ИНСТРУКЦИЯ
по безопасности при работе в мессенджере MAX
для преподавателей, сотрудников и студентов ВВГУ

Редакция 1.1 от 19.11.2025 г.

Мессенджер MAX широко применяется во Владивостокском государственном университете для деловой коммуникации. От того, насколько грамотно и безопасно преподаватели, сотрудники и студенты пользуются им, напрямую зависят конфиденциальность и сохранность персональных данных, переписки и служебной информации.

Данная инструкция, основанная на официальной документации MAX, предназначена для преподавателей, сотрудников и студентов университета и поможет им:

- настроить базовую защиту;
- избежать типичных рисков;
- обеспечить максимально безопасную работу в сервисе при решении повседневных задач.

ВНИМАНИЕ!

Для дополнительной защиты вашего аккаунта **настоятельно рекомендуется установить пароль для входа в MAX** (см. ниже, п.1.1).

В целях безопасности **НИКОГДА И НИ ПРИ КАКИХ ОБСТОЯТЕЛЬСТВАХ НЕ СООБЩАЙТЕ 6-ЗНАЧНЫЙ КОД ИЗ SMS И/ИЛИ ПАРОЛЬ ДЛЯ ВХОДА В MAX КОМУ БЫ ТО НИ БЫЛО.** Это предотвратит несанкционированный доступ третьих лиц к вашему аккаунту в MAX.

1. НАСТРОЙКА ПАРАМЕТРОВ БЕЗОПАСНОСТИ И КОНФИДЕНЦИАЛЬНОСТИ

1.1. Установка пароля для входа в MAX

Установка **пароля для входа** – это способ усилить безопасность вашего аккаунта в MAX за счет так называемой двухфакторной аутентификации (2FA), при которой вход в профиль, помимо 6-значного кода из SMS, дополнительно подтверждается вторым фактором – паролем. Благодаря этому, даже если злоумышленник каким-либо образом узнает 6-значный код для входа в мессенджер, он все равно не сможет войти в ваш профиль MAX, поскольку не будет знать пароля. Вы самостоятельно устанавливаете этот пароль в настройках вашего аккаунта.

Для установки пароля для входа в MAX:

1. Перейдите в раздел **Профиль → Приватность.**
2. Выберите пункт **Пароль для входа.**
3. Нажмите **Установить пароль.**
4. Укажите пароль, который будет использоваться при новом входе в профиль.
5. Установите подсказку (не обязательно).
6. Укажите адрес электронной почты. Он будет использоваться для восстановления доступа к аккаунту, если вы забудете пароль.
7. На указанный адрес электронной почты будет отправлен код подтверждения. Введите его.
8. Нажмите **Перейти в настройки**, чтобы завершить процесс установки пароля. Двухфакторная аутентификация настроена.

Изменить или отключить пароль для входа в MAX можно в том же меню: **Профиль → Приватность → Пароль для входа.**

Примечание: на мобильном устройстве вход в **Профиль** располагается в правом нижнем, а на компьютере и в браузере – в левом нижнем углу окна приложения.

1.2. Настройки приватности в приложении

Перейдите в **Профиль → Приватность** и настройте параметры приватности в соответствии с таблицей.

Таблица 1. Параметры приватности в мессенджере MAX

Наименование параметра	Назначение параметра	Варианты настройки параметра
Поиск по номеру телефона	Ограничение круга людей, которые могут найти вас по номеру телефона в MAX	• Все • Контакты Во втором случае ваш контакт в MAX получится найти по номеру телефона только при условии, что вы и ваш собеседник есть друг у друга в телефонной книге.
Звонки	Ограничение круга людей, которые могут вам звонить в MAX	• Все • Контакты Во втором случае позвонить вам через MAX получится только при условии, что вы и ваш собеседник есть друг у друга в телефонной книге.
Приглашения	Ограничение круга людей, которые могут приглашать вас в чат	• Все • Контакты Во втором случае пригласить вас в чат получится только при условии, что вы и приглашающий есть друг у друга в телефонной книге.
Предупреждение о файлах для установки	Активация дополнительного предупреждения о попытке передачи, загрузки или открытия	• Да • Нет

	файлов, которые могут содержать вредоносные программы	Рекомендуется включить эту опцию, чтобы снизить риск заражения вредоносными файлами.
Статус «в сети»	Настройка видимости вашего статуса «в сети»	• Контакты (ваш статус в сети видят только ваши контакты) • Никто (ваш статус «в сети» не видит никто)

1.3. Безопасный режим

В MAX есть специальный безопасный режим. Это набор настроек приватности, в которых вы можете:

- скрыть свой профиль из поиска;
- принимать звонки только от людей из списка контактов;
- получать приглашения в чаты только с людьми из списка контактов.

Безопасный режим автоматически включает настройки, при которых найти вас и связаться с вами получится только в случае, если вы и ваш собеседник есть друг у друга в телефонной книге или профиль собеседника добавлен в контакты MAX.

Как активировать безопасный режим:

1. Перейдите в **Профиль → Приватность**.
2. Нажмите на переключатель справа от надписи «Безопасный режим».
3. Нажмите кнопку «Включить».

Примечание: безопасный режим можно активировать только в мобильном приложении.

1.4. Управление активными сессиями

Регулярно проверяйте список устройств, с которых выполнен вход в ваш аккаунт:

1. Откройте **Профиль → Приватность**.
2. В разделе «Сессии» проверьте список активных устройств.
3. Завершите сессии на незнакомых или неиспользуемых устройствах, используя пункт меню «Завершить все сессии кроме текущей».

1.5. Черный список

В MAX имеется черный список, т.е. список тех, кто не может вам писать, звонить и добавлять в чаты. Для того чтобы добавить собеседника в черный список в мобильном приложении, перейдите в список чатов или контактов, нажмите на соответствующий чат/контакт и удерживайте палец до появления меню с дополнительными действиями. В появившемся меню выберите пункт «Заблокировать».

Примечание: в приложениях MAX для ПК и в веб-версии добавить контакт в черный список можно, щелкнув правой кнопкой мыши по соответствующему чату/контакту и выбрав в появившемся меню пункт «Заблокировать».

Управлять черным списком можно через меню **Профиль → Приватность → Черный список.**

1.6. Управление разрешениями мобильного приложения MAX

MAX запрашивает доступ к различным функциям вашего устройства. Управление разрешениями мобильного приложения MAX осуществляется через настройки телефона. В таблице ниже показано, как предоставить приложению MAX максимально возможные разрешения (если этого не было сделано при установке приложения).

Таблица 2. Управление разрешениями мобильного приложения MAX

Android	Подключить контакты Перейдите в **Настройки телефона** → **Приложения** → **Все приложения** → **MAX** → **Разрешения приложений** → **Контакты** → **Разрешить** Включить уведомления Перейдите в **Настройки** телефона → **Приложения** → **Все приложения** → **MAX** → **Уведомления** → **Показывать все уведомления** приложения MAX Доступ к камере Перейдите в **Настройки** телефона → **Приложения** → **Все приложения** → **MAX** → **Разрешения приложений** → **Камера** → **Разрешить** Галерея Перейдите в **Настройки** телефона → **Приложения** → **Все приложения** → **MAX** → **Разрешения приложений** → **Файлы и медиаконтент** → **Разрешить** Доступ к микрофону Перейдите в **Настройки** телефона → **Приложения** → **Все приложения** → **MAX** → **Разрешения приложений** → **Микрофон** → **Разрешить**
iPhone	Подключить контакты Перейдите в **Настройки** телефона → **Приложения** → **MAX** → **Контакты** → разрешить **Полный доступ** Включить уведомления Перейдите в **Настройки** телефона → **Приложения** → **MAX** → **Уведомления** → включить **Допуск уведомлений** Доступ к камере Перейдите в **Настройки** телефона → **Приложения** → **MAX** → включить **Камера** Фото Перейдите в **Настройки** телефона → **Приложения** → **MAX** → Фото → разрешить **Полный доступ** Доступ к микрофону Перейдите в **Настройки** телефона → **Приложения** → **MAX** → включить **Микрофон**

2. ПРАВИЛА БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ И ЗАЩИТА ОТ МОШЕННИЧЕСТВА

2.1. Общие принципы цифровой гигиены

Не делитесь в любых мессенджерах, в том числе в MAX, чувствительной информацией: не отправляйте пароли, финансовые данные, сканы документов или любую другую информацию, утечка которой может вам навредить.

Что НЕ СЛЕДУЕТ отправлять через MAX:

- пароли от любых систем и сервисов;
- банковские реквизиты и данные карт;
- сканы паспортов, СНИЛС, водительских удостоверений и других документов;
- персональные данные (как свои, так и принадлежащие другим лицам);
- коды двухфакторной аутентификации;
- конфиденциальную служебную информацию;
- информацию, составляющую коммерческую или государственную тайну.

2.2. Правила безопасности при использовании мессенджеров

Несмотря на меры безопасности, которые предпринимают разработчики мессенджера MAX и других мессенджеров, их пользователи нередко становятся жертвами мошенников. Для защиты от мошенничества придерживайтесь нескольких простых правил.

1. Никогда не сообщайте:

- коды из SMS;
- пароли от любых систем и сервисов;
- данные банковских карт;
- ПИН-коды.

2. Проверяйте поступающую информацию:

- перезванивайте на официальные номера организаций;
- перезванивайте людям при получении от них подозрительных сообщений;
- проверяйте подлинность ссылок;
- не переходите по подозрительным ссылкам;
- не открывайте подозрительные документы;
- не устанавливайте подозрительные программы.

3. Будьте бдительны! Вот типичные признаки мошенничества, которые должны вас насторожить:

- вам позвонили или написали сообщение и представились ректором, проректором университета, главным бухгалтером, директором института, заведующим кафедрой, сотрудником полиции, ФСБ, Центробанка, Росфинмониторинга, Роскомнадзора и т.д.;
- требуют перевести деньги, в том числе «на безопасный счет»;
- запрашивают коды из SMS;
- давят и запугивают;
- предлагают установить дополнительное ПО для «защиты»;
- требуют от вас немедленных действий.

Действия при обнаружении мошенничества

1. Немедленно прекратите общение с мошенниками.
2. Не выполняйте их требования.
3. Заблокируйте подозрительный контакт.
4. Подайте жалобу через функционал MAX (см. ниже).
5. Обратитесь в правоохранительные органы.
6. Уведомите службу безопасности университета (если предполагаемое мошенничество касается университета).
7. Если передали банковские данные – немедленно свяжитесь с банком.

2.3. Функция подачи жалобы

В мессенджере MAX имеется кнопка «Пожаловаться», которая позволяет пользователям отправлять жалобы модераторам мессенджера.

Когда подавать жалобу:

- спам и массовые рассылки;
- мошенничество и фишинг;
- оскорбления и угрозы;
- распространение вредоносных ссылок;
- попытки социальной инженерии.

Как подать жалобу:

1. Нажмите на подозрительное сообщение.
2. Выберите «Пожаловаться» (на компьютере или в браузере – щелкните по нему правой кнопкой мыши).
3. Укажите причину жалобы.
4. Подтвердите отправку.

3. Дополнительные меры безопасности

3.1. Резервное копирование важной информации

Ни один мессенджер, в том числе MAX, не гарантирует постоянное хранение переписки, поэтому целесообразно сохранять важную информацию и файлы на локальном компьютере, в облачном хранилище; делать и сохранять копии или скриншоты важных фрагментов переписки.

3.2. Безопасность учетной записи

Регулярно:

- проверяйте активные сессии (см. п. 1.4);
- обновляйте приложение до последней версии;
- проверяйте настройки приватности (они могут меняться после обновлений);
- меняйте пароль для входа в MAX (см. п. 1.1).

При смене/утере телефона:

- необходимо завершить все активные сессии (см. п. 1.4);
- рекомендуется измените пароль для входа в MAX (см. п. 1.1).

Мессенджер MAX – это полезный инструмент для оперативной деловой коммуникации в университете. Однако, как и любой цифровой сервис, он требует ответственного и осознанного использования. При соблюдении всех рекомендаций, изложенных в данной инструкции, использование мессенджера MAX будет максимально безопасным и эффективным.