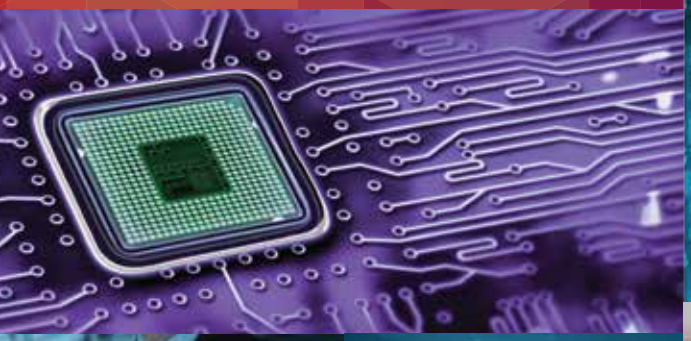
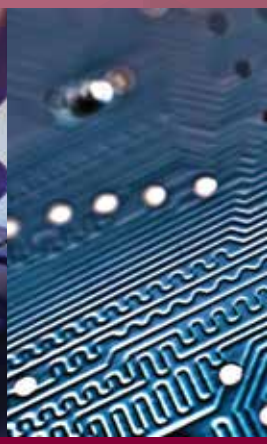
НАДЕЖНАЯ ЗАЩИТА



НАША ЗАБОТА



ДОВЕРЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

ANCUD
· ANGSTREM CUSTOM DESIGN ·

СОДЕРЖАНИЕ

КОМПЛЕКСНАЯ ЗАЩИТА ВАШЕЙ ИНФОРМАЦИИ

Ю.В. РОМАНЕЦ, ГЕНЕРАЛЬНЫЙ ДИРЕКТОР ФИРМЫ «АНКАД»

В современных условиях при построении системы защиты для критически важных объектов особое значение уделяется уязвимостям, связанным с наличием закладок в аппаратном или программном обеспечении. Фирма «АНКАД» разрабатывает доверенные российские средства защиты информации и построенные на их основе средства вычислительной техники, гарантирующие невозможность внедрения закладок на этапе производства в России. Использование отечественных решений полностью соответствует заданному руководством РФ курсу на импортозамещение в сфере вычислительной техники и связи.

Уникальная практика технического развития позволяет Фирме «АНКАД» оставаться лидером в сфере систем информационной безопасности на протяжении четверти века. Объединяя в своём штате высококлассных специалистов, мы ставим своей целью на регулярной основе развивать и пополнять базу специальных знаний в сфере шифртехники, а также создавать доверенные отечественные комплексы и средства вычислительной техники с интегрированными средствами защиты информации, включая криптографические.

Техническое совершенствование продукции и технологий Фирмы «АНКАД» напрямую зависят от мнения заказчиков и клиентов компании. Коллектив фирмы благодарен Вам за доверие к нашим разработкам, конструктивную критику, пожелания и комментарии, которые помогают усовершенствовать выпускаемые нами изделия.

Фирма «АНКАД» - ведущий разработчик и поставщик систем защиты информации, используемых для построения защищенных информационных и телекоммуникационных систем и комплексов.

Фирма «АНКАД» образована в 1991 году, за годы работы получила огромный опыт научно-исследовательских и конструкторских работ, создания и доработки систем защиты информации по требованиям заказчиков.

Приоритетом фирмы является защита информации, составляющей государственную тайну, с высокими грифами секретности.

ФИРМА «АНКАД» РЕЗИДЕНТ ОСОБОЙ ЭКОНОМИЧЕСКОЙ ЗОНЫ РОСОЭЗ® Зеленоград

Нам доверяют защиту своих информационных систем, в основном, крупные государственные и коммерческие организации, министерства, силовые ведомства - те, кому необходима надежная защита информации.
Фирма «АНКАД» открыта для совместных разработок с компаниями-интеграторами, обеспечивает профессиональную и легитимную поддержку заказчиков в вопросах защиты информации, организует для них консультации и семинары.

Широкая линейка продуктов Фирмы «АНКАД» под торговой маркой КРИПТОН/Crypton хорошо известна в России и за ее пределами. Это инновационные продукты (защищенные российскими патентами), созданные на основе отечественных криптоалгоритмов.

Продукция Фирмы «АНКАД» соответствует самым высоким требованиям стандартов и системы сертификации ФСБ и ФСТЭК России.

Компетенция специалистов Фирмы «АНКАД» позволяет организовать разработку средств защиты информации любой сложности и на любой платформе, включая разработку специальной элементной базы с реализацией разнообразных алгоритмов обработки информации. Мы можем предложить провести заказное проектирование на самом высоком технологическом уровне, чтобы обеспечить наибольшую независимость разрабатываемой техники двойного применения от зарубежных поставок и производств в интересах обеспечения национальной безопасности.

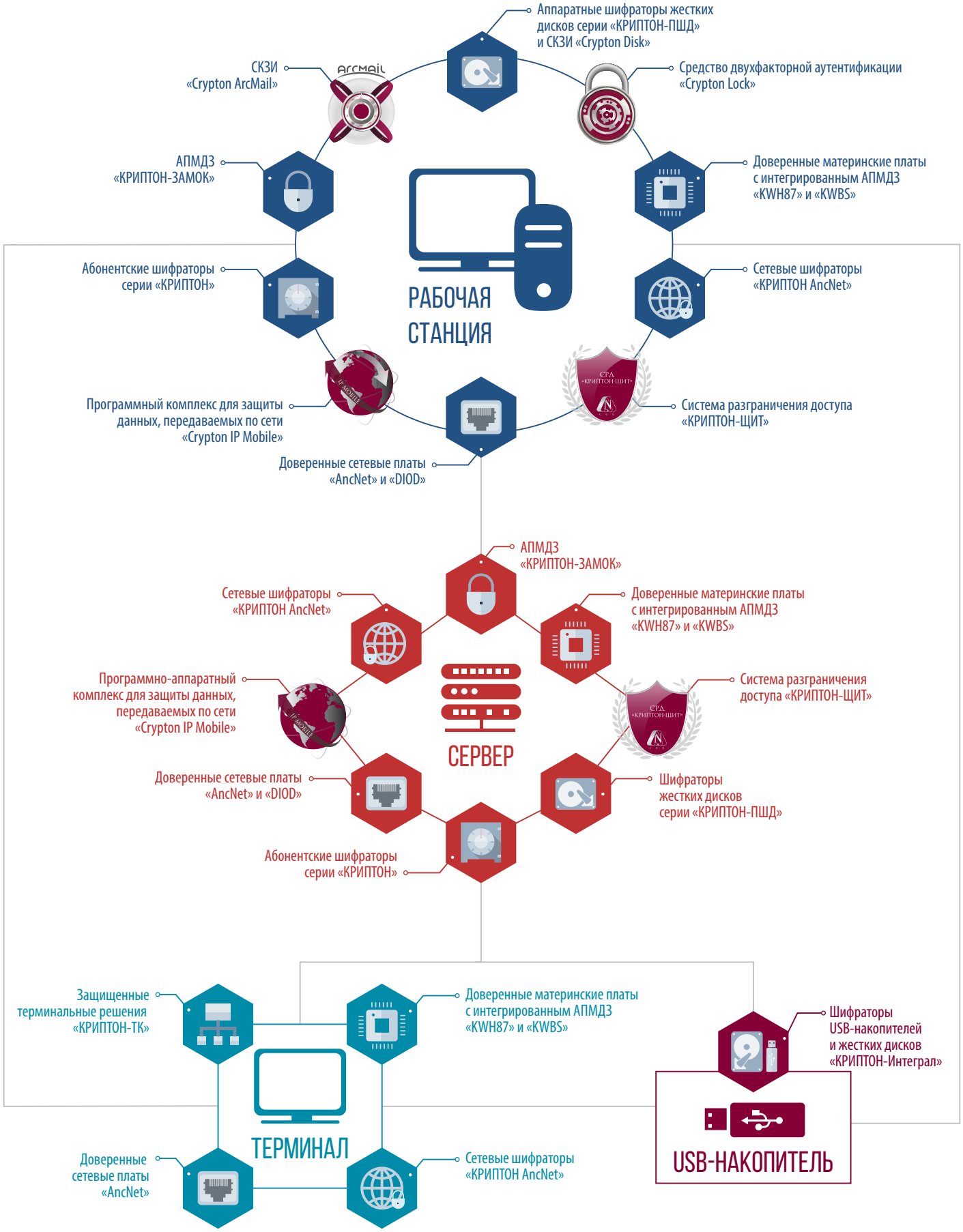
ПРОДУКЦИЯ, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ЗАЩИТЫ СВЕДЕНИЙ, СОСТАВЛЯЮЩИХ ГОСУДАРСТВЕННУЮ ТАЙНУ

Наименование	Описание	Тип реализации
АПМДЗ «КРИПТОН-ЗАМОК»	Комплекс, обеспечивающий защиту от несанкционированного доступа к компьютеру.	Программно-аппаратный
«КРИПТОН-ПШД» «КРИПТОН-Интеграл»	Средства, предназначенные для криптографической защиты информации, хранящейся на жестких дисках и USB-накопителях.	Программно-аппаратный
«КРИПТОН AncNet»	Семейство устройств, позволяющих выполнять криптографическую защиту данных, передаваемых в сеть.	Программно-аппаратный
«КРИПТОН-8, 10»	Абонентские шифраторы, выполняющие шифрование и контроль целостности блоков информации по запросам прикладного программного обеспечения.	Программно-аппаратный
СРД «КРИПТОН-ЩИТ»	Система, обеспечивающая разграничение доступа к программным ресурсам компьютера.	Программно-аппаратный
«КРИПТОН-ТК»	Комплекс, позволяющий создавать инфраструктуру «тонкий клиент» с интегрированными механизмами защиты информации.	Программно-аппаратный

ПРОДУКЦИЯ, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Наименование	Описание	Тип реализации
АПМДЗ «КРИПТОН-ЗАМОК»	Комплекс, обеспечивающий защиту от несанкционированного доступа к компьютеру.	Программно-аппаратный
СРД «КРИПТОН-ЩИТ»	Система, обеспечивающая разграничение доступа к программным ресурсам компьютера.	Программно-аппаратный
«AncNet»	Доверенные сетевые адаптеры, предназначенные для надежной передачи данных в компьютерных сетях.	Аппаратный
«DIOD»	Сетевые интерфейсные адаптеры, позволяющие решить задачу одностороннего обмена данными между компьютерами.	Аппаратный Программно-аппаратный
«Crypton IP Mobile»	Комплекс, служащий для защиты данных, передаваемых по компьютерным сетям.	Программно-аппаратный Программный
«Crypton Lock»	Средство защиты информации, предназначенное для обеспечения санкционированного доступа на компьютер под управлением операционной системы семейства MS Windows.	Программный
«Crypton Disk»	Комплекс, предназначенный для создания шифрованных логических дисков.	Программный
«Crypton ArcMail»	Комплекс, предоставляющий единый интерфейс электронной подписи, сжатия и шифрования объектов файловой системы: файлов и каталогов.	Программный

СХЕМА ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС «КРИПТОН-ТК»

Программно-аппаратный комплекс «КРИПТОН-ТК» позволяет создать инфраструктуру «тонкий клиент» с интегрированными механизмами защиты информации.
«КРИПТОН-ТК» предназначен для обработки сведений, содержащих государственную тайну вплоть до грифа «Совершенно секретно».

СЕРТИФИЦИРОВАНО ФСБ

WINDOWS

«КРИПТОН ТК-LEX»

«КРИПТОН ТК-ИК»

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Единая двухфакторная аутентификация

Для доступа к терминалу и программному обеспечению пользователя на сервере приложений используется единая двухфакторная аутентификация по идентификатору Touch Memory (TM) или смарт-карте и паролю пользователя.

Доверенная загрузка

Использование АПМДЗ позволяет проводить аутентификацию пользователей до загрузки ОС, проверку целостности файлов на серверах, запрет загрузки с любых носителей, кроме разрешенных.

Удаленная загрузка ОС

Удаленная загрузка ОС на терминалы позволяет избежать преднамеренной модификации ОС терминала с целью несанкционированного ввода/вывода информации.

Аппаратное шифрование сетевого трафика

Использование сетевого адаптера с аппаратным шифрованием сетевого трафика по ГОСТ 28147-89 позволяет надежно защитить информацию, передаваемую по локальной сети, в процессе работы пользователей.

Централизованное администрирование

Все права пользователей, зарегистрированные терминалы, разрешенные приложения и т.д. хранятся в единой базе данных, что позволяет администрировать систему централизованно с любого разрешенного терминала.

Интеграция с Active Directory (AD)

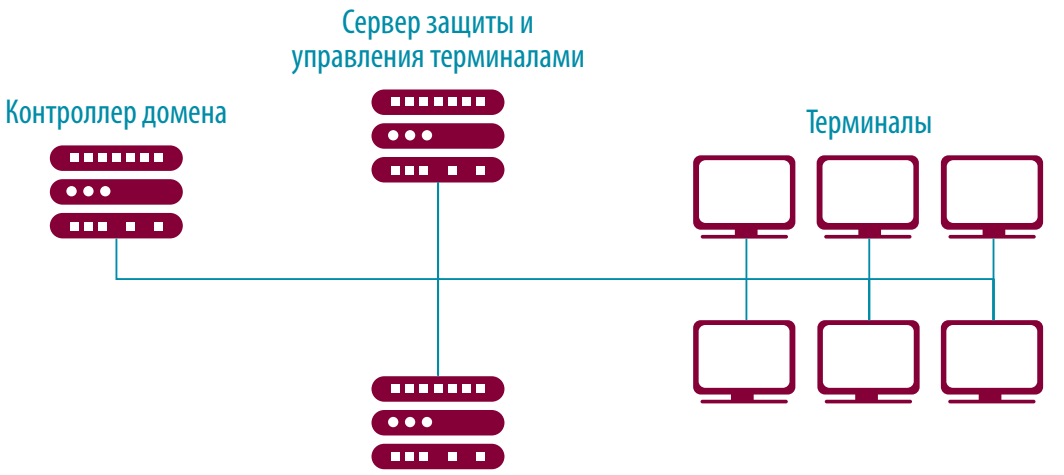
ПАК «КРИПТОН-ТК» интегрируется с Active Directory (синхронизация групп безопасности, информация о пользователях), что позволяет использовать широкий спектр ПО, получающего необходимую информацию из AD.

Реестр Аутентифицирующих Носителей

Все носители TM или смарт-карты, используемые в ПАК «КРИПТОН-ТК», должны быть заранее зарегистрированы в Реестре Аутентифицирующих Носителей администратором безопасности, что запрещает использование неконтролируемых носителей администраторами и пользователями системы.

СОСТАВ КОМЛЕКСА

Наименование	Назначение
Контроллер домена	Необходим для корректной работы нескольких серверов приложений и единого входа в сеть.
Сервер защиты и управления терминалами (возможно совмещение с контроллером домена)	Является основным местом хранения информации о различных объектах распределенной системы, а также активным компонентом системы, осуществляющим ряд функций по ее управлению.
Сервер приложений	Специализированный сервер, на котором будут выполняться все пользовательские приложения.
Терминал	Рабочее место пользователей защищенной инфраструктуры «тонкого клиента».



ЗАЩИЩЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА НА ПРИМЕРЕ «КРИПТОН-ТК»

ПОДДЕРЖИВАЕМЫЕ НА ТЕРМИНАЛАХ ВНЕШНИЕ УСТРОЙСТВА

СОСТАВ КОМПЛЕКСА

- Аппаратно-программные модули доверенной загрузки семейства «КРИПТОН».
- Сетевые адаптеры «AncNet» или «КРИПТОН AncNet».
- Программное обеспечение сервера защиты и управления терминалами.
- Программное обеспечение сервера приложений.
- Собственная сертифицированная клиентская терминальная операционная система «АнкадОС-ТК» со встроенными средствами безопасности и управления.

КОМПЛЕКСНОЕ РЕШЕНИЕ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фирма «АНКАД» представляет линейку российских доверенных комьютеров «Kraftway», построенных на основе отечественных материнских плат с интегрированными средствами защиты информации.

ТЕРМИНАЛЬНАЯ СТАНЦИЯ, РАБОЧАЯ СТАНЦИЯ И СЕРВЕР

ОТЛИЧИТЕЛЬНЫЕ ОСОБЕННОСТИ КОМПЬЮТЕРОВ ЛИНЕЙКИ

- Замкнутый цикл производства в России, включающий в себя спецпроверки и специсследования.
- Доверенная аппаратная платформа российского производства с интегрированными функциями безопасности.
- Аппаратный контроль системных шин, гарантирующий неизменность BIOS компьютера.
- Аппаратный ДСЧ (опционально).
- Универсальная доверенная UEFI среда для запуска модулей безопасности.
- Антивирусная защита на уровне UEFI.
- Двухфакторная аппаратная аутентификация.
- Защищенное хранилище ключевой информации.
- Контроль целостности программных компонентов системы.
- Прозрачное аппаратное шифрование хранимой информации (опционально).
- Шифрование данных, передаваемых по сети (опционально).
- Возможность обработки информации с различным уровнем конфиденциальности, вплоть до сведений, составляющих государственную тайну.

ГОТОВЫЕ РЕШЕНИЯ

Терминальная станция

Идеально подходит в качестве терминала в защищенной архитектуре «тонкого клиента». В распоряжении пользователя встроенные аппаратные средства доверенной загрузки, возможность аппаратного шифрования передаваемых данных, защищенное энергонезависимое хранилище для запускаемого ПО.

Сервер

Современный высокопроизводительный сервер в защищенном исполнении обеспечивает безопасное хранение информации, построение защищенных каналов связи для удаленных сотрудников, разграничение доступа к внутренним ресурсам, централизованное управление.

Рабочая станция

Применяется для требовательных систем автоматизированного проектирования, больших баз данных и многофункциональных сред разработки. Надежная рабочая станция позволит вести разработку проектов любой сложности в защищенной среде. Результаты разработки будут надежно защищены.

ОСНОВА ЗАЩИЩЕННЫХ КОМПЬЮТЕРОВ - ОТЕЧЕСТВЕННАЯ АППАРАТНАЯ ПЛАТФОРМА

 Материнская плата «KWH87»	СЕРТИФИЦИРОВАНО ФСБ  Материнская плата «KWBS»
Форм-фактор Micro ATX	Форм-фактор «уменьшенный» Micro ATX
Поддержка процессоров Intel® Core 4 поколения, сокет LGA1150 (Core i7, i5, i3, Pentium, Celeron)	Четырехъядерный процессор Intel® Celeron
Оперативная память до 32ГБ DDR3-1600/1333	Оперативная память до 8ГБ DDR3L-1066
Чипсет INTEL H87	Чипсет SoC Intel® BayTrail
Интерфейсы SATA, USB 2.0/3.0, COM, LPT, RJ45, HDMI, VGA, Audio	Интерфейсы SATA, USB 2.0/3.0, COM, LPT, RJ45, SFP, HDMI, VGA, Audio
Видео Intel HD Graphics (возможна установка видеокарт NVIDIA GeForce и ATI Radeon)	Видео Intel HD Graphics

ПРЕИМУЩЕСТВО - НЕИЗВЛЕКАЕМЫЙ МОДУЛЬ АПМДЗ «КРИПТОН-ВИТЯЗЬ»

Главной особенностью системных плат производства компании «Kraftway» является интеграция в них неизвлекаемого аппаратно-программного модуля доверенной загрузки, предназначенного для двухфакторной аутентификации пользователя, разграничения доступа пользователя к ресурсам компьютера, контроля целостности установленной на компьютере программной среды, управления и совместной работы со встроенными средствами защиты информации серии «КРИПТОН».

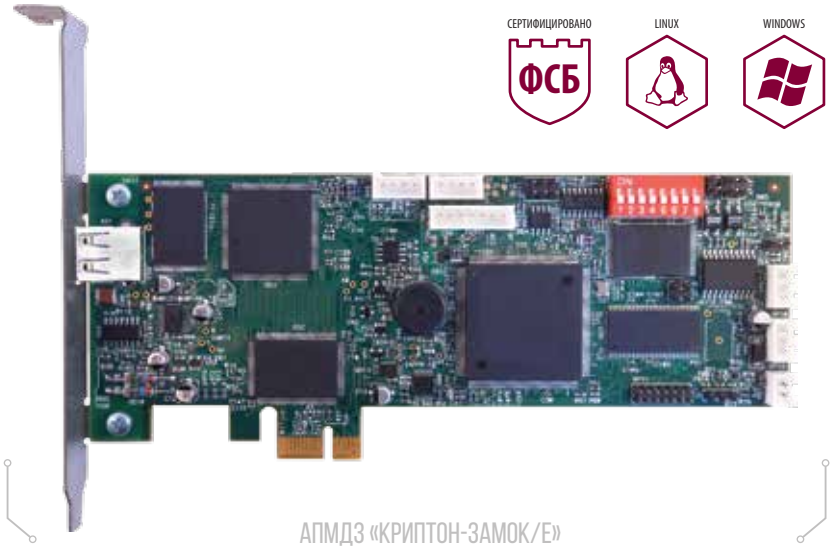
- Начинает работу сразу после подачи питания
- Контроль целостности BIOS
- Доверенная загрузка ОС
- Гарантированная работоспособность комплекса

РАЗНОУРОВНЕВАЯ ЗАЩИТА ИНФОРМАЦИИ

Компьютеры линейки позволяют формировать систему защиты, исходя из вида обрабатываемой информации.

АППАРАТНО-ПРОГРАММНЫЙ МОДУЛЬ ДОВЕРЕННОЙ ЗАГРУЗКИ «КРИПТОН-ЗАМОК»

«КРИПТОН-ЗАМОК» – комплекс средств, предназначенный для контроля и разграничения доступа пользователя к компьютеру и его аппаратным ресурсам, контроля целостности установленной на компьютере программной среды, а также для управления устройствами криптографической защиты информации серии «КРИПТОН».



АПМДЗ «КРИПТОН-ЗАМОК/E»

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Идентификация и аутентификация — Идентификация и усиленная аутентификация пользователей до загрузки операционной системы компьютера. Поддерживаются электронные ключевые носители, такие как iButton и смарт-карты.

Принудительная блокировка ПК — Блокировка доступа к компьютеру при обнаружении попытки несанкционированного доступа.

Создание нескольких профилей защиты — Многопользовательская структура модуля позволяет надежно разграничить ресурсы компьютера.

Контроль целостности — Подсчет эталонных значений контрольных сумм объектов и проверка текущих значений гарантирует неизменность конфигурации программной среды.

Доверенная загрузка — Принудительная загрузка операционной системы с выбранного устройства в соответствии с индивидуальными полномочиями пользователя. Аппаратная защита от несанкционированной загрузки операционной системы с гибкого диска, CD-ROM, DVD-ROM и USB-устройств.

Удаленное управление — Организация удаленного централизованного управления позволяет контролировать действия пользователей администратором, настраивать учетные записи, хранить базу данных пользователей на сервере.

Многоконтурность — Управление доступом к накопителям жестких, гибких дисков и блокировкой сетевых адаптеров позволяет создавать несколько контуров защиты.

РЕШАЕМЫЕ ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

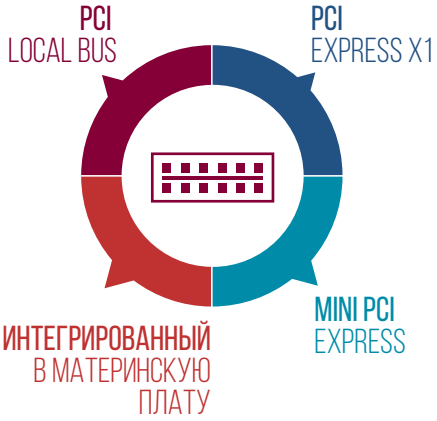
Функции устройства «КРИПТОН-ЗАМОК» по управлению аппаратными шифраторами семейства «КРИПТОН» и его многофункциональный программный интерфейс обусловливают возможность построения на базе данного устройства разнообразных комплексных решений по обеспечению безопасности компьютерных систем.

Модульная структура изделий «КРИПТОН-ЗАМОК» позволяет настраивать и дорабатывать их под конкретные требования заказчиков, благодаря чему возможно построение многоуровневых систем защиты, адаптированных для различных информационных систем.

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ

• Алгоритм шифрования аутентифицирующей информации в изделиях «КРИПТОН-ЗАМОК» соответствует требованиям ГОСТ 28147-89.
• Возможность разрешить некоторым пользователям осуществлять загрузку ОС с внешних носителей. Остальные пользователи загружают ОС только через сетевой адаптер, произведенный фирмой «АНКАД», или с одного из накопителей на жёстком диске компьютера, который специально подготовлен администратором.
• «КРИПТОН-ЗАМОК» поставляется в нескольких модификациях, которые могут быть использованы для защиты как конфиденциальной информации, так и для защиты информации, составляющей государственную тайну (до грифа «Совершенно секретно» включительно).

ВАРИАНТЫ ИНТЕРФЕЙСОВ УСТРОЙСТВ



«КРИПТОН-ПШД» И «КРИПТОН-ИНТЕГРАЛ»

СЕРТИФИЦИРОВАНО ФСБ

Устройства «КРИПТОН-ПШД» и «КРИПТОН-Интеграл» предназначены для криптографической защиты сведений, составляющих государственную тайну, хранящихся на жестких дисках компьютера и на USB-носителях.

ПРОХОДНЫЕ ШИФРАТОРЫ «КРИПТОН-ПШД» И «КРИПТОН-ИНТЕГРАЛ»

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Прозрачное шифрование данных

Шифрование информации на жестком диске или съемном USB-носителе осуществляется по алгоритму ГОСТ 28147-89 прозрачным методом, т. е. автоматически и незаметно (после однократной настройки) как для пользователя, так и для операционной системы.

Независимость от ОС и файловых систем

Вся записываемая на носитель информация шифруется целиком, включая служебные данные, что обеспечивает независимость использования устройств как от операционной системы, так и от файловых систем.

Функции электронного замка и доверенной загрузки

Проходные шифраторы работают в составе комплексов, включающих также АПМДЗ «КРИПТОН-ЗАМОК», который выполняет управление шифраторами и загрузку в них ключевой информации.

Автоматическое перешифрование данных

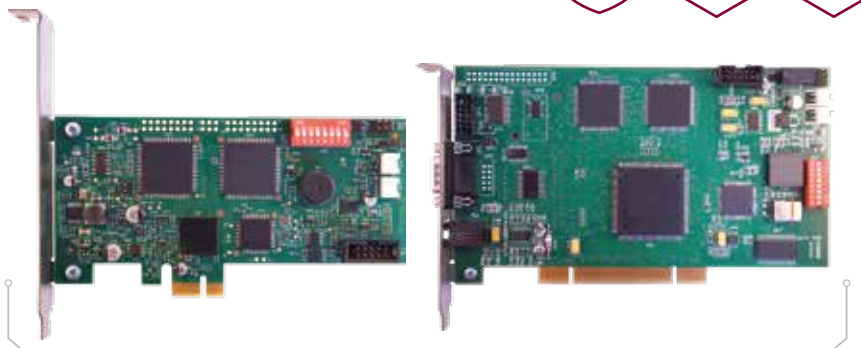
Для обеспечения гарантированной защиты данных модуль «КРИПТОН-ПШД/SATA 3.0» после каждого старта компьютера производит автоматическое перешифрование данных на жестком диске.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ ПРОХОДНЫХ ШИФРАТОРОВ

Устройство	«КРИПТОН-ПШД»			«КРИПТОН-Интеграл»
	«КРИПТОН-ПШД/IDE»	«КРИПТОН-ПШД/SATA»	«КРИПТОН-ПШД/SATA 3.0»	
Интерфейсы жестких дисков	ATA/ATAPI-6	Serial ATA 1.0a	Serial ATA 3.0	USB 2.0 Serial ATA 1.0a
Скорость шифрования	до 10 Мбайт/с	до 30 Мбайт/с	до 120 Мбайт/с	до 30 Мбайт/с
Носитель ключевой информации	устройство памяти Touch Memory DS 1993L-F5 ….DS 1996L-F5, смарт-карты			

«КРИПТОН-8» И «КРИПТОН-10»

Устройства «КРИПТОН-8» и «КРИПТОН-10» представляют собой абонентские шифраторы, выполняющие шифрование и контроль целостности блоков информации по запросам прикладного программного обеспечения.



АБОНЕНТСКИЕ ШИФРАТОРЫ «КРИПТОН-10» И «КРИПТОН-8»

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Шифрование информации

В устройствах реализован алгоритм шифрования ГОСТ 28147-89. Шифрование выполняется непосредственно в устройстве, что исключает возможность несанкционированного вмешательства в процесс шифрования и гарантирует целостность алгоритма.

Защита от НСД к ключевой информации

Загрузка ключей шифрования в «КРИПТОН-8» или «КРИПТОН-10» выполняется напрямую с ключевого носителя, минуя оперативную память и системную шину компьютера, что исключает возможность несанкционированного перехвата ключей или их модификации.

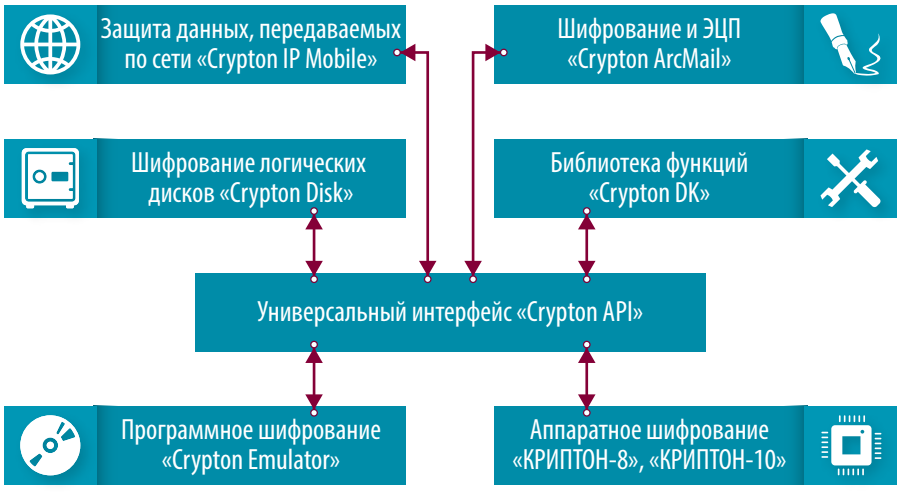
Работа с прикладным ПО

Функциональные возможности устройств «КРИПТОН-8» и «КРИПТОН-10» могут быть использованы через универсальный интерфейс «Crypton API», доступный в виде библиотеки функций «Crypton DK» при разработке собственного ПО.

ПРОГРАММНЫЕ СРЕДСТВА ШИФРОВАНИЯ И ЭЛЕКТРОННОЙ ПОДПИСИ

Программный шифратор «Crypton Emulator» выполняет функции шифрования и расчета имитовставок согласно алгоритму ГОСТ 28147-89, а также функции управления криптографическими ключами.

В арсенале Фирмы «АНКАД» имеются различные программные средства, предназначенные для криптографической защиты информации с использованием функций как программного, так и аппаратного шифратора.



СРД «КРИПТОН-ЩИТ»

СЕРТИФИЦИРОВАНО ФСБ · СЕРТИФИЦИРОВАНО ФСТЭК · WINDOWS

Система разграничения доступа (СРД) «КРИПТОН-ЩИТ» представляет собой программно-аппаратный комплекс средств защиты информации, обеспечивающий защиту от несанкционированного доступа к информации.

«КРИПТОН-ЩИТ» функционирует как на автономных персональных компьютерах, так и на средствах вычислительной техники, объединенных в локальную сеть.

ОСНОВНЫЕ ВОЗМОЖНОСТИ

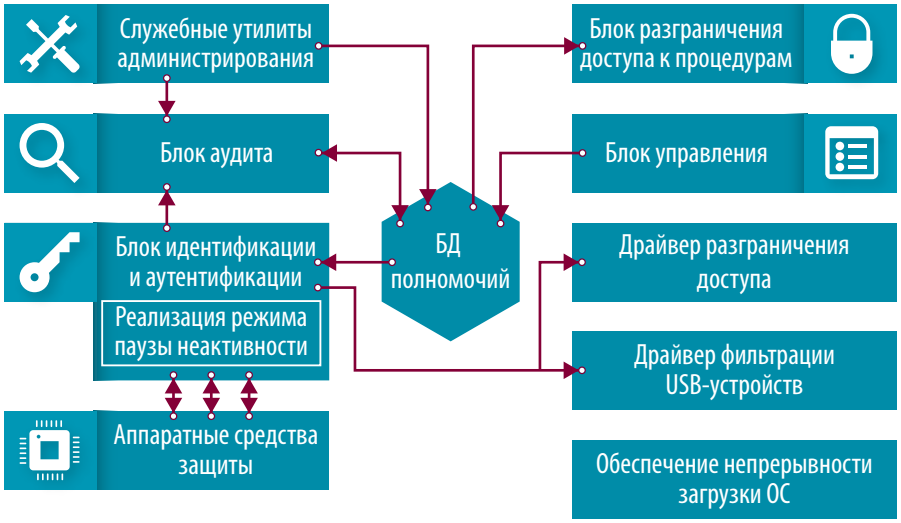
Идентификация и аутентификация пользователей — Реализована единая идентификация и аутентификация для пользователя с формированием профиля прав доступа.

Разграничение доступа к компьютеру — В СРД используются мандатный и дискреционный принципы разграничения доступа к ресурсам ОС компьютера. Разграничение доступа для всех процессов и пользователей производится на уровне ядра ОС.

Разграничение доступа к периферийным устройствам — Выполняется дополнительное разграничение доступа к USB-устройствам, принтерам (с регистрацией печати) и сетевым соединениям, что позволяет надежно защитить данные от утечек через внешние устройства.

Централизованное администрирование — Интегрированная централизованная настройка и описание пользователей, ресурсов и прав доступа пользователей к ресурсам.

АРХИТЕКТУРА СИСТЕМЫ



ТРЕБОВАНИЯ

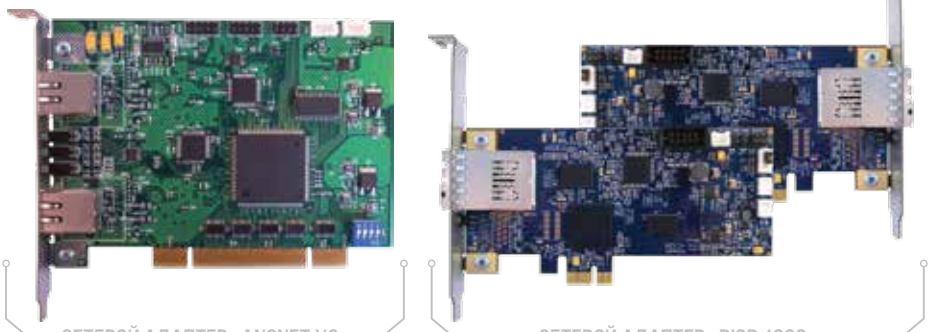
Система «КРИПТОН-ЩИТ» функционирует на уровне микроядра операционной системы Windows, независимо от встроенных в ОС средств контроля доступа.

СРД «КРИПТОН-ЩИТ» работает в одном из вариантов:

- совместно с АПМДЗ «КРИПТОН-ЗАМОК»;
- с использованием электронного ключа «Рутокен».

«ANCNET» И «DIOD»

Сетевые адаптеры «AncNet» предназначены для доверенной передачи данных в компьютерных сетях с возможностью разграничения доступа к ним. Изделия серии «DIOD» позволяют решить задачу гарантированного одностороннего обмена данными между компьютерами.



СЕТЕВОЙ АДАПТЕР «ANCNET X2»

СЕТЕВОЙ АДАПТЕР «DIOD 1000»

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Аппаратное разграничение доступа
Устройство «AncNet» может аппаратно включаться или отключаться (под управлением АПМДЗ «КРИПТОН-ЗАМОК») на ранних стадиях загрузки компьютера, что позволяет осуществлять разграничение доступа пользователя к компьютерным сетям.

Две сетевые карты в одной
Сетевой адаптер «AncNet x2» позволяет управлять доступом к двум компьютерным сетям с использованием одной сетевой карты.

Совместимость
Устройства «AncNet» совместимы со всеми типами активного сетевого оборудования и сетевыми адаптерами зарубежных производителей.

Однонаправленная связь
Сетевой адаптер «DIOD» обеспечивает строго одностороннюю передачу данных. Осуществляет отправку и запись файлов в указанную папку на принимающем компьютере.

Каскадное использование
Устройства «DIOD» можно использовать каскадно для передачи данных из общедоступной сети в сеть с высоким уровнем конфиденциальности.

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Устройство	«AncNet»	«DIOD»
Стандарты передачи данных	IEEE 802.3 (2000 Edition), 802.3u, 802.3x	IEEE 802.3 (2000 Edition), 802.3u, 802.3x
Сетевая среда	10/100BASE-TX, 100BASE-FX, 1000BASE-SX, 1000BASE-TX	100BASE-FX, 1000BASE-SX
Стандарт системной шины	PCI Local BUS Revision 2.1, 2.2 или PCI Express x1	PCI Local BUS Revision 2.1, 2.2 или PCI Express x1

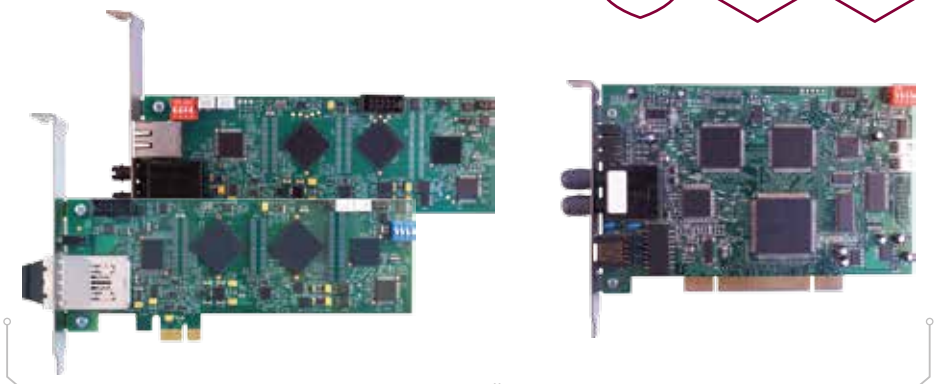
ВАРИАНТЫ ПОСТАВКИ УСТРОЙСТВА «DIOD»

- Комплект плат однонаправленной связи.
- Платы однонаправленной связи совместно с программным обеспечением.
- Готовые программно-аппаратные комплексы однонаправленной связи.

«КРИПТОН ANCNET»

СЕРТИФИЦИРОВАНО ФСБ LINUX WINDOWS

Устройство «КРИПТОН AncNet» представляет собой отечественный сетевой адаптер, предназначенный, в первую очередь, для защиты канала сетей, в которых ведется обработка информации, содержащей сведения, составляющие государственную тайну (до грифа «Совершенно секретно» включительно).



ВАРИАНТЫ ИСПОЛНЕНИЯ УСТРОЙСТВА «КРИПТОН ANCNET»

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Передача данных по сети
«КРИПТОН AncNet» выполняет прием и передачу кадров формата Ethernet II по протоколам семейства IPv4.

Прозрачное шифрование данных
Защита данных путем шифрования содержимого информационных частей IP-пакетов по алгоритму ГОСТ 28147-89 и контроль целостности данных выполняются прозрачным методом, т.е. незаметно для пользователя и операционной системы.

Контроль целостности
Подсчет контрольных сумм объектов гарантирует неизменность передаваемых по сети данных.

Взаимодействие с АПМДЗ «КРИПТОН-ЗАМОК»
Устройство «КРИПТОН AncNet» работает в составе комплекса с изделием АПМДЗ «КРИПТОН-ЗАМОК», который обеспечивает разграничение доступа к компьютерным сетям и загрузку ключей шифрования в устройство со смарт-карт и идентификаторов Touch Memory (iButton).

ОСНОВНЫЕ ХАРАКТЕРИСТИКИ

Устройство	«КРИПТОН AncNet Pro»	«КРИПТОН AncNet Express»	«КРИПТОН AncNet 1000»
Стандарты передачи данных	IEEE 802.3 (2000 Edition), 802.3U, 802.3X	IEEE 802.3 (2000 Edition)	
Сетевая среда	100BASE-FX, 100BASE-TX, 10BASE-T		1000BASE-SX
Стандарт системной шины	PCI Local BUS Revision 2.1, 2.2	PCI Express x1 rev.1.0/1.0a/1.1	
Скорость передачи данных по сети с шифрованием	до 70 Мбит/с	до 70 Мбит/с	до 400 Мбит/с

«CRYPTON IP MOBILE» И «CRYPTON VPN»

СЕРТИФИЦИРОВАНО ФСБ LINUX WINDOWS

СКЗИ «Crypton IP Mobile» предназначен для защиты данных, передаваемых по компьютерным сетям. Главная задача комплекса - создать поверх общедоступных сетей виртуальные частные сети (VPN) с прозрачным шифрованием информации и контролем целостности данных.

ПАК «CRYPTON VPN»

ОСНОВНЫЕ ВОЗМОЖНОСТИ

Организация виртуальных частных сетей — Комплекс позволяет создавать защищенный доступ удаленных сотрудников в корпоративную сеть, а также объединять несколько сетей.

Шифрование трафика — Шифрование информации осуществляется по алгоритму ГОСТ 28147-89 прозрачным методом, т. е. автоматически и незаметно для пользователя.

Фильтрация IP-трафика — Фильтрация враждебного трафика возможна на сетевом и транспортном уровнях. «Crypton IP Mobile» также поддерживает обработку фрагментированных пакетов и трансляцию сетевых адресов (NAT).

Централизованное администрирование — Возможность централизованного управления криптографическими ключами и локальными политиками безопасности.

КОМПОНЕНТЫ ПРОДУКТА

Наименование	Назначение
VPN Server	Защита серверов
VPN Gate	Защита подсетей
VPN Client	Защита отдельных клиентских компьютеров
Local Administrator	Формирование политик безопасности для VPN Server/Gate/Client
Crypton IP Mobile ЦГК	Генерация криптографических ключей

АППАРАТНАЯ РЕАЛИЗАЦИЯ

Программно-аппаратный комплекс «Crypton VPN» - это законченное решение, предназначенное для защиты передаваемой информации в компьютерных сетях, включающее программное обеспечение «Crypton IP Mobile» и выполняющее функции криптографического маршрутизатора с шифрованием трафика в соответствии с ГОСТ 28147-89.

СЧИТЫВАТЕЛИ СМАРТ-КАРТ

«КРИПТОН-ССК» представляет собой доверенный считыватель, предназначенный для построения систем защиты с использованием смарт-карт в качестве носителей ключевой и/или аутентифицирующей информации.

«КРИПТОН-ССК/ДСЧ» является разновидностью доверенного считывателя и отличается наличием встроенного датчика случайных чисел.

Ридеры могут подключаться непосредственно к АПМДЗ по интерфейсу USB или по интерфейсу 1-Wire, который предназначен для подключения iButton. Возможно подключение ридера к компьютеру через порт USB.

В считывателях используются микропроцессорные смарт-карты ISO 7816-3 (протокол T=0) class A, B, на микросхеме К5016ВГ1, имеющей сертификат ФСБ России.

«КРИПТОН-ССК» И СМАРТ-КАРТЫ

USB-УСТРОЙСТВА

«РУТОКЕН S» И «РУТОКЕН S MICRO»

Российское средство аутентификации и защиты информации «Рутокен» разработано совместно компанией «Актив» и Фирмой «АНКАД».

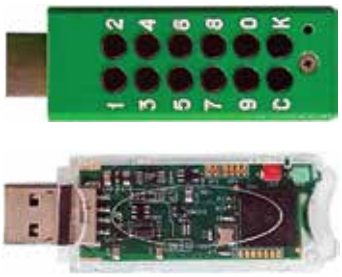
USB-устройство «MikToken», основанное на использовании микросхемы К5016ВГ1, разработано Фирмой «АНКАД» совместно с компанией ОАО «НИИМЭ и Микрон» (сертификат ФСБ).

Во многих отечественных государственных и коммерческих проектах используются USB-ключи в различных форм-факторах, которые предоставляют следующие основные функции:

- защищенное хранение данных;
- генерация и хранение криптографических ключей и аутентифицирующей информации пользователей;
- возможность использования токена в качестве одного из факторов аутентификации;
- криптографическая обработка информации в соответствии с отечественными криптостандартами.

ДОВЕРЕННЫЕ НОСИТЕЛИ ИНФОРМАЦИИ «ОЗОН»

Устройства серии «ОЗОН» подключаются к USB-порту, специальному разъему компьютера или к устройству «КРИПТОН-Интеграл», который обеспечивает шифрование данных. Доверенные носители реализуют различные механизмы защиты хранящейся на них информации.



ДОВЕРЕННЫЕ НОСИТЕЛИ «ОЗОН»

УСТРОЙСТВА TOUCH MEMORY

Традиционно используемые для работы с ключевой информацией идентификаторы Touch Memory (iButton) и различные варианты коннекторов (внешнее и внутреннее подключение, с защитой от высокого напряжения) позволят удовлетворить спрос любого заказчика.

УСТРОЙСТВО TOUCH MEMORY

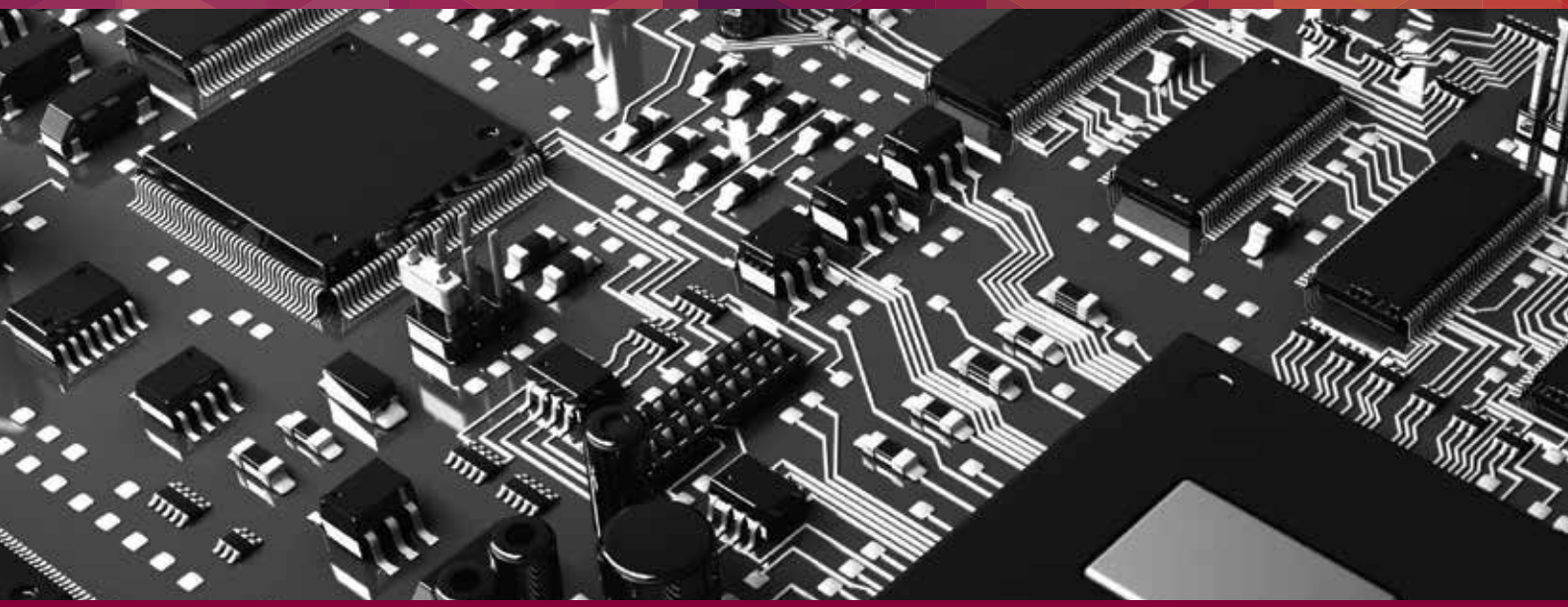
ФИРМА «АНКАД» ДЕЙСТВУЕТ НА ОСНОВАНИИ ЛИЦЕНЗИЙ ФСБ, СВР, ФСТЭК И МО

Орган действия	Дата	Номер	Срок	Вид деятельности
УФСБ	27.06.2011	19687	27.06.2016	Осуществление работ, связанных с использованием сведений, составляющих государственную тайну.
УФСБ	22.04.2015	26174	27.06.2016	Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.
ФСБ	25.07.2011	10959 С	25.07.2016	Осуществление работ, связанных с созданием средств защиты информации, содержащей сведения, составляющие государственную тайну.
ФСБ	25.07.2011	10960 М	25.06.2016	Осуществление мероприятий и (или) оказание услуг в области защиты государственной тайны.
ФСБ	29.06.2012	12310 К	бессрочно	Осуществление разработки и производства средств защиты конфиденциальной информации.
ФСБ	29.06.2012	12311 Н	бессрочно	Осуществление разработки, производства, распространения шифровальных (криптографических) средств, выполнения работ и оказания услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств.
ФСТЭК	14.11.2012	267	14.11.2017	Проведение работ, связанных с созданием средств защиты информации.
ФСТЭК	01.11.2012	1057	бессрочно	Деятельность по разработке и производству средств защиты конфиденциальной информации.
ФСТЭК	01.11.2012	1869	бессрочно	Деятельность по технической защите конфиденциальной информации.
СВР	25.07.2014	993	25.07.2019	Проектирование и изготовление систем и средств, предназначенных для хранения, накопления, передачи, приема, обработки и защиты (кроме защиты от утечки по техническим каналам) в российских загранучреждениях информации, составляющей государственную тайну, или устанавливаемых в помещениях, где такая информация циркулирует.
СВР	25.07.2014	992	25.07.2019	Осуществление работ в российских загранучреждениях, связанных с использованием сведений, составляющих государственную тайну, при монтаже, вводе в эксплуатацию, ремонте и техническом обслуживании средств защиты информации.
МО	20.06.2014	1073	20.06.2019	Деятельность в области создания средств защиты информации.

АККРЕДИТАЦИЯ

ФСБ	24.09.2010	АФ-109	24.09.2015	Исследования функциональных свойств программного обеспечения информационных и телекоммуникационных систем на соответствие требованиям информационной безопасности для информации, не содержащей сведения, составляющие государственную тайну.
Банк России	25.09.2007		бессрочно	Участие в закрытых конкурсах, проводимых Банком России по видам деятельности: «Обеспечение безопасности защиты информации», «Информатизация» и «Образовательные услуги».

ANCUD



ООО Фирма «АНКАД»

124498, г. Москва, г. Зеленоград,

проезд 4806, дом 5, строение 20

Тел.: +7 (499) 731-0000, 732-1313

marketing@ancud.ru

www.ancud.ru

2015