КОД БЕЗОПАСНОСТИ

SECRET NET

Сертифицированное средство защиты информации от несанкционированного доступа к рабочим станциям и серверам

ПРЕИМУЩЕСТВА

- ШИРОКИЕ ВОЗМОЖНОСТИ ДЛЯ КОНТРОЛЯ УТЕЧЕК И КАНАЛОВ РАСПРОСТРАНЕНИЯ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ
- КОРПОРАТИВНАЯ ПОЛИТИКА ИСПОЛЬЗОВАНИЯ РАЗЛИЧНЫХ ТИПОВ ВНЕШНИХ НОСИТЕЛЕЙ
- ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ, ОПЕРАТИВНЫЙ МОНИТОРИНГ И АУДИТ БЕЗОПАСНОСТИ
- ПОДДЕРЖКА ТЕРМИНАЛЬНЫХ РЕШЕНИЙ И VDI-ИНФРАСТРУКТУРЫ
- ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ КЛИЕНТАМИ, ЗАЩИЩЕННЫМИ СЗИ SECRET NET LSP ДЛЯ ОС GNU/LINUX
- МАСШТАБИРУЕМАЯ СИСТЕМА ЗАЩИТЫ – ДЕСЯТКИ ТЫСЯЧ ЗАЩИЩЕННЫХ КОМПЬЮТЕРОВ В ENTERPRISE-ИНФРАСТРУКТУРАХ

ВОЗМОЖНОСТИ

ЗАЩИТА ВХОДА В СИСТЕМУ

- Усиленная аутентификация пользователей по паролю и/или электронному идентификатору. Поддерживаются eToken PRO, eToken PRO (Java), iKey, Rutoken S, Rutoken ЭЦП, Rutoken Lite, JaCarta, ESMART и iButton.
- Предусмотрены дополнительные механизмы защиты при входе доменных пользователей в систему, а также возможность входа по стандартным сертификатам.
- Централизованное управление паролями и электронными идентификаторами доменных пользователей, имеющих доступ к компьютерам с установленным СЗИ Secret Net LSP.

ЦЕНТРАЛИЗОВАННОЕ УПРАВЛЕНИЕ, МОНИТОРИНГ И АУДИТ

- Наличие собственных механизмов централизованного управления политиками и программы управления пользователями позволяет не вносить изменения в службу Active Directory при внедрении СЗИ Secret Net.
- Возможность выбора СУБД для сервера безопасности – Oracle Database или MS SQL Server.
- Оперативный мониторинг в режиме реального времени с возможностью наглядного отображения состояния каждой станции, сервера и группы объектов с учетом критичности события.
- Расширенные возможности по работе с журналами (квитирование событий НСД, поиск, печать, автоматическая архивация) и получению различных отчетов о состоянии системы.
- Возможность подключения к контуру управления Secret Net компьютеров, работающих под управлением ОС Linux и защищенных СЗИ Secret Net LSP.

КОНТРОЛЬ ПЕЧАТИ

- Разграничение доступа к принтерам с возможностью ограничения категорий конфиденциальности документов, выводимых на печать.
- Гибкая настройка маркировки и теневое копирование распечатываемых документов.

КОНТРОЛЬ УТЕЧЕК

- Полномочное управление доступом на основе категорий конфиденциальности ресурсов (файлов, каталогов, устройств, принтеров и сетевых интерфейсов) и прав допуска пользователей.
- Контроль печати и отчуждения конфиденциальной информации.
- Теневое копирование отчуждаемой информации.
- Гарантированное уничтожение данных.

ДОВЕРЕННАЯ ИНФОРМАЦИОННАЯ СРЕДА

- Защита компьютера от несанкционированной загрузки с внешних носителей.
- Замкнутая программная среда с широкими возможностями по настройке.
- Контроль целостности программ и данных.
- Функциональный самоконтроль подсистем Secret Net.

КОНТРОЛЬ УСТРОЙСТВ

- Контроль неизменности аппаратной конфигурации компьютера в процессе работы компьютера.
- Большой список контролируемых внешних устройств (USB, PCMCIA, Secure Digital и любые внешние диски) и широкие возможности по их контролю.
- Централизованные политики использования отчуждаемых носителей в организации. Включая управление механизмом контроля устройств на компьютерах, защищенных СЗИ Secret Net LSP.

ЗАЩИТА ТЕРМИНАЛЬНОЙ И VDI-ИНФРАСТРУКТУРЫ

- Обеспечивается вход по идентификатору и контроль устройств, подключаемых к терминальному серверу с тонких клиентов.
- Контроль подключения устройств к виртуальной машине средствами VDI.

СЦЕНАРИИ ПРИМЕНЕНИЯ

ЗАЩИТА ENTERPRISE-ИНФРАСТРУКТУР

Результат:

- Обеспечен централизованный мониторинг и управление защитой рабочих станций на базе ОС Windows и Linux.
- Сокращены временные и материальные затраты на развертывание и администрирование системы защиты в филиалах.
- Снижены риски несанкционированной активности привилегированных пользователей.
- Сокращено время расследования инцидентов безопасности в региональных офисах.

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ

Результат:

- Информационная система приведена в соответствие требованиям нормативных документов.
- Минимизированы финансовые и временные затраты на реализацию СОИБ в соответствии с требованиями регуляторов.
- Минимизированы финансовые, репутационные и юридические риски, связанные с невыполнением требований регуляторов.

МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ

Результат:

- Минимизированы финансовые потери от инцидентов, связанных с информационной безопасностью.
- Повышена скорость реакции на инцидент и оперативность расследования инцидентов ИБ.

ЗАЩИТА ОТ ВНУТРЕННИХ УГРОЗ

Результат:

- Минимизация финансовых и репутационных рисков, связанных с утечкой конфиденциальной информации.
- Настроены политики безопасности для сотрудников различных служб при работе с конфиденциальной информацией:
  - с финансовыми документами;
  - с базой данных клиентов;
  - с интеллектуальной собственностью организации;
  - с банковской тайной;
  - с персональными данными.

  Сотрудники получают доступ только к своим рабочим данным, нивелирован риск финансовых и репутационных потерь из-за утечек конфиденциальной информации.

СЕРТИФИКАТЫ

ФСТЭК России и Минобороны России.

СВТ 3 / НДВ 2, для защиты АС до класса 1Б включительно (в т.ч. защита гостайны с грифом «совершенно секретно»), ИСПДн до УЗ1 включительно и ГИС до 1 класса включительно.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка Secret Net может осуществляться как напрямую, силами специалистов «Код Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера – партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов – обращается в службу технической поддержки вендора.
Существует несколько пакетов технической поддержки:


Базовый


Стандартный


Расширенный


VIP

КАТАЛОГ УСЛУГ	ПАКЕТ ПОДДЕРЖКИ			
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	VIP
Доступность услуги	8x5, e-mail, телефон		24x7, e-mail, телефон	
Приоритет	Низкий	Средний	Высокий	Первоочередной
Количество обращений	Не ограничено			
Консультирование по установке и использованию продукта	●	●	●	●
Доступ на форум по продукту и к базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Личный кабинет на веб-портале	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Регистрация обращений на веб-портале		●	●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

О КОМПАНИИ «КОД БЕЗОПАСНОСТИ»

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

+7 (495) 982-30-20 (многоканальный) info@securitycode.ru www.securitycode.ru