



# JaCarta PKI и Microsoft Outlook 2016

---

Шифрование и подпись электронных писем

Листов: 19

Автор: Dmitry Shuralev

## Аннотация

Настоящий документ описывает настройку **Microsoft Office 2016** для реализации шифрования писем и добавления электронной подписи к письмам с использованием цифровых сертификатов, хранящихся на электронных ключах **JaCartaPKI**.

Настоящий документ, включая подбор и расположение иллюстраций и материалов в нём, является объектом авторских прав и охраняется в соответствии с законодательством Российской Федерации. Обладателем исключительных авторских и имущественных прав является ЗАО "Аладдин Р.Д.". Использование этих материалов любым способом без письменного разрешения правообладателя запрещено и может повлечь ответственность, предусмотренную законодательством РФ.

Информация, приведённая в данном документе, предназначена исключительно для ознакомления и не является исчерпывающей. Состав продуктов, компонент, их функции, характеристики, версии, доступность и пр. могут быть изменены компанией "Аладдин Р.Д." без предварительного уведомления. Все указанные данные о характеристиках продуктов основаны на международных или российских стандартах и результатах тестирования, полученных в независимых тестовых или сертификационных лабораториях, либо на принятых в компании методиках. В данном документе компания "Аладдин Р.Д." не предоставляет никаких ни явных, ни подразумеваемых гарантий.

Владельцем товарных знаков Аладдин, Aladdin, JaCarta, логотипов и правообладателем исключительных прав на их дизайн и использование, патентов на соответствующие продукты является ЗАО "Аладдин Р.Д.".

Владельцем товарных знаков Apple, iPad, iPhone, Mac OS, OS X является корпорация AppleInc. Владельцем товарного знака IOS является компания Cisco (CiscoSystems, Inc). Владельцем товарного знака WindowsVista и др. — корпорация Microsoft (MicrosoftCorporation). Названия прочих технологий, продуктов, компаний, упоминающихся в данном документе, могут являться товарными знаками своих законных владельцев.

Сведения, приведённые в данном документе, актуальны на дату его публикации.

При перепечатке и использовании данных материалов либо любой их части ссылки на ЗАО "Аладдин Р.Д." обязательны.

© ЗАО "Аладдин Р.Д.", 1995–2017. Все права защищены.


# Оглавление

|  |           |
|--|-----------|
| <b>Введение</b>                                  | <b>4</b>  |
| Требования к инфраструктуре                      | 4         |
| Принцип работы                                   | 5         |
| Для чего нужно шифровать сообщения?              | 5         |
| Что подтверждает цифровая подпись?               | 6         |
| Поддерживаемые модели электронных ключей         | 6         |
| <b>Настройка и проверка шифрования и подписи</b> | <b>7</b>  |
| Настройка параметров безопасности                | 7         |
| Отправка и получение подписанного сообщения      | 12        |
| Отправка и получение зашифрованного сообщения    | 14        |
| <b>Контакты, техническая поддержка</b>           | <b>17</b> |
| <b>Регистрация изменений</b>                     | <b>18</b> |

# Введение

---

Программное обеспечение **Microsoft Outlook** на протяжении многих лет является наиболее популярным офисным и домашним инструментом в мире для работы с электронной почтой. По сути, ПО является полноценным органайзером, предоставляющим функции календаря, планировщика задач, записной книжки и менеджера контактов. Кроме того, **MS Outlook** позволяет отслеживать работу с документами пакета **Microsoft Office**.

 В настоящем документе показаны примеры на базе Outlook2016, но его можно использовать и для других более старых версий.

Используя цифровой сертификат, записанный на электронный ключ **JaCartaPKI**, пользователь может с лёгкостью подписать и зашифровать электронное сообщение, тем самым обеспечить защиту сообщения и вложения.


## Требования к инфраструктуре

### Серверная часть

WindowsServerролью контроллера домена(ADDC)

WindowsServerролью центра сертификации(ADCA)

WindowsServerролью почтового сервераMicrosoftExchange

 Указанные роли могут быть развернуты в рамках одного физического или виртуального сервера Windows. Настоящий документ не рассматривает настройку указанных серверных ролей.

### Клиентская часть

Любая клиентская версия Windows с установленным ПО MicrosoftOutlook и "Единый Клиент JaCarta".

## Принцип работы

Шифрование электронных писем и выработка/проверка электронной подписи играют важную роль при обеспечении информационной безопасности. У пользователей есть электронный ключ **JaCartaPKI** с цифровым сертификатом и ключевой парой (открытый и закрытый ключи). Третья сторона (Центр сертификации или Удостоверяющий центр) удостоверяет по цифровому сертификату его законного владельца.

**Электронная подпись почтовых сообщений** производится отправителем почтового сообщения с использованием своего закрытого ключа. При помощи открытого ключа можно проверить правильность цифровой подписи, а также посмотреть информацию об отправителе.

Для **шифрования почтовых сообщений** два пользователя сначала должны обменяться подписанными сообщениями. Почтовое сообщение шифруется отправителем при помощи открытого ключа получателя. Таким образом, любой может зашифровать сообщение для пользователя при помощи открытого ключа, но только владелец закрытого ключа может расшифровать сообщение.

Для надёжной сохранности сертификат и ключ необходимо хранить на **USB-токене** или **смарт-карте JaCartaPKI**. При использовании **JaCartaPKI** только легальный пользователь сможет прочесть зашифрованное для него сообщение. Центр сертификации и почтовый сервер необходимы в инфраструктуре, но настройка **электронной подписи** и **шифрования почтовых сообщений** не зависит от них. Настройка ЭП и шифрования почтовых сообщений сводится к настройке программы почтового клиента.

Электронный ключ **JaCartaPKI**, в отличие от других известных способов хранения, обеспечивает неизвлекаемость ключевой информации на USB-токене или смарт-карте. Неизвлекаемое хранение подразумевает, что ключ из токена или карты не попадает никуда извне, например, на жёсткий диск компьютера или в оперативную память. А при обращении к информации на электронном ключе требуется знание PIN-кода, неправильный ввод которого приведёт к блокировке устройства. Это в свою очередь защищает от подбора комбинации PIN-кода, сводя количество попыток к определённому значению, например, 3.

## Для чего нужно шифровать сообщения?

Если Вам нужно обеспечить конфиденциальность сообщения электронной почты, защитить сам текст письма и все вложения, то можно зашифровать это письмо. Шифрование сообщения в Outlook означает, что читаемый обычный текст преобразуется в зашифрованные данные. Расшифровать сообщение для прочтения может только получатель, у которого есть закрытый ключ, соответствующий открытому ключу, использованному для его шифрования. Для получателей, которые не имеют соответствующего закрытого ключа, будет отображаться искажённый текст.

## Что подтверждает цифровая подпись?

- **Подлинность.**


Цифровая подпись подтверждает личность подписавшего.

- **Целостность.**

Цифровая подпись подтверждает, что содержимое документа не было изменено или подделано после заверения.

- **Неотказуемость.**

Цифровая подпись подтверждает происхождение заверенного содержимого. Подписавший не может отрицать свою связь с подписанным содержимым.

 Независимо от времени получения сертификата подписи и состояния его отзыва считается, что подписанные документы с действующей отметкой времени содержат действительные подписи.

## Поддерживаемые модели электронных ключей



### USB-токены:

- JaCarta PKI;
- JaCarta PKI/Flash;
- JaCarta PKI/ГОСТ;
- JaCarta PKI/ГОСТ/Flash.

### Смарт-карты:

- JaCarta PKI;
- JaCarta PKI/ГОСТ.

 Для смарт-карт требуется считыватель ASEDriVeIIIUSB.

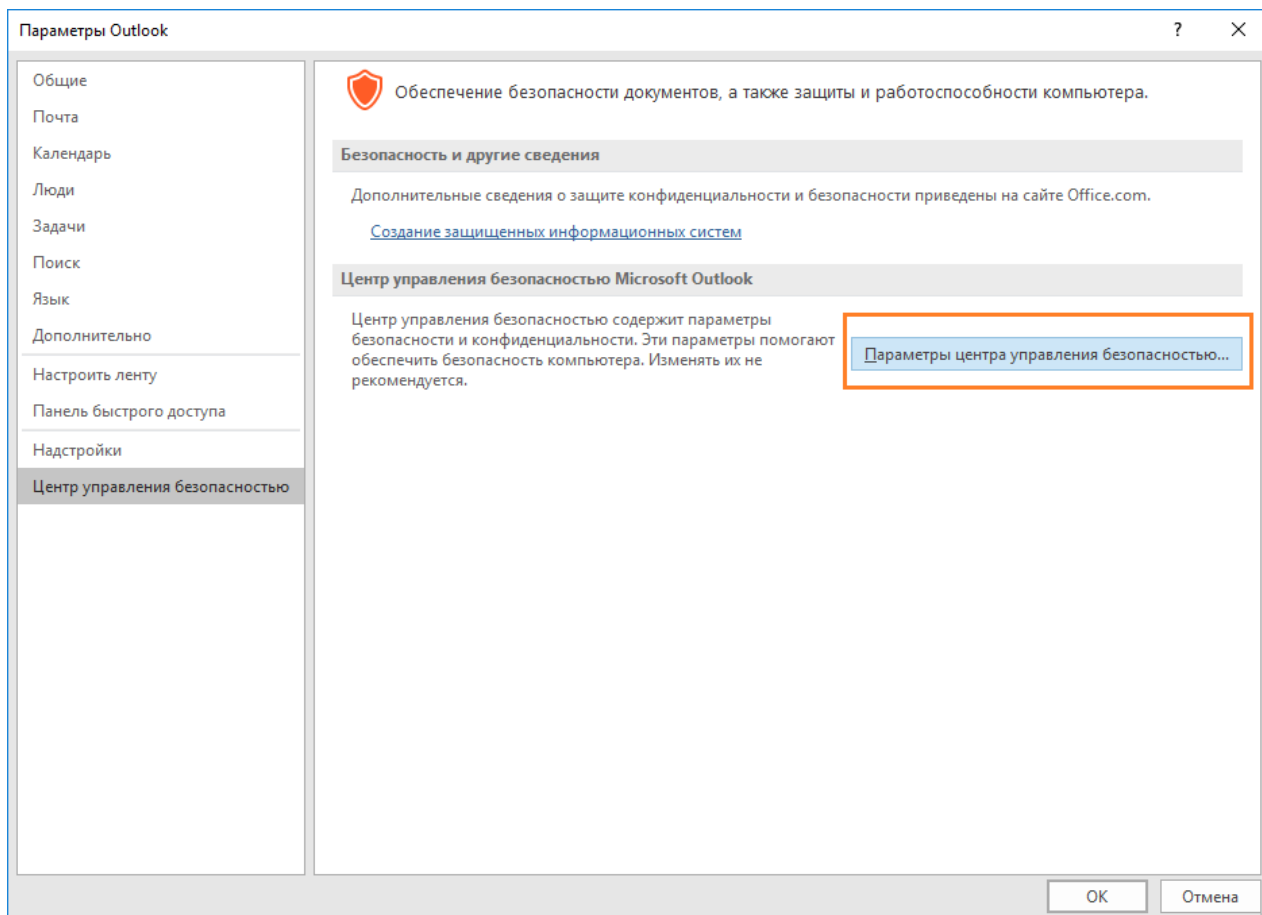
# Настройка и проверка шифрования и подписи

## Настройка параметров безопасности

В главном окне **Outlook 2016** выберите **Файл -> Параметры**.

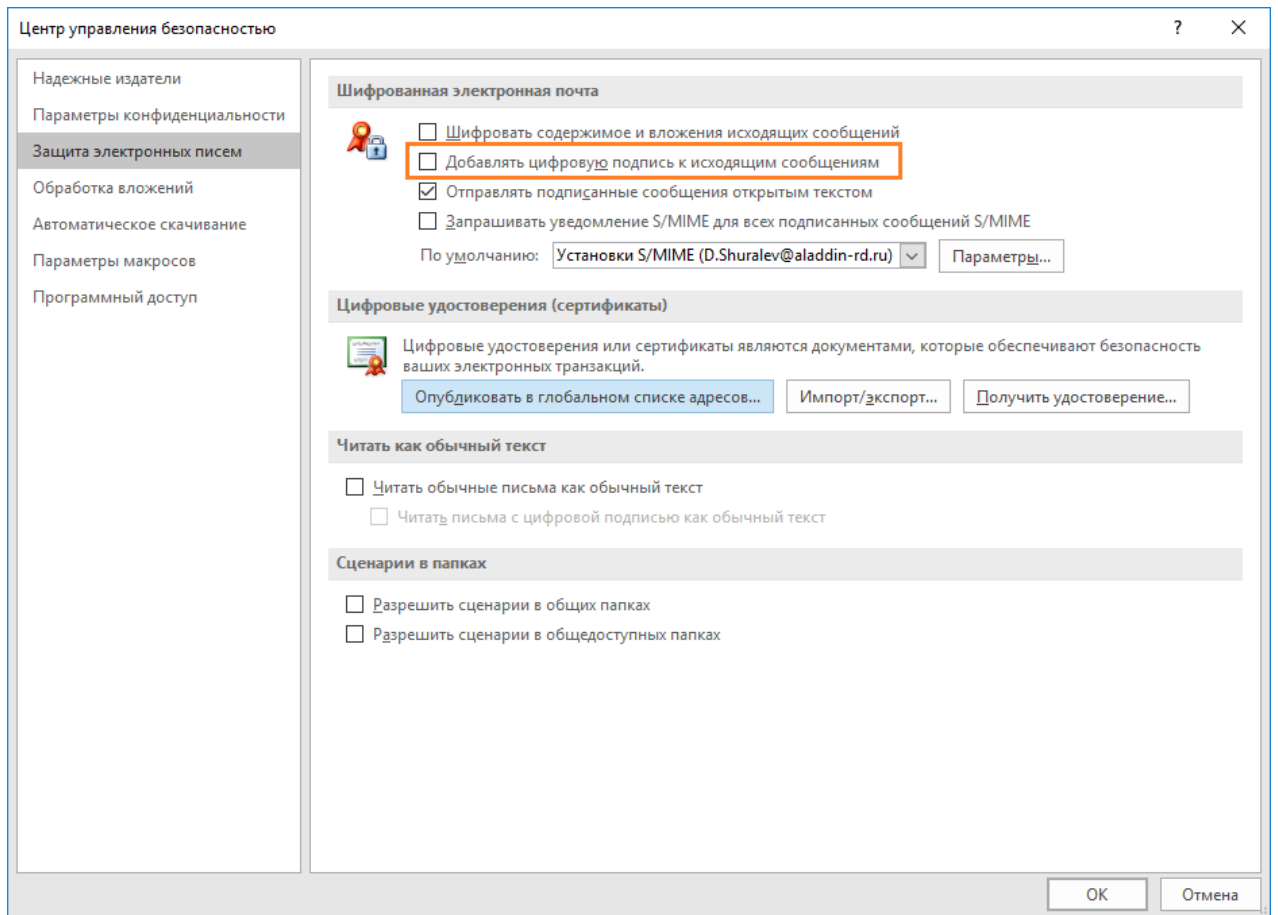
The screenshot shows the 'Сведения об учетной записи' (Account Information) settings page in Outlook 2016. On the left is a blue navigation pane with the following options: Сведения (selected), Открыть и экспортировать, Сохранить как, Сохранить вложения, Печать, Учетная запись Office, Параметры, and Выход. The main content area is titled 'Сведения об учетной записи' and displays the account '@aladdin-rd.ru' on Microsoft Exchange. Below the account name is a '+ Добавить учетную запись' button. There are four main sections, each with an icon and a title: 1. 'Настройка учетных записей' (Account Settings) with a gear icon, description: 'Измените параметры для этой учетной записи или установите больше соединений.' and a checkbox 'Доступ к этой учетной записи на веб-сайте' with the URL 'https://aladdin.ru/owa/'. 2. 'Автоответы (нет на работе)' (Out of Office) with a calendar icon, description: 'Используйте автоответы для уведомления других пользователей о том, что вы отсутствуете на рабочем месте, находитесь в отпуске или не имеете возможности отвечать на сообщения электронной почты.' 3. 'Средства очистки' (Cleanup Tools) with a trash can icon, description: 'Управляйте размером почтового ящика, используя очистку папки "Удаленные" и архивацию.' 4. 'Правила и оповещения' (Rules and Alerts) with a mail icon, description: 'Используйте правила и оповещения для организации входящих сообщений электронной почты и получения обновлений при добавлении, изменении или удалении элементов.'

В отобразившемся окне в левом меню выберите **Центр управления безопасностью** и справа нажмите **Параметры центра управления безопасностью**.

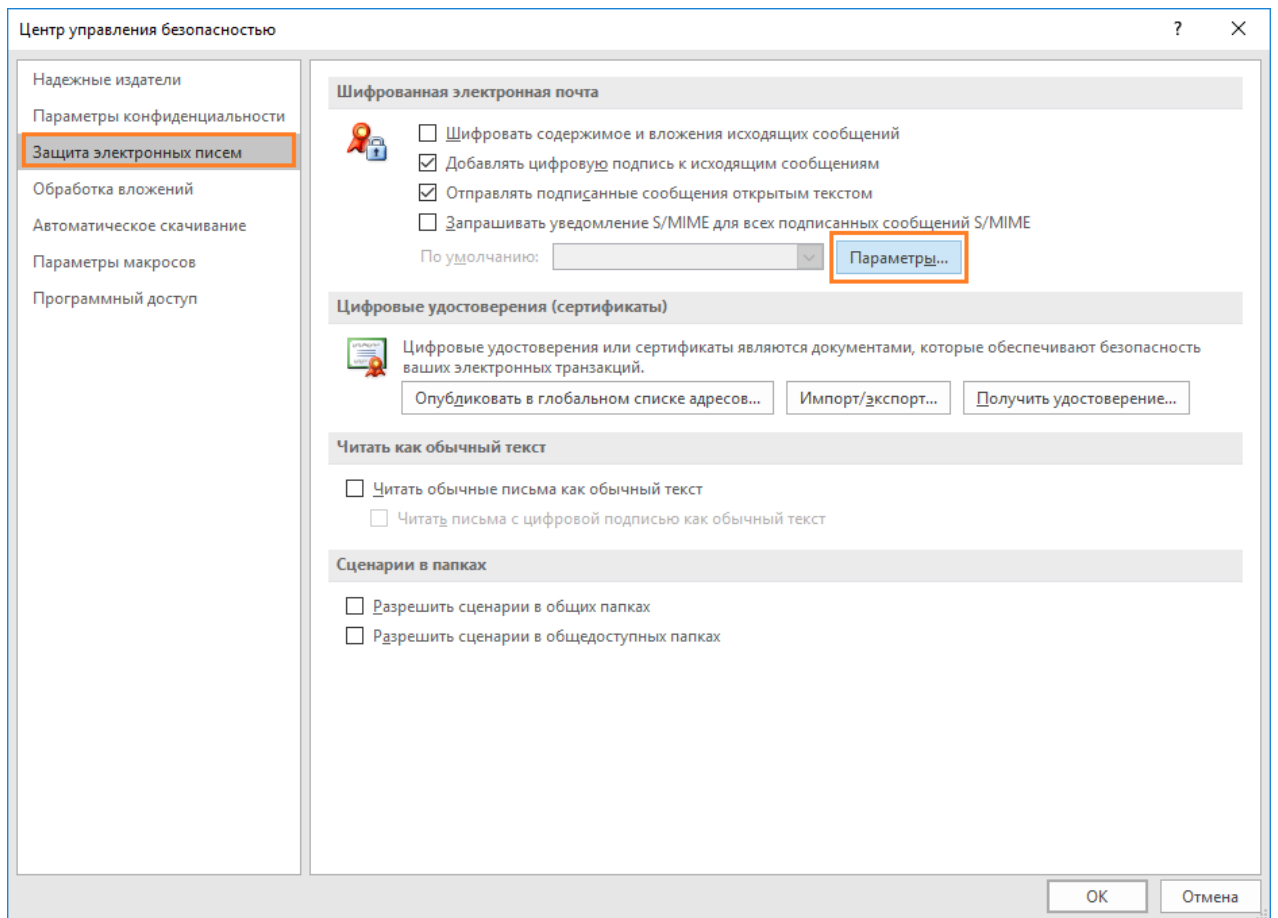




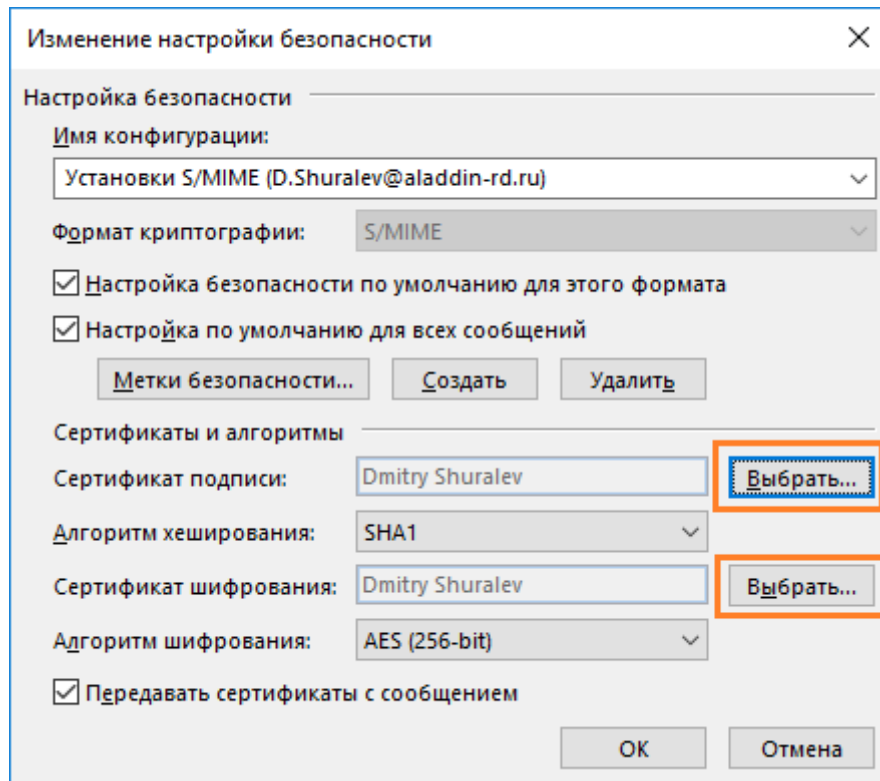
В окне **Центр управления безопасностью** выберите **Защита электронных писем**, отметьте пункт **Добавлять цифровую подпись к исходящим сообщениям**.



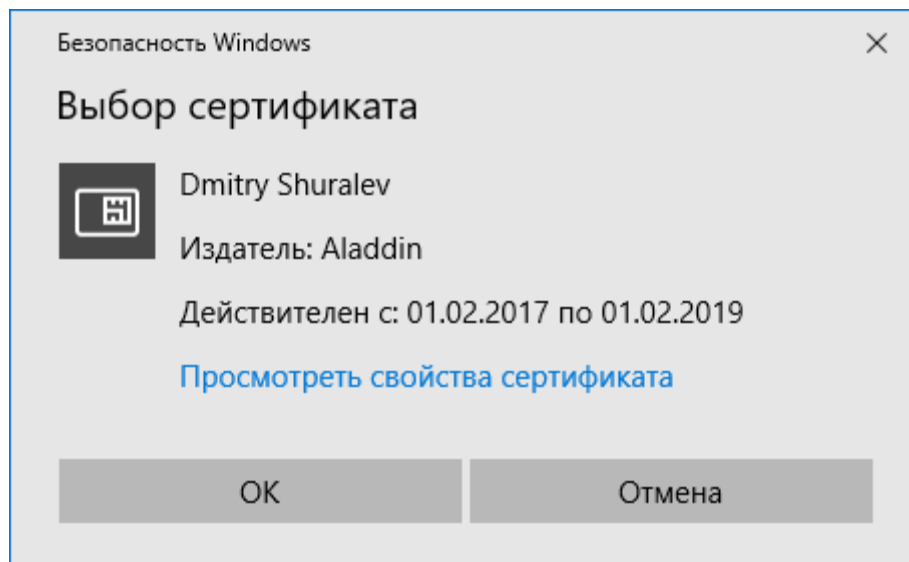
Нажмите **Параметры**.



В отобразившемся окне выберите **сертификат подписи алгоритм хэширования**. В случае если необходимо выполнить ещё и шифрование, то укажите **сертификат шифрования и алгоритм шифрования**. В настоящем примере для подписи и шифрования используется один сертификат пользователя, находящийся на **USB-токене JaCartaPKI**.



В открывшемся окне можно выбрать нужный сертификат и посмотреть его свойства. Нажмите ОК.



# Отправка и получение подписанного сообщения

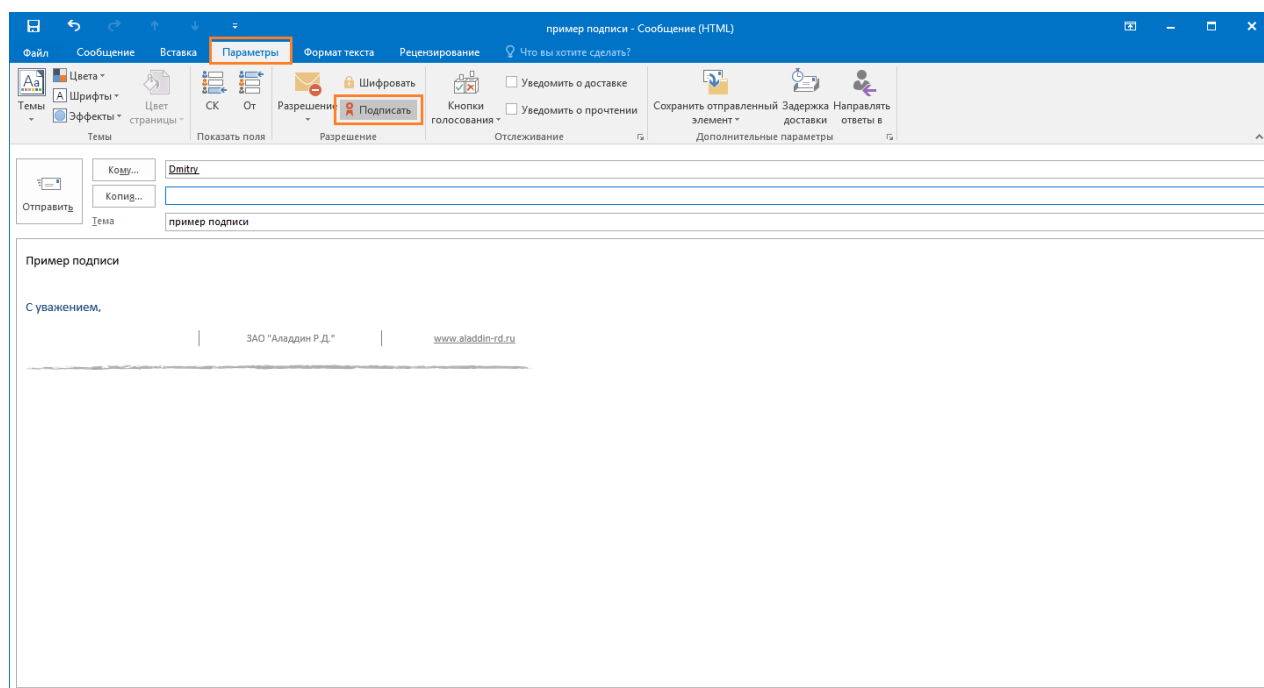
Перейдите в главное меню **Outlook 2016** и создайте **новое письмо** для произвольного получателя.

Заполните необходимые поля для отправки, выберите **Параметры -> Подпись**.

Нажмите **Подпись**.

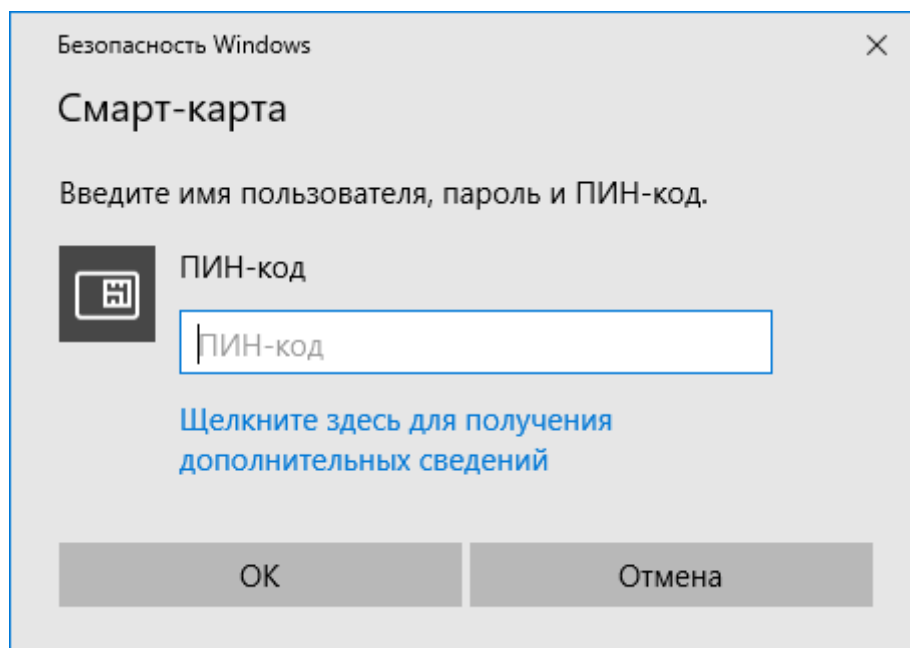



Кнопки **Подписать** и **Шифровать** доступны только после настроек параметров электронной подписи и шифрования почтовых сообщений. При нажатии кнопки **Подписать** или **Шифровать** не происходит подписи или шифрования сообщения, подпись и шифрование происходят непосредственно перед отправкой сообщения, после ввода PIN-кода.

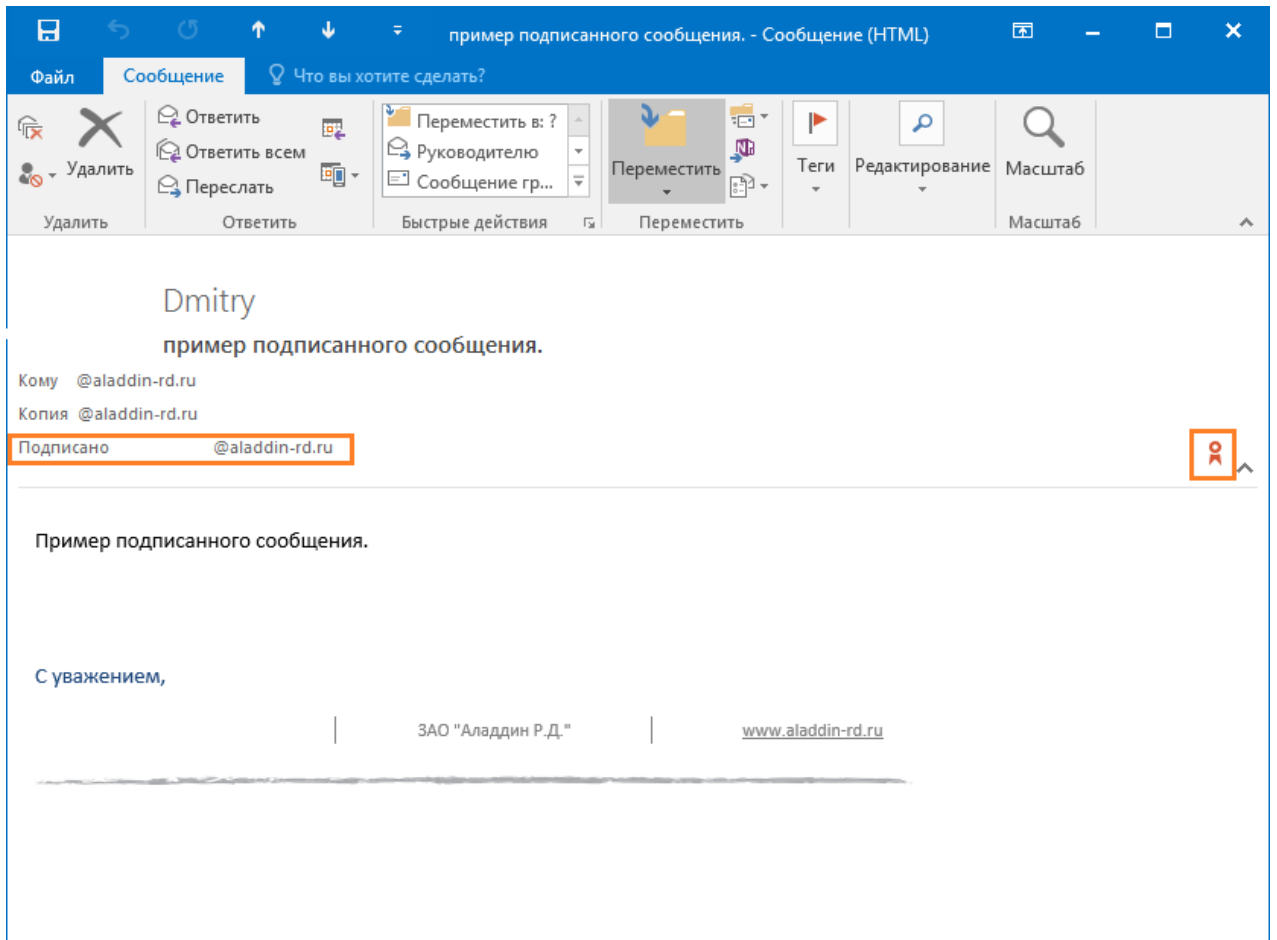



В предыдущем окне нажмите **Отправить**, отобразится окно ввода PIN-кода.

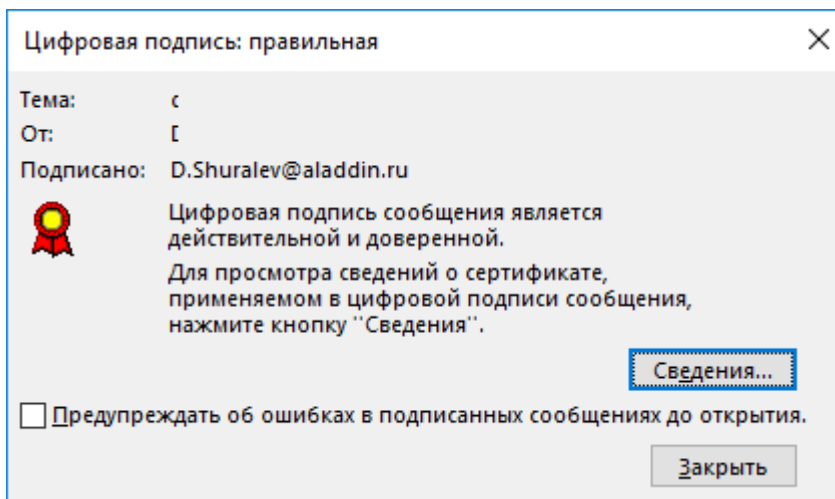
Введите PIN-код и нажмите **ОК**.



Полученное письмо с подписью будет иметь специальную пометку в виде печати  и дополнительное поле **Подписано**.



Для просмотра свойств подписи щёлкните значок .



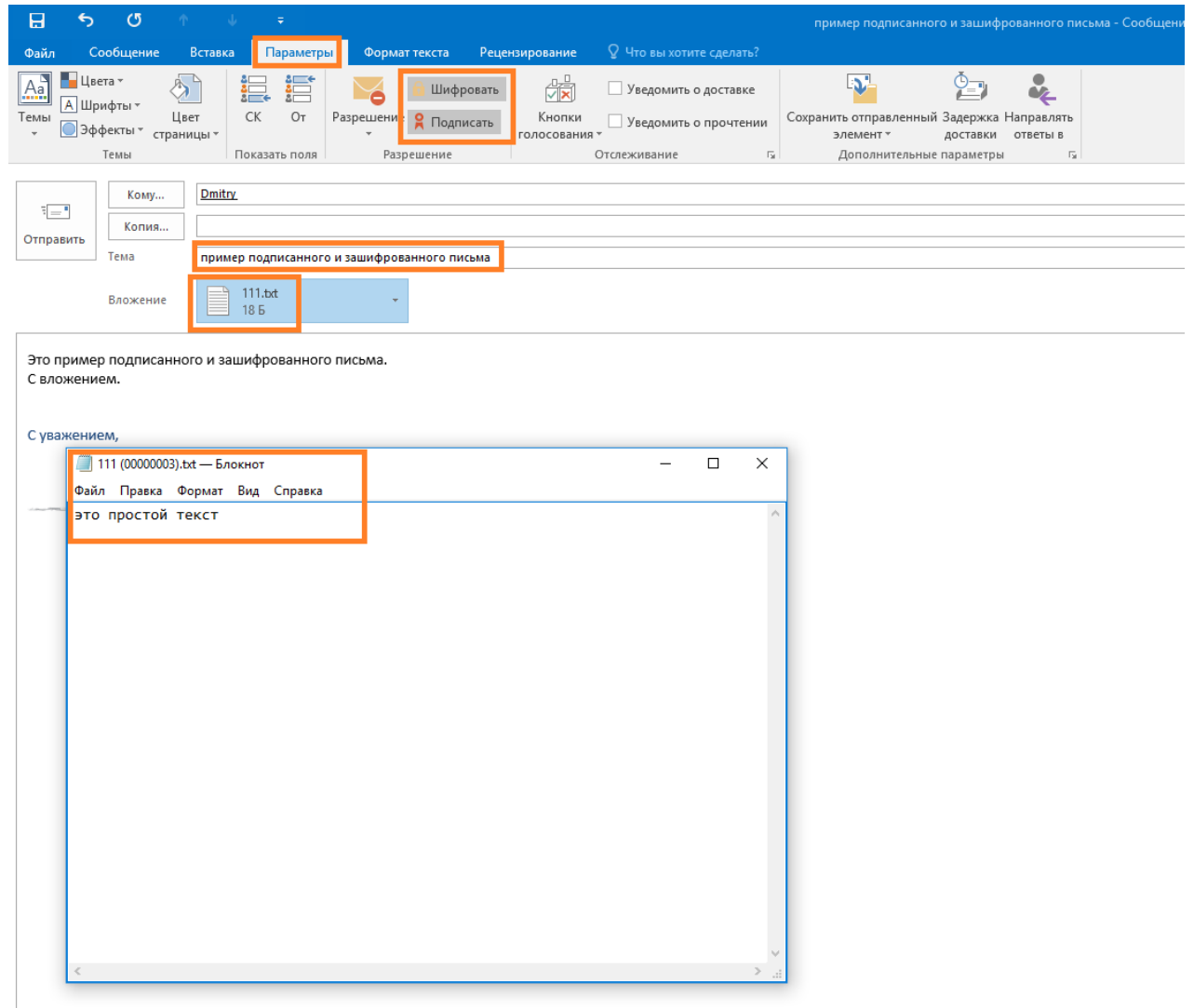
# Отправка и получение зашифрованного сообщения

Перейдите в главное меню **Outlook 2016** и создайте **новое письмо** для произвольного получателя.

Заполните необходимые поля для отправки, выберите **Параметры -> Подпись**.

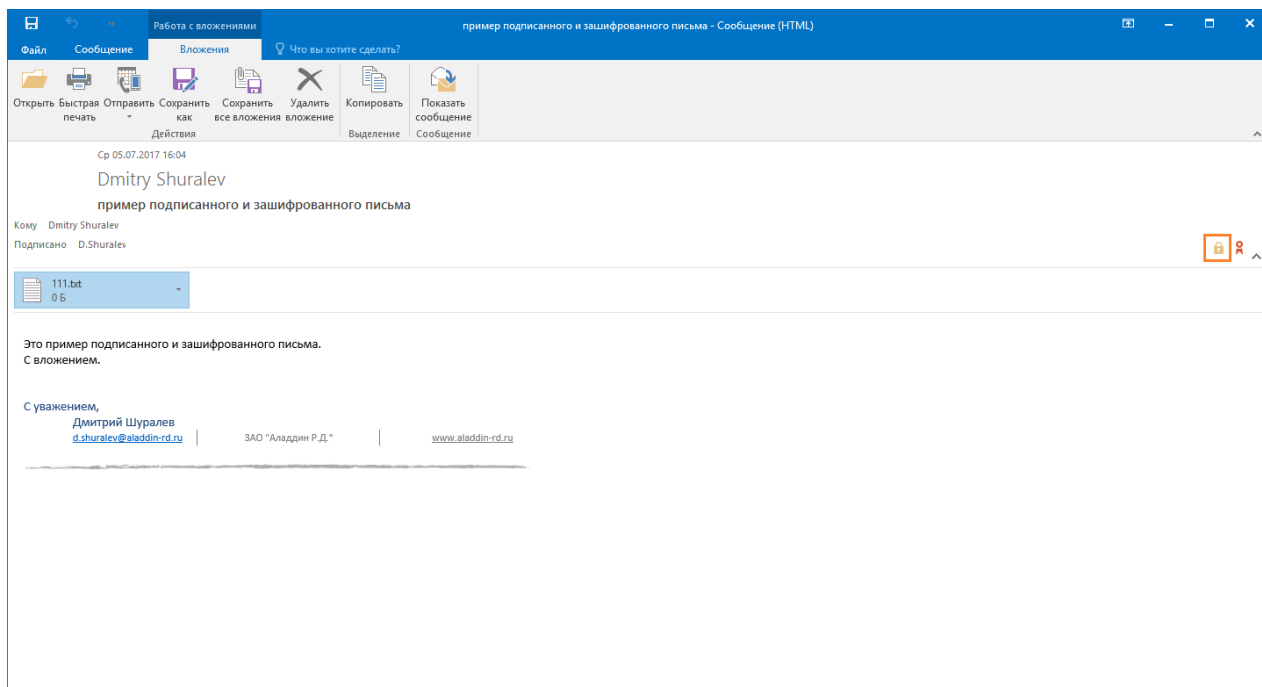
Нажмите **Подпись**, нажмите **Шифрование**.


В письмо вложите произвольный документ, например, .txt файл.

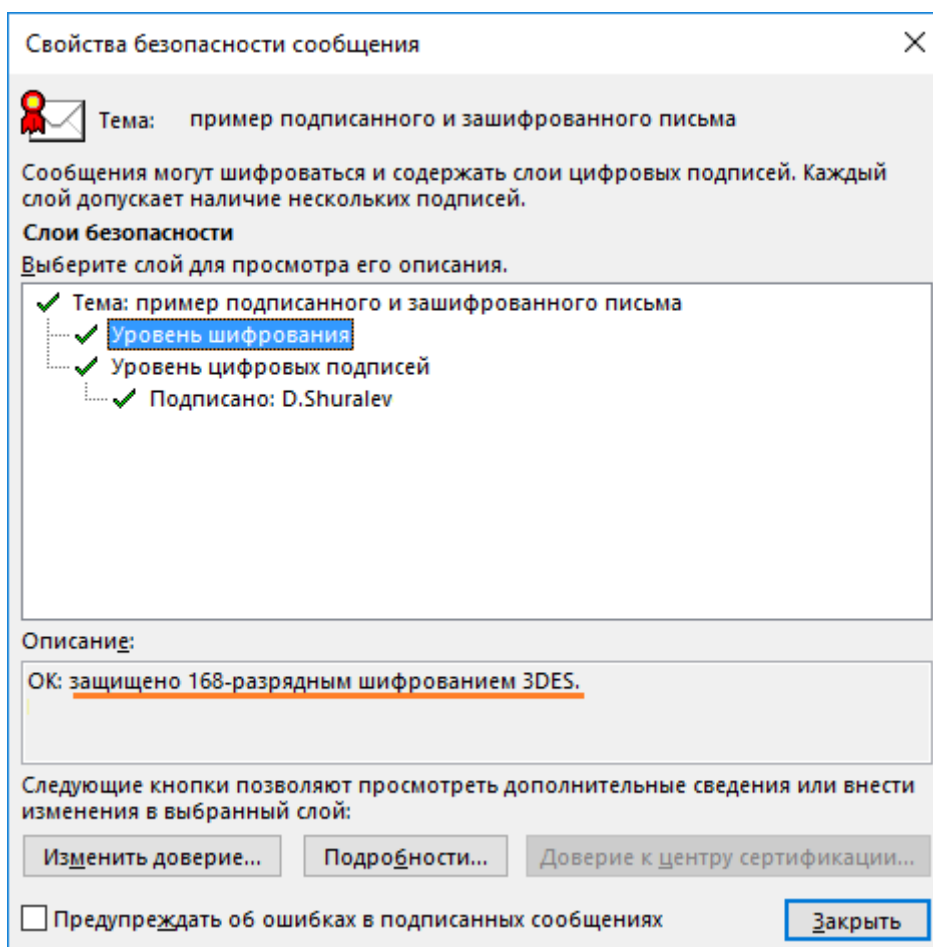




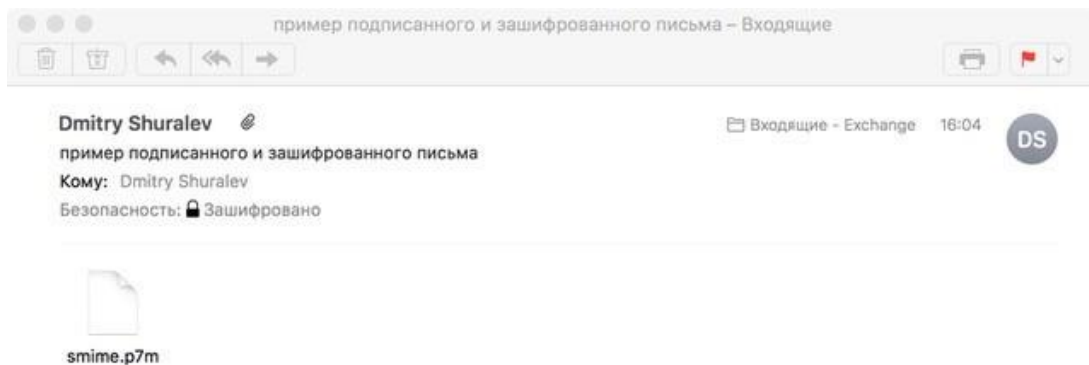
Кнопки **Подписать** и **Шифровать** доступны только после настроек параметров электронной подписи и шифрования почтовых сообщений. При нажатии кнопки **Подписать** или **Шифровать** не происходит подписи или шифрования сообщения, подпись и шифрование происходят непосредственно перед отправкой сообщения, после ввода PIN-кода.



Полученное зашифрованное письмо будет иметь специальную пометку в виде замка , нажав на который можно посмотреть свойства безопасности сообщения, в том числе алгоритм шифрования.



Если это письмо будет перехвачено злоумышленником или даже сам легитимный пользователь откроет его из стороннего места, без сертификата, то ничего, кроме темы, ему доступно не будет, так как письмо надёжно зашифровано алгоритмом 3DES.



На этом настройка и проверка шифрования и подписи электронных писем в **Microsoft Outlook 2016** завершена.



# Контакты, техническая поддержка

---

## Офис (общие вопросы)

Адрес: 129226, Москва, ул. Докукина, д. 16, стр. 1, компания "Аладдин Р.Д."

Телефоны: +7 (495) 223-00-01 (многоканальный), +7 (495) 988-46-40

Факс: +7 (495) 646-08-82

E-mail: [aladdin@aladdin-rd.ru](mailto:aladdin@aladdin-rd.ru) (общий)

Web: [www.aladdin-rd.ru](http://www.aladdin-rd.ru)

Время работы: ежедневно с 10:00 до 19:00, кроме выходных и праздничных дней

## Техподдержка

Служба техподдержки принимает запросы только в письменном виде через Web-сайт:

**[www.aladdin-rd.ru/support/index.php](http://www.aladdin-rd.ru/support/index.php)**

Для оперативного решения Вашей проблемы укажите используемый Вами продукт, его версию, подробно опишите условия и сценарии применения, по возможности, снабдите сообщение снимками экрана, примерами исходного кода.

# Регистрация изменений

---

| Версия | Изменения                 |
|--------|---------------------------|
| 1.0    | Исходная версия документа |
|        |                           |
|        |                           |



Лицензии ФСТЭК России № 0037 и № 0054 от 18.02.03, № 2874 от 18.05.12  
Лицензии ФСБ России № 12632 Н от 20.12.12, № 24530 от 25.02.14  
Лицензия Министерства обороны РФ № 1384 от 22.08.16  
Система менеджмента качества компании соответствует требованиям стандарта ISO/ИСО 9001-2011  
Сертификат СМК ГОСТ Р ИСО 9001-2011 № РОСС RU.ИС72.К00082 от 10.07.15  
Apple Developer

© ЗАО "АладдинР.Д.", 1995–2017. Все права защищены.

Тел. +7 (495) 223-00-01 Email: [aladdin@aladdin-rd.ru](mailto:aladdin@aladdin-rd.ru) Web: [www.aladdin-rd.ru](http://www.aladdin-rd.ru)