



# Безопасность и конфиденциальность на [monday.com](https://monday.com)



# Ответы на часто задаваемые вопросы

## Получите ответы на все вопросы

В этом документе вы найдете ответы на часто задаваемые вопросы о безопасности и конфиденциальности на платформе monday.com, безопасности приложения и инфраструктуры, а также сведения об API и о том, как мы реагируем на инциденты. Мы постарались осветить здесь наиболее распространенные темы, но если у вас есть дополнительные вопросы или желание уточнить информацию, вы можете в любое время обратиться в нашу службу поддержки по адресу [support@monday.com](mailto:support@monday.com).

### Содержание

Корпоративная безопасность .....	1
Безопасность приложения .....	4
Безопасность инфраструктуры .....	7
Реагирование на инциденты .....	9
Варианты интеграции .....	10

## Корпоративная безопасность

### 1 В. Есть ли у monday.com официальная программа информационной безопасности?

О. Да. Эта программа составлена с учетом требований местного и международного законодательства, стандартов и норм, применимых к деятельности monday.com. Она определяет, какие меры и средства контроля мы разработали и применяем для защиты сервиса monday.com и данных клиентов. Эта программа составлена на основе стандарта ISO 27001. Область ее действия распространяется на всю организацию monday.com, включая ее дочерние компании, сотрудников, подрядчиков, субподрядчиков, партнеров и иных лиц, создающих, поддерживающих, осуществляющих хранение, обработку или передачу информации платформы monday.com или ее пользователей, а также осуществляющих доступ к ней в связи с предоставлением услуг, оказываемых monday.com.

## 2 В. Каким нормам, стандартам и сертификатам в области безопасности и конфиденциальности данных соответствует monday.com на дату создания этого документа?

О. У нас есть следующие сертификаты, отчеты и программы, обеспечивающие соблюдение нами требований законодательных и иных нормативных актов:



Вы найдете все наши сертификаты [здесь](#).

## 3 В. Есть ли у monday.com специально назначенные сотрудники, занимающиеся обеспечением безопасности?

О. Да. Наши мероприятия в сфере обеспечения безопасности осуществляются и контролируются Службой безопасности, а также имеющим более широкие полномочия Советом безопасности, в состав которого входят представители из отделов инфраструктуры, управления исследованиями и разработкой, операционного отдела и ИТ.

## 4 В. Есть ли у monday.com официальный процесс реагирования на изменения в законодательстве, нормативных и иных актах в области конфиденциальности данных?

О. Наш Совет по защите конфиденциальности, в который входят представители юридического отдела, группы обеспечения конфиденциальности и службы безопасности и который возглавляется Уполномоченным по защите данных, непрерывно отслеживает изменения в применимом законодательстве, нормативных и иных актах в области конфиденциальности данных. Совет отвечает за соблюдение нами принципа «Конфиденциальность по умолчанию» (Privacy by Design) и регулярно оценивает последствия новых или предлагаемых вариантов развития продукта и иных инициатив с точки зрения защиты данных.

**5 В. Соответствует ли платформа monday.com стандарту безопасности данных индустрии платежных карт PCI-DSS?**

О. На платформе monday.com используется система обработки платежей, сертифицированная по стандарту PCI-DSS; таким образом, все операции оплаты кредитными картами через используемую нами стороннюю систему обработки платежей соответствуют стандарту PCI-DSS. Сервис monday.com не сертифицирован по стандарту PCI-DSS и, соответственно, не обрабатывает платежную информацию, поэтому данные, в отношении которых требуется соблюдение требований PCI-DSS, на платформе не хранятся.

**6 В. Есть ли у monday.com программа повышения осведомленности об информационной безопасности?**

О. Да. В рамках процедуры первичной адаптации персонала, а также на постоянной основе (не реже раза в год) наши сотрудники проходят инструктаж в отношении своих обязанностей по соблюдению информационной безопасности.

Каждый квартал у нас проходят недели безопасности и конфиденциальности, призванные повысить осведомленность всех сотрудников компании. Кроме того, для разработчиков регулярно проводятся инструктажи (как минимум, раз в год) для ознакомления с мировым опытом в разработке на началах информационной безопасности.

**7 В. Как часто пересматриваются политики информационной безопасности monday.com?**

О. Наши политики информационной безопасности пересматриваются не реже раза в год или в случае существенного изменения нашего сервиса или нашей позиции в отношении обеспечения безопасности и конфиденциальности данных.

**8 В. Есть ли у monday.com Уведомление о конфиденциальности/Политика конфиденциальности?**

О. Да, с нашей Политикой конфиденциальности можно ознакомиться [здесь](#).

**9 В. Привлекает ли monday.com подрядчиков/субподрядчиков по обработке данных, которые получают доступ к персональным данным пользователей?**

**О.** Да, для обеспечения работы нашего сервиса мы пользуемся услугами нескольких субподрядчиков по обработке данных. Список таких субподрядчиков (обрабатывающих данные от имени и в интересах пользователей) с указанием их местоположения и вида оказываемых ими услуг доступен здесь.

По этой же ссылке можно также подписаться на получение по электронной почте уведомлений в случае изменения списка таких субподрядчиков.

## **Безопасность приложения.**

**10 В. Какие данные собирает monday.com?**

**О.** После создания аккаунта мы сохраняем такие персональные данные, как полное имя пользователя, адрес электронной почты и номер телефона. Состав данных, которые мы сохраняем при использовании вами сервиса monday.com, зависит от того, как именно вы используете сервис, а также от типа данных (например, текст, файлы и др.), которые вы или ваши авторизованные пользователи, зарегистрированные в сервисе, отправляют или загружают на платформу monday.com. Дополнительную информацию об этом можно найти в нашей [Политике конфиденциальности](#).

**11 В. Как обеспечивается защита доступа пользователей к сервису monday.com?**

**О.** Доступ к monday.com осуществляется с использованием следующих способов аутентификации:

- Учетные данные: имя пользователя (обычно адрес электронной почты) и пароль.
- Мы также поддерживаем использование сервисов внешних поставщиков удостоверений, таких как SSO Google (служба единого входа Google — только для тарифов 'Pro' и 'Корпоративный'), Okta, OneLogin и пользовательский SAML 2.0 (только для тарифа 'Корпоративный').
- Кроме того, администратор аккаунта может активировать двухфакторную аутентификацию (2FA) по SMS или через приложение для аутентификации.

## **12 В. Позволяет ли monday.com настраивать политику паролей?**

**О.** Мы предлагаем администраторам два варианта настроек надежности паролей в аккаунте: не менее 8 символов без повторяющихся и последовательных символов; не менее 8 символов без повторяющихся и последовательных символов и с обязательным использованием хотя бы одной цифры (123), буквы в нижнем регистре (abc) и буквы в верхнем регистре (ABC).

## **13 В. Используете ли вы шифрование для данных пользователей monday.com? Какие методологии шифрования данных применяются?**

**О.** Да, в сервисе monday.com используются следующие способы шифрования данных пользователей:

- Для шифрования хранимых данных используется алгоритм AES-256.
- Данные, передаваемые по открытым сетям, шифруются с помощью протокола TLS 1.3 (минимум TLS 1.2).
- Пароли пользователей хешируются с солью.

## **14 В. Как обеспечивается безопасность разработки кода для monday.com?**

**О:** Мы используем стандарты оценки уязвимостей OWASP Top 10 и CVSS для обеспечения безопасности в рамках всего цикла разработки программного обеспечения. Весь код, написанный нашими разработчиками, подвергается статистическому анализу и экспертной оценке для обеспечения его качества перед развертыванием. Мы непрерывно оцениваем и проверяем наше приложение на наличие уязвимостей во время и после развертывания.

## 16 В. В течение какого времени monday.com хранит мои данные? Что с ними произойдет, если я прекращу пользоваться сервисом?

О. Клиенты monday.com сохраняют полный контроль над загруженными данными и могут изменить или удалить их в любой момент в течение срока действия подписки средствами, доступными им через пользовательский интерфейс monday.com. Вы можете направить запрос на удаление своих данных в рамках процедуры закрытия аккаунта, выполняемой с панели администратора monday.com. После этого все отправленные вами данные будут удалены в течение 90 дней: в течение первых 30 дней можно отозвать запрос, а следующие 60 дней отводятся на удаление этих данных из наших баз данных и баз данных субподрядчиков по обработке данных. Кроме того, вы можете сохранить данные своего аккаунта даже после его закрытия и отмены подписки. В этом случае нашей текущей политикой предусмотрено сохранение данных, однако при этом мы не берем на себя каких-либо обязательств по конкретному сроку хранения и можем по истечении любого периода удалить данные как с уведомлением, так и без него.

Обратите внимание, что данные из аккаунта можно в любой момент экспортировать в двух форматах:

- доски — в Excel;
- данные всего аккаунта — через панель администратора в виде zip-архива с Excel-таблицами и файлами, загруженными в аккаунт (это действие доступно только администраторам).

## В. Предоставляет ли monday.com журналы аудита с информацией о действиях пользователей на платформе?

О. Да, журналы предоставляются в двух форматах:

- действия на уровне досок фиксируются в [журнале действий](#);
- сведения об успешных/неудачных попытках входа в систему фиксируются в [журнале аудита](#).

**18 В. Какие роли доступны для авторизации в приложении monday.com?**

О. В нашем сервисе доступны следующие роли: администратор, участник, гость и наблюдатель. Подробнее об этом читайте в [этой статье](#).

Помимо ролей, контроль доступа в нашем сервисе осуществляется с помощью таких функций, как [рабочие области](#), [типы досок](#), [разрешения на уровне досок](#), и [разрешения на уровне столбцов](#).

**19 В. Дает ли monday.com возможность третьим лицам сообщать об уязвимостях в системе безопасности сервиса?**

О. Да, об уязвимостях в системе безопасности сервиса можно сообщать по адресу [security@monday.com](mailto:security@monday.com), или через форму HackerOne, доступ к которой можно получить [здесь](#).

## Безопасность инфраструктуры

**20 В. Где расположены центры обработки данных monday.com?**

О. monday.com — полностью облачный сервис с хостингом в инфраструктуре Amazon Web Services, которая физически находится в Северной Вирджинии, и с несколькими разными зонами доступности, а узел для аварийного восстановления (DR) развернут в другом регионе.

Некоторые данные резервного копирования хранятся в Google Cloud Platform (США, несколько регионов). В этих ЦОД реализованы передовые средства физической и экологической безопасности, в результате чего обеспечивается высокая отказоустойчивость инфраструктуры. Более подробные сведения о методах обеспечения безопасности соответствующих сервисов доступны на следующих сайтах:

[страница о безопасности AWS;](#)

[страница о безопасности GCP.](#)



**21 В. Доступна ли локальная версия monday.com?**

О. monday.com — полностью облачный сервис, у нас нет его версии в локальной среде.

**22 В. Как часто выполняется резервное копирование данных?**

В. Мы последовательно выполняем резервное копирование данных пользователей каждые 5 минут и распределяем зашифрованные резервные копии по нескольким зонам доступности AWS, где они хранятся в течение 25 дней. Кроме того, в другом регионе AWS у нас развернут узел аварийного восстановления. Резервные копии данных журнала действий сохраняются в GCP (США, несколько регионов), где они хранятся в течение 7 дней.

**23 В. Есть ли у monday.com план аварийного восстановления?**

О. Да. В нашем плане аварийного восстановления описан порядок действий в случае возникновения чрезвычайных ситуаций, затрагивающих нашу производственную среду, включая восстановление основной функциональности сервиса с DR-площадки. Тестирование проводится не реже двух раз в год.

**24 В. Есть ли у monday.com политика физической безопасности?**

О. Да. Наш сервис является полностью облачным, и ни одна часть его инфраструктуры не развернута в локальной среде. К мерам обеспечения физической безопасности в нашем офисе относится контроль доступа на основе идентификации личности сотрудников, круглосуточное видеонаблюдение и система сигнализации.

**25 В. Как обеспечивается доступность сервиса?**

О. Чтобы свести к минимуму влияние на состояние системы отказа одного или нескольких компонентов, мы используем архитектуру микросервисов. Для обеспечения дополнительного резервирования используется несколько

соответствующему персоналу, коммуникациям (внутренним и внешним), расследованию, минимизации последствий и проведению ретроспективного (post-mortem) анализа. Для дополнительной информации см. раздел 7 «Управление инцидентами, связанными с персональными данными, и уведомления о них» нашего [Соглашения об обработке данных](#).

**29 В. Каким образом monday.com проинформирует меня, если в результате инцидента или утечки были скомпрометированы мои персональные данные?**

О. Форма уведомления зависит от типа, характера и масштаба инцидента. Как минимум, мы отправим письмо администратору(ам) вашего аккаунта. Вы будете проинформированы, насколько это возможно, о характере утечки, неблагоприятных последствиях, о которых известно monday.com, а также о действиях, предпринятых или запланированных monday.com.

## Варианты интеграции

**30 В. Возможен ли доступ к monday.com через API?**

О. Да, с документацией к нашему API GraphQL можно ознакомиться [здесь](#).

**31 В. Поддерживает ли monday.com дальнейшие интеграции с сервисом?**

О. Да, Помимо нашего API, для создания настраиваемых рабочих процессов мы также поддерживаем интеграции с [другими программными решениями](#), в т.ч. Zoom, Slack, Zendesk, Microsoft Teams, Salesforce и Outlook. Это дополнительная возможность, которую можно отключить через панель администратора.

зон доступности AWS; кроме того, у нас есть несколько альтернативных поставщиков услуг.

В соответствии с условиями Соглашения об уровне сервиса ([SLA](#)) для корпоративных клиентов мы гарантируем доступность 99,9%. Кроме того, доступность наших сервисов можно отслеживать на [странице статуса](#), которая также позволяет подписаться на обновления по электронной почте или SMS.

**26 В. Применяет ли monday.com передовой опыт разработки защищенных архитектур?**

О. Да, мы имеем статус [AWS Advanced Technology Partner](#). Он является подтверждением того, что компания AWS тщательно проверила сервис monday.com с точки зрения инфраструктуры, безопасности, применения лучших методик проектирования и т.п.

**27 В. Поддерживает ли monday.com безопасное удаление данных пользователей?**

A: Yes. Our service is hosted on AWS, with certain data backed up to GCP. Both cloud computing providers implement proprietary data distribution and deletion strategies to allow for safe storage and deletion of sensitive data in a multi-tenant environment.

Storage media decommissioning is performed by the aforementioned providers using the techniques detailed in NIST 800-88.

## Реагирование на инциденты

**28 В. Есть ли у monday.com официальный план реагирования на инциденты безопасности?**

О. Да. В нашем плане реагирования на инциденты безопасности описаны внутренние рекомендации по обнаружению инцидентов, их эскалированию