

Инструкция по работе с антивирусом «Айс Щит»

Оглавление

1. Введение
 2. Интерфейс и структура программы
 3. Вход в личный кабинет
 - 3.1. Где вводить номер
 - 3.2. Как происходит подтверждение
 4. Личный кабинет
 - 4.1. Подписки и возможности тарифов
 - 4.2. Активация по коду
 - 4.3. Привязка и отвязка устройств
 5. Основные разделы программы
 - 5.1. Профиль
 - 5.2. Защита (главный экран)
 - 5.3. Поиск угроз
 - Полное сканирование
 - Быстрое сканирование
 - Сканирование по расписанию
 - 5.4. Режимы защиты
 - 5.5. Обновления баз
 - 5.6. Журнал угроз
 - 5.7. Настройки программы
 - 5.8. Поддержка
 6. Реакция на угрозы
 7. Как исключить файлы из проверки
 8. Поддержка
-

1. Введение

"Айс Щит" — универсальный антивирусный продукт, предназначенный для защиты компьютера от вирусов, троянов, вредоносных программ, веб-угроз и прочих атак.

Система включает:

- Сканер файлов

- Защиту в реальном времени
 - Веб-защиту
 - Искусственный интеллект
 - Обновляемые базы угроз
 - Облачную проверку
-

2. Интерфейс

Слева находится панель переключения разделов:

Домой

Профиль

Защита

Режимы

Обновление

Журнал

Настройки

Поддержка

3. Вход в личный кабинет

! Важное уточнение:

Программа НЕ спрашивает телефон при первом запуске.

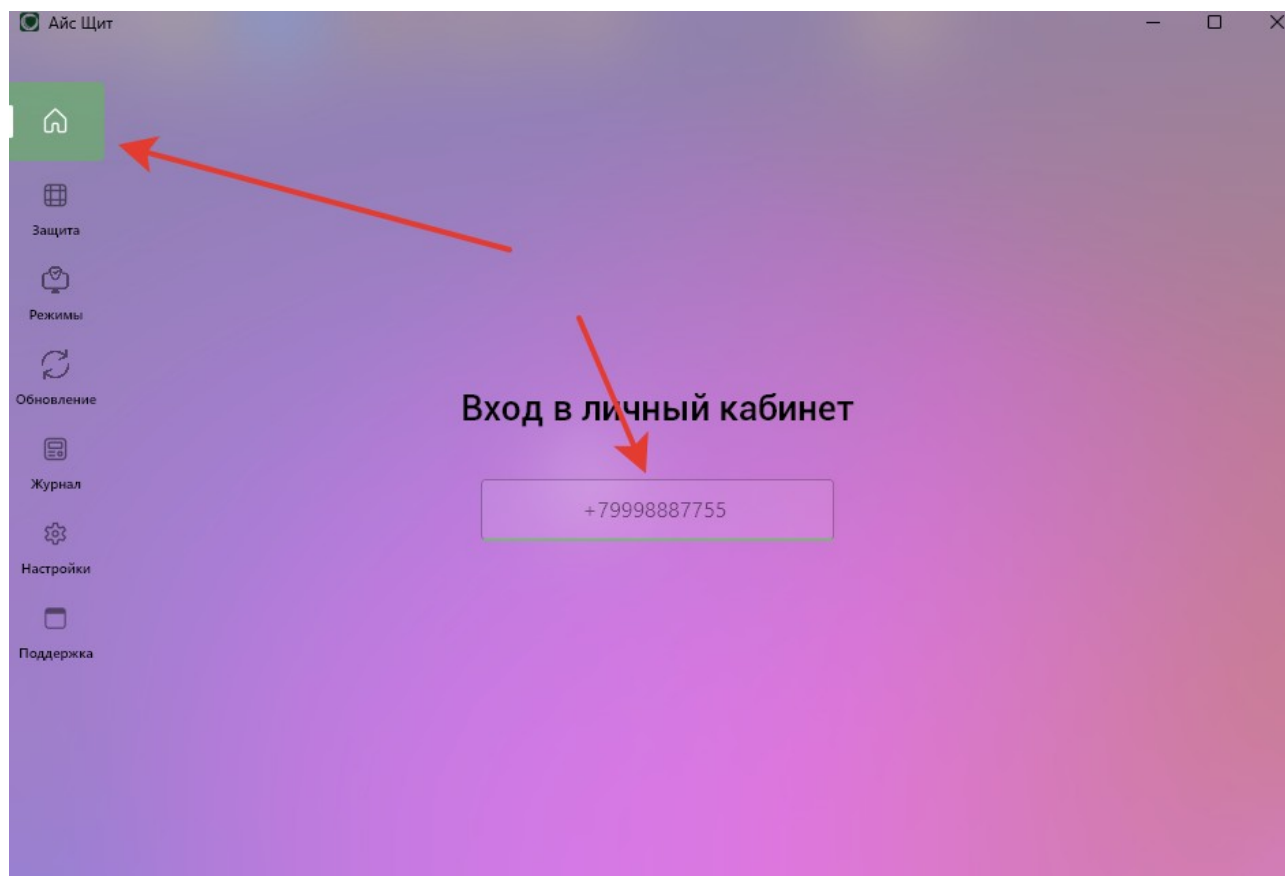
Она открывается на вкладке "Защита".

Чтобы войти в личный кабинет:

3.1. Шаг 1 — нажмите "Профиль"

Вы попадёте на окно входа

3.2. Шаг 2 — введите номер телефона



3.3. Подтверждение телефона

Подтверждение происходит через:

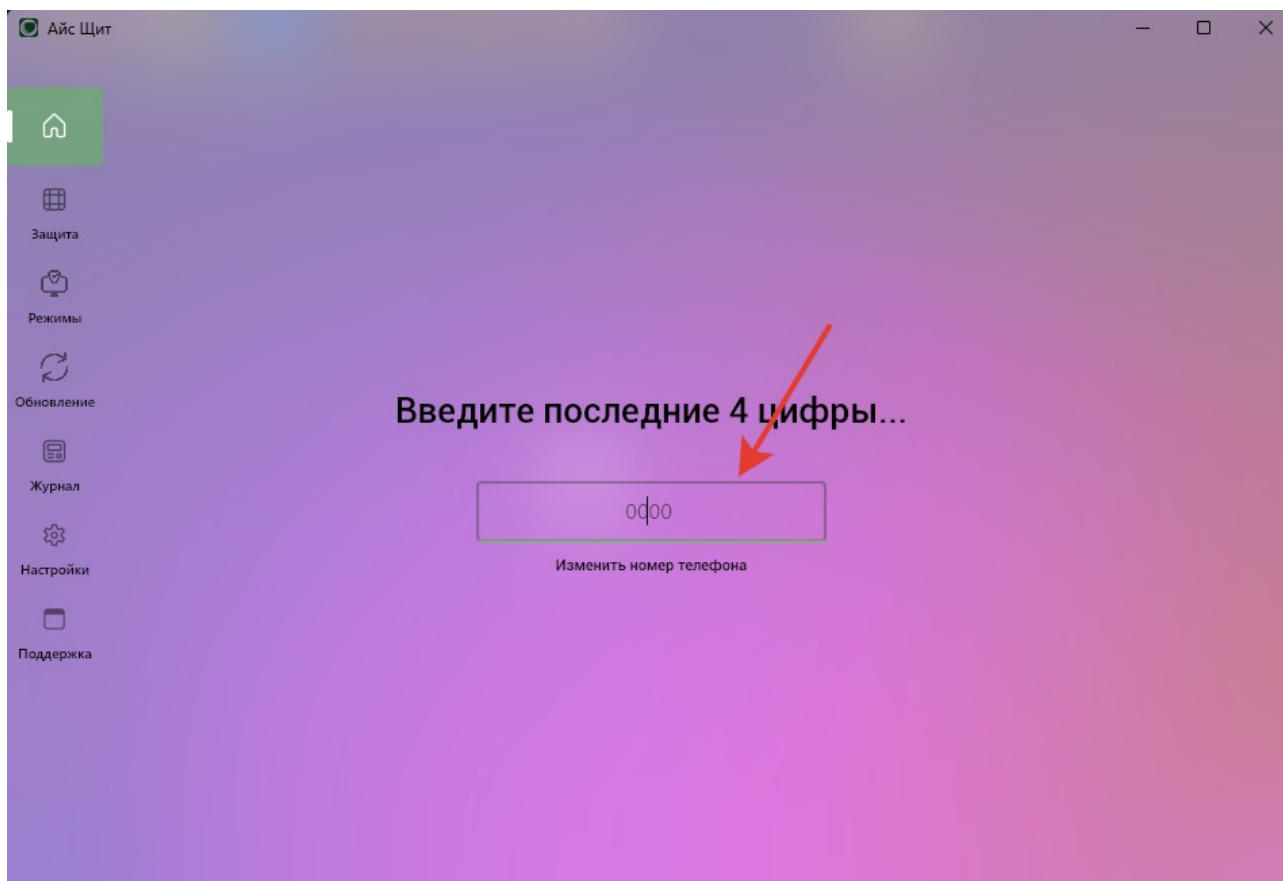
- звонок на номер
- либо автоответчик
- либо последние 4 цифры номера

Нужно:

■ Ввести в поле последние **4 цифры**

— или —

■ Прослушать код в голосовом сообщении



4. Личный кабинет

В нём есть:

- подписки
- количество устройств
- данные учётной записи
- поле для активации кода
- список привязанных устройств

4.1. Тарифы

Тариф — это активная подписка, которая определяет, какие именно возможности антивируса доступны пользователю.

Тариф влияет на:

- срок работы защиты
- сколько устройств можно защитить
- доступ к обновлениям

- работу облачных функций
- работу защиты в реальном времени
- поддержку и техподдержку
- доступные модули защиты

Когда срок тарифа заканчивается:

- защита отключается
- модули перестают обновляться
- новые устройства привязать нельзя
- программы могут начать выдавать предупреждения

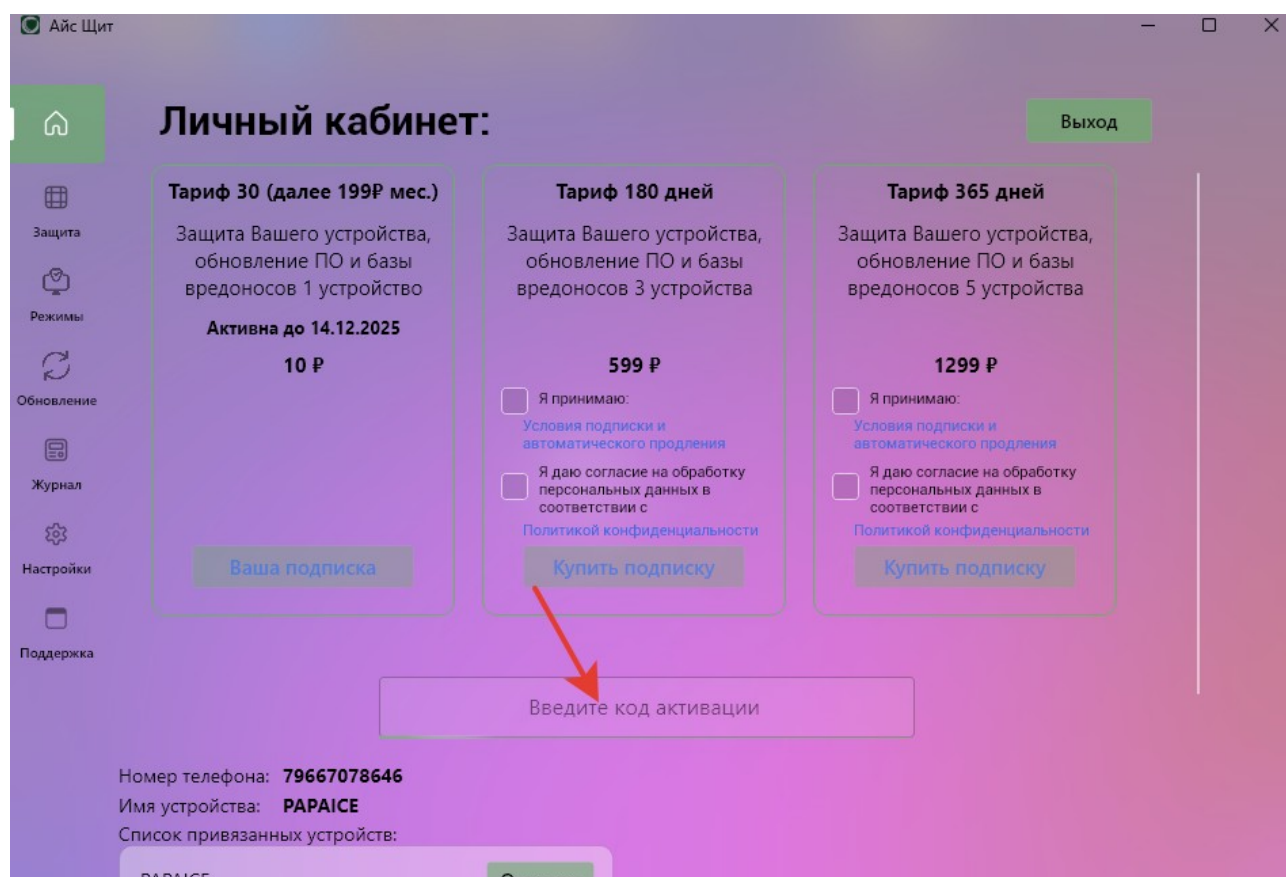
4.2. Активация через код

Если у вас есть:

- промокод
- ключ активации

Вводим в поле:

"Введите код активации"



4.3. Привязка устройств

Если устройство **ещё не привязано** — появится кнопка:

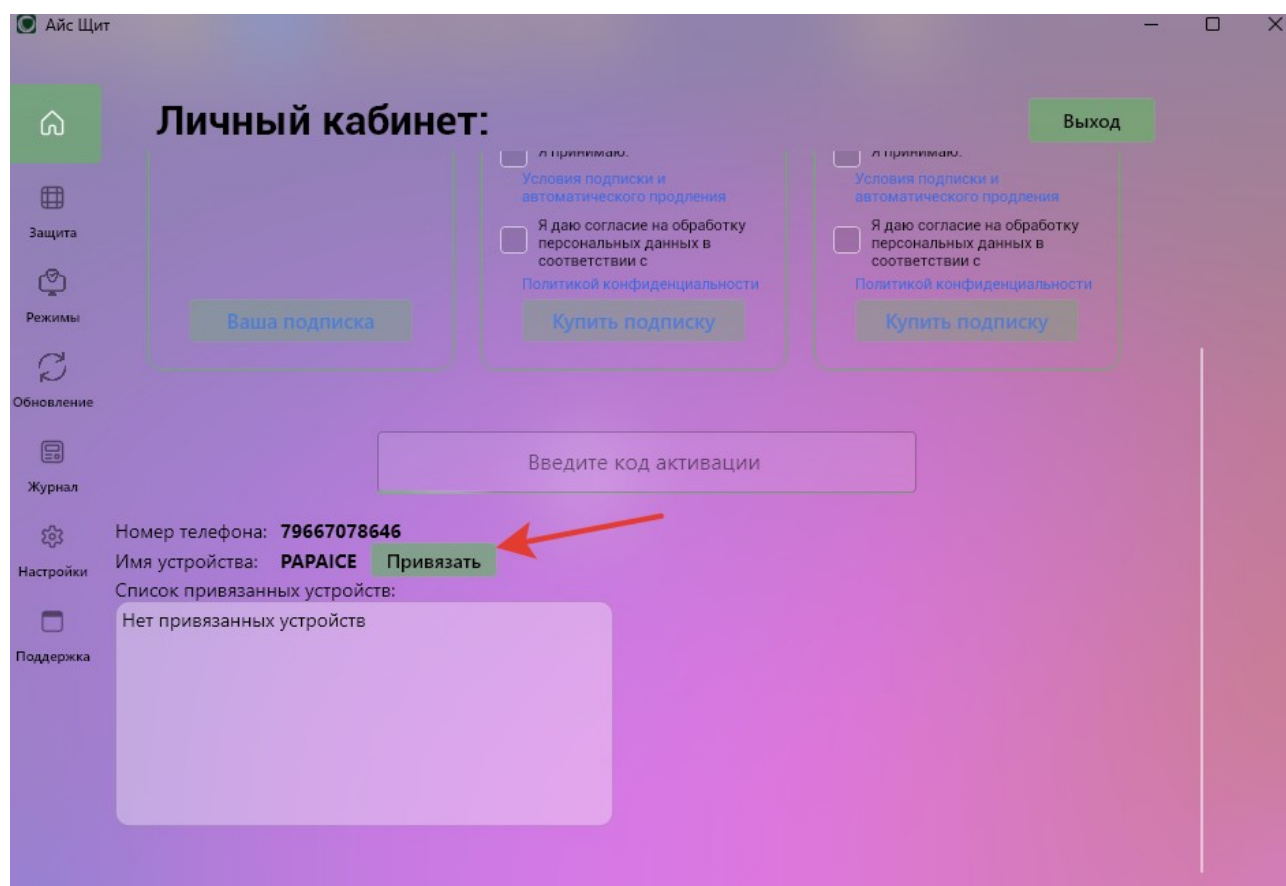
Привязать

Если уже привязано, будет список устройств и кнопка:

Отвязать

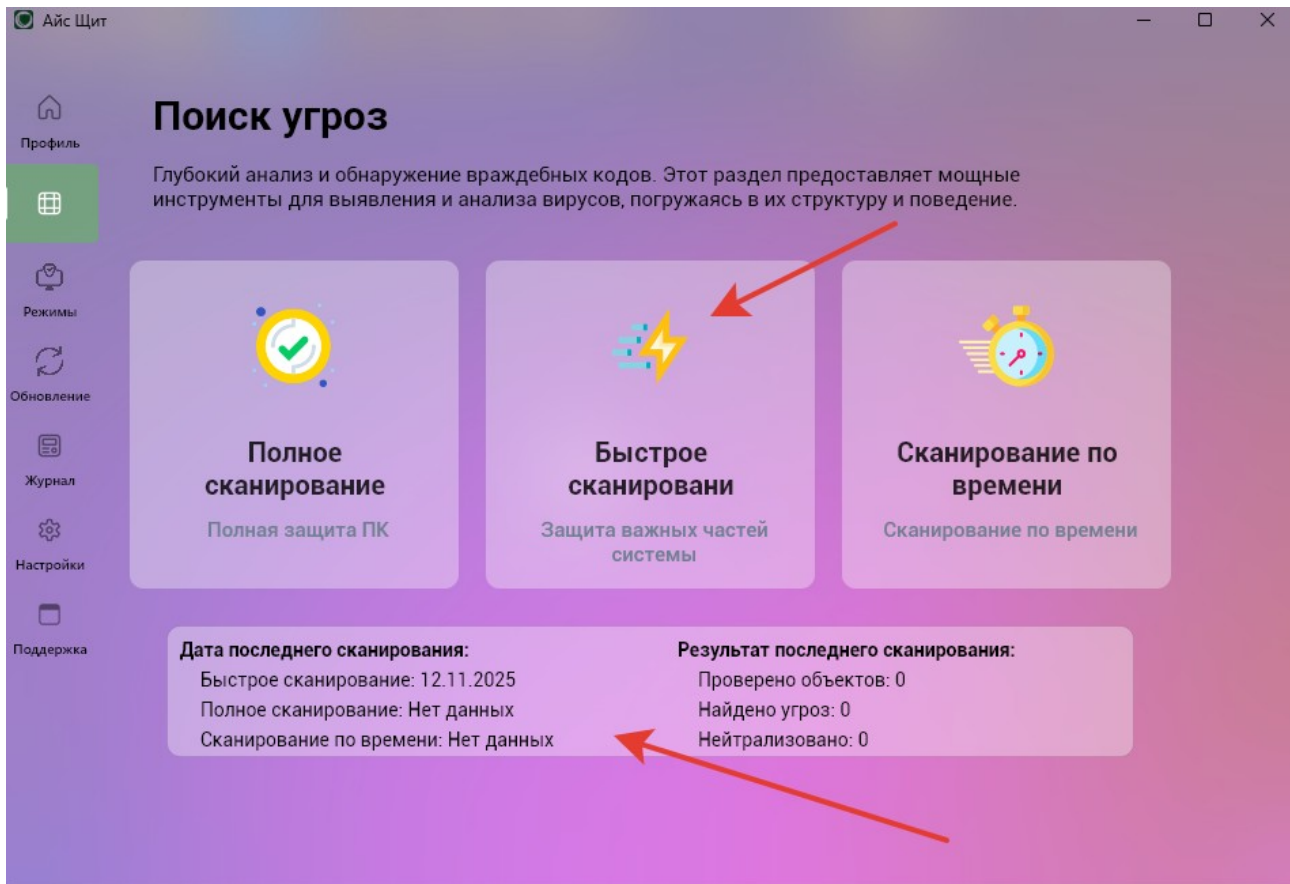
⚠ **Важно:**

Количество устройств зависит от тарифа.



5. Основные разделы

5.1. Защита (главный экран)



Раздел, который открывается первым.

Тут можно:

- начать сканирование
- увидеть состояние системы

5.2. Поиск угроз

1) Полное сканирование

Проверяет весь компьютер:

- системные папки
- скрытые файлы
- всю файловую систему

2) Быстрое сканирование

Проверяет:

- основные зоны заражения
- системные процессы

3) Сканирование по времени

Функция **сканирования по времени** — это автоматическая проверка системы, которая запускается **без участия пользователя**, строго по заранее заданному графику.

Она позволяет обеспечить постоянную защиту **даже если вы забыли запустить проверку вручную**.

Можно выбрать:

- день недели
- время
- тип сканирования

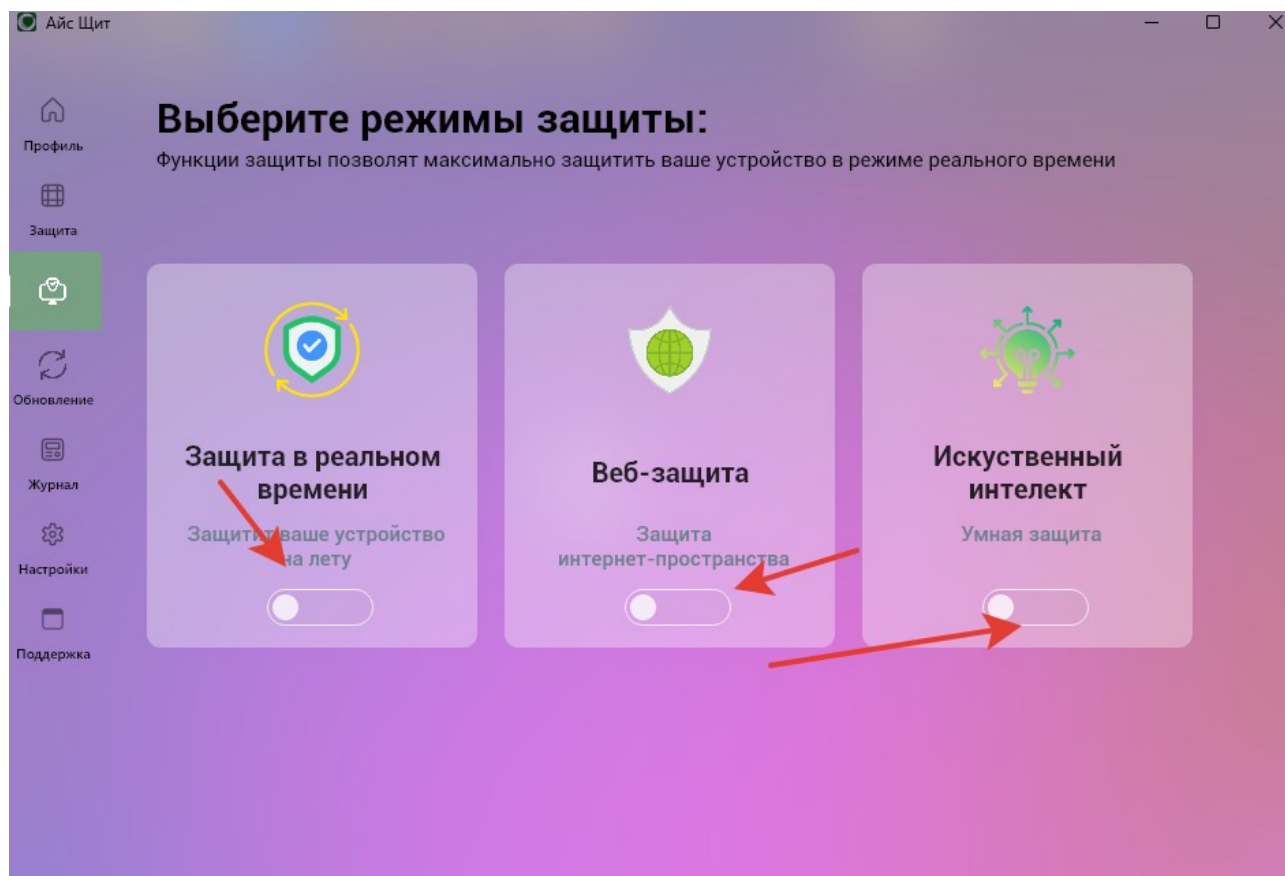
Нажимаем:

Применить

Сканирование по расписанию особенно полезно, если:

- ✓ компьютер работает круглосуточно
 - ✓ вы часто скачиваете файлы
 - ✓ пользуетесь флешками
 - ✓ нужно регулярное автоматическое лечение
 - ✓ вы хотите систематически проверять ПК, но не вручную
 - ✓ вы системный администратор и управляете несколькими ПК
-

5.3. Режимы защиты



Раздел "**Режимы**" позволяет управлять тремя ключевыми механизмами, обеспечивающими постоянную, активную и интеллектуальную защиту вашего устройства.

Эти режимы работают **в фоновом режиме**, не мешая пользователю, и предотвращают угрозы **ещё до того, как они нанесут вред системе**.

Защита в реальном времени

Защита в реальном времени — это механизм, который **активно сканирует все действия в системе**, а именно:

- ✓ Файлы, которые открываются
- ✓ Программы, которые запускаются
- ✓ Файлы, которые скачиваются из интернета
- ✓ Архивы при распаковке
- ✓ Файлы, которыми обмениваются программы

Веб-защита

Веб-защита фильтрует вредоносные URL.

Искусственный интеллект

Определяет неизвестные угрозы

Они включаются переключателем.

5.5. Обновления

Раздел сообщает:

- нужен ли апдейт
- какие базовые модули устарели

Есть кнопка:

Обновить — принудительная проверка обновления .

5.6. Журнал

Здесь отображается:

- название угрозы
- путь к файлу

в данном разделе есть возможность восстановить файл из временного хранилища либо удалить полностью.

5.7. Настройки

Параметры:

- автозапуск(запускать ли программу вместе с windows)
 - автообновления(программа сама будет обновлять все компоненты по мере появления)
 - рекламные уведомления
 - уведомления о блокировке сайтов
-

6. Журнал

Если найден вирус:

Экран:

Найдено 1 вредоносных объектов

Указано:

- Уровень уверенности
- Путь к вирусу

Доступны 2 действия:

 **Восстановить**

(если это ложное срабатывание)

 **Удалить**

(если это угроза)

7. Исключения из проверки

Раздел:

Файловая защита

Можно:

- Добавить файл
- Добавить папку

Это полезно для:

- модов
- игр
- разработчиков
- подписанных программ

Записи можно удалить кнопкой с корзиной.

8. Поддержка

Есть 2 варианта:

Telegram-бот

Email-поддержка