



КОД БЕЗОПАСНОСТИ

SECRET NET LSP

Сертифицированное средство защиты
от несанкционированного доступа
для ОС семейства GNU/Linux

ПРЕИМУЩЕСТВА



УДОБСТВО АДМИНИСТРИРОВАНИЯ
БЛАГОДАРЯ НАЛИЧИЮ ГРАФИЧЕСКИХ И
КОНСОЛЬНЫХ СРЕДСТВ УПРАВЛЕНИЯ



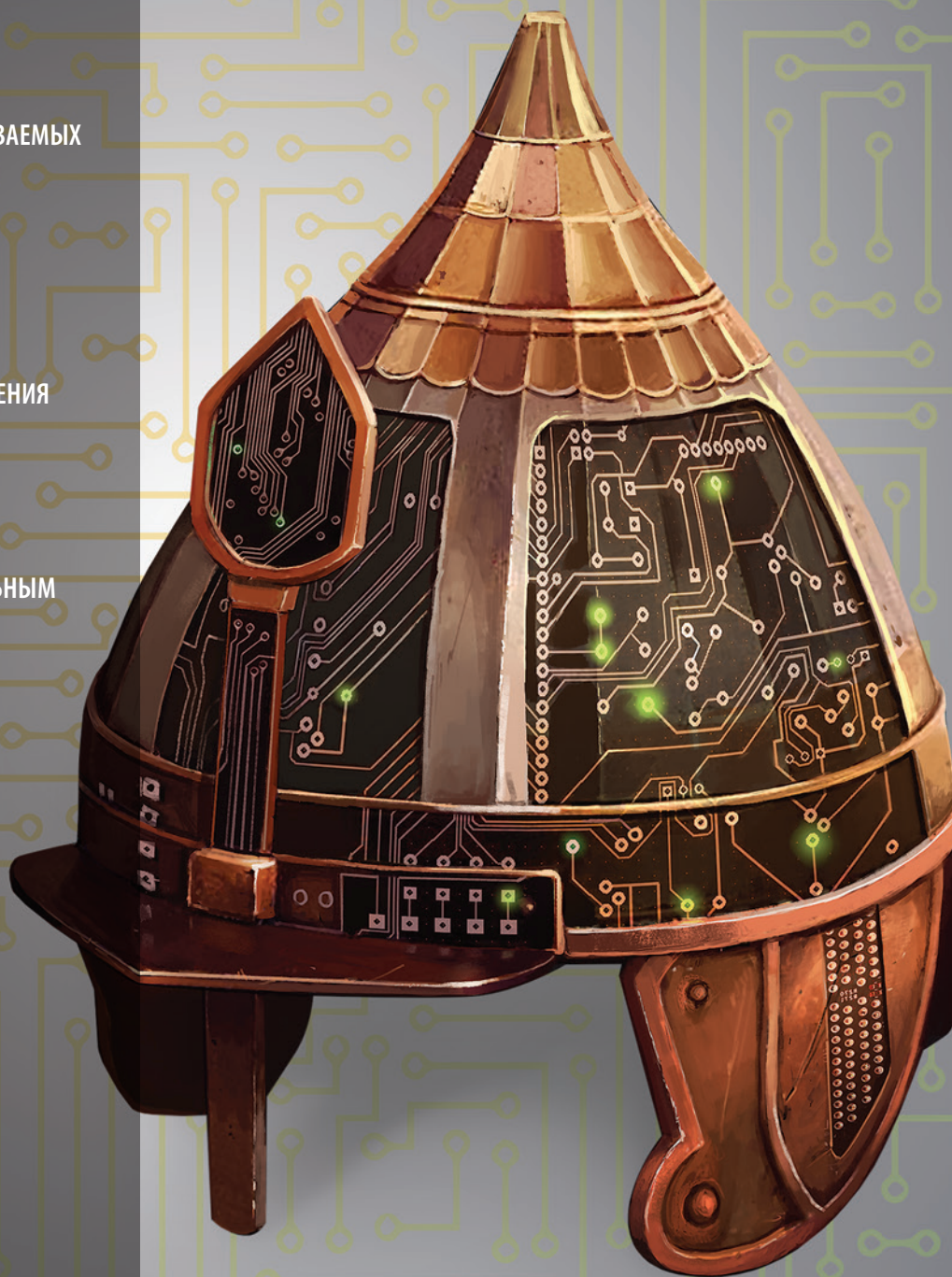
ШИРОКИЙ СПИСОК ПОДДЕРЖИВАЕМЫХ
ДИСТРИБУТИВОВ LINUX



ПОДДЕРЖКА СРЕДСТВ
ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ
SECRET NET STUDIO



СОВМЕСТИМОСТЬ С ТЕРМИНАЛЬНЫМ
СЕРВЕРОМ ПОД УПРАВЛЕНИЕМ
ОС WINDOWS



ВОЗМОЖНОСТИ

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Контроль входа пользователей в систему по логину/паролю или с использованием электронных идентификаторов.

РАЗГРАНИЧЕНИЕ ДОСТУПА К РЕСУРСАМ

Механизм дискреционного разграничения доступа для контроля и управления правами доступа пользователей и групп пользователей к объектам файловой системы – файлам и каталогам.

РАЗГРАНИЧЕНИЕ ДОСТУПА К ВНЕШНИМ УСТРОЙСТВАМ

Разграничение доступа пользователей и групп пользователей к шинам USB, SATA, IEEE 1394 и подключаемым к ним устройствам в целях предотвращения несанкционированной утечки информации с защищаемого компьютера.

КОНТРОЛЬ ЦЕЛОСТНОСТИ

Контроль целостности ключевых компонентов Secret Net LSP и критических объектов файловой системы. Настройка режимов реакции на нарушение целостности объектов.

РЕГИСТРАЦИЯ СОБЫТИЙ ИБ И ГЕНЕРАЦИЯ ОТЧЕТОВ

Фиксация событий безопасности в журнале. Включает события, связанные с доступом пользователей к защищаемым файлам, устройствам и узлам вычислительной сети. Фильтрация событий безопасности, контекстный поиск в журнале безопасности.

АУДИТ ДЕЙСТВИЙ ПОЛЬЗОВАТЕЛЕЙ

Аудит действий субъектов с защищаемыми объектами файловой системы и сетевых соединений, аудит отчуждения информации. Возможность автоматического построения отчетов по результатам аудита.

ЗАТИРАНИЕ ОСТАТОЧНОЙ ИНФОРМАЦИИ

Уничтожение (затирание) содержимого конфиденциальных файлов при их удалении пользователем. Очистка освобождаемых областей оперативной памяти компьютера и запоминающих устройств (жестких дисков, внешних запоминающих устройств).

ИНТЕГРАЦИЯ СО СРЕДСТВАМИ УПРАВЛЕНИЯ SECRET NET STUDIO

СЗИ Secret Net LSP может использоваться совместно со средствами управления СЗИ Secret Net Studio. Контроль подключаемых устройств, управление защитными подсистемами и мониторинг событий НСД через сервер безопасности Secret Net Studio.

РАСШИРЕНИЕ ФУНКЦИОНАЛЬНОСТИ ОС

Обновление общесистемного ПО и расширение функциональности системы без необходимости дожидаться сертификации обновления системных компонентов. Возможность создания различных по функциональности решений на базе дистрибутива Linux и защита этих решений с использованием Secret Net LSP.

ПОДДЕРЖКА ШИРОКОГО СПИСКА ДИСТРИБУТИВОВ ОС GNU/LINUX

Secret Net LSP может устанавливаться на следующие ОС:

- MCBC 5.0;
- Astra Linux Special Edition 1.4/1.5;
- CentOS 6.5/7.1/7.2/7.3 x86/x64;
- Debian 7.6/8.0 x64;
- Red Hat Enterprise Linux 6.5/7.0/7.2/7.3 x86/x64;
- Oracle Linux 7.2/7.3 x86/x64;
- ContinentOS 4.2 x86/x64.

СЦЕНАРИИ ПРИМЕНЕНИЯ

ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ 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.

СООТВЕТСТВИЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ ТРЕБОВАНИЯМ ФСТЭК РОССИИ

Результат:

- Минимизация финансовых и репутационных рисков, связанных с невыполнением требований регуляторов.
- Информационная система приведена в соответствие требованиям нормативных документов.

ЗАЩИТА ГЕТЕРОГЕННЫХ СЕТЕЙ

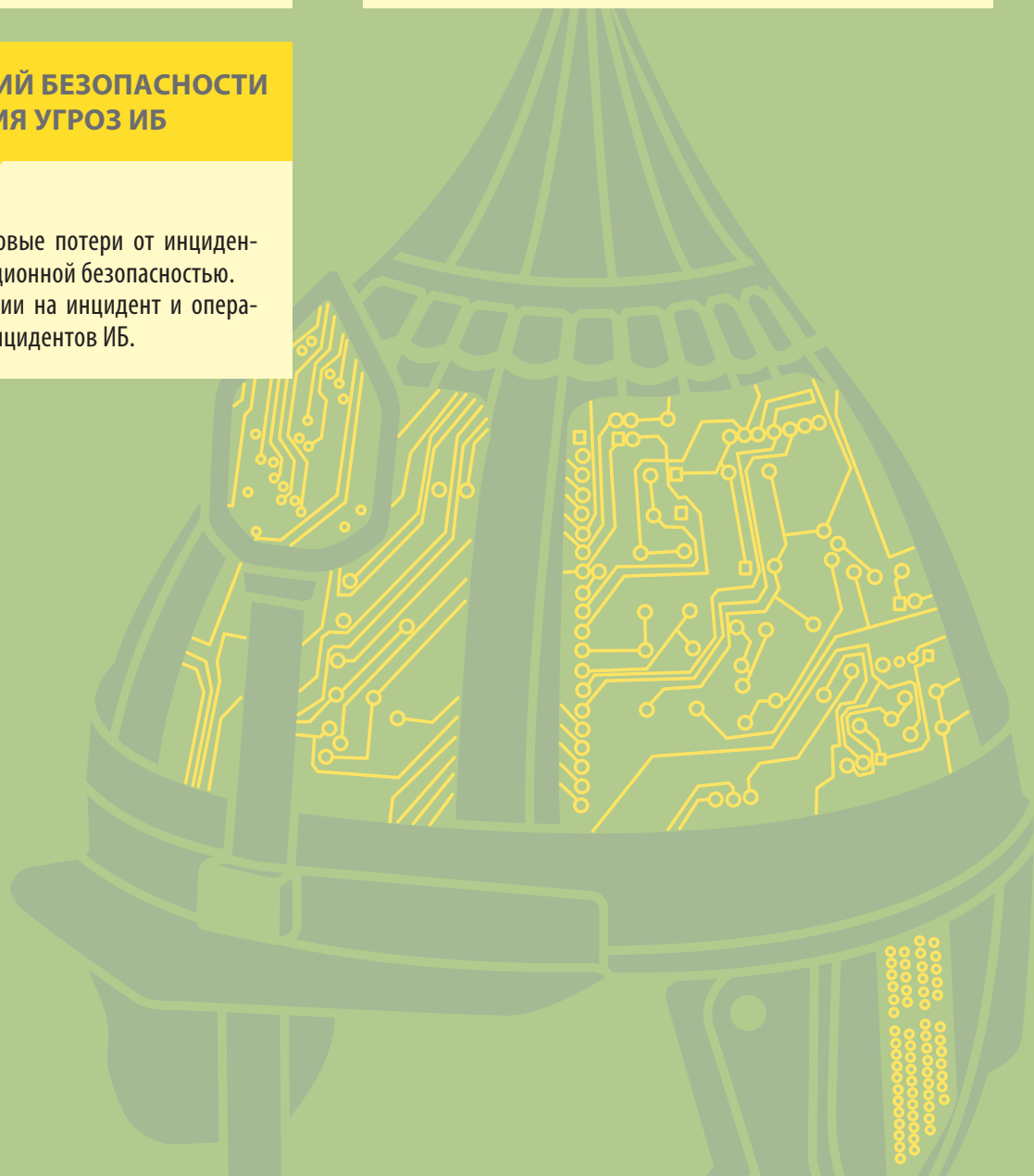
Результат:

- Обеспечен централизованный мониторинг и управление защитой рабочих станций на базе ОС Windows и Linux.

МОНИТОРИНГ СОБЫТИЙ БЕЗОПАСНОСТИ ДЛЯ ВЫЯВЛЕНИЯ УГРОЗ ИБ

Результат:

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



СЕРТИФИКАТЫ



ФСТЭК России

СВТ5/НДВ4, для защиты АС до класса 1Г включительно, ИСПДн до УЗ1 включительно и ГИС до К1 включительно и АСУ ТП до К1 включительно

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка Secret Net LSP 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
Способ обращения в ТП	e-mail	веб-портал, e-mail	телефон, веб-портал, e-mail	
Приоритет	Низкий	Средний	Высокий	Наивысший
Консультирование по установке и использованию продукта	●	●	●	●
Доступ к Базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Работа над инцидентами в режиме 8x5 (рабочие дни МСК 10:00–18:00)	●	●	●	●
Регистрация и контроль обращений на веб-портале		●	●	●
Работа над критичными инцидентами в режиме 24x7			●	●
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 международным и отраслевым стандартам.

+7 (495) 982-30-20 (многоканальный)

info@securitycode.ru

www.securitycode.ru