Kaspersky Embedded Systems Security

Комплексная защита встраиваемых систем и устаревших компьютеров

kaspersky

Встраиваемые системы: отрасли и устройства

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

Windows 11 | Windows 10 IoT | Windows Embedded 8 | Windows Embedded POSReady 2009 | Windows Embedded POSReady 7 | Windows XP Embedded | Linux

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
- APT-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*:

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

По уникальным устройствам*:

Место	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

Примеры из реальной жизни

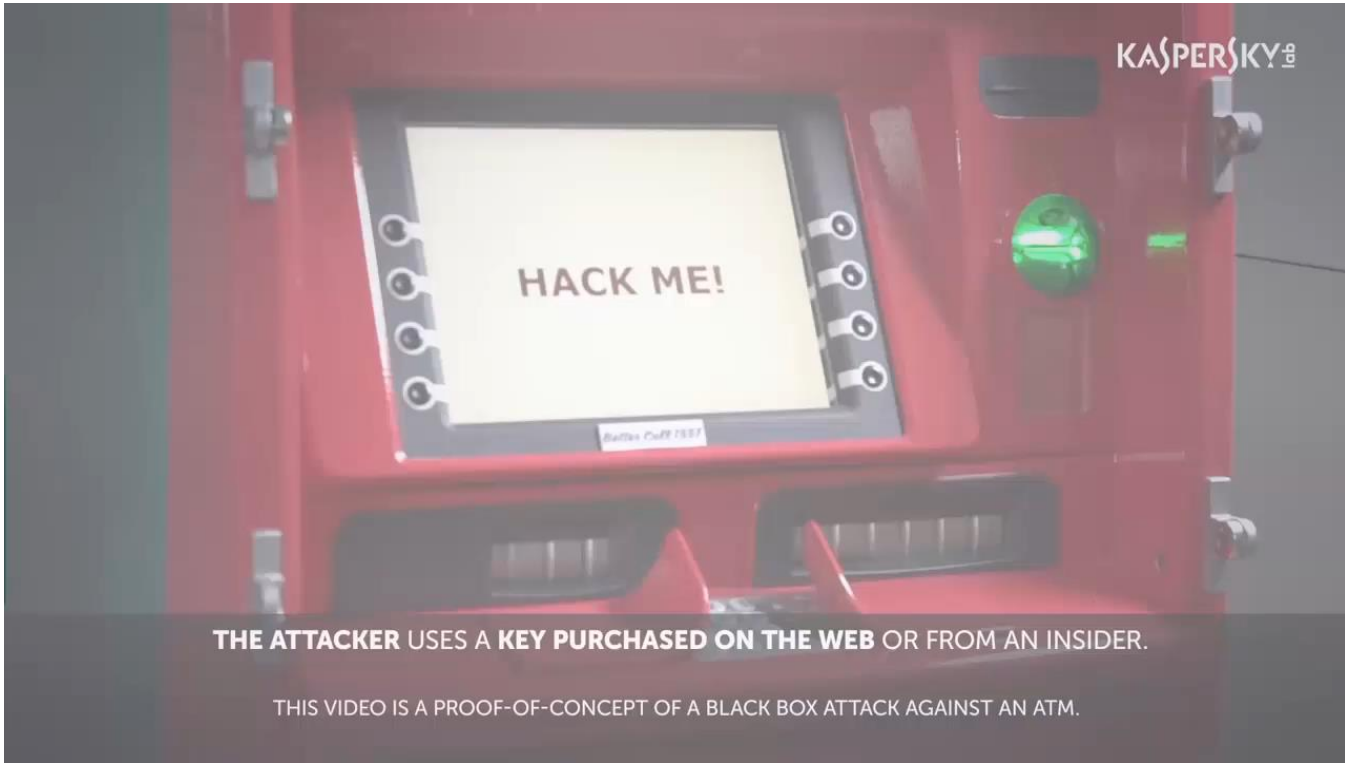
Атака через QR

- 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

Примеры из реальной жизни - 2

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!



Примеры из реальной жизни - 3

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 на экранная 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 кредами, 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

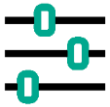
- Отсутствие постоянных пользователей
- Свободный доступ
- Обслуживание сторонними подрядчиками

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

What about Linux?

Linux растет!

- 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

Комплексная защита встраиваемых систем

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 PCI DSS

Оптимизированные системные требования

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

Инструменты контроля

- Контроль запуска программ
- Контроль распространения ПО
- Контроль устройств

Защита от вредоносного ПО

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

Защита сети

- Защита от сетевых угроз
- Управление сетевым экраном

* Доступно в версии Compliance Edition

** Доступно только в Windows приложении

Kaspersky Embedded Systems Security для Linux: новое приложение в составе продукта

Поддержка отечественных дистрибутивов

- ALT
- AlterOS
- Astra
- EMIAS
- Атлант
- GosLinux
- РЕД ОС
- ROSA Linux

Поддержка зарубежных дистрибутивов

- AlmaLinux
- Amazon Linux
- CentOS
- Debian
- Linux Mint
- OpenSuSE
- Oracle Linux
- 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

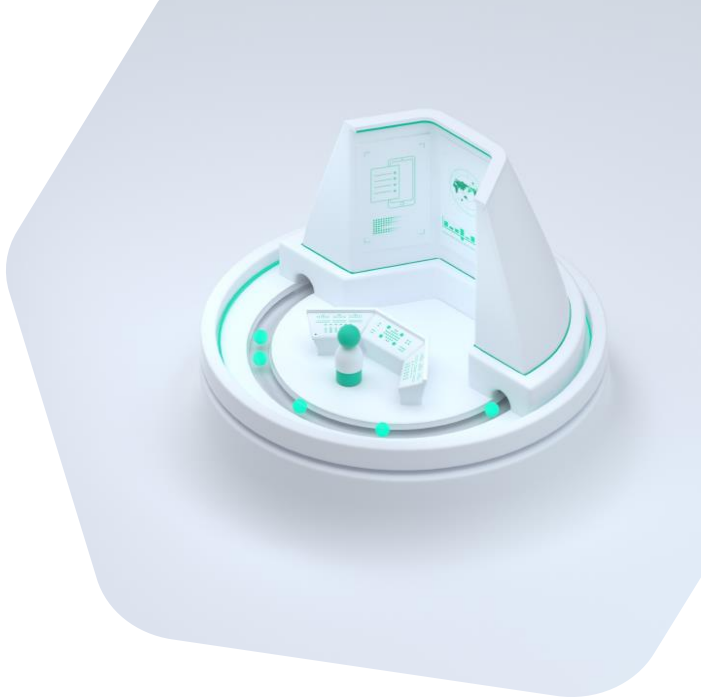
- Антивирус
- Поведенческий анализ
- Контроль приложений
- Контроль периферии
- Защита от сетевых атак
- Мониторинг изменений в системе
- Управление брандмауэром
- Интеграция с SIEM
- Облачная защита
- Централизованное управление вместе с другими решениями «Лаборатории Касперского»

Linux vs. Windows: различия в функциональности

Функция	KESS для Windows	KESS для Linux
Антивирус	√	√
Облачная защита	√	√
Защита от эксплойтов	√	x
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	√	x
Управление файерволлом	√	√
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 сильныестороны

- 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?

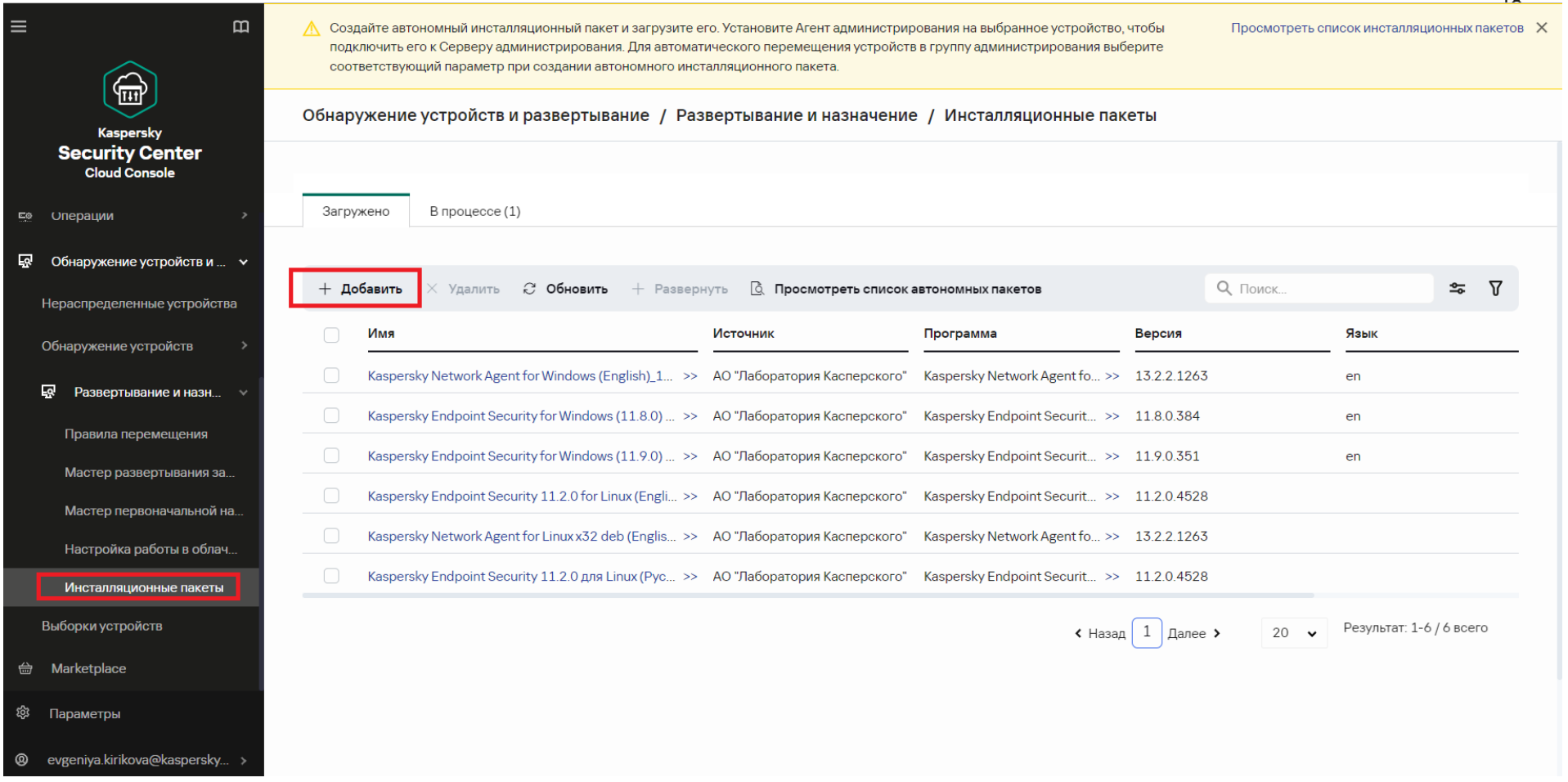
- Обычные EPP-решения, в том числе приложения Kaspersky Endpoint Security, работают только на небольшой части встраиваемых систем, произведенных за последнее время.
- Мы не тестировали приложения Kaspersky Endpoint Security на встраиваемых системах и не можем гарантировать их правильную работу.
- Для 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

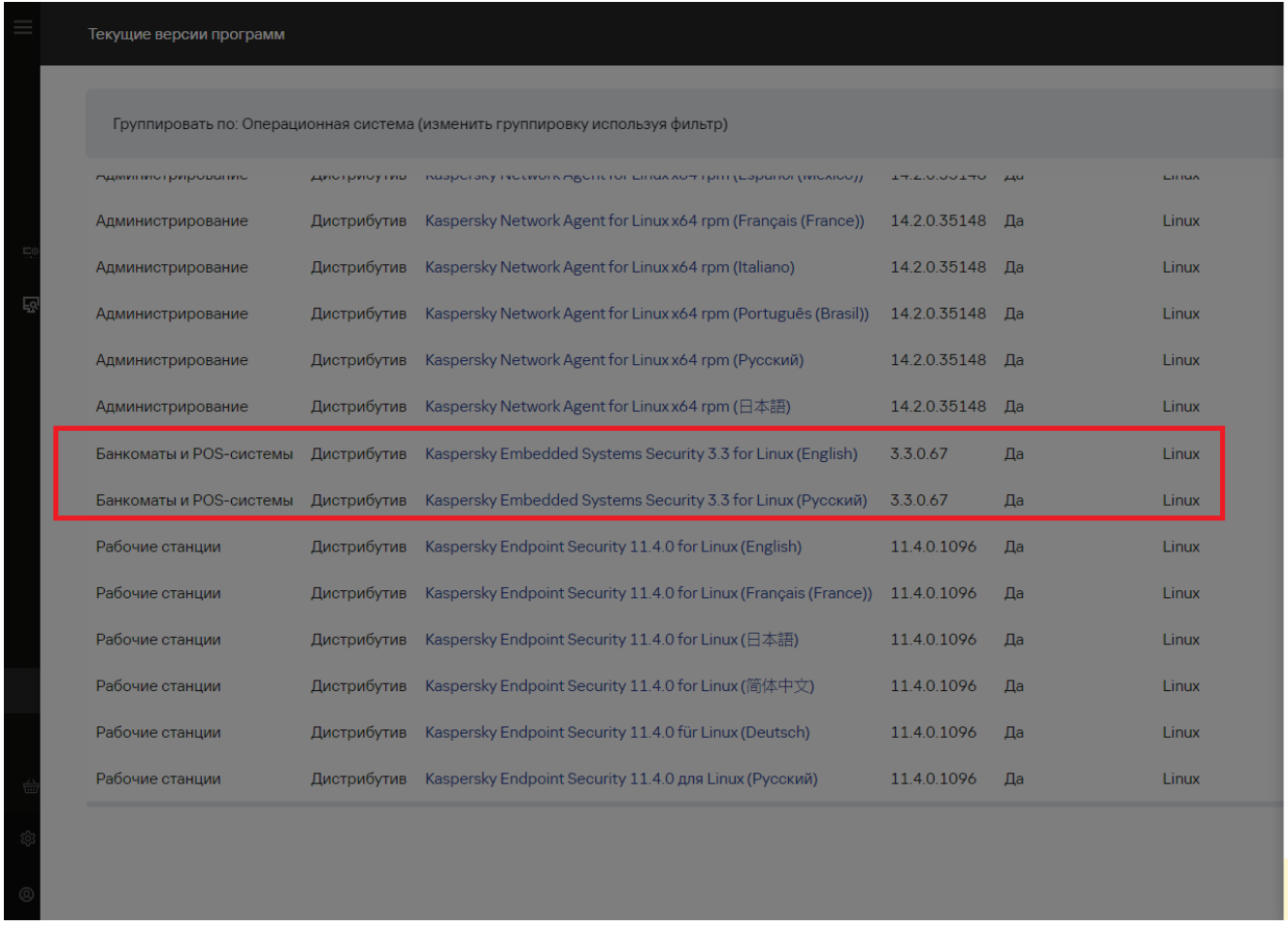
kaspersky

October 2021

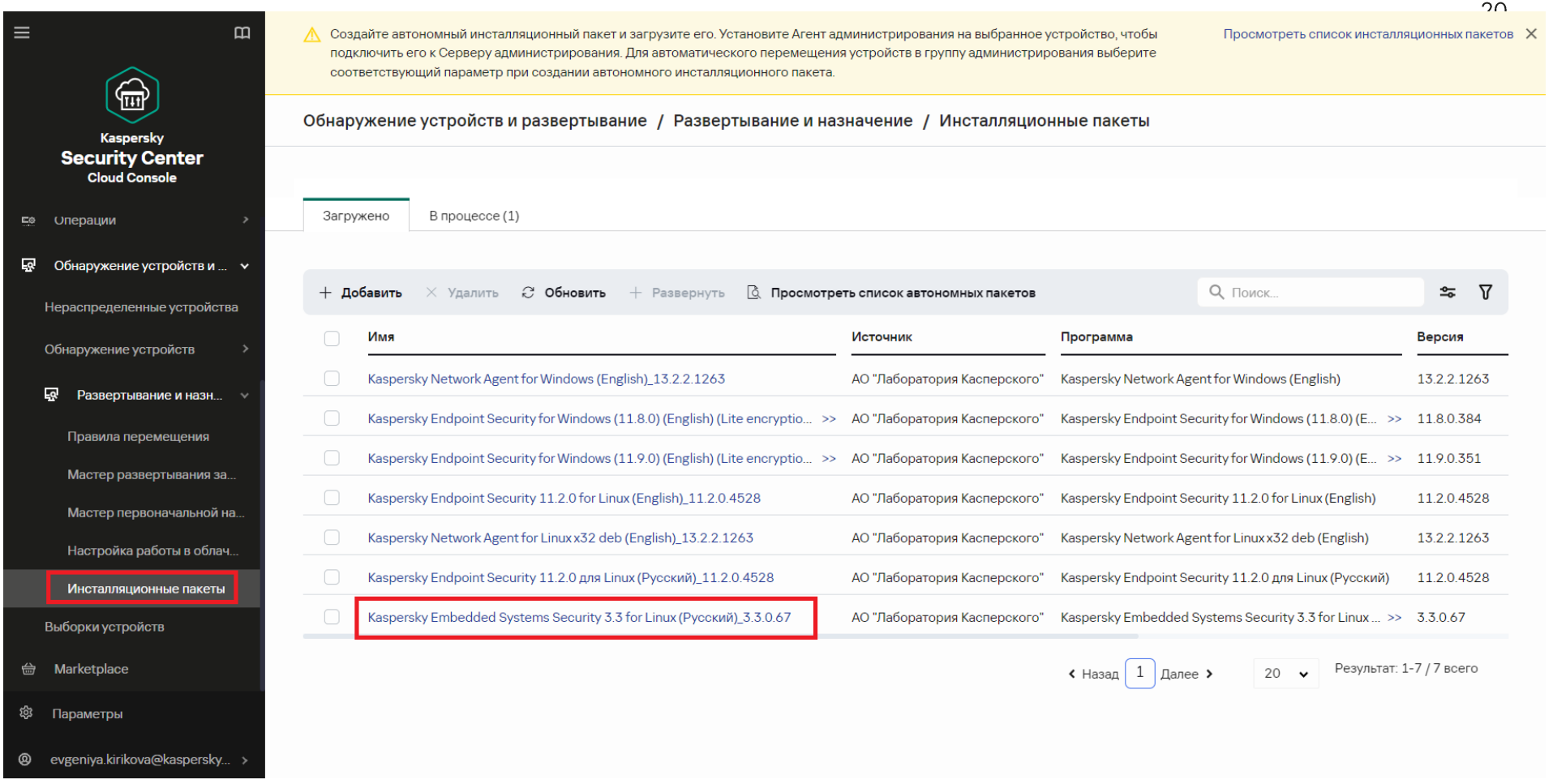
KSC: Добавляем нужные установочные пакеты



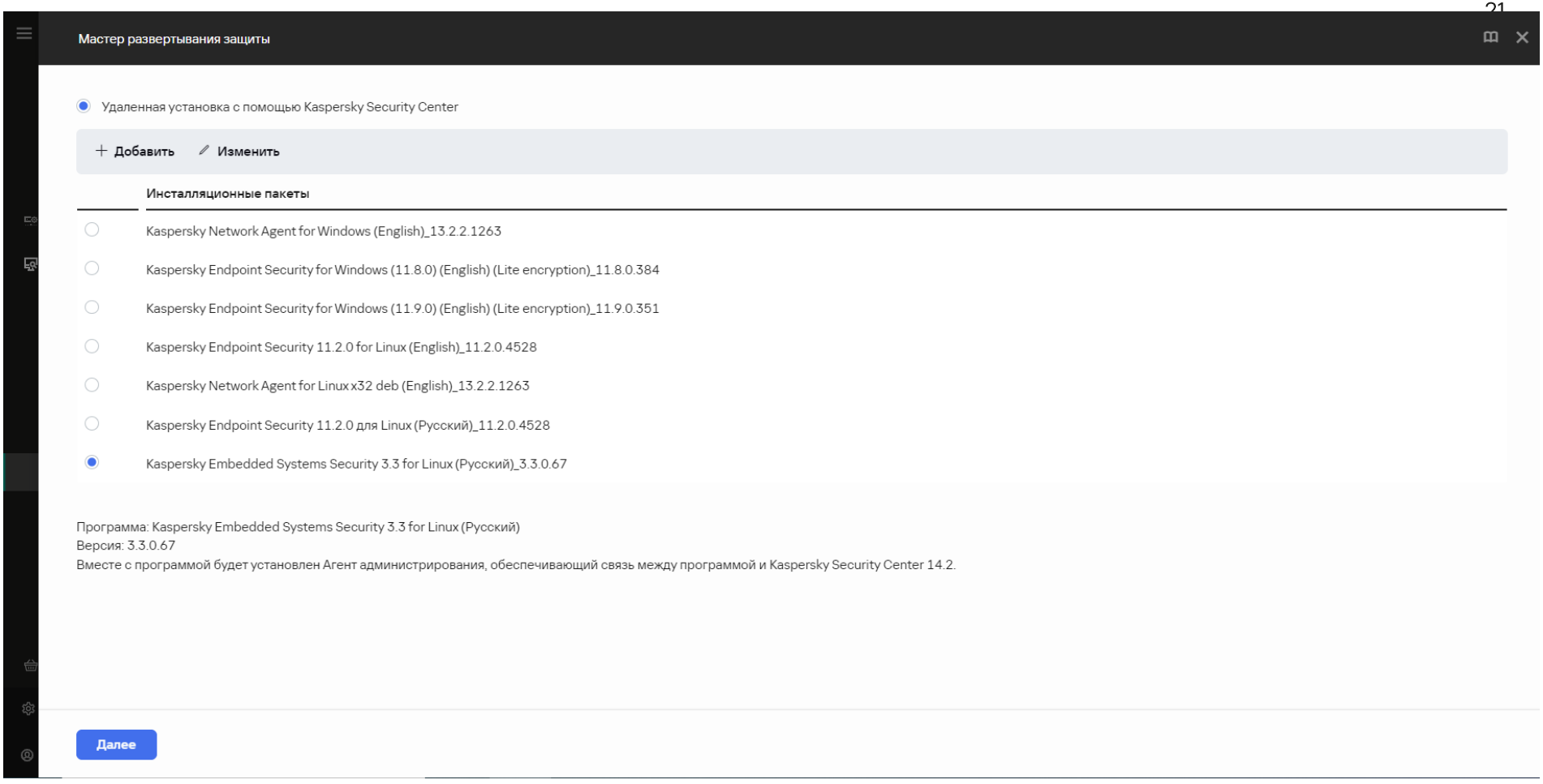
KSC: Добавляем нужные установочные пакеты



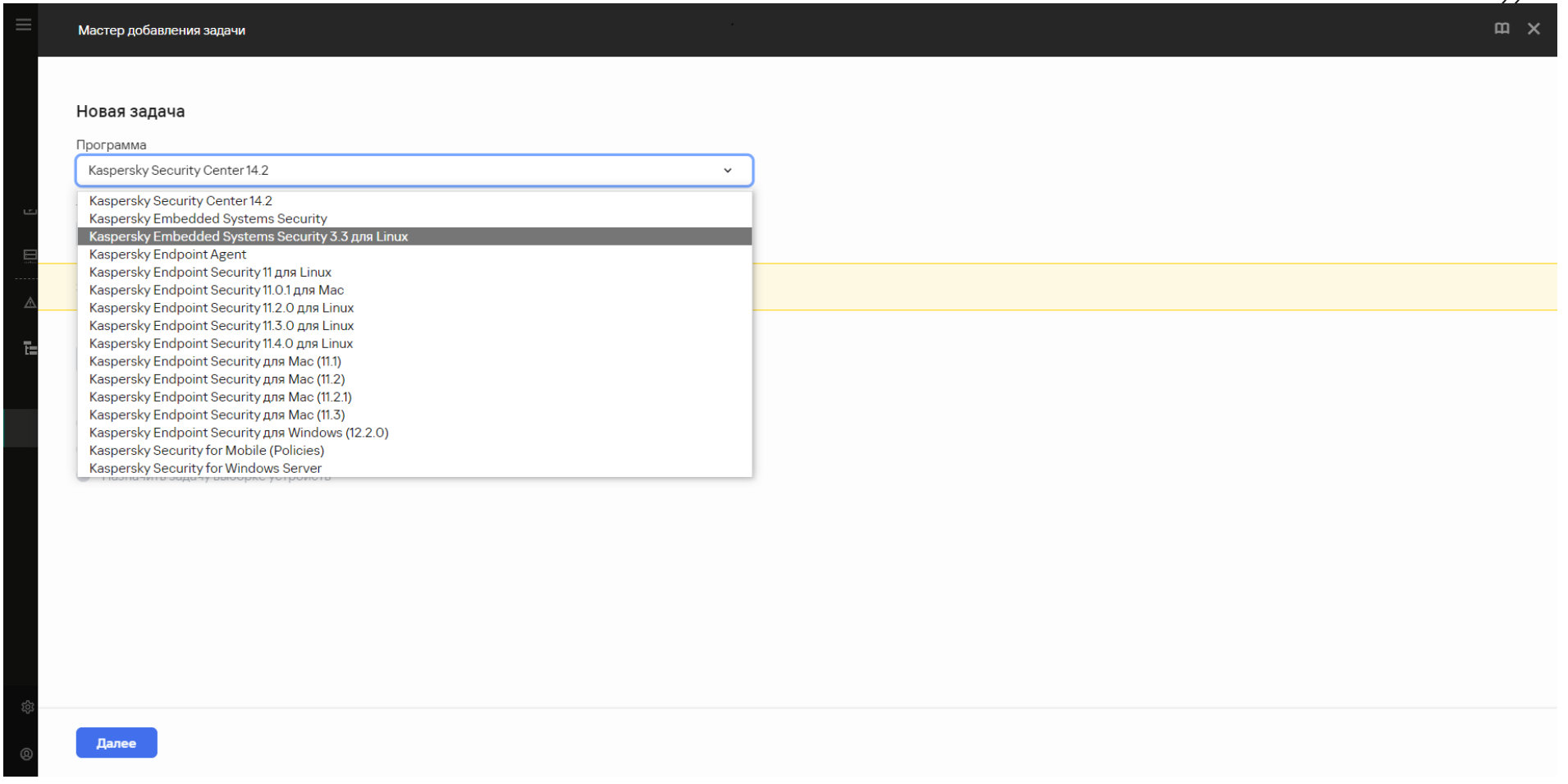
KSC: Добавляем нужные установочные пакеты



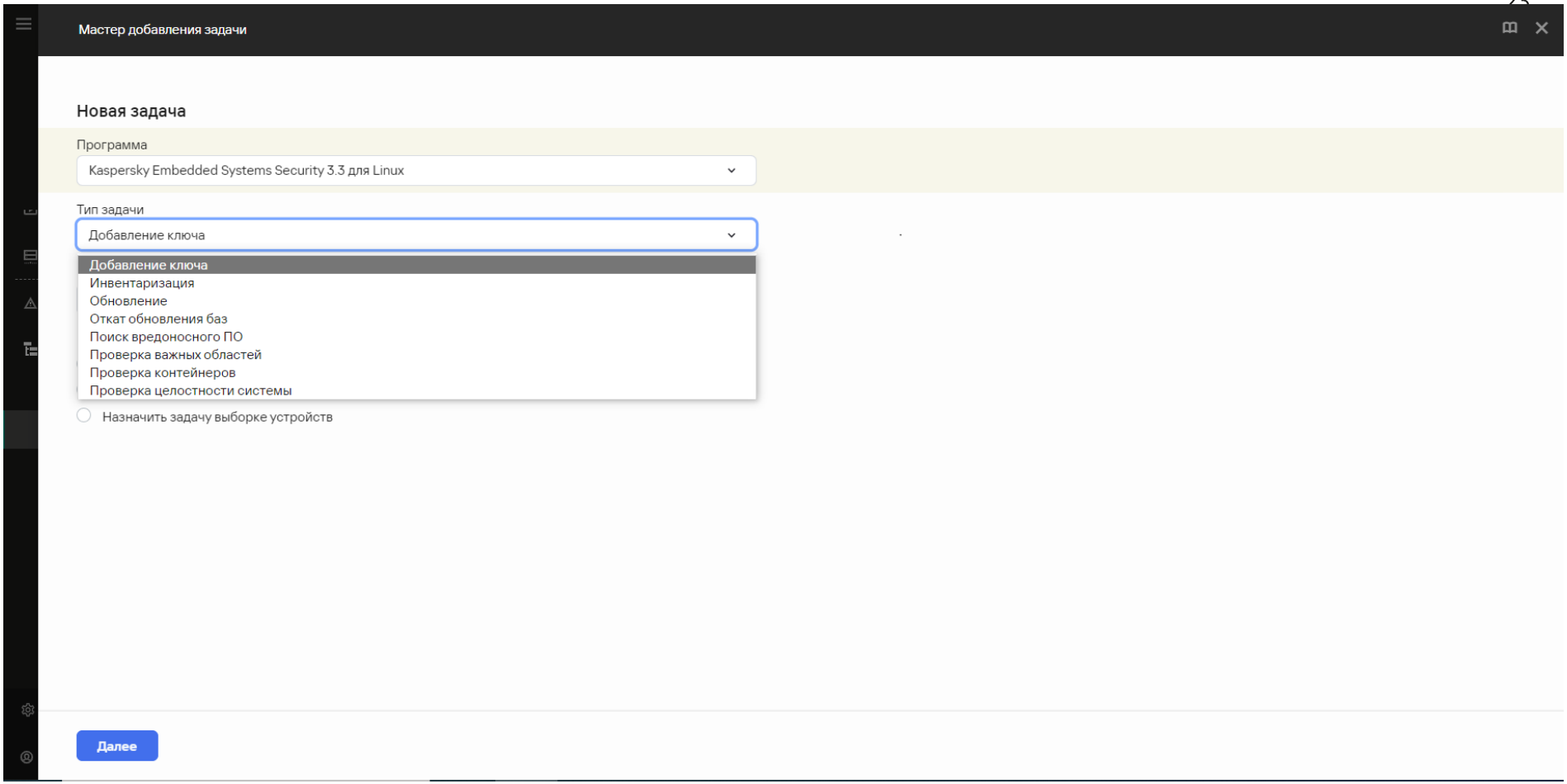
KSC: Удаленно устанавливаем KESS для Linux



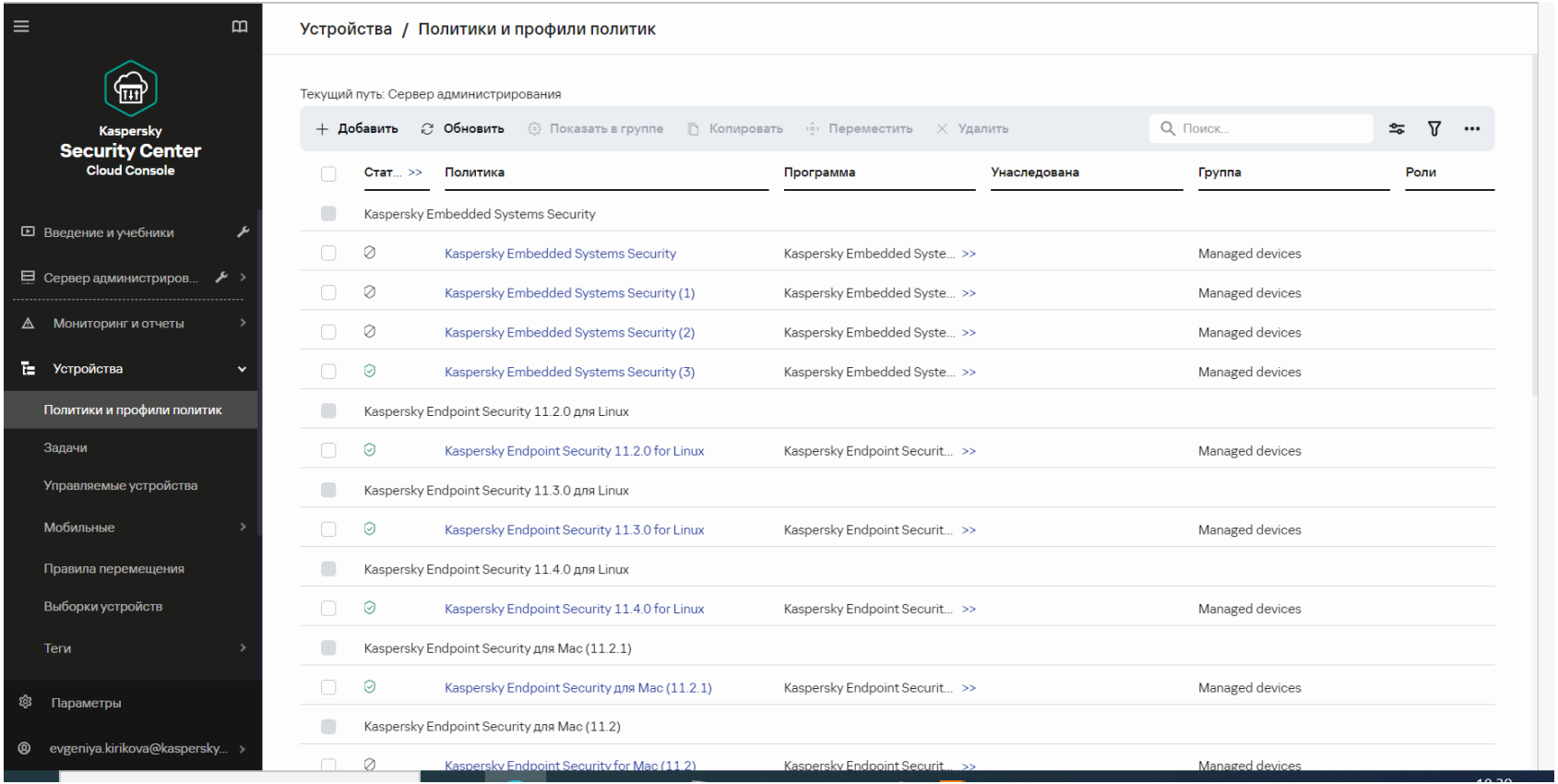
KSC: Создаем задачу развертывания



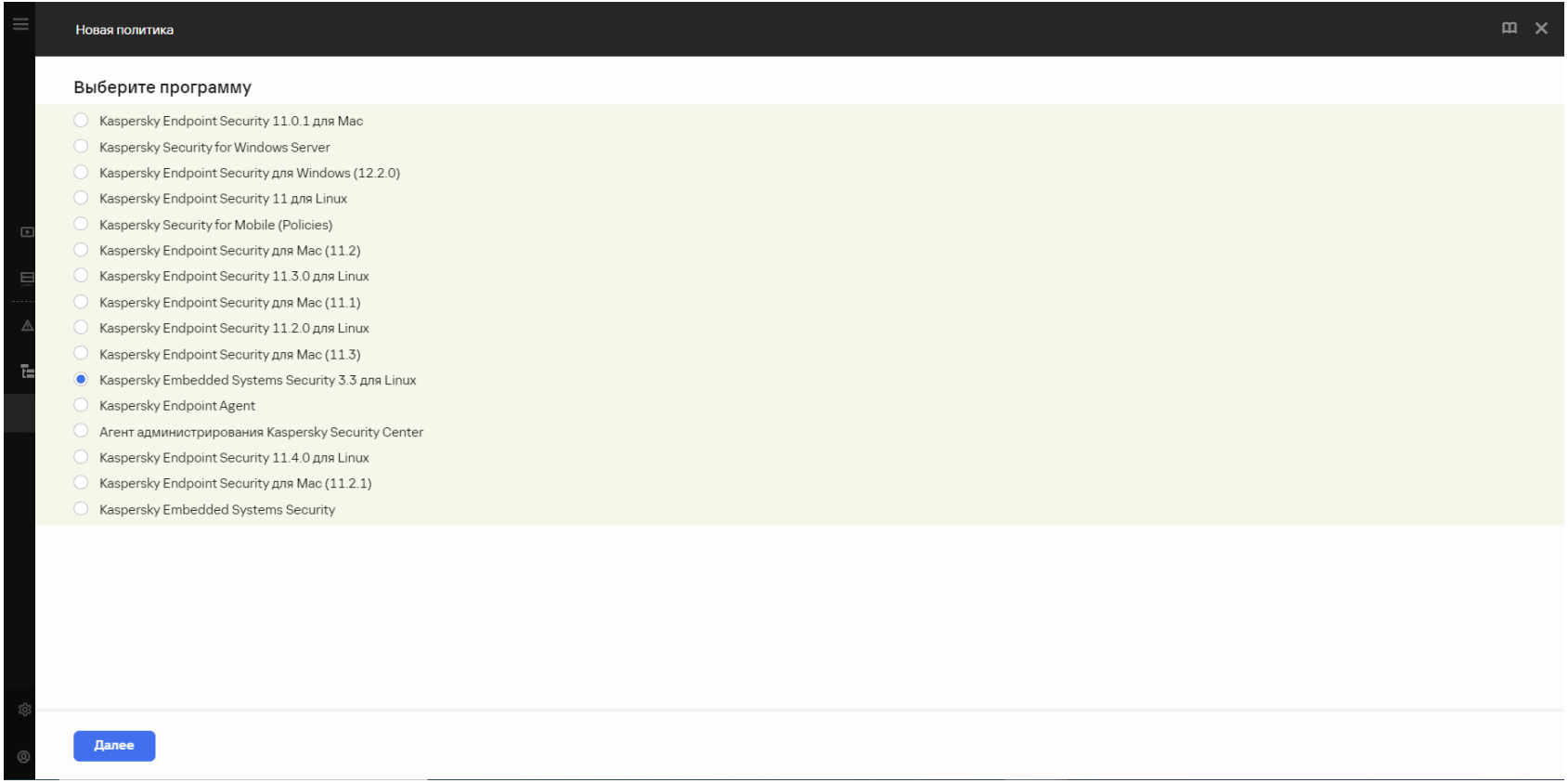
KSC: Добавляем ключ



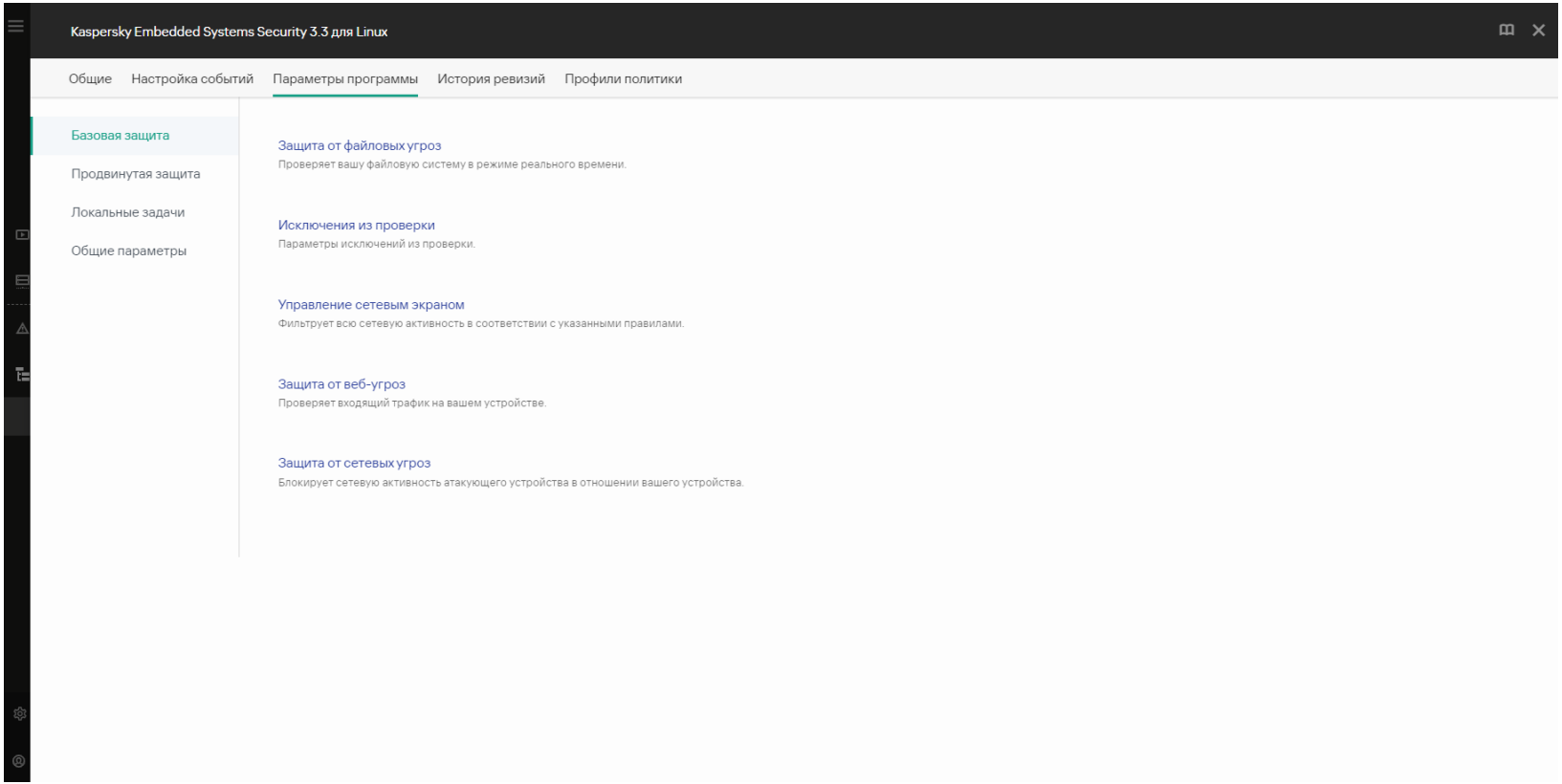
KESS для Linux : политики



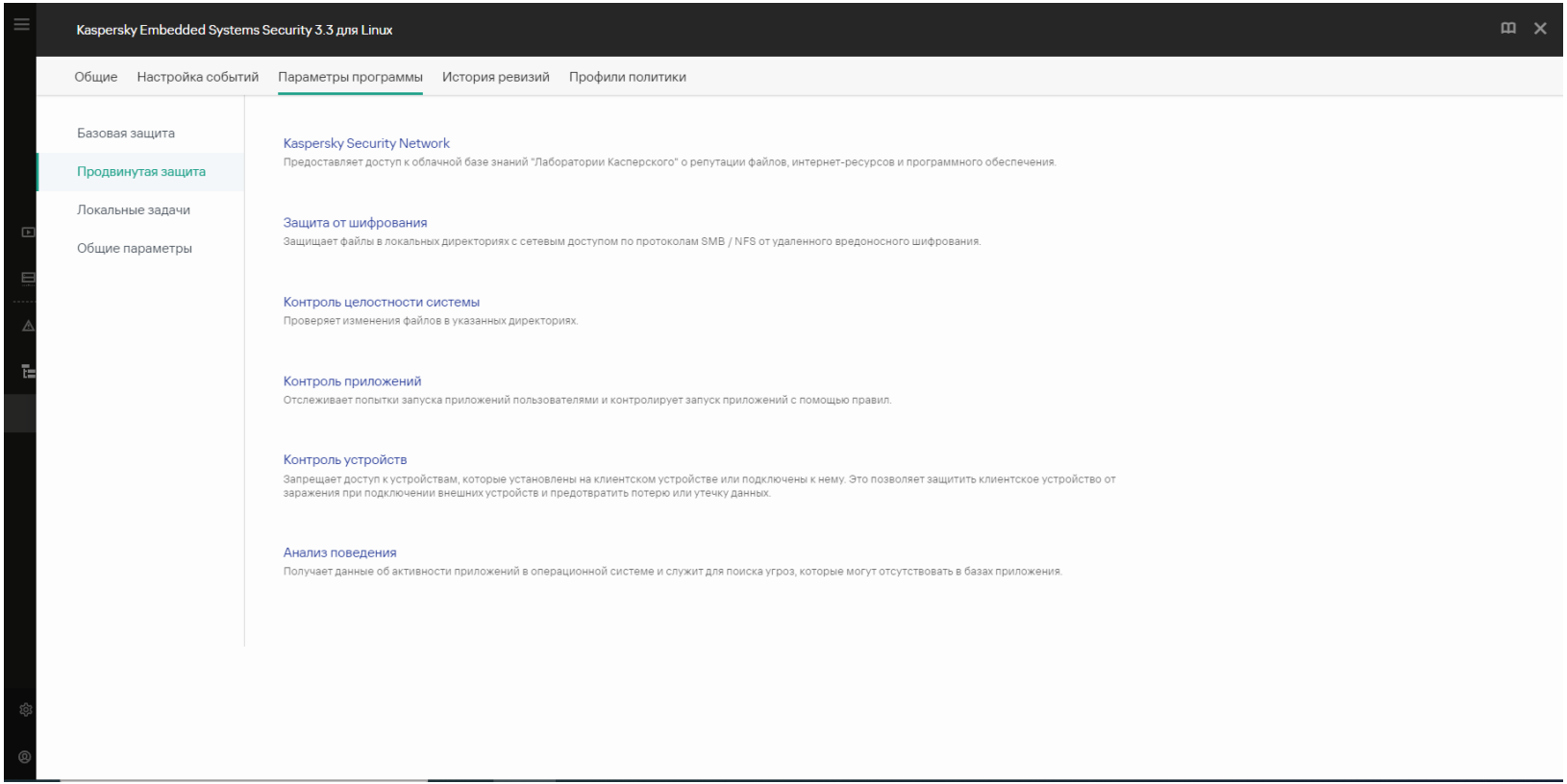
KESS для Linux : политики



KESS для Linux : политики – базовая защита



KESS для Linux: политики – продвинутая защита



Остались вопросы?

Страница продукта:
www.kaspersky.ru/enterprise-security/embedded-systems

kaspersky