

# Kaspersky Embedded Systems Security

---

Комплексная защита встраиваемых  
систем и устаревших компьютеров

kaspersky

## Отрасли



Финансовый сектор



Транспорт и туризм (продажа билетов)



Розничная торговля



Ресторанный и гостиничный бизнес



Здравоохранение



Государственный  
и некоммерческий сектор



Развлечения

## Устройства



Банкоматы



Билетные автоматы



Бензоколонки



Кассы



POS-терминалы



Медицинское оборудование



Устаревшие компьютеры



Игровые автоматы

# Векторы атаки на встраиваемые системы



## Атаки на физическом уровне

- Атаки методом «черного ящика»
- Замена панели для ввода ПИН-кода / использование скиммеров
- Скрытые камеры
- Взрывы



## Атаки на уровне сети

- Уязвимости VPN-подключения
- АРТ-атаки
- Удаленная установка



## Атаки на уровне ПО

- Удаленная / локальная установка вредоносного ПО
- Анализаторы памяти (снифферы) / атаки на ОС
- Заражение / изменение связующего ПО



Более половины успешных атак на встраиваемые системы проходят при участии инсайдеров – сотрудников компании или сторонних поставщиков услуг

## Угрозный ландшафт реактивировался

### Факты:

Количество инцидентов снова растет

Производители оборудования – тоже мишени

Прогноз: значительный рост атак

По количеству детектов\*:

Мес то	Зловред
1	HydraPOS
2	Abaddon
3	Prilex
4	Ploutus
5	Backoff
6	RawPOS
7	RatankbaPOS
8	POSBrut
9	MajikPOS
10	ModPipePOS

По уникальным устройствам\*:

Мес то	Зловред
1	Abaddon
2	HydraPOS
3	RawPOS
4	Prilex
5	RatankbaPOS
6	Backoff
7	MajikPOS
8	Plotus
9	ShieldPOS
10	MajikPOS

\* Данные на 08.2023



## Атака через QR

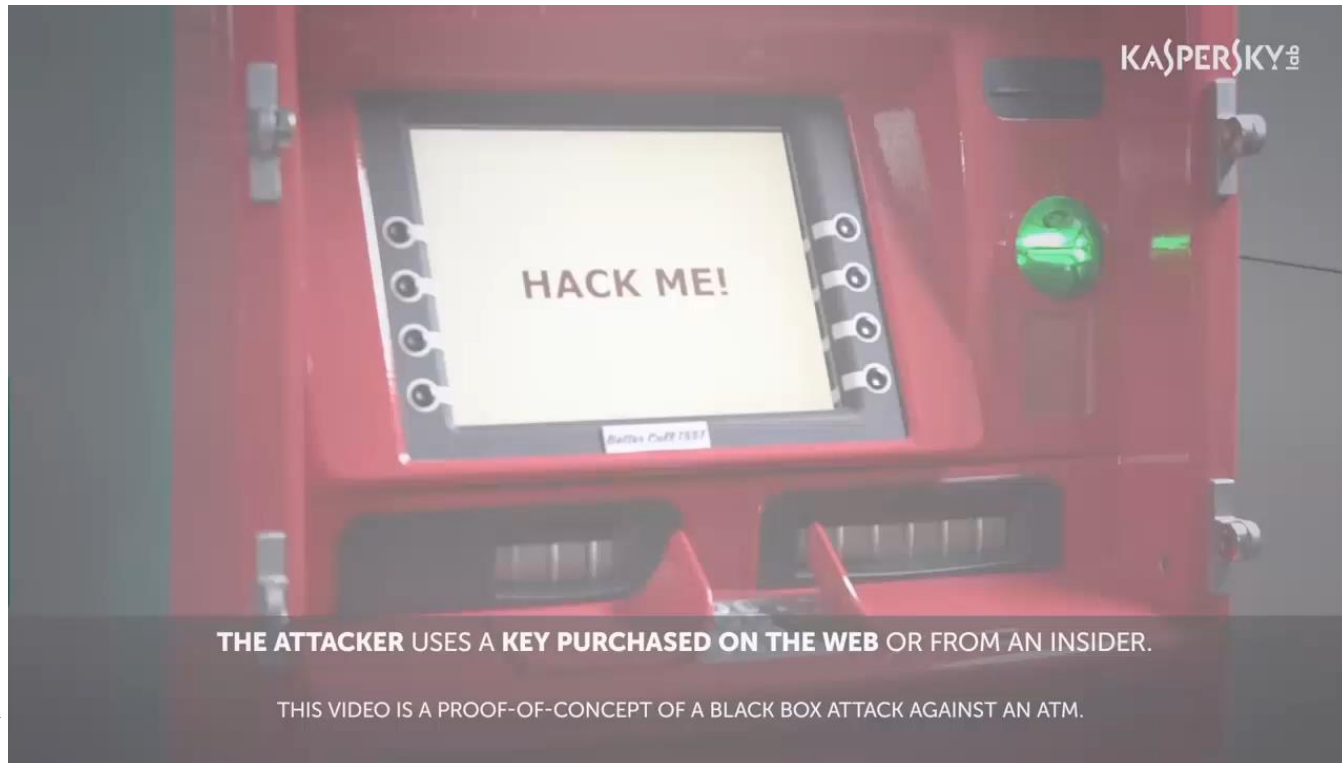
- Специальный QR код переключает сканер в режим эмуляции клавиатуры
- Через цепочку уязвимостей повышает привилегии
- Хакер получает доступ к произвольным файлам системы
- С помощью утилиты тестирования оборудования можно выдать деньги





### Атака с «черным ящиком»

- Открываем банкомат
- Вешаем в разрыв между диспенсером и комп.системой Raspberry Pi (с другой стороны – в USB)
- Анализируем протокол управления диспенсером БЕЗ потери связи с ним
- Просим диспенсер: «Дай денег!» на его «родном языке»
- Профит!





### Случай №1: Защита банкомата решением конкурента

- Не смог заблокировать USB программной (Device Control?)
- Raspberry Pi на USB порт + эмуляция клавиатурного ввода
- Успешный БРУТФОРС пароля защитного решения
- **Защита деактивирована!**



### Случай №2: Защита банкомата решением конкурента + ошибки админа

- Ненужные привилегии аккаунта пользователя
- Незаблокированные сочетания клавиш
- Незаблокированная наэкранный клавиатура
- **Защитное решение отключено!**



### Случай №3: кассовый аппарат крупного RU ретейлера.

- Легкий выход из режима киоска
- Множество незаблокированных функций
- Массивные недостатки в архитектуре спец ПО – plaintext логи с кредитами, и даже данными карт клиентов
- Утилита для открытия ящика с деньгами
- **Заходи кто хочешь, бери что хочешь!**

# Почему традиционная защита не подходит для встраиваемых систем?



## Среда

- Отсутствие постоянных пользователей
- Свободный доступ
- Обслуживание сторонними подрядчиками



## Технические особенности

- Устаревшее ПО
- Слабое аппаратное обеспечение
- Слабый канал связи



## Специфика работы

- Финансовые транзакции
- Обработка персональных данных
- Работа с электронными медицинскими картами



## Программное обеспечение

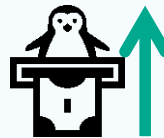
- ОС Windows для встраиваемых систем или основанная на Linux платформа
- Фиксированный набор программ
- Нечастое изменение конфигурации





## Linux растёт!

- Глобальный рынок Linux оценен в **\$5.33 млрд** в 2021, и планирует вырасти до **\$22.15 млрд** до 2029 с CAGR **19.8%**



## Больше встраиваемых систем на Linux

- Крупные компании принадлежащие типичным для использования встроенных систем мигрируют с Windows и **выбирают Linux**



## Хакеры фокусируются на Linux

- Существующие техники и инструменты **адаптируются** против встроенных систем
- Разрабатываются новые техники и инструменты

# Kaspersky Embedded Systems Security

---

Обзор продукта

kaspersky

## Управление и отчетность

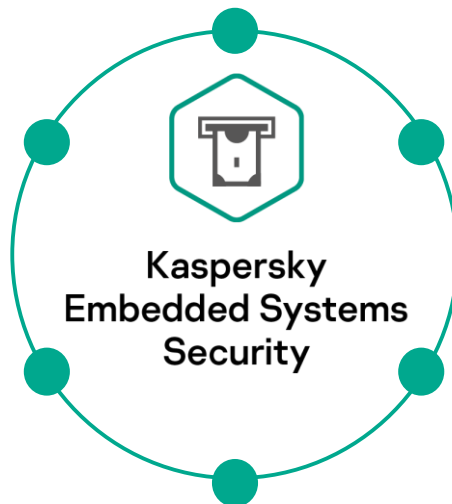
- Централизованное управление, управление через интерфейс командной строки или графический интерфейс
- Доступны локальная или облачная SaaS-консоль
- Интеграция с SIEM-системами, в т. ч. сторонних\* производителей

## Мониторинг целостности системы и контроль соответствия требованиям\*

- Мониторинг целостности файлов
- Мониторинг доступа к реестру\*\*
- Анализ журналов
- Соответствие стандарту PCIDSS

## Инструменты контроля

- Контроль запуска программ
- Контроль распространения ПО
- Контроль устройств



## Защита сети

- Защита от сетевых угроз
- Управление сетевым экраном

## Оптимизированные системные требования

- ОЗУ: от 256 МБ
- ОС: Windows XP и более поздние версии, Linux OS
- Скорость подключения: от 56 кбит/с

## Защита от вредоносного ПО

- Опциональна (можно отключить)
- Проверка - постоянная и по требованию
- Защита от эксплойтов
- Защита от программ-вымогателей

\* Доступно в версии Compliance Edition

\*\* Доступно только в Windows приложении

## Поддержка отечественных дистрибутивов

- ALT
- AlterOS
- Astra
- EMIAS
- Атлант
- GosLinux
- РЕДОС
- ROSA Linux

## Поддержка зарубежных дистрибутивов

- AlmaLinux
- AmazonLinux
- CentOS
- Debian
- Linux Mint
- OpenSuSE
- OracleLinux
- RHEL
- Rocky
- SuSE Enterprise

## Низкие системные требования

- Процессор: Core2Duo 1,86ГГц
- Память: 1Гб (32бит) / 2Гб (64бит)
- Диск: свободное место от 4Гб, раздел обмена (Swap не менее 1Гб)

## Отечественное решение

- Включен в состав Российского ПО
- Запланирована сертификация ФСТЭК

## Богатый набор технологий

- Антивирус
- Поведенческий анализ
- Контроль приложений
- Контроль периферии
- Защита от сетевых атак
- Мониторинг изменений в системе
- Управление брандмауэром
- Интеграция с SIEM
- Облачная защита
- Централизованное управление вместе с другими решениями «Лаборатории Касперского»

## Linux vs. Windows: различия в функциональности

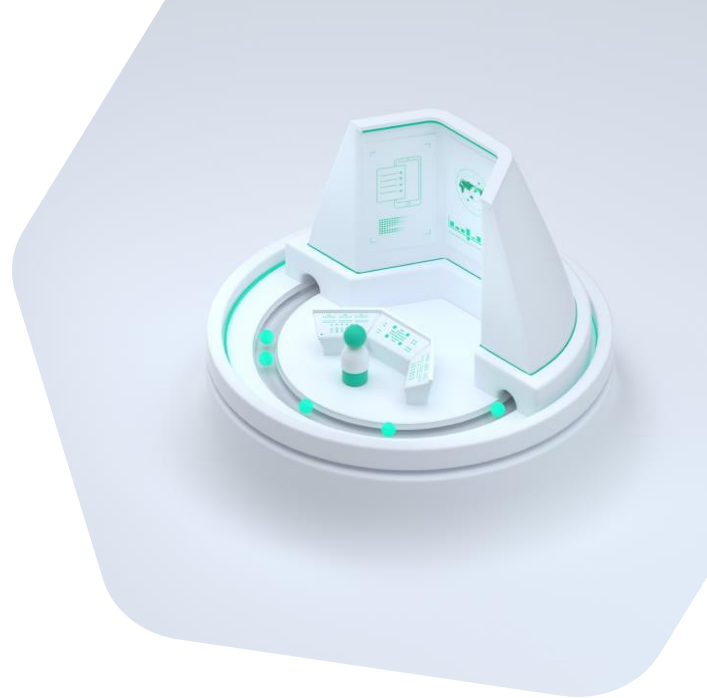
Функция	KESS для Windows	KESS для Linux
Антивирус	✓	✓
Облачная защита	✓	✓
Защита от эксплойтов	✓	✗
Сетевая защита	✓	✓
Контроль запуска приложений	✓	✓
Контроль устройств	✓	✓
Инвентаризация устройств	✓	✓
Планировщик задач инвентаризации	✓	✓
Поддержка доверенных устройств	✓	✓
Автосканирование USB при подключении устройств	✓	✓

Функция	KESS для Windows	KESS для Linux
Анализ логов	✓	✗
Управление файрволлом	✓	✓
Режим Default Deny	✓	✓
Поддержка исключений и доверенных приложений	✓	✓
Контроль целостности защиты	✓	✓
Мониторинг изменений файлов и папок	✓	✓
Мониторинг изменений реестра Windows	✓	N/A
Централизованное управление	✓	✓
Ролевая модель управления	✓	✓
Интеграция с SIEM	✓	✓

# Ключевые преимущества перед основными конкурентами

## **Отечественные конкуренты: наши сильные стороны**

- Собственная защита мирового уровня от вредоносного ПО
- Возможность выбора компонентов решения для установки в зависимости от сценариев защиты и доступных системных ресурсов
- Мониторинг изменений в системе и анализ логов
- Поддержка Windows и Linux в одном продукте
- Поддержка доверенных подключаемых устройств и автоматическое сканирование USB устройств при подключении
- Инвентаризация используемых программ и устройств
- Контроль запуска программ и поддержка сценария «запрет по умолчанию»



# Ключевые преимущества перед основными конкурентами

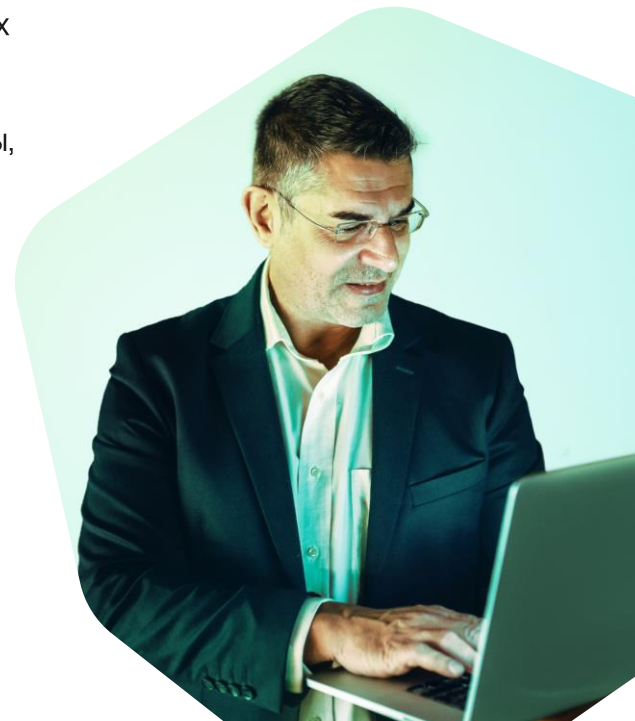
## **Зарубежные конкуренты: наши преимущества**

- Отечественное решение
- Одни из самых низких системных требований (особенно для Windows)
- Поддержка Windows XP
- Поддержка опциональных уровней защиты
- Поддержка Windows и Linux в одном продукте
- Поддержка доверенных подключаемых устройств и автоматическое сканирование USB устройств при подключении
- Не только блокировка устройства, но и защита от вредоносного ПО мирового уровня



## Kaspersky Security для бизнеса или Kaspersky Embedded Systems Security?

- Обычные EPP-решения, в том числе приложения Kaspersky Endpoint Security, работают только на небольшой части встраиваемых систем, произведенных за последнее время.
- Мы не тестировали приложения Kaspersky Endpoint Security на встраиваемых системах и не можем гарантировать их правильную работу.
- Для контроля соответствия требованиям нужны специальные уровни защиты, которые зачастую используются только на серверах и встроенных системах и недоступны в стандартных EPP-решениях.
- Kaspersky Embedded Systems Security – это специализированное решение, в котором используются тщательно отобранные, протестированные и улучшенные уровни защиты, совместимые с большинством встраиваемых систем и сценариев. Для таких устройств мы рекомендуем использовать Kaspersky Embedded Systems Security, а не Kaspersky Security для бизнеса.





# Демо



kaspersky

---

October 2021

# KSC: Добавляем нужные установочные пакеты

18

⚠️ Создайте автономный установочный пакет и загрузите его. Установите Агент администрирования на выбранное устройство, чтобы подключить его к Серверу администрирования. Для автоматического перемещения устройств в группу администрирования выберите соответствующий параметр при создании автономного установочного пакета.

[Просмотреть список установочных пакетов](#) ✕

Обнаружение устройств и развертывание / Развертывание и назначение / Установочные пакеты

Загружено

В процессе (1)

+ Добавить

✕ Удалить

↻ Обновить

+ Развернуть

🔍 Просмотреть список автономных пакетов

🔍 Поиск...

⚙️ 🔍

<input type="checkbox"/>	Имя	Источник	Программа	Версия	Язык
<input type="checkbox"/>	Kaspersky Network Agent for Windows (English)_1...	>> АО "Лаборатория Касперского"	Kaspersky Network Agent fo... >>	13.2.2.1263	en
<input type="checkbox"/>	Kaspersky Endpoint Security for Windows (11.8.0) ... >>	АО "Лаборатория Касперского"	Kaspersky Endpoint Securit... >>	11.8.0.384	en
<input type="checkbox"/>	Kaspersky Endpoint Security for Windows (11.9.0) ... >>	АО "Лаборатория Касперского"	Kaspersky Endpoint Securit... >>	11.9.0.351	en
<input type="checkbox"/>	Kaspersky Endpoint Security 11.2.0 for Linux (Engli... >>	АО "Лаборатория Касперского"	Kaspersky Endpoint Securit... >>	11.2.0.4528	
<input type="checkbox"/>	Kaspersky Network Agent for Linux x32 deb (Englis... >>	АО "Лаборатория Касперского"	Kaspersky Network Agent fo... >>	13.2.2.1263	
<input type="checkbox"/>	Kaspersky Endpoint Security 11.2.0 для Linux (Рус... >>	АО "Лаборатория Касперского"	Kaspersky Endpoint Securit... >>	11.2.0.4528	

< Назад 1 Далее >

20 ▾

Результат: 1-6 / 6 всего



Kaspersky  
Security Center  
Cloud Console

Операции >

Обнаружение устройств и ... ▾

Нераспределенные устройства

Обнаружение устройств >

Развертывание и назн... ▾

Правила перемещения

Мастер развертывания за...

Мастер первоначальной на...

Настройка работы в облач...

**Установочные пакеты**

Выборки устройств

Marketplace

Параметры

evgeniya.kirikova@kaspersky... >

# KSC: Добавляем нужные установочные пакеты

10

Текущие версии программ

Группировать по: Операционная система (изменить группировку используя фильтр)

Администрирование	Дистрибутив	Kaspersky Network Agent for Linux x64 rpm (Français (France))	14.2.0.35148	Да	Linux
Администрирование	Дистрибутив	Kaspersky Network Agent for Linux x64 rpm (Italiano)	14.2.0.35148	Да	Linux
Администрирование	Дистрибутив	Kaspersky Network Agent for Linux x64 rpm (Português (Brasil))	14.2.0.35148	Да	Linux
Администрирование	Дистрибутив	Kaspersky Network Agent for Linux x64 rpm (Русский)	14.2.0.35148	Да	Linux
Администрирование	Дистрибутив	Kaspersky Network Agent for Linux x64 rpm (日本語)	14.2.0.35148	Да	Linux
Банкоматы и POS-системы	Дистрибутив	Kaspersky Embedded Systems Security 3.3 for Linux (English)	3.3.0.67	Да	Linux
Банкоматы и POS-системы	Дистрибутив	Kaspersky Embedded Systems Security 3.3 for Linux (Русский)	3.3.0.67	Да	Linux
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security 11.4.0 for Linux (English)	11.4.0.1096	Да	Linux
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security 11.4.0 for Linux (Français (France))	11.4.0.1096	Да	Linux
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security 11.4.0 for Linux (日本語)	11.4.0.1096	Да	Linux
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security 11.4.0 for Linux (简体中文)	11.4.0.1096	Да	Linux
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security 11.4.0 für Linux (Deutsch)	11.4.0.1096	Да	Linux
Рабочие станции	Дистрибутив	Kaspersky Endpoint Security 11.4.0 для Linux (Русский)	11.4.0.1096	Да	Linux

## Kaspersky Embedded Systems Security 3.3 for Linux (Русский)

Область защиты	Банкоматы и POS-системы
Тип	Дистрибутив
Используется в управляемой сети	Нет
Версия	3.3.0.67
Добавлен	19.07.2023 16:23:40
Операционная система	Linux
Язык	ru

Загрузить и создать установочный пакет

# KSC: Добавляем нужные установочные пакеты



Создайте автономный установочный пакет и загрузите его. Установите Агент администрирования на выбранное устройство, чтобы подключить его к Серверу администрирования. Для автоматического перемещения устройств в группу администрирования выберите соответствующий параметр при создании автономного установочного пакета.

[Просмотреть список установочных пакетов](#)

## Обнаружение устройств и развертывание / Развертывание и назначение / Установочные пакеты

Загружено

В процессе (1)

[+](#) [Добавить](#) [×](#) [Удалить](#) [↻](#) [Обновить](#) [+](#) [Развернуть](#) [🔍](#) [Просмотреть список автономных пакетов](#)



<input type="checkbox"/>	Имя	Источник	Программа	Версия
<input type="checkbox"/>	Kaspersky Network Agent for Windows (English)_13.2.2.1263	АО "Лаборатория Касперского"	Kaspersky Network Agent for Windows (English)	13.2.2.1263
<input type="checkbox"/>	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Lite encryptio... >>	АО "Лаборатория Касперского"	Kaspersky Endpoint Security for Windows (11.8.0) (E... >>	11.8.0.384
<input type="checkbox"/>	Kaspersky Endpoint Security for Windows (11.9.0) (English) (Lite encryptio... >>	АО "Лаборатория Касперского"	Kaspersky Endpoint Security for Windows (11.9.0) (E... >>	11.9.0.351
<input type="checkbox"/>	Kaspersky Endpoint Security 11.2.0 for Linux (English)_11.2.0.4528	АО "Лаборатория Касперского"	Kaspersky Endpoint Security 11.2.0 for Linux (English)	11.2.0.4528
<input type="checkbox"/>	Kaspersky Network Agent for Linux x32 deb (English)_13.2.2.1263	АО "Лаборатория Касперского"	Kaspersky Network Agent for Linux x32 deb (English)	13.2.2.1263
<input type="checkbox"/>	Kaspersky Endpoint Security 11.2.0 для Linux (Русский)_11.2.0.4528	АО "Лаборатория Касперского"	Kaspersky Endpoint Security 11.2.0 для Linux (Русский)	11.2.0.4528
<input type="checkbox"/>	Kaspersky Embedded Systems Security 3.3 for Linux (Русский)_3.3.0.67	АО "Лаборатория Касперского"	Kaspersky Embedded Systems Security 3.3 for Linux ... >>	3.3.0.67

[←](#) [Назад](#) 1 [Далее](#) [→](#)

20

Результат: 1-7 / 7 всего



Kaspersky  
Security Center  
Cloud Console

Операции >

Обнаружение устройств и ... >

Нераспределенные устройства

Обнаружение устройств >

Развертывание и назн... >

Правила перемещения

Мастер развертывания за...

Мастер первоначальной на...

Настройка работы в облач...

**Установочные пакеты**

Выборки устройств

Marketplace

Параметры

evgeniya.kirikova@kaspersky... >

## Мастер развертывания защиты

Удаленная установка с помощью Kaspersky Security Center

+ Добавить    ✎ Изменить

### Инсталляционные пакеты

- Kaspersky Network Agent for Windows (English)\_13.2.2.1263
- Kaspersky Endpoint Security for Windows (11.8.0) (English) (Lite encryption)\_11.8.0.384
- Kaspersky Endpoint Security for Windows (11.9.0) (English) (Lite encryption)\_11.9.0.351
- Kaspersky Endpoint Security 11.2.0 for Linux (English)\_11.2.0.4528
- Kaspersky Network Agent for Linux x32 deb (English)\_13.2.2.1263
- Kaspersky Endpoint Security 11.2.0 для Linux (Русский)\_11.2.0.4528
- Kaspersky Embedded Systems Security 3.3 for Linux (Русский)\_3.3.0.67

Программа: Kaspersky Embedded Systems Security 3.3 for Linux (Русский)

Версия: 3.3.0.67

Вместе с программой будет установлен Агент администрирования, обеспечивающий связь между программой и Kaspersky Security Center 14.2.

Далее

# KSC: Создаем задачу развертывания

Мастер добавления задачи

## Новая задача

Программа

Kaspersky Security Center 14.2

- Kaspersky Security Center 14.2
- Kaspersky Embedded Systems Security
- Kaspersky Embedded Systems Security 3.3 для Linux**
- Kaspersky Endpoint Agent
- Kaspersky Endpoint Security 11 для Linux
- Kaspersky Endpoint Security 11.0.1 для Mac
- Kaspersky Endpoint Security 11.2.0 для Linux
- Kaspersky Endpoint Security 11.3.0 для Linux
- Kaspersky Endpoint Security 11.4.0 для Linux
- Kaspersky Endpoint Security для Mac (11.1)
- Kaspersky Endpoint Security для Mac (11.2)
- Kaspersky Endpoint Security для Mac (11.2.1)
- Kaspersky Endpoint Security для Mac (11.3)
- Kaspersky Endpoint Security для Windows (12.2.0)
- Kaspersky Security for Mobile (Policies)
- Kaspersky Security for Windows Server

Далее

## Мастер добавления задачи

### Новая задача

Программа

Kaspersky Embedded Systems Security 3.3 для Linux

Тип задачи

Добавление ключа

Добавление ключа

Инвентаризация

Обновление

Откат обновления баз

Поиск вредоносного ПО

Проверка важных областей

Проверка контейнеров

Проверка целостности системы

Назначить задачу выборке устройств

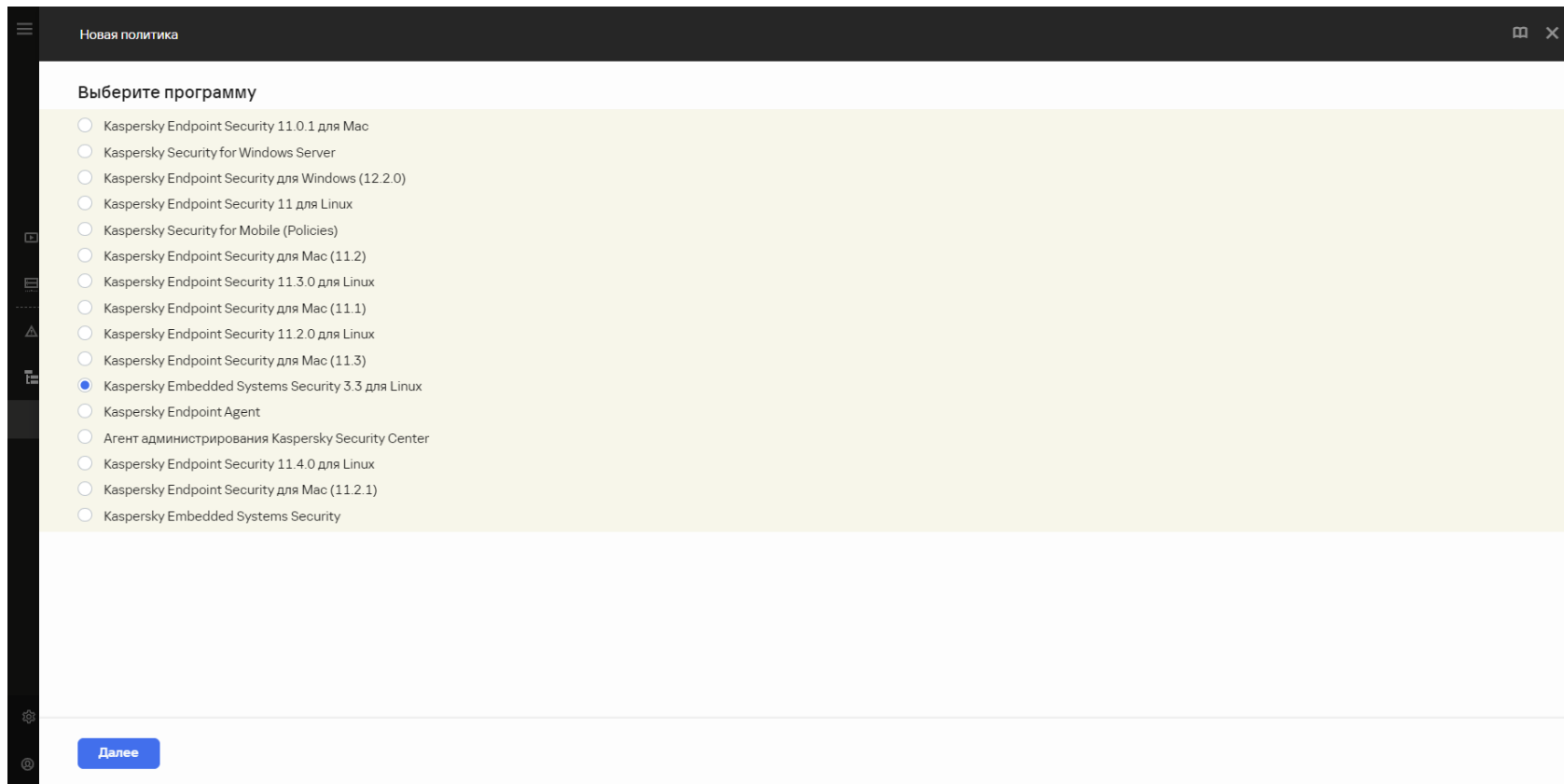
Далее

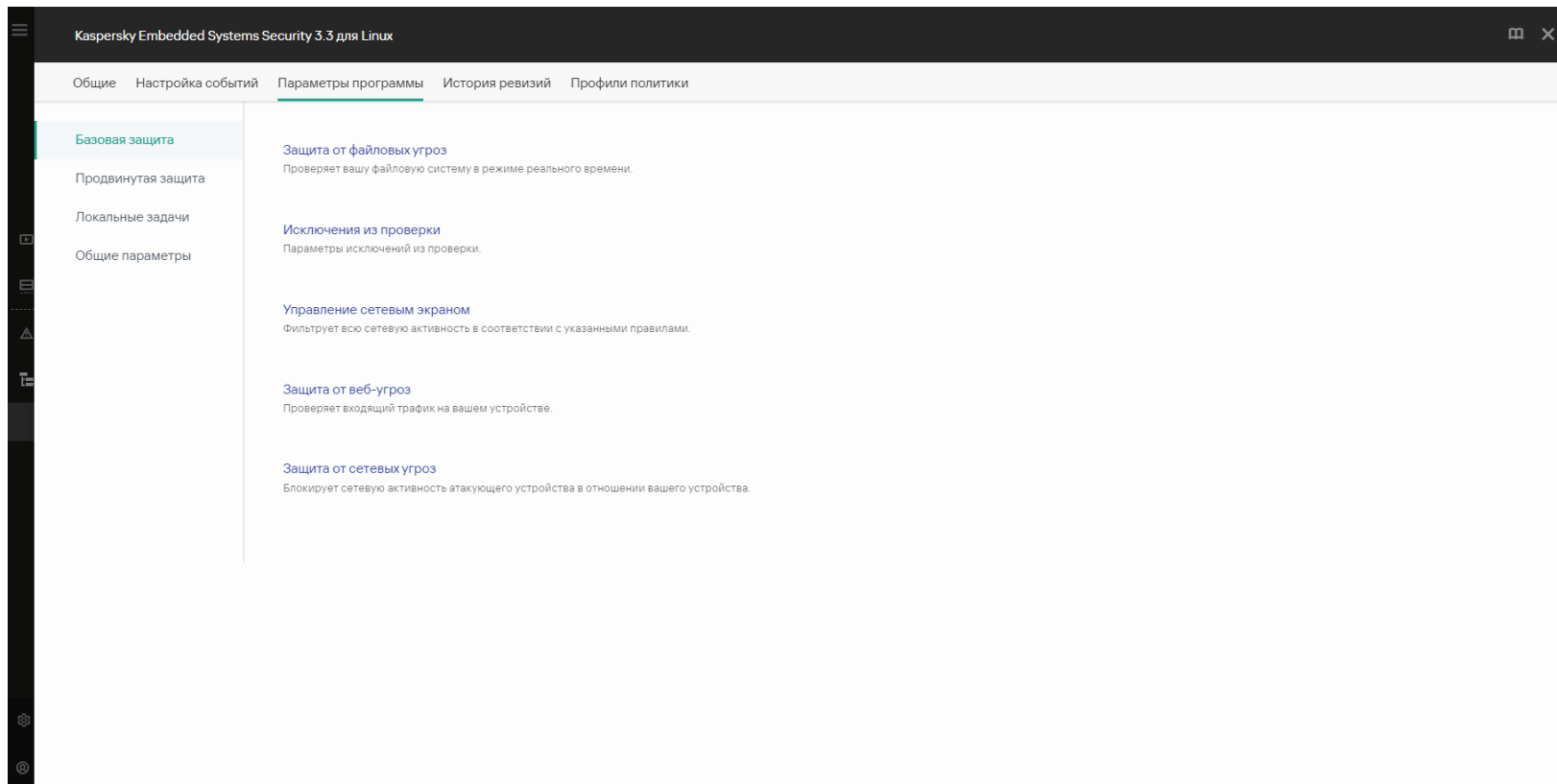
The screenshot displays the Kaspersky Security Center Cloud Console interface. The left sidebar contains navigation options: Введение и учебники, Сервер администрирования, Мониторинг и отчеты, Устройства, Политики и профили политик (selected), Задачи, Управляемые устройства, Мобильные, Правила перемещения, Выборки устройств, Теги, Параметры, and user information (evgeniya.kirikova@kaspersky...).

The main content area is titled "Устройства / Политики и профили политик" and shows the current path: "Сервер администрирования". Below this is a toolbar with actions: + Добавить, Обновить, Показать в группе, Копировать, Переместить, Удалить, and a search bar. A table lists various security policies:

<input type="checkbox"/>	Стат... >>	Политика	Программа	Унаследована	Группа	Роли
<input type="checkbox"/>		Kaspersky Embedded Systems Security				
<input type="checkbox"/>	✓	<a href="#">Kaspersky Embedded Systems Security</a>	<a href="#">Kaspersky Embedded Syste... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>	✓	<a href="#">Kaspersky Embedded Systems Security (1)</a>	<a href="#">Kaspersky Embedded Syste... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>	✓	<a href="#">Kaspersky Embedded Systems Security (2)</a>	<a href="#">Kaspersky Embedded Syste... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>	✓	<a href="#">Kaspersky Embedded Systems Security (3)</a>	<a href="#">Kaspersky Embedded Syste... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>		Kaspersky Endpoint Security 11.2.0 для Linux				
<input type="checkbox"/>	✓	<a href="#">Kaspersky Endpoint Security 11.2.0 for Linux</a>	<a href="#">Kaspersky Endpoint Securit... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>		Kaspersky Endpoint Security 11.3.0 для Linux				
<input type="checkbox"/>	✓	<a href="#">Kaspersky Endpoint Security 11.3.0 for Linux</a>	<a href="#">Kaspersky Endpoint Securit... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>		Kaspersky Endpoint Security 11.4.0 для Linux				
<input type="checkbox"/>	✓	<a href="#">Kaspersky Endpoint Security 11.4.0 for Linux</a>	<a href="#">Kaspersky Endpoint Securit... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>		Kaspersky Endpoint Security для Mac (11.2.1)				
<input type="checkbox"/>	✓	<a href="#">Kaspersky Endpoint Security для Mac (11.2.1)</a>	<a href="#">Kaspersky Endpoint Securit... &gt;&gt;</a>		Managed devices	
<input type="checkbox"/>		Kaspersky Endpoint Security для Mac (11.2)				
<input type="checkbox"/>	✓	<a href="#">Kaspersky Endpoint Security for Mac (11.2)</a>	<a href="#">Kaspersky Endpoint Securit... &gt;&gt;</a>		Managed devices	







# KESS для Linux: политики – продвинутая защита

The screenshot displays the configuration window for Kaspersky Embedded Systems Security 3.3 for Linux. The window title is "Kaspersky Embedded Systems Security 3.3 для Linux". The main menu includes "Общие", "Настройка событий", "Параметры программы", "История ревизий", and "Профили политики". The left sidebar lists "Базовая защита", "Продвинутая защита" (highlighted), "Локальные задачи", and "Общие параметры". The main content area shows the following settings:

- Kaspersky Security Network**  
Предоставляет доступ к облачной базе знаний "Лаборатории Касперского" о репутации файлов, интернет-ресурсов и программного обеспечения.
- Защита от шифрования**  
Защищает файлы в локальных директориях с сетевым доступом по протоколам SMB / NFS от удаленного вредоносного шифрования.
- Контроль целостности системы**  
Проверяет изменения файлов в указанных директориях.
- Контроль приложений**  
Отслеживает попытки запуска приложений пользователями и контролирует запуск приложений с помощью правил.
- Контроль устройств**  
Запрещает доступ к устройствам, которые установлены на клиентском устройстве или подключены к нему. Это позволяет защитить клиентское устройство от заражения при подключении внешних устройств и предотвратить потерю или утечку данных.
- Анализ поведения**  
Получает данные об активности приложений в операционной системе и служит для поиска угроз, которые могут отсутствовать в базах приложения.

# Остались вопросы?



Страница продукта:  
[www.kaspersky.ru/enterprise-security/embedded-systems](http://www.kaspersky.ru/enterprise-security/embedded-systems)

kaspersky