НКЦКИ
НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Веб-сайт: cert.gov.ru
E-mail: threats@cert.gov.ru



# Распространение ВПО с использованием легитимного инструментария

ALRT-20230608.1 | 8 июня 2023 г.

Уровень угрозы: КРИТИЧЕСКИЙ

TLP: WHITE

| | |
|---|---|
| Описание угрозы | Специалистами НКЦКИ зафиксирован ряд компьютерных инцидентов, в рамках которых злоумышленниками для распространения ВПО внутри атакованных инфраструктур применялись штатные механизмы легитимных инструментов.<br>Одним из таких инструментов является механизм доставки обновлений, реализованный в Kaspersky Security Center.<br>Для минимизации возможностей злоумышленников по внедрению ВПО на все устройства организации, подключенные к Kaspersky Security Center, рекомендуем применить меры защиты для Сервера администрирования, разработанные компанией АО «Лаборатория Касперского». Руководство доступно на официальном сайте компании по ссылке: https://support.kaspersky.com/KSC/14.2/ru-RU/245736.htm |
| Рекомендации по нейтрализации угрозы | Руководство по усилению защиты Kaspersky Security Center 14 Windows<br><br>Программа Kaspersky Security Center предназначена для централизованного решения основных задач по управлению и обслуживанию системы защиты сети организации. Приложение предоставляет администратору доступ к детальной информации об уровне безопасности сети организации. Kaspersky Security Center позволяет настраивать все компоненты защиты, построенной на основе программ "Лаборатории Касперского".<br>Сервер администрирования Kaspersky Security Center имеет полный доступ к управлению защитой клиентских устройств и является важнейшим компонентом системы защиты организации. Поэтому для Сервера администрирования требуются усиленные меры защиты.<br>В Руководстве по усилению защиты описаны рекомендации и особенности настройки Kaspersky Security Center и его компонентов для снижения рисков его компрометации.<br>Руководство по усилению защиты содержит следующую информацию:<br>• выбор схемы развертывания Сервера Администрирования;<br>• настройка безопасного подключения к Серверу Администрирования;<br>• настройка учетных записей для работы с Сервером администрирования;<br>• управление защитой Сервера администрирования;<br>• управление защитой клиентских устройств;<br>• настройка защиты управляемых приложений;<br>• обслуживание Сервера администрирования; |

- передача информации в сторонние системы.

## Развертывание Сервера администрирования

### Архитектура Сервера администрирования

В общем случае на выбор архитектуры централизованного управления влияют расположение защищаемых устройств, доступы из смежных сетей, схемы обновления баз и другие параметры.

На начальном этапе проработки архитектуры мы рекомендуем ознакомиться с компонентами Kaspersky Security Center и их взаимодействием между собой, а также со схемами трафика данных и использования портов.

На основании этой информации нужно сформировать архитектуру, определяющую:

- расположение Сервера администрирования и подключение к сети;
- организацию рабочих мест администраторов и способы подключения к Серверу администрирования;
- способ установки Агента администрирования и программы защиты;
- использование точек распространения;
- использование виртуальных Серверов администрирования;
- использование иерархии Серверов администрирования;
- схему обновления антивирусных баз;
- другие информационные потоки.

### Выбор устройства для Сервера администрирования

Сервер администрирования рекомендуется устанавливать на выделенный сервер в инфраструктуре. Если на сервере отсутствует стороннее программное обеспечение, это позволит настроить параметры безопасности с учетом требований Kaspersky Security Center и без зависимости от требований стороннего программного обеспечения.

Сервер администрирования может быть развернут как на физическом сервере, так и на виртуальной машине. Убедитесь, что выбранное устройство соответствует аппаратным и программным требованиям.

## Расположение Сервера администрирования

Устройства, управляемые Сервером администрирования, могут располагаться:

- в локальном сегменте сети;
- в интернете;
- в демилитаризованной зоне (DMZ).

При этом Сервер администрирования также может быть расположен в следующих сегментах: технологическом, корпоративном, сегментах демилитаризованной зоны (DMZ).

При использовании Kaspersky Security Center для управления защитой изолированного сегмента сети, рекомендуется разворачивать Сервер администрирования в сегменте демилитаризованной зоны (DMZ). Это позволит организовать полноценное сегментирование сетей и минимизировать возможные обращения в защищаемый сегмент, сохранив при этом возможности по управлению устройствами и доставке обновлений.

## Ограничение установки Сервера администрирования на контроллер домена, терминальный сервер или пользовательское устройство

Категорически не рекомендуется устанавливать Сервер администрирования на контроллер домена, терминальный сервер или пользовательское устройство.

Рекомендуется предусмотреть функциональное разделение ключевых устройств сети. Это позволит сохранить работоспособность разных систем при выходе устройства из строя или при его компрометации. В это же время такой подход позволит реализовать различные политики безопасности для каждого устройства.

Например, ограничения безопасности, применяемые к контроллеру домена, могут значительно снизить производительность Сервера администрирования и привести к невозможности использования некоторых его функций. Если привилегированный доступ к контроллеру домена получит злоумышленник, он может изменить, повредить или уничтожить базу данных Active Directory Domain Services (AD DS). При этом также будут скомпрометированы все системы и учетные записи, управляемые Active Directory.

## Учетные записи для установки и запуска Сервера администрирования

Рекомендуется запустить установку Сервера администрирования под учетной записью локального администратора, чтобы избежать использования учетных записей домена для доступа к базе данных Сервера администрирования. Набор необходимых учетных записей и их прав зависит от выбранного типа СУБД, местоположения СУБД и способа создания базы данных Сервера администрирования.

При установке Kaspersky Security Center автоматически формируются группы пользователей KLAdmins и KLOperators. Этим группам предоставляются права на подключение к Серверу администрирования и на работу с его объектами.

В зависимости от того, под какой учетной записью проводится установка Kaspersky Security Center, группы KLAdmins и KLOperators создаются следующим образом:

- Если установка проводится под учетной записью пользователя, входящего в домен, группы создаются на устройстве с Сервером администрирования и в домене, в который входит устройство с Сервером администрирования.
- Если установка проводится под учетной записью системы, группы создаются только на устройстве с Сервером администрирования.

Чтобы избежать создания групп KLAdmins и KLOperators в домене и, как следствие, присвоения прав для управления Сервером администрирования вне устройства, на котором он установлен, рекомендуется проводить установку Kaspersky Security Center под локальной учетной записью.

При установке Сервера администрирования выберите учетную запись, под которой Сервер администрирования будет запускаться как служба. По умолчанию приложение создает локальную учетную запись KL-AK-*, под которой будет запускаться служба Сервера администрирования (klserver).

Служба Сервера администрирования при необходимости может запускаться под выбранной учетной записью. При этом учетная запись должна обладать различными правами для подключения к СУБД. Для обеспечения безопасности используйте непривилегированную учетную запись для запуска службы Сервера администрирования.

Во избежание некорректных параметров доступа для учетной записи Сервера администрирования рекомендуется создавать ее автоматически.

Исключение Сервера администрирования из домена

Не рекомендуется включать в домен устройство с Сервером администрирования (если оно используется). Это позволит разграничить права управления Kaspersky Security Center и избежать получения доступа к управлению в случае компрометации домена.

## Безопасность соединения

### Использование TLS

Рекомендуется запретить небезопасные подключения к Серверу администрирования. Например, при настройке Сервера администрирования, рекомендуется не включать подключения по HTTPпротоколу к Серверу администрирования.

Обратите внимание, что по умолчанию часть HTTP-портов Сервера администрирования закрыта. Оставшийся порт используется Веб-сервером Kaspersky Security Center (8060). Этот порт можно ограничить параметрами сетевого экрана устройства с Сервером администрирования.

### Строгие параметры TLS

Рекомендуется использовать протокол TLS версии 1.2 или выше и ограничить или запретить использование небезопасных алгоритмов шифрования.

Вы можете настроить протоколы шифрования (TLS), используемые Сервером администрирования. При этом учитывайте, что на момент выпуска определенной версии Сервера администрирования параметры протокола шифрования по умолчанию настроены так, чтобы обеспечить безопасную передачу данных.

### Ограничение доступа к базе данных Сервера администрирования

Рекомендуется ограничить доступ к базе данных Сервера администрирования. Например, вы можете разрешить доступ только с устройства с Сервером администрирования. Это позволит снизить вероятность взлома базы Сервера администрирования данных через известные уязвимости.

Вы можете настроить параметры в соответствии с руководством по эксплуатации используемой базы данных, а также предусмотреть закрытые порты на сетевых экранах.

## Запрет удаленной аутентификации с учетными записями Windows

Запрет на SSPI-подключения с удаленных адресов возможен с помощью специального флага LP_RestrictRemoteOsAuth. Этот флаг позволяет запретить удаленную аутентификацию на Сервере администрирования для учетных записей Windows, локальных или доменных.

Чтобы переключить флаг LP_RestrictRemoteOsAuth в режим запрета SSPI-подключений с удаленных адресов:

1. С помощью утилиты klscflag укажите значение флага LP_RestrictRemoteOsAuth: klscflag.exe -fset -pv .core/.independent -s KLLIM -n LP_RestrictRemoteOsAuth -t d -v 1
2. Перезапустите службу Сервера администрирования.

Флаг LP_RestrictRemoteOsAuth не работает, если удаленная аутентификация выполняется через Kaspersky Security Center Web Console или Консоль администрирования, установленную на том же устройстве, что и Сервер администрирования.

## Аутентификация Microsoft SQL Server

Если вы используете Microsoft SQL Server в качестве СУБД Сервера администрирования, нужно защитить от несанкционированного доступа данные Kaspersky Security Center, передаваемые в базу данных или получаемые от нее, а также данные, хранящиеся в этой базе данных. Для этого требуется настроить использование безопасного соединения между Kaspersky Security Center и SQL Server. Самый надежный способ обеспечить безопасную связь - это установить Kaspersky Security Center и SQL Server на одном устройстве и использовать механизм совместной памяти для обеих программ. Во всех других случаях рекомендуется использовать сертификат SSL/TLS для аутентификации экземпляра SQL Server.

## Настройка списка разрешенных IP-адресов для подключения к Серверу администрирования

По умолчанию пользователи могут войти в Kaspersky Security Center с любого устройства, на котором установлена Kaspersky Security Center Web Console или Консоль администрирования на основе Microsoft Management Console (MMC). Настроить Сервер администрирования можно таким образом, чтобы пользователи

могли подключаться к нему только с устройств с разрешенными IP-адресами. В этом случае, если злоумышленник похитит учетную запись Kaspersky Security Center, он сможет подключиться к Kaspersky Security Center только с тех IPадресов, которые добавлены в разрешенные.

## Учетные записи и авторизация

### Использование двухэтапной проверки Сервера администрирования

Kaspersky Security Center предоставляет пользователям Kaspersky Security Center Web Console и Консоли администрирования возможность использовать двухэтапную проверку на основе стандарта RFC 6238 (TOTP: Time-Based One-Time Password algorithm).

Если для вашей учетной записи включена двухэтапная проверка, каждый раз при входе в Kaspersky Security Center Web Console или в Консоль администрирования вы вводите свое имя пользователя, пароль и дополнительный одноразовый код безопасности. Если вы используете доменную аутентификацию для своей учетной записи, вам необходимо ввести только дополнительный одноразовый код безопасности. Для того чтобы получить одноразовый код безопасности, вам нужно установить приложение проверки подлинности на своем компьютере или мобильном устройстве.

Существуют как программные, так и аппаратные аутентификаторы (токены), поддерживающие стандарт RFC 6238. Например, к программным аутентификаторам относятся Google Authenticator, Microsoft Authenticator, FreeOTP.

Категорически не рекомендуется устанавливать приложение проверки подлинности на том же устройстве, с которого выполняется подключение к Серверу администрирования. Например, вы можете установить приложение для проверки подлинности на мобильном устройстве.

### Использование двухфакторной аутентификации операционной системы

Для авторизации на устройстве с Сервером администрирования рекомендуется использовать многофакторную аутентификацию (MFA) с использованием токена, смарт-карты или другого способа.

### Запрет на сохранение пароля администратора

При использовании Консоли администрирования не рекомендуется сохранять пароль администратора в диалоговом окне подключения к Серверу администрирования.

Также при работе с Сервером администрирования через Kaspersky Security Center Web Console не рекомендуется сохранять пароль администратора в браузере на устройстве пользователя.

### Авторизация внутреннего пользователя

По умолчанию пароль внутренней учетной записи пользователя Сервера администрирования должен соответствовать следующим требованиям:

- Длина пароля должна быть от 8 до 16 символов.
- Пароль должен содержать символы как минимум трех групп списка ниже:
  - верхний регистр (A-Z);
  - нижний регистр (A-Z) (a-z);
  - числа (0-9);
  - специальные символы (@ # $ % ^ & * - _ ! + = [ ] { } | : ' , . ? / \ ` ~ " ( ) ;).
- Пароль не должен содержать пробелов, символов Юникода или комбинации "." и "@", когда "." расположена перед "@".

По умолчанию максимальное количество попыток ввода пароля равно 10. Вы можете изменить количество попыток ввода пароля.

Пользователь Kaspersky Security Center может вводить неверный пароль ограниченное количество раз. После этого учетная запись пользователя блокируется на час.

### Отдельная группа администрирования для устройства с Сервером администрирования

Для Сервера администрирования рекомендуется создать выделенную группу администрирования. Предоставьте этой группе особые права доступа и создайте политику безопасности для нее.

Чтобы избежать умышленного понижения уровня защиты Сервера администрирования рекомендуется ограничить список учетных записей, которые могут управлять этой группой администрирования.

## Группы KLAdmins и KLOperators

Группы пользователей KLAdmins и KLOperators создаются автоматически во время установки Kaspersky Security Center. Группе KLAdmins предоставлены все права. Группе KLOperators предоставлены права на Чтение и Выполнение. Набор прав, предоставленных группе KLAdmins, недоступен для изменения.

С помощью стандартных средств администрирования операционной системы можно просмотреть группы KLAdmins и KLOperators и внести изменения в состав этих групп.

При разработке регламентов работы с Сервером администрирования нужно определить, потребуется ли специалисту информационной безопасности полный доступ (и включение в группу KLAdmins) для решения штатных задач.

Большинство базовых задач администрирования могут быть распределены между подразделениями организации (или разными сотрудниками одного подразделения) и, как следствие, между различными учетными записями. Также может быть выполнено разграничение по доступу к группам администрирования в Kaspersky Security Center. В результате можно реализовать такую модель использования, при которой авторизация под учетными записями из группы KLAdmins будет нестандартным поведением, что можно рассматривать как инцидент.

Если установка Kaspersky Security Center проводилась под системной учетной записью, группы создаются только на устройстве с Сервером администрирования. В этом случае рекомендуем убедиться, что в группу включены только учетные записи, созданные во время установки Kaspersky Security Center. Не рекомендуется добавлять в группу KLAdmins другие группы пользователей (локальные и/или доменные), которые были созданы автоматически во время установки Kaspersky Security Center. Группа KLAdmins должна включать единичные непривилегированные учетные записи.

Если установка выполнялась под учетной записью пользователя, входящего в домен, группы KLAdmins и KLOperators создаются как на Сервере администрирования, так и в домене, в который входит Сервер администрирования. Рекомендуется применить аналогичный подход как и в случае с установкой под системной учетной записью.

## Ограничить членство в роли "Главный администратор"

Рекомендуется ограничить членство пользователей в роли "Главный администратор".

По умолчанию после установки Сервера администрирования роль "Главный администратор" присвоена группе локальных администраторов устройства и созданной группе KLAdmins. Это удобно для управления, но критично с точки зрения безопасности, так как роль "Главный администратор" имеет очень широкий набор привилегий – назначение этой роли пользователям должно быть строго регламентировано.

Локальных администраторов можно исключить из списка пользователей, имеющих права администратора Kaspersky Security Center. Роль "Главный администратор" нельзя удалить из группы KLAdmins. В нее можно включить учетные записи группы KLAdmins, которые будут использоваться для управления Сервером администрирования.

В случае использования доменной аутентификации, рекомендуется ограничить привилегии учетных записей администраторов домена в Kaspersky Security Center. По умолчанию этим учетным записям присвоена роль "Главный администратор". Также администратор домена может включить свою учетную запись в группу KLAdmins с целью получения роли "Главный администратор". Чтобы этого избежать, в параметрах безопасности Kaspersky Security Center можно добавить группу "Администраторы домена" ("Domain Admins") и определить для нее запрещающие правила. Эти правила будут приоритетнее разрешающих.

Также можно использовать предопределенные роли пользователей с уже настроенным набором прав.

## Настройка прав доступа к функциям программы

Рекомендуется использовать возможности гибкой настройки прав доступа пользователей и групп пользователей к разным функциям Сервера администрирования.

Управление доступом на основе ролей позволяет создавать типовые роли пользователей с заранее настроенным набором прав и присваивать эти роли пользователям в зависимости от их служебных обязанностей.

Основные преимущества ролевой модели управления доступом:

- простота администрирования;
- иерархия ролей;
- принцип наименьшей привилегии;
- разделение обязанностей.

Вы можете воспользоваться встроенными ролями и присвоить их определенным сотрудникам на основе должностей либо создать полностью новые роли.

При настройке ролей требуется уделить особое внимание привилегиям, связанным с изменением состояния защиты устройства и удаленной установкой стороннего программного обеспечения:

Управление группами администрирования.

- Операции с Сервером администрирования.
- Удаленная установка.
- Изменение параметров хранения событий и отправки уведомлений.

  Эта привилегия позволяет настроить уведомления, которые запускают скрипт или исполняемый модуль на устройстве с Сервером администрирования при возникновении события.

### Отдельная учетная запись для удаленной установки приложений

Помимо базового разграничения прав доступа, рекомендуется ограничить возможность удаленной установки приложений для всех учетных записей (кроме "Главного администратора" или иной специализированной учетной записи).

Рекомендуется использовать отдельную учетную запись для удаленной установки приложений.

Вы можете назначить роль или разрешения отдельной учетной записи.

### Обеспечение безопасности привилегированного доступа Windows

Рекомендуется рассмотреть рекомендации Microsoft по обеспечению безопасности привилегированного доступа. Чтобы просмотреть эти рекомендации, перейдите в раздел Обеспечение безопасности привилегированного доступа .

Одной из ключевых рекомендаций является развертывание рабочих станций с привилегированным доступом (PAW) .

### Использование управляемых учетных записей служб (MSA) и групповых управляемых учетных записей служб (gMSA) для запуска служб Сервера администрирования

В Active Directory существует специальный тип учетных записей для безопасного запуска служб – MSA/gMSA . Kaspersky Security Center поддерживает управляемые учетные записи службы (MSA) и групповые управляемые

учетные записи службы (gMSA). Если такие учетные записи используются в вашем домене, вы можете выбрать одну из них в качестве учетной записи для службы Сервера администрирования.

### Регулярный аудит всех пользователей

Рекомендуется проводить регулярный аудит всех пользователей на устройстве, где установлен Сервер администрирования. Это позволит реагировать на некоторые типы угроз безопасности, связанные с возможной компрометацией устройства.

## Управление защитой Сервера администрирования

### Выбор программы защиты Сервера администрирования

Выбор приложения для защиты устройства, на котором установлен Сервер администрирования, зависит от типа развертывания Сервера администрирования и общей стратегии защиты.

Если вы разворачиваете Сервер администрирования на выделенном устройстве, рекомендуется выбрать программу Kaspersky Endpoint Security для защиты устройства с Сервером администрирования. Это позволит применить все имеющиеся технологии для защиты устройства, в том числе модули поведенческого анализа.

Если Сервер администрирования устанавливается на уже существующее в инфраструктуре устройство, использованное ранее для выполнения других задач, рекомендуются следующие приложения защиты:

- Kaspersky Industrial CyberSecurity for Nodes. Эту программу рекомендуется устанавливать на устройства, входящие в промышленную сеть. Kaspersky Industrial CyberSecurity for Nodes – это программа, имеющая сертификаты совместимости с различными производителями промышленного программного обеспечения.
- Рекомендованные программы безопасности. Если Сервер администрирования установлен на устройство с другим программным обеспечением, нужно ознакомиться с рекомендациями производителя программного обеспечения по использованию антивирусных программ (возможно, уже существуют рекомендации по выбору программы защиты, и, вероятно, вам потребуется выполнить настройку доверенной зоны).

## Создание отдельной политики безопасности для защиты программы

Для приложения защиты Сервера администрирования нужно создать отдельную политику безопасности. Эта политика должна отличаться от политики безопасности для клиентских устройств. Такой подход позволит задать максимально подходящие параметры безопасности для Сервера администрирования, не влияя при этом на уровень защиты других устройств.

Рекомендуется разделить устройства на группы, определив устройство с Сервером администрирования в отдельную группу администрирования, для которой вы затем можете создать специальную политику безопасности

## Модули защиты

Если отсутствуют особые рекомендации от производителя стороннего программного обеспечения, установленного на том же устройстве, что и Сервер администрирования, рекомендуется активировать и настроить все доступные модули защиты (после проверки их работы в течение определенного времени).

## Настройка сетевого экрана устройства с Сервером администрирования

На устройстве с Сервером администрирования рекомендуется настроить сетевой экран таким образом, чтобы ограничить число устройств, с которых администраторы могут подключаться к Серверу администрирования через Консоль администрирования либо Kaspersky Security Center Web Console.

По умолчанию Сервер администрирования использует порт 13291 для подключения к Консоли администрирования и порт 13299 для подключения к Kaspersky Security Center Web Console.

Рекомендуется ограничить число устройств, с которых Сервер администрирования может управляться по этим портам.

## Запрет на запуск панели управления

Если вы установили Сервер администрирования на устройство под управлением Microsoft Windows и используете приложение с модулем контроля запуска программ, можно запретить запуск панели управления (control.exe) для непривилегированных пользователей, например для группы администраторов.

В таком случае, после создания указанных запрещающих правил контроля запуска программ, пользователи с правами предустановленной роли Администратора потеряют возможность контролировать другие учетные записи сети, в том числе изменять имена учетных записей и пароли.

## Управление защитой клиентских устройств

Инсталляционные пакеты хранятся в папке общего доступа Сервера администрирования, во вложенной папке Packages. Если лицензионные ключи будут добавлены в инсталляционный пакет, они могут быть доступны на чтение всем пользователям, имеющим права на чтение этой папки общего доступа.

Для того чтобы избежать компрометации лицензионного ключа, не рекомендуется добавлять лицензионные ключи в инсталляционные пакеты.

Рекомендуется использовать автоматическое распространение лицензионных ключей на управляемые устройства, выполнять развертывание с помощью задачи Добавление лицензионного ключа для управляемой программы, и добавлять код активации или файл ключа на устройства вручную.

## Правила автоматического перемещения устройств между группами администрирования

Рекомендуется ограничить использование правил автоматического перемещения устройств между группами администрирования.

Использование правил автоматического перемещения может привести к тому, что на устройство будут распространены политики, предоставляющие более широкий набор привилегий, чем было до перемещения.

Перемещение клиентского устройства в другую группу администрирования может привести к распространению на него параметров политик. Эти параметры политик могут быть нежелательны к распространению на гостевые и недоверенные устройства.

Эта рекомендация, не относится к первоначальному распределению устройств по группам администрирования.

### Требования к безопасности к устройствам с точками распространения и шлюзам соединений

Устройства с установленным Агентом администрирования могут использоваться в качестве точки распространения и выполнять следующие функции:

- Распространять обновления и инсталляционные пакеты, полученные от Сервера администрирования, на клиентские устройства в группе.
- Выполнять удаленную установку программ сторонних производителей и программ "Лаборатории Касперского" на клиентские устройства.
- Опрашивать сеть с целью обнаружения новых устройств и обновления информации об уже известных устройствах. Точка распространения может использовать те же методы обнаружения устройств, что и Сервер администрирования.

Размещение точек распространения в сети организации используется для следующего:

- уменьшение нагрузки на Сервер администрирования;
- оптимизация трафика;
- предоставление Серверу администрирования доступа к устройствам в труднодоступных частях сети.

С учетом доступных возможностей рекомендуется защитить, в том числе физически, устройства, выполняющие роль точек распространения, от любого типа несанкционированного доступа.

### Ограничение автоматического назначения точек распространения

Для упрощения администрирования и сохранения работоспособности сети рекомендуется воспользоваться автоматическим назначением точек распространения. Однако в промышленных и небольших сетях рекомендуется избегать автоматического назначения точек распространения, так как на точки распространения могут быть, например, переданы конфиденциальные сведения учетных записей, используемых для работы задач принудительной удаленной установки средствами операционной системы.

В промышленных и небольших сетях вы можете назначить точки распространения вручную.

При необходимости вы также можете просмотреть Отчет о работе точек распространения.

## Настройка защиты управляемых приложений

### Политики управляемых приложений

Рекомендуется создать политику для каждого вида используемого приложения и компонента Kaspersky Security Center (Агент администрирования, KasperskyEndpointSecurity для Windows,KasperskyEndpoint Agent и другие). Политика должна применяться ко всем управляемым устройствам (корневой группе администрирования) или к отдельной группе, в которую автоматически попадают новые управляемые устройства в соответствии с настроенными правилами перемещения.

### Установка пароля на выключение защиты и удаление приложения

**Чтобы злоумышленники не могли отключить программы безопасности "Лаборатории Касперского", рекомендуется установить пароль для выключения защиты и удаления программ безопасности "Лаборатории Касперского".** Вы можете установить пароль, например, для Kaspersky Endpoint Security для Windows , Kaspersky Security для Windows Servers, Агента администрирования и других программ "Лаборатории Касперского". После включения защиты паролем рекомендуется заблокировать эти параметры, закрыв их "замком".

### Использование Kaspersky Security Network

Во всех политиках управляемых приложений и в свойствах Сервера администрирования рекомендуется использовать Kaspersky Security Network (KSN) и принять актуальное Положение о KSN. При обновлении Сервера администрирования вы также можете принять обновленное Положение о KSN. Когда использование облачных служб запрещено законодательством или иными нормативными актами, вы можете не включать KSN.

### Регулярная проверка управляемых устройств

Для всех групп устройств вам нужно создать задачу, периодически запускающую полную проверку устройств.

### Обнаружение новых устройств

Рекомендуется должным образом настроить параметры обнаружения устройств: настроить интеграцию с Active Directory и указать диапазоны IP-адресов для обнаружения новых устройств.

В целях безопасности вы можете использовать группу администрирования по умолчанию, в которую попадают все новые устройства, и политики по умолчанию, применяемые к этой группе.

### Определение папки общего доступа

Если Сервер администрирования развернут на устройстве под управлением Windows, при выборе существующей папки общего доступа, (которая используется, например, для размещения инсталляционных пакетов и хранилища обновляемых баз) рекомендуем убедиться, что права на чтение предоставлены группе "Все" (Everyone), а права на запись – группе KLAdmins.

## Обслуживание Сервера администрирования

### Резервное копирование данных Сервера администрирования

Резервное копирование данных позволяет восстановить данные Сервера администрирования без их потери.

По умолчанию задача резервного копирования создается автоматически после установки Kaspersky Security Center и выполняется периодически с сохранением резервных копий в соответствующей директории.

Пользователь может изменить параметры задачи резервного копирования:

- увеличить частоту резервного копирования;
- определить особую директорию для сохранения копий;
- изменить пароль для резервной копии.

При хранении резервных копий в директории, отличной от директории по умолчанию, рекомендуется ограничить ACL этой директории. Учетные записи Сервера администрирования и сервера базы данных Сервера администрирования должны иметь доступ на запись в этой директории.

### Обслуживание Сервера администрирования

Обслуживание Сервера администрирования позволяет сократить объем базы данных, повысить производительность и надежность работы программы. Рекомендуется обслуживать Сервер администрирования не реже раза в неделю.

Обслуживание Сервера администрирования выполняется с помощью соответствующей задачи.

Во время обслуживания Сервера администрирования программа выполняет следующие действия:

- проверяет базу данных на наличие ошибок;
- перестраивает индексы базы данных;
- обновляет статистику базы данных;
- сжимает базу данных (при необходимости).

### Обновление операционной системы и стороннего программного обеспечения на устройстве с Сервером администрирования

Настоятельно рекомендуется регулярно выполнять установку обновлений операционной системы и стороннего программного обеспечения на устройстве с Сервером администрирования.

Клиентским устройствам не требуется постоянное подключение к Серверу администрирования, поэтому после установки обновлений можно безопасно перезагрузить устройство с Сервером администрирования. Все события, зарегистрированные на клиентских устройствах во время простоя Сервера администрирования, отправляются на него после восстановления соединения.

## Передача событий в сторонние системы

### Мониторинг и отчеты

Для своевременного реагирования на инциденты безопасности вы можете настроить функции мониторинга и параметры отчетов.

### Экспорт событий в SIEM-системы

Для максимально быстрого выявления инцидентов до того, как будет нанесен существенный ущерб, рекомендуется использовать передачу событий в SIEM-систему.

### Уведомление по электронной почте о событиях аудита

Kaspersky Security Center позволяет получать информацию о событиях, произошедших в процессе работы Сервера администрирования и программ "Лаборатории Касперского", установленных на управляемых устройствах. Для своевременного реагирования на возникновение нештатных ситуаций рекомендуется настроить отправку Сервером администрирования уведомлений о публикуемых им событиях аудита, критических событиях, событиях отказа функционирования и предупреждениях.

Поскольку события аудита являются внутрисистемными, они регистрируются редко и количество уведомлений о подобных событиях вполне приемлемо для почтовой рассылки.