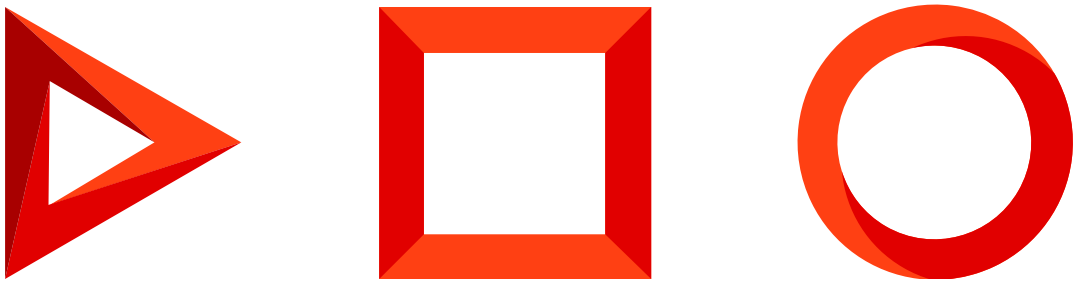
Creatio Academy

Настройка домена для рассылок

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

Настроить верификацию для провайдера UniOne

ПРОДУКТЫ: MARKETING

Если вы планируете отправлять рассылки в Creatio с помощью провайдера UniOne, то верифицируйте ваш email-адрес и корпоративный домен.

В этом случае получатели, которые используют MS Outlook, Hotmail, Gmail и большинство других современных почтовых сервисов, увидят в строке отправителя, что сообщение прислано с сервера вашего почтового провайдера от вашего имени.

Например, в строке отправителя может отобразиться подобный текст: “UniOne_Ivanov <postman1847554@usndr.com>; on behalf of; UniOne_Ivanov <ivanov.alexej@gmail.com>” либо “UniOne_Ivanov ivanov.alexej@gmail.com с домена usndr.com”.

Провайдер UniOne не позволяет отправлять тестовые письма с помощью бесплатных почтовых служб (например, Gmail, Yahoo! Mail, iCloud и т. д.).

Для использования функциональности рассылок пользователям Creatio on-site необходимо предварительно настроить интеграцию с сервисом массовых рассылок. Подробнее читайте в статье “Настройка email-рассылок”.

Чтобы верифицировать ваши email-адреса и домен, выполните следующие шаги:

1. Получите SPF- и DKIM-записи, а также дополнительный параметр отправки рассылок. Подробнее >>>
2. Укажите SPF- и DKIM-записи и дополнительный параметр в DNS-зоне вашего домена. Подробнее >>>

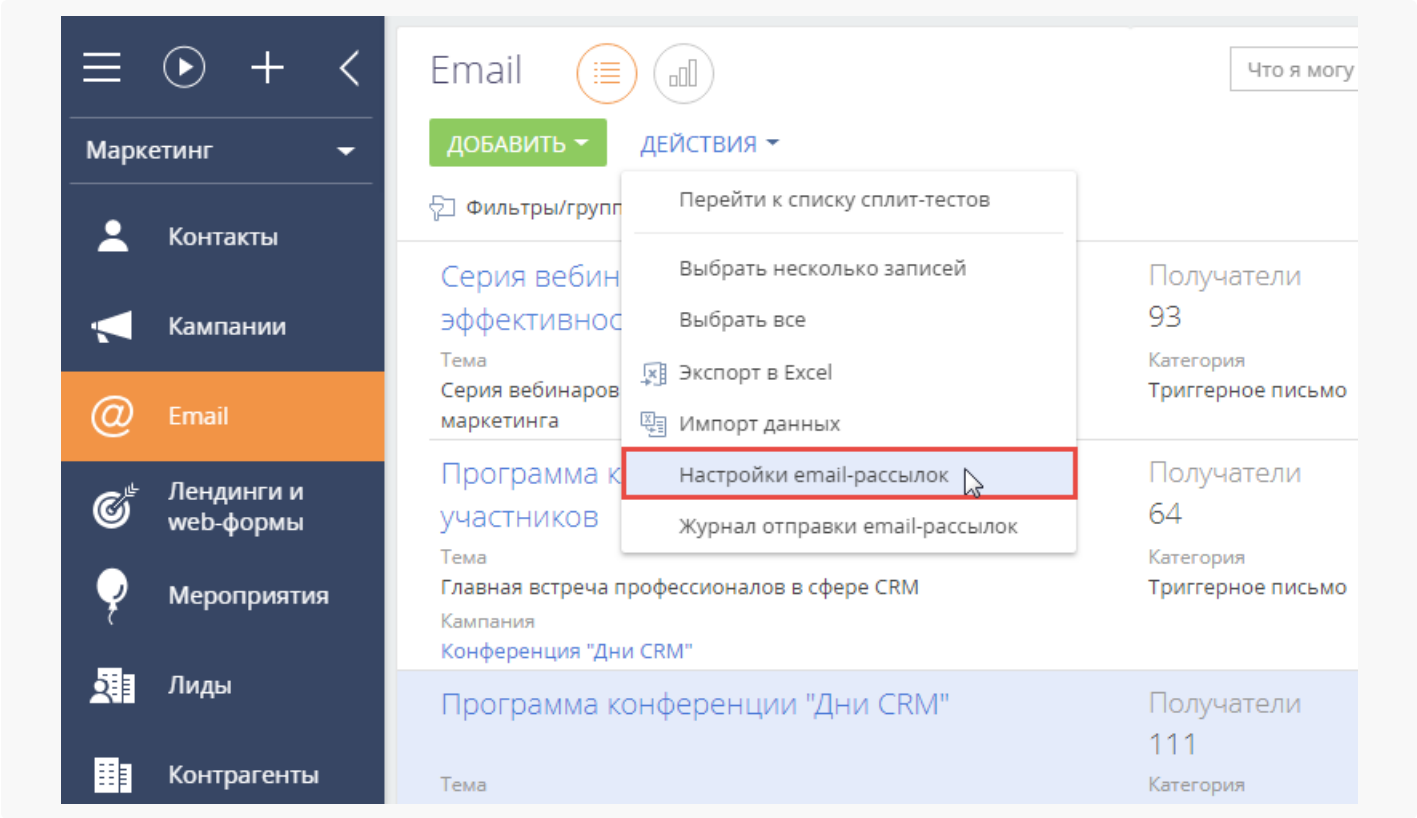
> **Важно.** Один домен может быть верифицирован только для одного приложения Creatio. Если вы используете два разных приложения Creatio, то вы не сможете верифицировать один и тот же домен для обоих.

3. Для корректной отправки писем на адреса группы mail.ru дополнительно настройте сервис Postmaster.mail.ru и Feedbak Loop. Подробнее >>>

Получить записи SPF, DKIM и дополнительный параметр отправки

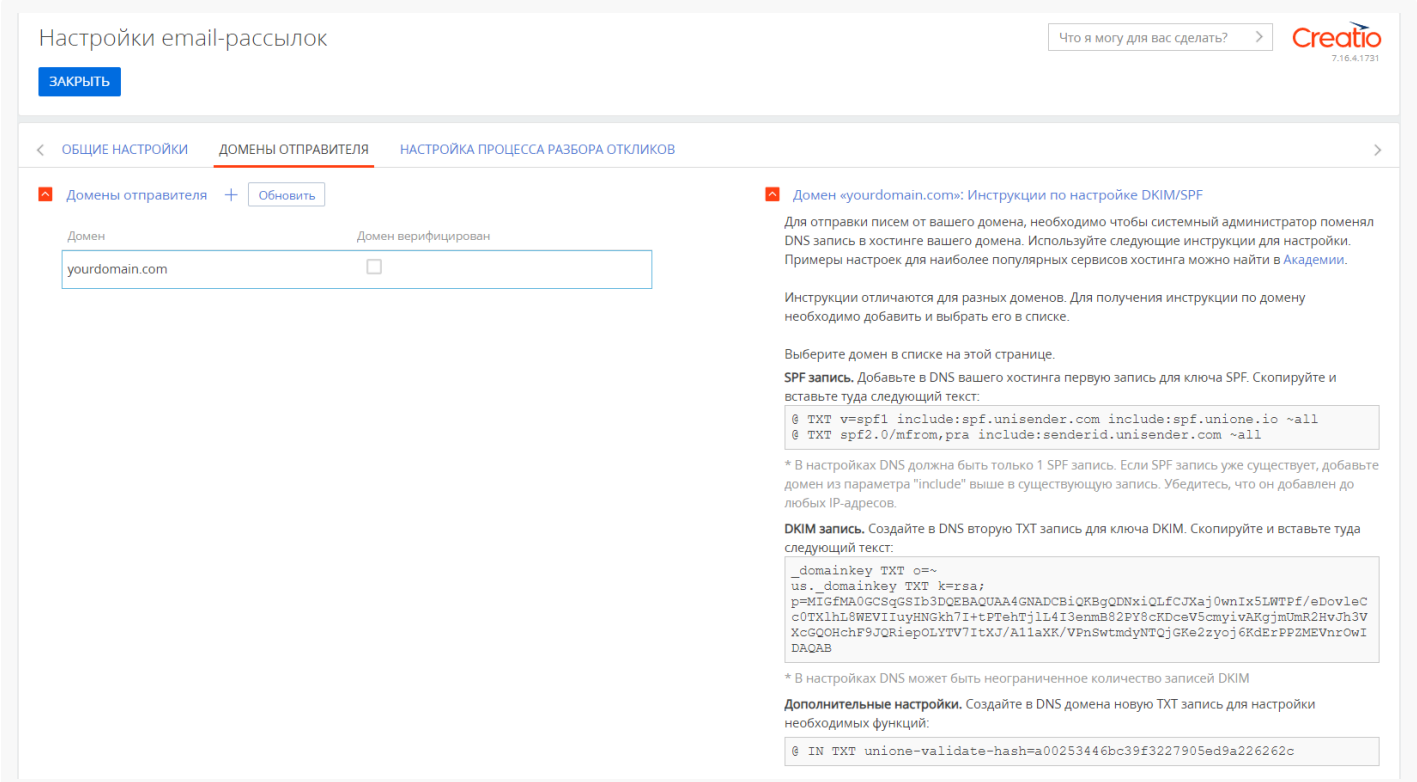
Дополнительный параметр необходим для того, чтобы провайдер рассылок дал разрешение на отправку писем. Этот параметр настраивается один раз и действителен всех адресов данного домена. SPF- и DKIM-записи и дополнительный параметр верификации генерируются автоматически в разделе **Email**. Для получения этих записей в разделе **Email** в меню [*Действия*] выберите **Настройки email-рассылок** (Рис. 1).

Рис. 1 — Переход на страницу настройки email-рассылок



Все необходимые записи будут автоматически сгенерированы в поле **Инструкции по настройке DKIM/SPF** на вкладке **Домены отправителя** (Рис. 2).

Рис. 2 — Ключи DKIM/SPF для указанного домена



На заметку. DKIM/SPF настройки отличаются для каждого отдельного домена. Нужно добавить и выбрать каждый домен, чтобы получить разные инструкции. При использовании провайдера UniOne только домены верифицированных email-адресов могут быть добавлены на вкладку [*Домены отправителя*].

Выполнить настройки в DNS-зоне домена

Чтобы настроить возможность отправки писем, необходимо указать дополнительный параметр отправки в DNS-зоне вашего домена. Чтобы верифицировать почтовый домен при использовании провайдера рассылок UniOne, необходимо добавить записи SPF, DKIM и политику DMARC в DNS-зону настроек почтового домена, иначе не гарантируется высокий уровень репутации домена и доставляемости писем. Если не заполнить хотя бы один из перечисленных параметров, то домен будет считаться недействительным и отправка писем с него выполняться не будет.

Для настройки:

1. Укажите дополнительный параметр в DNS-зоне вашего домена.

   Скопируйте сгенерированную запись **дополнительного параметра** из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
@	in TXT	unione-validate-hash=XXXXXXXXXX

   В приведенной записи XXXXXXXXXX — это уникальный ключ для каждого домена клиента. Ключ формируется автоматически и доступен на вкладке [*Домены отправителя*].

   Если ключ не был сгененирован, обратитесь в службу поддержки Creatio.

   В зависимости от DNS-редактора в поле “Host / Name” DNS-зоны может понадобиться указать символ "@", имя домена, или не указывать ничего. Обратитесь к вашему хостинг-провайдеру для получения информации о том, как правильно ввести это значение.

2. Укажите SPF-записи в DNS-зоне вашего домена.

1. Если в DNS-зоне вашего домена еще нет **SPF-записи**, вам нужно ее скопировать из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
@	TXT	v=spf1 include:spf.unisender.com ~all
@	TXT	spf2.0/mfrom,pra include:senderid.unisender.com ~all

1. Если TXT-запись с SPF информацией уже существует, то в конец первой и второй строк этой записи, перед последним оператором (как правило, это **?all**, **~all**, или **-all**), необходимо добавить:

Название	Тип	Значение
Запись SPF1 (первая строка)	TXT	include:spf.unisender.com
Запись SPF2 (вторая строка)	TXT	include:senderid.unisender.com

В зависимости от DNS-редактора в поле “Имя” DNS-зоны может понадобиться указать символ "@", имя домена, или не указывать ничего. Обратитесь к вашему хостинг-провайдеру для получения информации о том, как правильно ввести это значение.

Важно. UniOne выделяет 24 часа на проверку домена после генерации ключей SPF/DKIM. Если процесс задерживается, свяжитесь со службой поддержки Creatio, чтобы успешно завершить проверку.

2. Укажите DKIM-запись в DNS-зоне вашего домена и выполните соответствующую настройку записей DKIM:
   Скопируйте сгенерированную запись **DKIM** из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
_domainkey	TXT	o=~
us._domainkey	TXT	k=rsa; p=XXXXXXXXXXXXXXXXXXXXX

   В приведенной записи XXXXXXXXXXXXXXXXXXXXX — это уникальный ключ для каждого домена клиента. Ключ формируется автоматически и доступен на вкладке [*Домены отправителя*].

3. Настройте DMARC в DNS-зоне вашего домена

   Проверка DMARC добавляется только после того, как были добавлены записи SPF и DKIM, и сообщает серверу-получателю, что делать с письмами, отправленными с домена, который не был верифицирован. Для UniOne настройка политики DMARC является необязательной, но рекомендуемой для повышения репутации домена. Чтобы активировать DMARC, добавьте в записи DNS домена правило в виде записи TXT:

Название	Тип	Значение
_dmarc	TXT	v=DMARC1;p=none;

   Тег **v** указывает версию протокола, а **p** — способ обработки писем, которые не прошли проверку. Больше информации о протоколе в доступно в статье о DMARC в Википедии.

Настроить корректную отправку писем на адреса группы mail.ru

При отправке рассылок на адреса группы mail.ru, например, inbox.ru, mail.ua, list.ru, bk.ru и т. д., необходимо выполнить дополнительные настройки:

- Добавить домены, с которых отправляются ваши рассылки, в сервис Postmaster.mail.ru.
- Настроить Feedback Loop (FBL).

> **На заметку.** О механизме получения обратной связи Feedback Loop читайте в статье “Как и зачем отслеживать отклики “Отправлено в спам”?”.

Отсутствие этих настроек приведет к тому, что в UniOne и Creatio не будут получены отклики почтовой системы на письма, помеченные получателями как спам. Повторная отправка рассылок таким получателям может повлиять на репутацию отправителя и привести к блокировке вашего домена почтовым сервисом.

Для настройки:

1. Зарегистрируйте новый почтовый ящик на Mail.ru и войдите в созданную учетную запись.
2. Перейдите по адресу https://postmaster.mail.ru/add/. Используя инструкцию на странице, добавьте домены, с которых вы отправляете рассылки.
3. На странице https://postmaster.mail.ru/settings/ настройте адреса для получения обратной связи по откликам “Это спам” с помощью механизма Feedback Loop:
   a. Для каждого вашего домена укажите адрес в формате fbl@ваш_домен. На него будут отправляться письма, на которые жалуются пользователи, в формате Abuse Reporting Format.
   b. Настройте автоматическое перенаправление писем с этого адреса на адрес fbl@unisender.com для обработки.

Настроить верификацию для провайдера Elastic Email

ПРОДУКТЫ: MARKETING

Если вы планируете отправлять рассылки в Creatio с помощью провайдера Elastic Email, то верифицируйте ваш email-адрес и корпоративный домен.

В этом случае получатели, которые используют MS Outlook, Hotmail, Gmail и большинство других современных почтовых сервисов, увидят в строке отправителя, что сообщение прислано с сервера вашего почтового провайдера от вашего имени. В строке отправителя может отобразиться такой текст: “Terrasoft <info@terrasoft.ua> via elasticemail.com”.

Чтобы верифицировать ваши email-адреса и домен, выполните следующие шаги:

1. Добавьте ваш корпоративный домен на страницу настройки email-рассылок. Подробнее >>>
2. Получите SPF- и DKIM-записи. Подробнее >>>
3. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена. Подробнее >>>

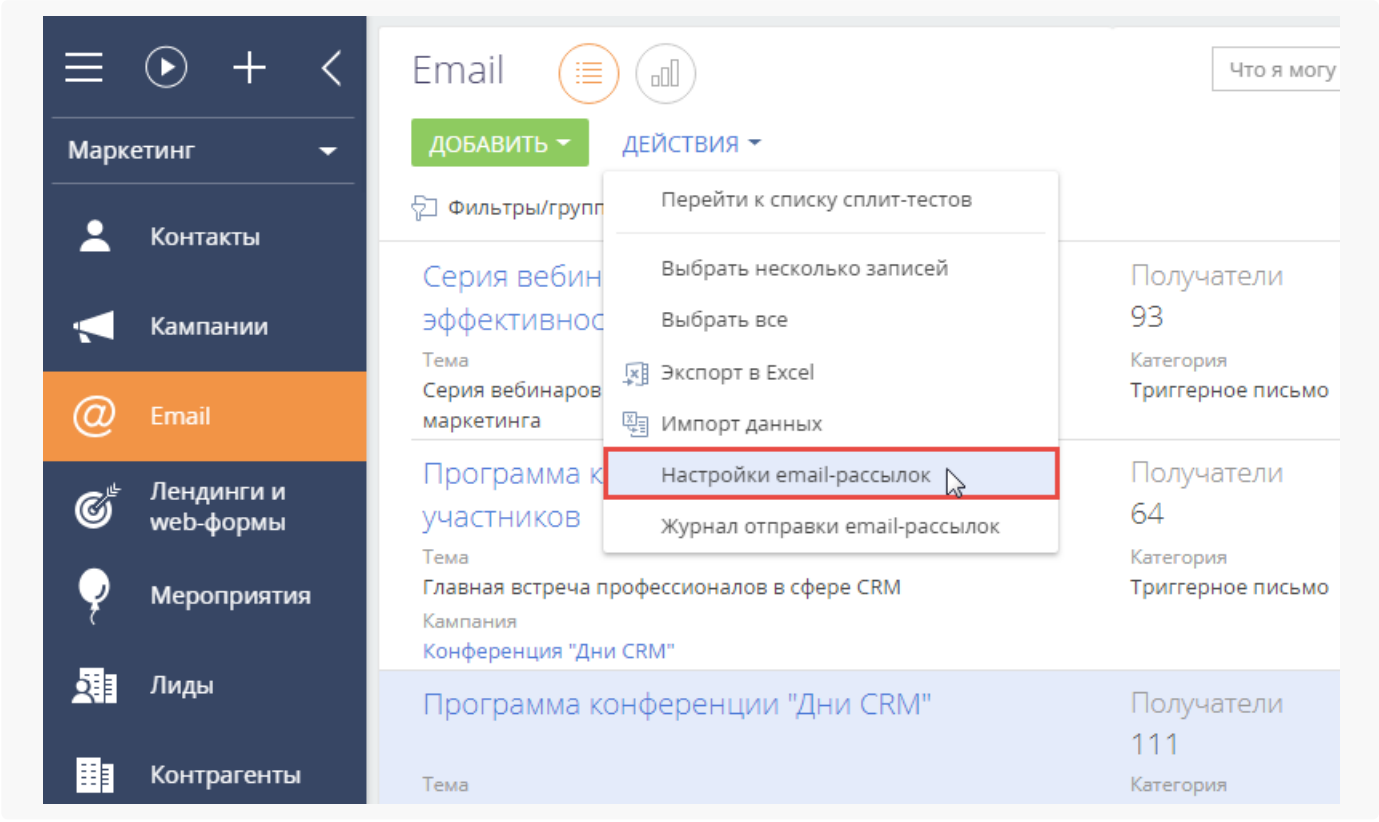
Важно. Если ваш домен не верифицирован, то Elastic Email ограничивает количество отправленных писем до 50 в день.

Добавить корпоративный домен на страницу настройки email-рассылок

До начала отправки массовых рассылок выполните настройки:

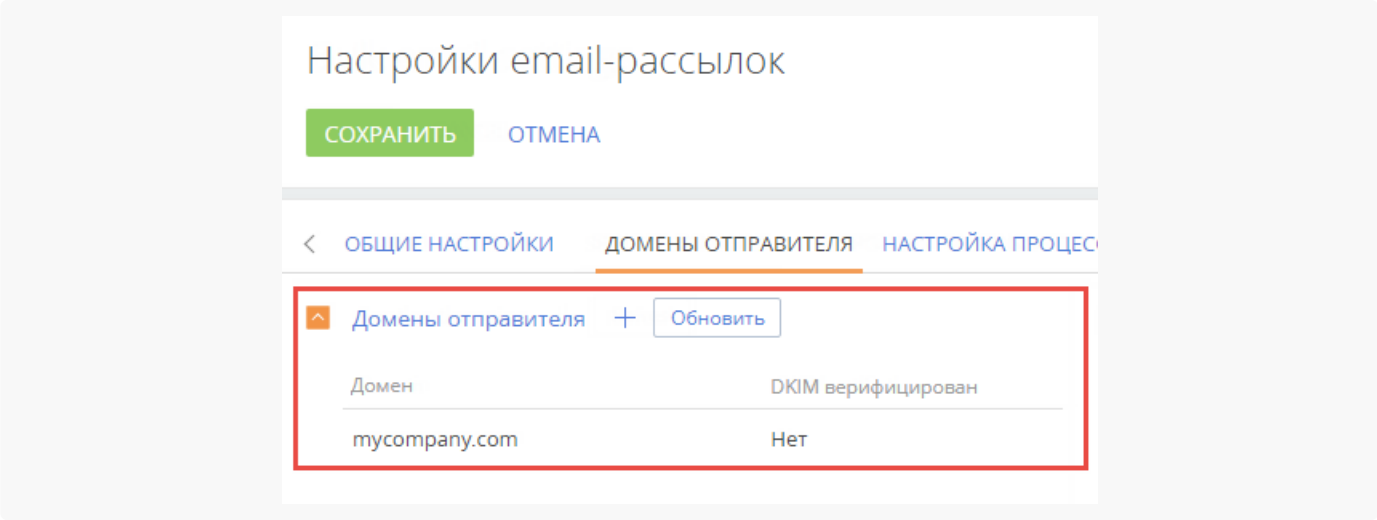
1. В разделе [*Email*] в меню [*Действия*] выберите [*Настройки email-рассылок*] (Рис. 1).

Рис. 1 — Переход на страницу настройки email-рассылок



2. На странице [*Настройки email-рассылок*] на вкладке [*Домены отправителя*] укажите домен вашего email-адреса, с которого будут отправляться рассылки, например “mycompany.com” (Рис. 2).

Рис. 2 — Вкладка [*Домены отправителя*]



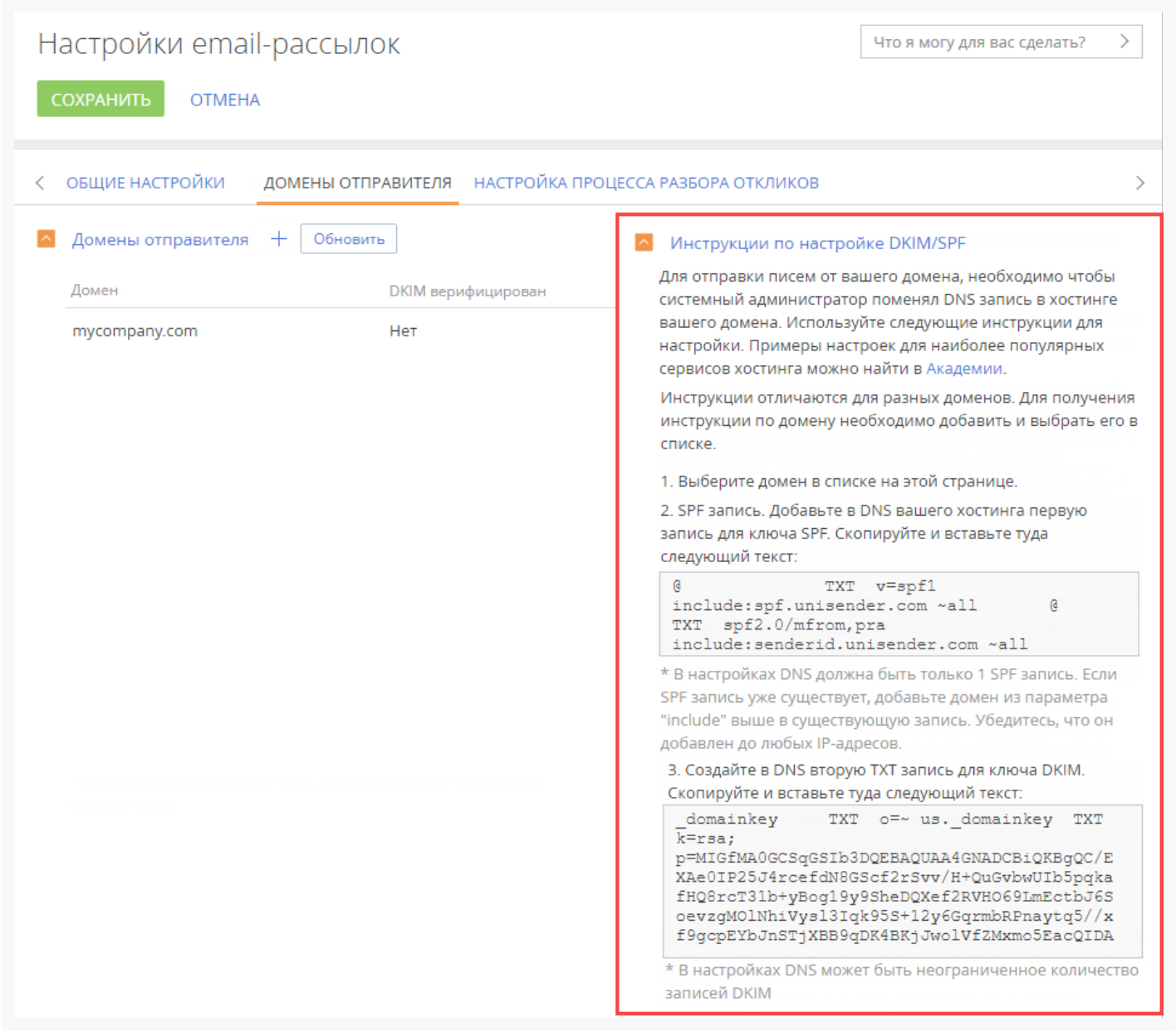
Получить SPF- и DKIM-записи

SPF- и DKIM-записи генерируются автоматически в разделе [*Email*] после добавления домена на страницу настройки email-рассылок.

Для получения этих записей в разделе [*Email*] в меню [*Действия*] выберите [*Настройки email-рассылок*].

SPF- и DKIM-записи будут автоматически сгенерированы в поле [*Инструкции по настройке DKIM/SPF*] на вкладке [*Домены отправителя*] (Рис. 3).

Рис. 3 — Ключи DKIM/SPF для указанного домена



SPF- и DKIM-записи провайдера Elastic Email одинаковы для всех доменов.

Выполнить настройки в DNS-зоне домена

Чтобы обеспечить высокий уровень репутации домена и доставляемости писем, необходимо добавить записи SPF, DKIM, Tracking Domain и политику DMARC в DNS-зону настроек почтового домена.

Для настройки:

1. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена:
2. Если в DNS-зоне вашего домена еще нет SPF-записи, то ее необходимо скопировать из поля [*Инструкции по настройке DKIM/SPF*] на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
@	TXT	v=spf1 a mx include:_spf.elasticemail.com ~all

3. Если у вас уже есть TXT-запись с SPF информацией, то в конец этой записи, перед ее последним оператором (как правило, это **?all**, **~all**, или **-all**) необходимо добавить следующую строку:

Название	Тип	Значение
@	TXT	include:_spf.elasticemail.com

На заметку. В зависимости от DNS-редактора в поле “Host / Name” DNS-зоны может понадобиться указать символ "@", имя домена, или не указывать ничего. Обратитесь к вашему хостинг-провайдеру для получения информации о том, как правильно ввести это значение.

4. Укажите DKIM-запись в DNS-зоне вашего домена. Для провайдера Elastic Email эта запись имеет такой вид:

Название	Тип	Значение
api._domainkey	TXT	k=rsa;t=s;p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCbmGbQMzYeMvxwtNQoXN0waGYaciuKx8mtMh5czguT4EZlJXuCt6V+l56mmt3t68FEX5JJ0q4ijG71BGoFRkl87uJi7LrQt1ZZmZCvrEII0YO4mp8sDLXC8g1aUAoi8TJgxq2MJqCaMyj5kAm3Fdy2tzftPCV/lbdiJqmBnWKjtwIDAQAB

На заметку. В некоторых настройках DNS в поле “Host/Name” может потребоваться ввести “api._domainkey.yourdomain.com”, заменив значение своим актуальным доменом.

5. Настройте Tracking Domain в DNS-зоне вашего домена.
Чтобы отследить переход по ссылке в полученном письме, Elastic Email переписывает адрес ссылки в шаблоне письма. Поэтому при переходе получателя по ссылке из письма в браузере сначала отобразится адрес с доменом "api.elasticemail.com" и только затем будет выполнена переадресация на указанную при отправке письма ссылку. Чтобы в первой ссылке для отслеживания был указан ваш домен, необходимо создать CNAME-запись в настройках DNS-домена:

Название	Тип	Значение
tracking	CNAME	api.elasticemail.com

6. Укажите SPF- и DKIM-записи в DNS-зоне вашего домена.
Проверка DMARC добавляется только после того, как были добавлены записи SPF и DKIM, и сообщает серверу-получателю, что делать с письмами, отправленными с домена, который не был верифицирован. Чтобы активировать DMARC, добавьте в записи DNS домена правило в виде записи

TXT:

Название	Тип	Значение
_dmarc	TXT	v=DMARC1;p=none;

Тег **v** указывает версию протокола, а **p** — способ обработки писем, которые не прошли проверку.

Больше информации о протоколе в доступно в статье о DMARC в Википедии.Подробная информация о настройке записей SPF, DKIM, Tracking Domain и DMARC доступна в инструкции на сайте провайдера Elastic Email.

Настроить верификацию для провайдера SendGrid

ПРОДУКТЫ: MARKETING

Если отправка рассылок в Creatio осуществляется с помощью SendGrid, то вам необходимо верифицировать ваш email-адрес и корпоративный домен, чтобы провайдер мог отправлять электронные письма от вашего имени.

Если ваши получатели используют MS Outlook, Hotmail, Gmail и большинство других современных почтовых сервисов, они могут увидеть в строке отправителя, что сообщение прислано с сервера вашего почтового провайдера от вашего имени.

На заметку. В строке отправителя может отобразиться такой текст: “Your Manager <info@creatio.com> via sendgrid.net”.

Процедура верификации домена для провайдера SendGrid состоит из следующих этапов:

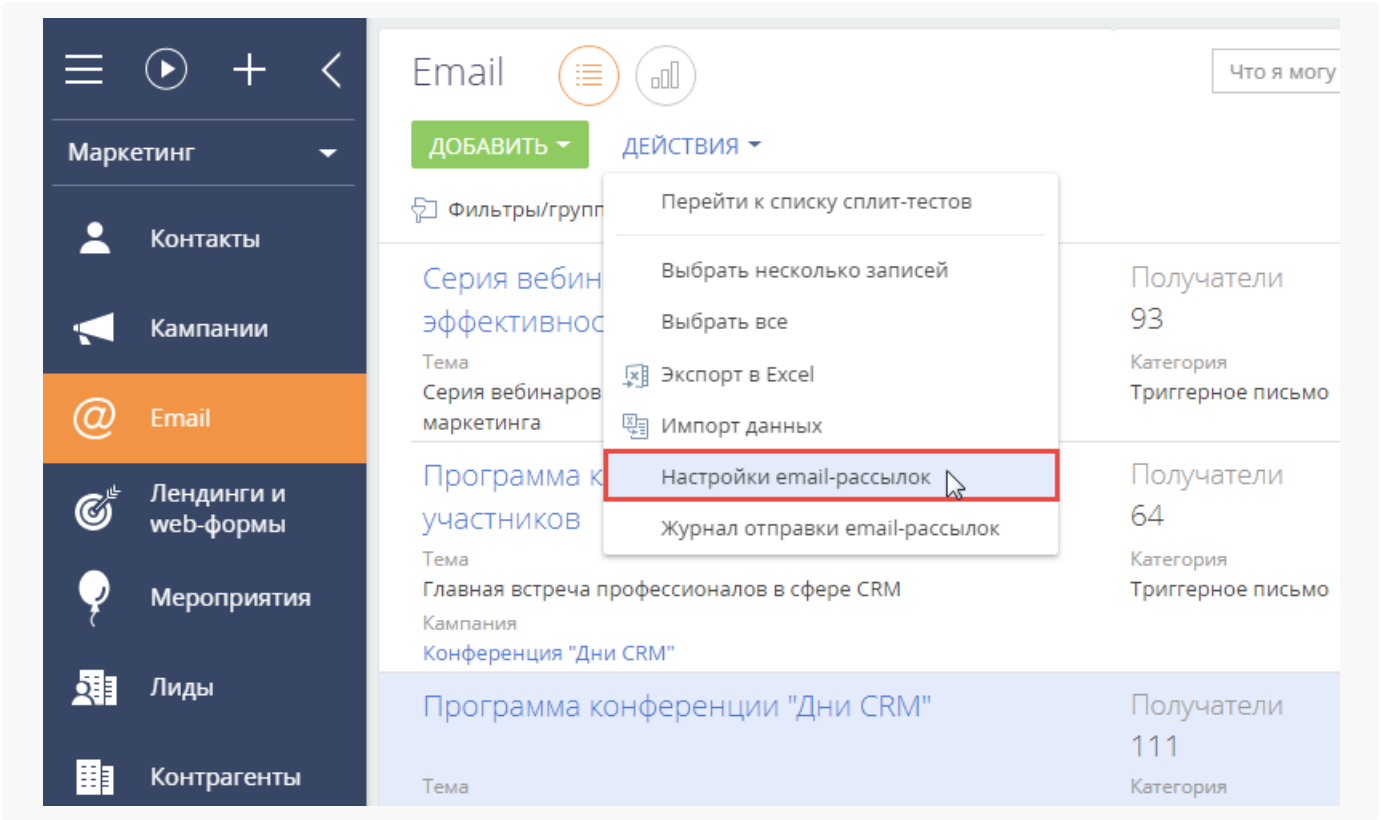
1. Добавьте ваш корпоративный домен на страницу настройки email-рассылок. Подробнее >>>
2. Получите MX-, SPF- и DKIM-записи. Подробнее >>>
3. Укажите MX-, SPF-, и DKIM-записи в DNS-зоне вашего домена. Подробнее >>>

Добавить ваш корпоративный домен на страницу настройки email-рассылок

Пользователям SendGrid нужно добавить корпоративный домен в Creatio до начала отправки массовых рассылок. Для этого:

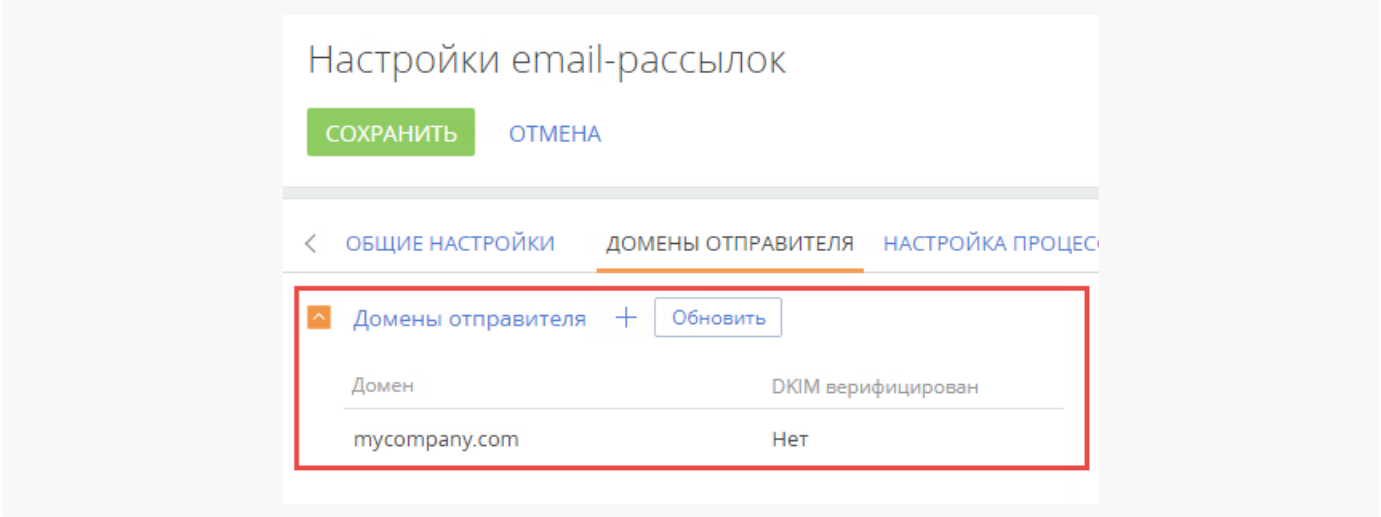
1. В разделе **Email** в меню **Действия** выберите **Настройки email-рассылок** (Рис. 1).

Рис. 1 — Переход на страницу настройки email-рассылок



2. На странице **Настройки email-рассылок** на вкладке **Домены отправителя** укажите домен вашего email-адреса, с которого будут отправляться рассылки, например “mycompany.com” (Рис. 2).

Рис. 2 — Вкладка [*Домены отправителя*]

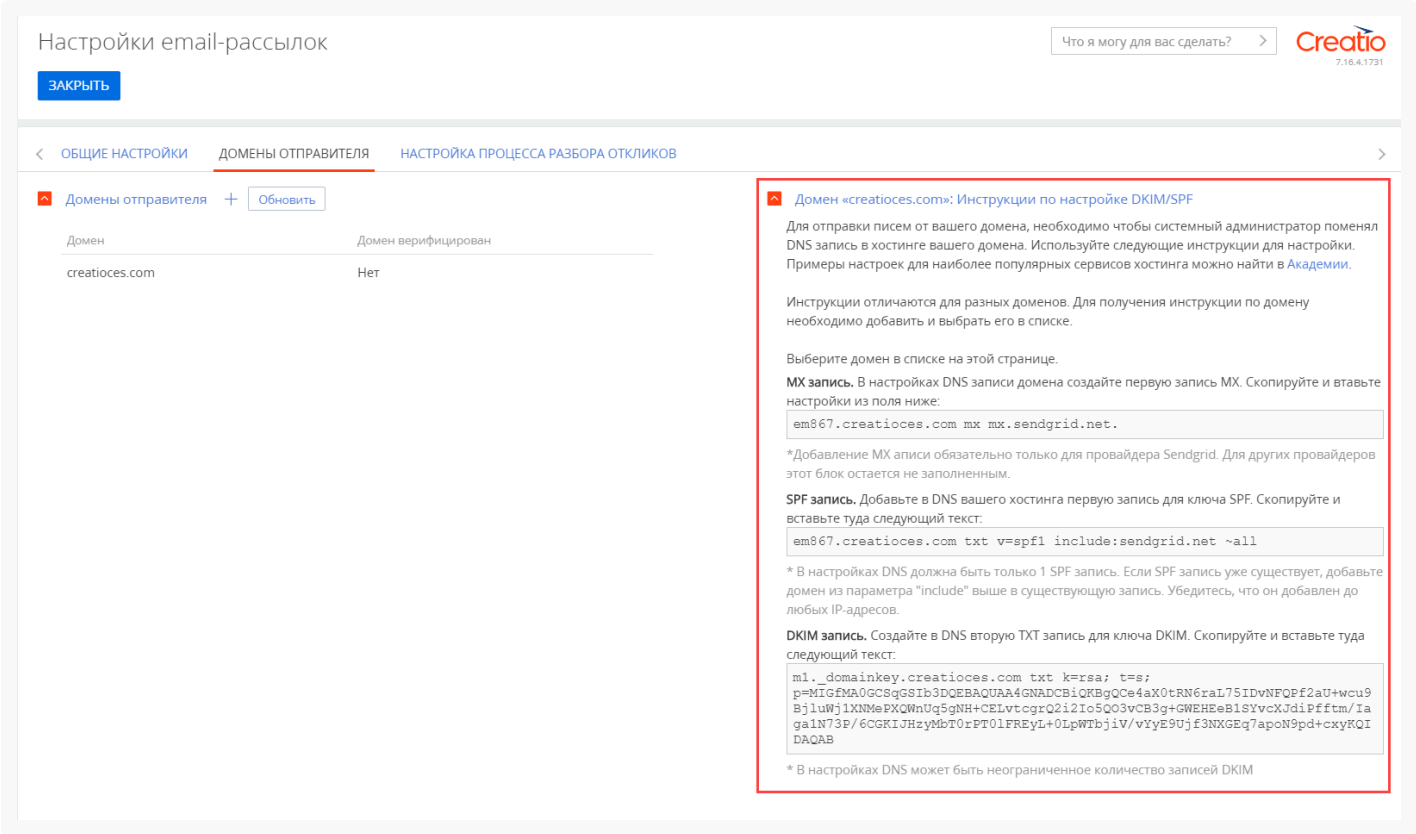


Получить ключи настройки для домена

MX-, SPF- и DKIM-записи генерируются автоматически в разделе **Email** после добавления домена на страницу настройки email-рассылок. Для получения этих записей в разделе **Email** в меню [*Действия*] выберите **Настройки email-рассылок**.

SPF- и DKIM-записи будут автоматически сгенерированы в поле **Инструкции по настройке DKIM/SPF** на вкладке **Домены отправителя** (Рис. 1).

Рис. 1— Ключи MX/DKIM/SPF для указанного домена



Важно. MX-, SPF- и DKIM-записи провайдера SendGrid отличаются для разных доменов.

Выполнить настройки в DNS-зоне вашего домена

Чтобы верифицировать почтовый домен при использовании провайдера рассылок SendGrid, необходимо добавить записи MX, SPF и DKIM в DNS-зону настроек почтового домена, иначе не гарантируется высокий уровень репутации домена и доставляемости писем.

На заметку. Рекомендуем также ознакомиться с примерами в статье “Рекомендации по настройке для популярных DNS-провайдеров”.

Указать MX-запись в DNS-зоне вашего домена

MX-запись — это основная запись в доменной зоне, указывающая на имена почтовых хостов домена. Почтовый сервер выполняет обязательную проверку наличия MX-записей в DNS-зоне домена и их соответствия IP-адресу отправителя. В случае отсутствия или несоответствия данных, удаленный сервер с высокой вероятностью откажет в отправке и получении электронной почты.

Синтаксис MX-записей отличается от SPF- и DKIM-записей наличием приоритетов.
Приоритет указывается в виде целого числа от нуля включительно и указывает для данного домена порядок проверки доступности почтовых серверов, если их используется несколько. Чем меньше число, тем выше приоритет. то есть, наивысший приоритет — 0. Допускается наличие в системе нескольких

MX-записей с равными приоритетами.

MX-запись будет выглядеть следующим образом:

Имя	Приоритет	Тип	Значение
subdomain.yourdomain.com	0	mx	mx.sendgrid.net.

Имя поддомена (subdomain) является уникальным и формируется провайдером.

Указать SPF-запись в DNS-зоне вашего домена

Скопируйте SPF-запись из поля **Инструкции по настройке DKIM/SPF** на странице **Настройки email-рассылок**. Запись будет выглядеть следующим образом:

Имя	Тип	Значение
subdomain.yourdomain.com	TXT	v=spf1 a mx include:_spf.sendgrid.com ~all

Имя поддомена (subdomain) является уникальным и формируется провайдером. Поэтому для каждого из поддоменов необходимо добавлять отдельную SPF-запись.

Указать DKIM-запись в DNS-зоне вашего домена

После настройки записи SPF необходимо добавить записи DKIM. Для провайдера SendGrid эта запись выглядит следующим образом:

Название	Тип	Значение
m1._domainkey	TXT	k=rsa; t=s; p=XXXXXXXXXXXXX

В приведенной записи XXXXXXXXXXXXX — это **индивидуальный ключ** для каждого домена клиента. Ключ формируется автоматически и доступен на вкладке [***Домены отправителя***].

В некоторых настройках DNS в поле “Host/Name” может потребоваться ввести “m1._domainkey.yourdomain.com”, заменив значение поддоменом, который был сформирован провайдером.

На заметку. Подробная информация о настройке записей MX, SPF и DKIM доступна в инструкции на сайте провайдера SendGrid.

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: ip4:<IP address> ip6:<IP address> include:<domain name> 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.

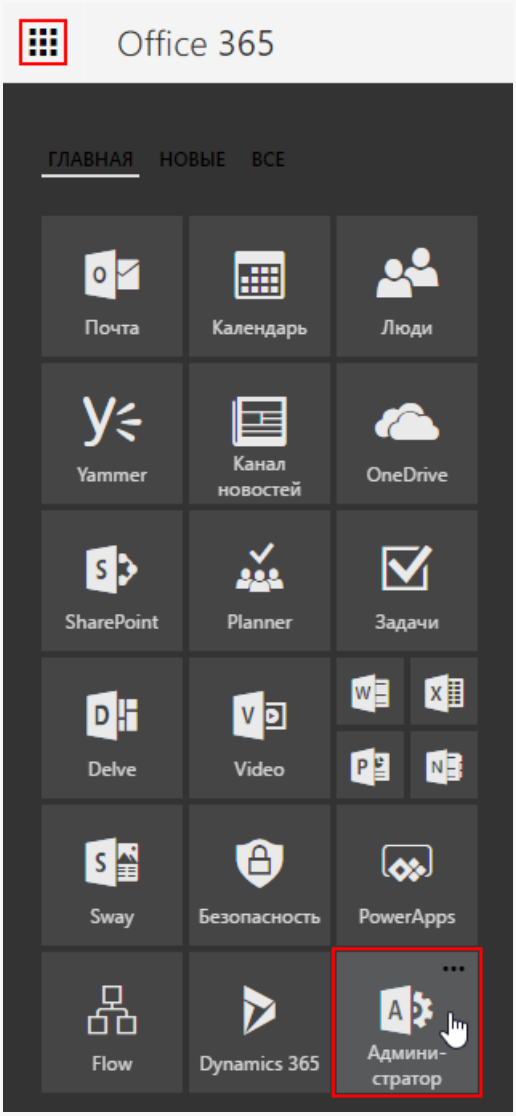
   Значение initialDomain — это домен, который вы использовали при регистрации в Office 365.

2. Включение DKIM.

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

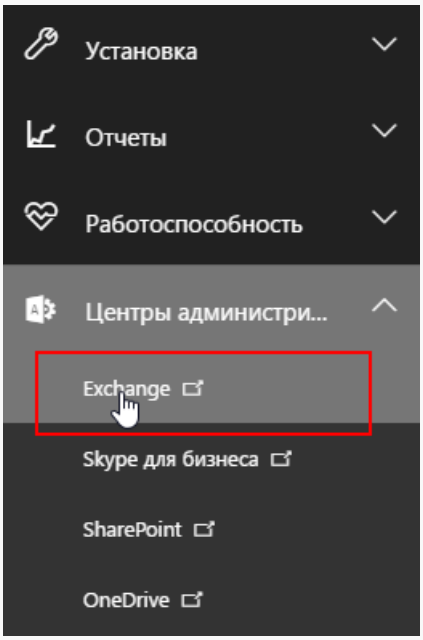
   a. В левом верхнем углу Office 365 нажмите на иконку запуска приложений и выберите элемент “Администратор” (Рис. 1).

Рис. 1 — Открытие меню администратора



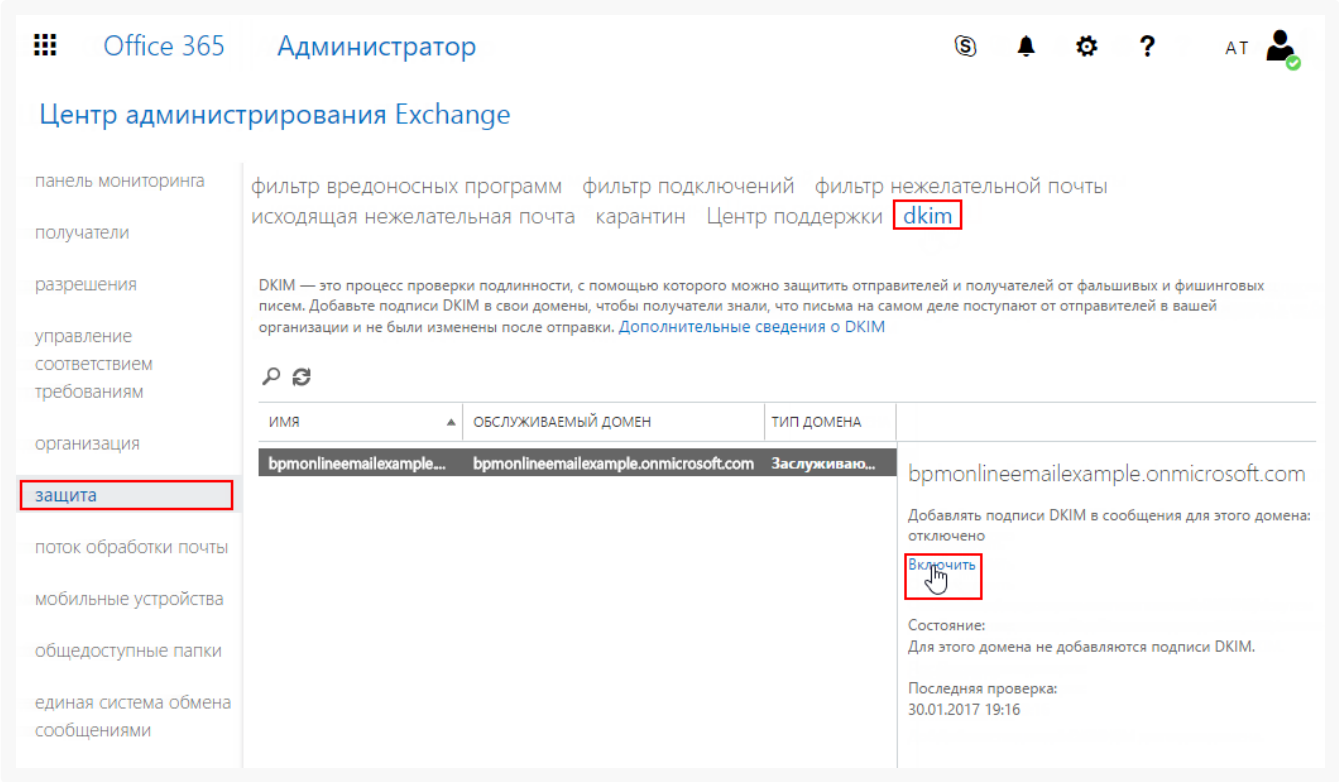
b. В области навигации слева внизу разверните пункт меню “Центры администрирования” и выберите элемент “Exchange” (Рис. 2).

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.