

F-Secure Mobile Security™ for S60

1. Установка и активация

Предыдущая версия Предыдущую версию F-Secure Mobile Anti-Virus удалять не требуется. Проверьте параметры F-Secure Mobile Security после установки новой версии.

Установка **Чтобы установить приложение, выполните следующие действия.**

- Загрузите файл установки на компьютер и переместите его на устройство;
- Загрузите файл установки на компьютер и установите продукт с помощью Nokia PC Suite или
- Загрузите файл установки непосредственно на устройство. Установка начнется автоматически.

После завершения установки перезапустите устройство, если отобразится соответствующий запрос. После выполнения установки необходимо выполнить активацию продукта. Защита вашего устройства приложением не будет осуществляться, если оно не активировано.

Активация **Чтобы начать активацию, выполните следующие действия.**

1. Откройте приложение. Откроется окно приветствия.
2. Нажмите кнопку **Далее**.
3. Выберите тип активации:
 - Чтобы активировать только функцию защиты от кражи, выберите тип активации **Только защита от кражи** и нажмите кнопку **Продолжить**.
 - Чтобы использовать полную лицензионную версию, выберите **Номер подписки** в качестве типа активации и нажмите кнопку **Далее**. Введите ваш номер подписки и нажмите **ОК**.
4. Нажмите кнопку **Да** и выберите точку доступа к Интернету, чтобы подключиться к службе обновления и запустить загрузку обновлений. Приложение подключается к службе обновлений и передает в нее ваш номер подписки. Во время выполнения первого обновления приложение загружает новейшую базу данных с описанием вирусов.
5. После загрузки всех необходимых обновлений приложение готово к работе. Чтобы завершить процесс активации, нажмите кнопку **Продолжить**.

После того как процесс активации завершен, произведите поиск вирусов на устройстве, чтобы убедиться, что вирусы на устройстве отсутствуют. См. раздел **Поиск вирусов** ниже.



Следует производить поиск вирусов при каждом запросе приложения на выполнение проверки.

2. Поиск вирусов

F-Secure Mobile Security работает в фоновом режиме и выполняет автоматическое сканирование файлов на наличие вирусов.

1. F-Secure Mobile Security показывает уведомление, если обнаруживает вирус при проверке в реальном времени. Выберите **Да**, чтобы сразу просмотреть зараженные файлы, или **Нет**, чтобы сделать это позже.
2. В окне просмотра вирусов содержится список зараженных файлов на устройстве и состояние файла (на карантине или восстановлен).

Чтобы просмотреть подробные сведения о зараженном файле:

1. Выполните прокрутку до зараженного файла и нажмите кнопку выбора.
2. Выберите **Просмотр**.
3. В представлении «О заражении» будут отображены следующие сведения: путь к зараженному файлу, имя этого файла, название вируса, которым заражен файл.

Обработка зараженных файлов

Чтобы обработать зараженные файлы, выполните следующие действия:

1. В окне просмотра вирусов выберите зараженный файл, который необходимо обработать.
2. Нажмите кнопку выбора.
3. Выберите одно из следующих действий:
 - **Удалить** – удалить зараженный файл. Рекомендуется выбирать эту команду. Файл будет полностью удален из устройства.
 - **Отправить на карантин** – отправить зараженный файл на карантин, если файл еще не на карантине. Файл, отправленный на карантин, блокируется и не может причинить вред устройству, когда приложение F-Secure Mobile Security включено.
 - **Восстановить** – восстановить файл, помещенный на карантин. При выборе этой команды с изолированного файла снимается блокировка. Вы получаете к нему доступ и можете использовать его на свой страх и риск.

3. Предотвращение несанкционированного сетевого трафика

В программном обеспечении F-Secure Mobile Security брандмауэр нормально работает в фоновом режиме. Он контролирует входящие и исходящие сведения из Интернета и сетевой трафик, а также защищает от попыток проникновения. Предварительно определенные уровни защиты для брандмауэра позволяют изменить степень защиты в соответствии с потребностями пользователя.


Выбор уровня защиты

Чтобы выбрать уровень защиты, выполните следующие действия:

1. Перейдите к меню **Настройки** и нажмите кнопку выбора.
2. Выберите **Брандмауэр** в списке выбора настроек.
3. Выберите нужный уровень защиты:
 - **Запретить все** – запрещает весь сетевой трафик.
 - **Высокий** – разрешает запуск наиболее часто используемых приложений и блокирует весь входящий трафик.
 - **Обычный** – разрешает все исходящие соединения и блокирует весь входящий трафик.
 - **Разрешить все** – разрешение всего сетевого трафика.
 - **Настраиваемый** – уровень, который разрешает сетевой трафик на основе настраиваемых пользователем правил. Чтобы изменить настраиваемый набор правил, выберите **Параметры > Изменить настраиваемые правила**, если выбран уровень защиты **Настраиваемый**.

4. Защита конфиденциальных сведений

Средство защиты от кражи исключает несанкционированное использование устройства или хранящихся на нем данных в случае кражи устройства.


-  Поскольку карты памяти можно легко удалить, для обеспечения безопасности храните конфиденциальные сведения в памяти устройства, которую можно заблокировать или очистить с помощью функции защиты от кражи.

Использование блокировки устройства

Средство защиты от кражи может автоматически заблокировать устройство в случае смены SIM-карты в нем. Заблокированное устройство можно разблокировать только с помощью кода блокировки.

Настройка блокировки устройства:

1. Перейдите к меню **Настройки** и нажмите кнопку выбора.
2. Выберите **Защита от кражи** в списке выбора настроек.
3. Введите **код блокировки**. Код блокировки должен содержать не менее 5 символов. Сохраните его в надежном месте.

-  Ваш код блокировки защищает настройки функции защиты от кражи. Перед изменением настроек функции защиты от кражи необходимо ввести текущий код блокировки.

4. Если требуется заблокировать устройство в случае смены SIM-карты, выберите **Да** рядом с пунктом **Блокировать при смене SIM-карты**.

Использование защиты от кражи в удаленном режиме

Функция удаленной защиты от кражи позволяет отправить на устройство текстовое SMS-сообщение с кодом блокировки, чтобы определить местоположение устройства, заблокировать его или стереть с него всю информацию.

Настройка удаленного режима для функции защиты от кражи

1. Перейдите к меню **Настройки** и нажмите кнопку выбора.
2. Выберите **Защита от кражи** в списке выбора настроек.
3. Чтобы иметь возможность заблокировать устройство в удаленном режиме, выполните следующие действия.
 - a. Введите **код блокировки**, если он еще не задан.
 - b. Включите функцию **Удаленная блокировка**.

Заблокированное устройство можно разблокировать только с помощью кода блокировки.


4. Чтобы иметь возможность стереть данные с устройства в удаленном режиме, выполните следующие действия.
 - a. Введите **код стирания**. Код стирания должен содержать минимум 8 символов. Сохраните его в надежном месте.
 - b. Включите функцию **Удаленное стирание**.

При очистке устройства все сохраненные на нем данные удаляются безвозвратно.

Чтобы заблокировать устройство или стереть с него все данные в удаленном режиме, выполните следующие действия.

Отправьте следующее SMS-сообщение на устройство.

- Чтобы заблокировать устройство, отправьте сообщение:
#LOCK#<код блокировки> (например, #LOCK#abcd1234)
- Чтобы стереть устройство, отправьте сообщение:
#WIPE#<код стирания> (например, #WIPE#abcd1234)
- Чтобы определить местоположение устройства, отправьте сообщение:
#LOCATE#<код блокировки> (например, #LOCATE#abcd1234)

-  *Anti-Theft не хранит данные о местоположении, сведения о местоположении находятся только в SMS-сообщении, отправленном вам.*

5. Защита при просмотре Интернета

Защита при просмотре Интернета предотвращает доступ к веб-узлам, которые могут выкрасть личные данные, включая номера кредитных карт, данные учетных записей и пароли.

Функция защиты при просмотре Интернета проверяет веб-узлы, просматриваемые с помощью веб-обозревателя по умолчанию. Если используется сторонний обозреватель, защита при просмотре Интернета не обеспечивается.



Выключите веб-обозреватель и очистите кэш, прежде чем включать защиту при просмотре Интернета.

Чтобы включить защиту при просмотре Интернета, выполните следующие действия.

1. Перейдите к меню **Настройки** и нажмите кнопку выбора.
2. Выберите **Защита при просмотре Интернета** в списке выбора настроек.
3. Включите параметр **Защита при просмотре Интернета**.
4. В поле **Используемая сеть** выберите режим работы защиты при просмотре Интернета: постоянно или только при использовании сети своего оператора.
 - Выберите **Только мой оператор**, чтобы защита при просмотре Интернета была активна, только когда используется сеть своего оператора.
 - Выберите **Все операторы**, чтобы защита была включена даже за пределами зоны действия своего оператора.

Положение о конфиденциальности

Функция защиты при просмотре Интернета может автоматически отправлять для анализа сведения о веб-узлах с вредоносным содержимым с целью повышения качества обслуживания. В настройках можно выбрать, какая информация должна передаваться для анализа.

Чтобы изменить режим конфиденциальности, выполните следующие действия.

1. Перейдите к меню **Настройки** и нажмите кнопку выбора.
2. Выберите **Другие настройки** в списке выбора настроек.
3. В области »Режим конфиденциальности« выберите один из следующих вариантов.
 - Выберите **Только статистика**, чтобы отправлять статистику о защите при просмотре Интернета и информацию о подключении к серверу.
 - Выберите **Разрешить все**, чтобы отправлять статистику и информацию о веб-узлах, которые не были проанализированы или имели вредоносное содержимое.



*Для обеспечения наилучшего качества обслуживания рекомендуется оставить режим конфиденциальности **Разрешить все**.*

Положение о конфиденциальности

Отправка информации не ставит под угрозу конфиденциальность пользователя.

Несмотря на то, что отправляемая информация может рассматриваться в некоторых юрисдикциях как личная, в процессе ее передачи обеспечивается надлежащая конфиденциальность. Информация передается по защищенным каналам, излишние личные сведения удаляются, после чего данные обрабатываются анонимно вместе с данными, полученными от других пользователей. Таким образом, эта информация никак не может быть связана с конкретными пользователями. Отправляемая информация не содержит данных учетной записи, IP-адреса или сведений о лицензии. Для обеспечения дополнительной безопасности информация передается в зашифрованном виде.

Отправляемая информация используется для усовершенствования защитных качеств предоставляемых служб и продуктов.

6. Обновление продукта

Автоматические обновления

F-Secure Mobile Security включает службу автоматического обновления, которая предусматривает регулярное обновление базы данных с описанием вирусов. Только обновленная база данных с описанием вирусов может защитить устройство от новейших вирусов. Функция автоматического обновления может использоваться после активации продукта.

Для выполнения обновления для приложения необходимо наличие активного подключения к Интернету. Если доступно подключение к Интернету, приложение проверяет, когда база данных с описанием вирусов обновлялась в последний раз. При необходимости выполняется загрузка обновлений.

Ручные версии

Чтобы обновить приложение, выполните следующие действия.

1. Перейдите к меню **Защита от вирусов** и нажмите кнопку выбора.
2. Выберите **Обновить сейчас**.
3. Выберите точку доступа в Интернет для подключения к серверу обновлений. Будет выполнена автоматическая загрузка последней версии базы данных с описанием вирусов, которая немедленно начнет использоваться.
4. После завершения обновления выберите ответ **Да** на вопрос, произвести ли поиск вирусов на устройстве. См. раздел **Поиск вирусов** выше.

Обновления версии

Если доступна новая версия F-Secure Mobile Security, отображается сообщение с предложением загрузить ее. По завершении обновления приложение автоматически перезапускается.

Техническая поддержка

В главном окне пользовательского интерфейса отображается сводка безопасности и текущее состояние.

Если в этом окне сообщается, что устройство не защищено, выполните следующие действия.

1. Перейдите к меню **Обзор безопасности** и нажмите кнопку выбора.
2. Выберите элемент с красным или желтым значком состояния и нажмите кнопку выбора, чтобы устранить проблему.

Для получения дополнительных сведений загрузите руководство пользователя *F-Secure Mobile Security for S60 User's Guide* (доступно на английском языке) с веб-узла <http://mobile.f-secure.com/>

Если возникли вопросы, ответы на которые не содержатся в руководствах или интерактивных службах, можно связаться с распространителем F-Secure или обратиться напрямую в корпорацию F-Secure.

ЗАЯВЛЕНИЕ ОБ ОТКАЗЕ ОТ ОТВЕТСТВЕННОСТИ

«F-Secure» и символ-треугольник являются охраняемыми товарными знаками корпорации F-Secure, названия продуктов, символы и логотипы F-Secure являются охраняемыми товарными знаками корпорации F-Secure. Все названия продуктов, упомянутые в данном документе, являются товарными знаками или охраняемыми товарными знаками соответствующих владельцев. Корпорация F-Secure отказывается от имущественного права по отношению к торговым знакам и названиям других продуктов. Хотя корпорация F-Secure прилагает все усилия для обеспечения точности приводимых сведений, корпорация F-Secure не будет нести ответственности за любые ошибки или пропуски фактов, имеющиеся в данном документе. Корпорация F-Secure сохраняет за собой право изменять сведения, приводимые в этом документе, без предварительного уведомления.

Компании, имена и даты, используемые в этом документе в качестве примеров, являются вымышленными, если не оговорено иное. Никакая часть настоящего документа не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами, будь то электронные или механические, если на то нет письменного разрешения корпорации F-Secure.

Этот продукт может быть защищен одним или несколькими патентами F-Secure, включая следующие:
GB2353372, GB2366691, GB2366692, GB2366693, GB2367933, GB2368233, GB2374260

© Корпорация F-Secure, 2009 г. Все права защищены.

