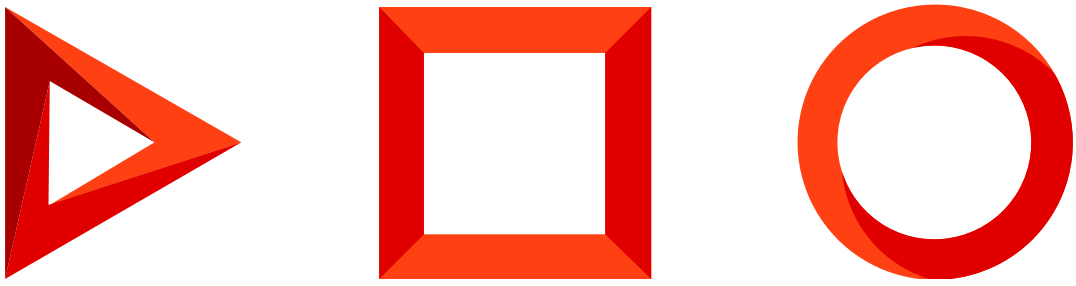
Creatio Academy

# Рекомендации для DNS

## Рекомендации по настройке для популярных DNS-провайдеров

Версия 8.0



Эта документация предоставляется с ограничениями на использование и защищена законами об интеллектуальной собственности. За исключением случаев, прямо разрешенных в вашем лицензионном соглашении или разрешенных законом, вы не можете использовать, копировать, воспроизводить, переводить, транслировать, изменять, лицензировать, передавать, распространять, демонстрировать, выполнять, публиковать или отображать любую часть в любой форме или посредством любые значения. Обратный инжиниринг, дизассемблирование или декомпиляция этой документации, если это не требуется по закону для взаимодействия, запрещены.

Информация, содержащаяся в данном документе, может быть изменена без предварительного уведомления и не может гарантировать отсутствие ошибок. Если вы обнаружите какие-либо ошибки, сообщите нам о них в письменной форме.

# Содержание

# Рекомендации по настройке для популярных DNS-провайдеров

ПРОДУКТЫ: MARKETING

В процессе работы с записями SPF и DKIM учитывайте следующие нюансы:

1. Чтобы изменения, внесенные в настройки DNS-сервера вашего домена вступили в силу, все новые и измененные записи должны пройти проверку на корректность. Время, которое занимает проверка, отличается для каждого провайдера и обычно занимает несколько часов из-за кеширования. Подробную информацию можно найти в документации сервера вашего домена.
2. Возможна ситуация, когда по истечении указанного времени добавленная DKIM-запись не проходит проверку. Причиной могут быть отличия в требованиях разных DNS-серверов к форматированию DKIM-записи. Например, некоторые DNS требуют установки символа “\” перед символом “;” в начале и конце значения DKIM-записи. Некоторые, наоборот, не требуют.
3. При создании DKIM-записи необходимо руководствоваться справочной информацией вашего хостинг-провайдера либо ответами службы поддержки.

Ниже приведены ссылки на сайты часто используемых DNS-провайдеров и описаны некоторые особенности форматирования DKIM-записи:

| | |
|---|---|
| Bluehost | DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми). |
| GoDaddy | DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми). |
| CloudFlare | DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми). |
| DynDNS | Поле, в которое вы вводите значение каждой записи, должно быть заключено в двойные кавычки. |
| MS Office 365 | DKIM-запись обычно форматируется в автоматическом режиме (управляющие символы записи заменяются соответствующими текстовыми). |

## Настроить SPF- и DKIM-записи в Microsoft 365

### Настройка SPF

Чтобы использовать личный домен в Microsoft 365, в настройки DNS необходимо добавить специальную текстовую SPF-запись, используя команды из таблицы:

| **Любая почтовая система (обязательно)** | **v=spf1** |
|---|---|
| Exchange Online | include:spf.protection.outlook.com |
| При использовании только Exchange Online | ip4:23.103.224.0/19 ip4:206.191.224.0/19 ip4:40.103.0.0/16 include:spf.protection.outlook.com |
| Microsoft 365 Germany, только Microsoft Cloud Germany | include:spf.protection.outlook.de |
| Сторонняя почтовая система | include:<доменное имя>, где <доменное имя> — это доменное имя сторонней почтовой системы. |
| Локальная почтовая система, например Exchange Online Protection с другой почтовой системой | Используйте один из следующих параметров для каждой дополнительной почтовой системы:<br>ip4:<IP address><br>ip6:<IP address><br>include:<domain name><br>где значение <IP address> — это IP-адрес другой почтовой системы, а <domain name> — доменное имя другой почтовой системы, которая отправляет сообщения от имени вашего домена. |
| Любая почтовая система (обязательно) | Это может быть одно из нескольких значений. Рекомендуется использовать значение -all. |

Например, если ваша организация использует только Microsoft 365 и у вас нет локальных почтовых серверов, то SPF-запись будет выглядеть следующим образом:

```
v=spf1 include:spf.protection.outlook.com -all
```

Это один из наиболее распространенных форматов SPF-записи для Microsoft 365. Такая запись подходит в большинстве случаев, независимо от того, где находится ваш центр данных Microsoft 365 — в США, Европе (в том числе, в Германии) или в другом месте.

Создав SPF-запись, обновите ее в службе DNS. Для домена можно создать только одну SPF-запись. Если такая запись уже существует, то следует обновить существующую запись, не добавляя новую.

После добавления SPF-записи выполните ее проверку. Более подробная информация о проверке SPF-записи доступна в статьях на сайте Microsoft.

## Настройка DKIM

Для настройки DKIM добавьте на стороне провайдера две CNAME-записи для каждого дополнительного домена и включите DKIM в Microsoft 365.

1. Добавление CNAME-записей.

   Для каждого домена, для которого требуется добавить подпись DKIM в DNS, необходимо добавить две CNAME-записи. Запись CNAME указывает, что каноническое имя домена является псевдонимом другого доменного имени. Используйте для записей следующий формат:

| | |
|---|---|
| Host name | selector1._domainkey.<domain>. |
| Points to address or value | selector1-<domainGUID>._domainkey.<initialDomain>. |
| TTL | 3600. |
| Host name | selector2._domainkey.<domain> |
| Points to address or value | selector2-<domainGUID>._domainkey.<initialDomain> |
| TTL | 3600. |

   В указанном примере selector1 и selector2 — это селекторы для Office 365. Названия этих селекторов не меняются.

   Значение domainGUID совпадает со значением domainGUID, указанным перед mail.protection.outlook.com в пользовательской записи MX для личного домена. Например, в записи creatio1-com.mail.protection.outlook.com это creatio1-com.

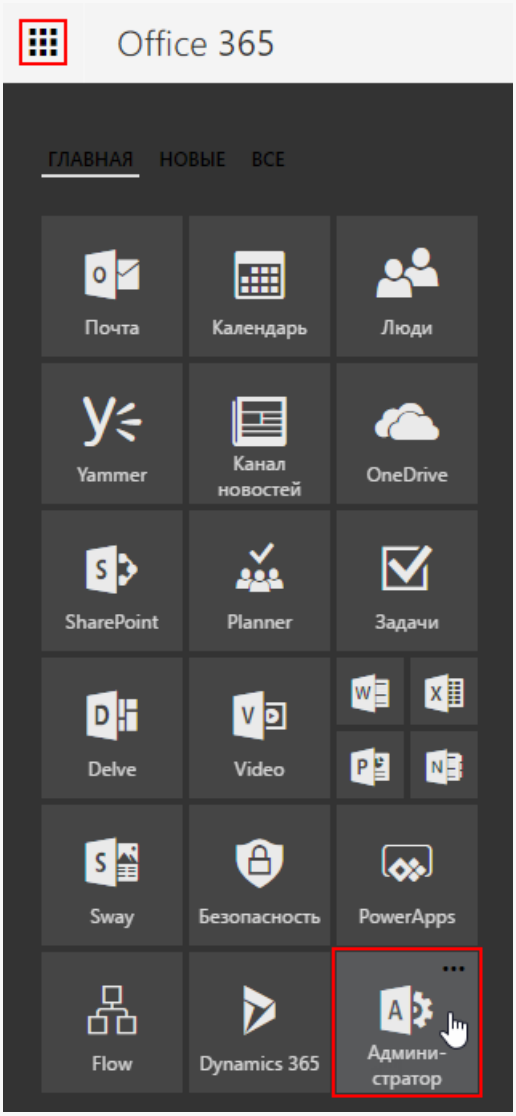
   Значение initialDomain — это домен, который вы использовали при регистрации в Office 365.

2. Включение DKIM.

   После добавления CNAME-записей в DNS включите подпись с помощью DKIM в Office 365.

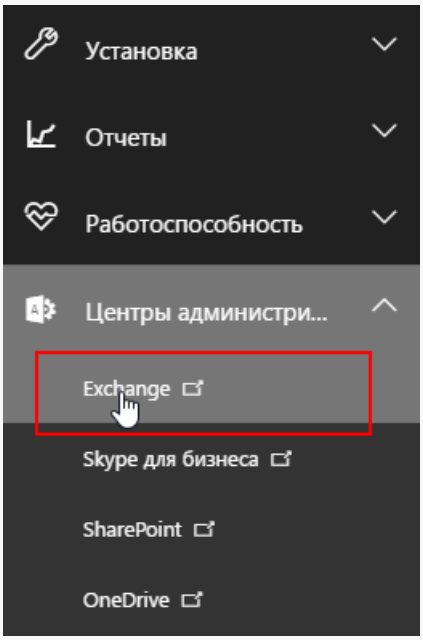
   a. В левом верхнем углу Office 365 нажмите на иконку запуска приложений и выберите элемент “Администратор” (Рис. 1).

Рис. 1 — Открытие меню администратора



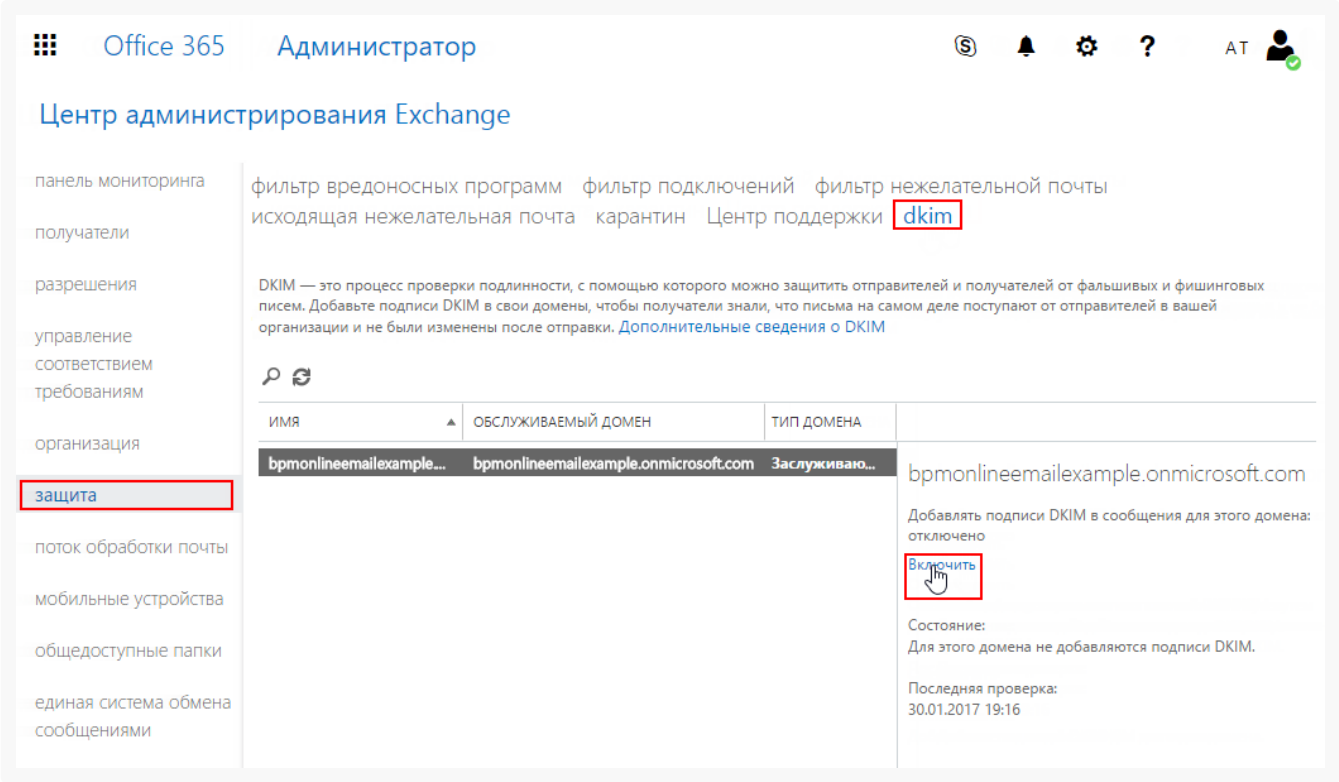

b. В области навигации слева внизу разверните пункт меню “Центры администрирования” и выберите элемент “Exchange” (Рис. 2).

Рис. 2 — Открытие Exchange




c. Откройте раздел “Защита” и выберите вкладку “dkim”. В списке доменов выберите домен, для которого требуется включить DKIM, а затем в области “Добавлять подписи DKIM в сообщения для этого домена” нажмите “Включить” (Рис. 3).

Рис. 3 — Включение DKIM для домена




Повторите этот шаг для каждого личного домена.