензионного соглашения и нажмите кнопку "Yes".

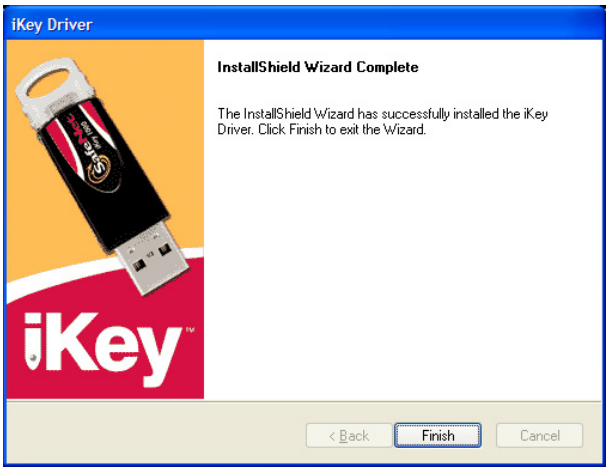
   Программа установки приступит к копированию файлов на жесткий диск компьютера. Ход процесса копирования отображается на экране в виде индикатора прогресса.

   После завершения процесса копирования на экране появится следующее диалоговое окно:



5. Нажмите кнопку "Close".

На экране появится следующее диалоговое окно:



6. Нажмите кнопку "Finish".

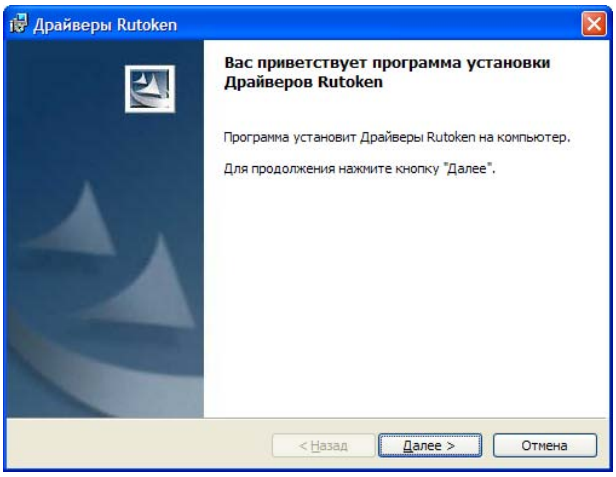
После завершения установки программного обеспечения СИА на базе iKey 2032 на защищаемый компьютер перезагрузите его операционную систему.

Rutoken

Для установки программного обеспечения:

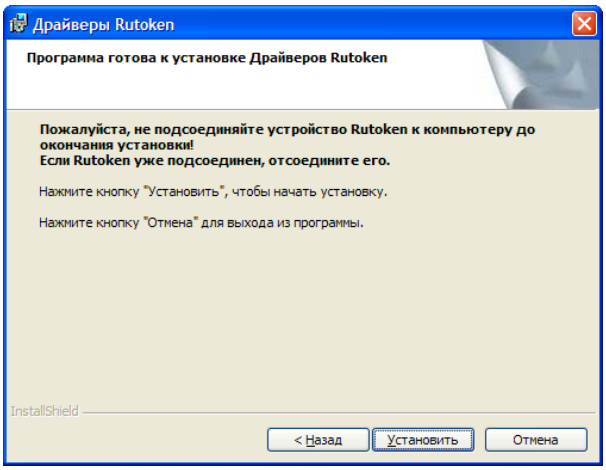
1. Запустите на исполнение файл программы установки.

   Программа выполнит подготовку к установке. После завершения подготовительных действий на экране появится стартовый диалог программы установки.



2. Нажмите кнопку "Далее >".

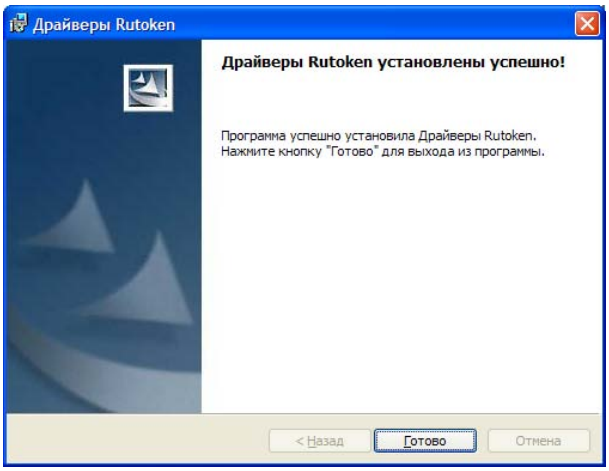
На экране появится следующее диалоговое окно:



3. Нажмите кнопку "Установить".

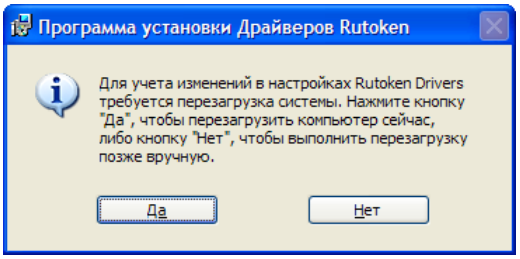
   Программа установки приступит к копированию файлов на жесткий диск компьютера. Ход процесса копирования отображается на экране в виде индикатора прогресса.

   После успешного выполнения процедуры установки на экране появится завершающий диалог программы установки:



4. Нажмите кнопку "Готово".

   На экране появится следующее окно:



5. Нажмите кнопку "Да".

Терминологический справочник

А	
Администратор безопасности	Лицо или группа лиц, ответственных за обеспечение безопасности системы, за реализацию и непрерывность соблюдения установленных административных мер защиты и осуществляющих постоянную организационную поддержку функционирования применяемых физических и технических средств защиты
Аппаратные средства защиты	Различные электронные устройства, которые выполняют (самостоятельно или в комплексе с другими средствами) функции защиты информации. Например, идентификацию и аутентификацию пользователей, блокировку загрузки операционной системы с внешних носителей, регистрацию событий, криптографические функции и др.
Аутентификация	Проверка регистрационной информации о пользователе
И	
Идентификатор	Уникальный признак субъекта (объекта) доступа, позволяющий однозначно выделить идентифицируемый субъект (объект) среди множества других субъектов (объектов). В качестве идентификатора может использоваться запоминаемый код, биометрический признак или устройство (контактная смарт-карта, бесконтактная смарт-карта, iButton, USB-ключ), в которое с помощью специальной технологии занесен идентификационный признак в виде кодовой информации
Идентификация	Распознавание субъекта (объекта) по присущему или присвоенному ему идентификационному признаку
К	
Контрольная сумма	Числовое значение, вычисляемое по специальному алгоритму и используемое для контроля неизменности данных
Контроль целостности	Проверка наличия несанкционированной модификации файлов и секторов жесткого диска защищаемого компьютера
Н	
НСД	Доступ субъектов к объекту в нарушение установленных в системе правил разграничения доступа
О	
Объект системы	Пассивный компонент системы, хранящий, принимающий или передающий информацию. Доступ к объекту подразумевает доступ к содержащейся в нем информации
П	
Порт ввода/вывода	Специальный интерфейс, необходимый для подсоединения внешних устройств (считыватели СИА, платы аппаратной поддержки, платы расширения, клавиатура, манипулятор "мышь", внешние модемы и т. п.) к компьютеру
С	
Считыватель СИА	Устройство в составе СИА, предназначенное для чтения (ввода) идентификационных признаков
Субъект системы	Активный компонент системы, обычно представляемый в виде пользователя или устройства, которые могут явиться причиной потока информации от объекта к объекту или изменения состояния системы

Документация

1	Средство защиты информации Secret Net 6. Принципы построения. Руководство администратора	RU.88338853.501410. 007 91 1
2	Средство защиты информации Secret Net 6. Установка, обновление и удаление. Руководство администратора	RU.88338853.501410. 007 91 2
3	Средство защиты информации Secret Net 6. Управление. Основные механизмы защиты. Руководство администратора	RU.88338853.501410. 007 91 3
4	Средство защиты информации Secret Net 6. Управление. Полномочное управление доступом и контроль печати. Руководство администратора	RU.88338853.501410. 007 91 4
5	Средство защиты информации Secret Net 6. Аудит. Руководство администратора	RU.88338853.501410. 007 91 5
6	Средство защиты информации Secret Net 6. Мониторинг и оперативное управление. Руководство администратора	RU.88338853.501410. 007 91 6
7	Средство защиты информации Secret Net 6. Конфигурирование. Руководство администратора	RU.88338853.501410. 007 91 7
8	Средство защиты информации Secret Net 6. Аппаратные средства. Руководство администратора	RU.88338853.501410. 007 91 8
9	Средство защиты информации Secret Net 6. Руководство пользователя	RU.88338853.501410. 007 92
10	Программно-аппаратный комплекс "Соболь". Версия 2.1. Руководство администратора	УВАЛ. 00300-58-01 91
11	Программно-аппаратный комплекс "Соболь". Версия 2.1. Руководство пользователя	УВАЛ. 00300-58-01 92
12	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство администратора	RU.40308570.501410. 001 91
13	Программно-аппаратный комплекс "Соболь". Версия 3.0. Руководство пользователя	RU.40308570.501410. 001 92