

StopPhish Report Outlook Plugin

Инструкция по установке
v2.1.0.0

StopPhish



Оглавление

1	Описание	2
1.1	Комплект поставки	2
1.2	Системные требования	2
1.3	Лицензионное соглашение	3
1.4	Предоставление/передача данных	4
2	Описание StopPhish Report Outlook Addin	5
2.1	Предварительные требования	5
2.2	Порядок работы надстройки	5
3	Установка	7
3.1	Предварительная настройка	7
3.2	Установка через Групповые Политики Windows	7
3.3	Установка через командную строку	11
4	Настройки	13
4.1	Описание настроек	13
	ISD EMAIL	13
	confirmMessage	13
	adminEmailNotFoundMessage	14
	gratitudeMessage	14
	exceptionWhileSendingReport	14
	reportEmailBody	15
	reportEmailSubject	15
	buttonLabel	15
	groupLabel	15
5	Удаление	16
5.1	Удаление групповой политики	16
5.2	Удаление плагина установленного вручную	16

Описание

1.1 Комплект поставки

- Пакеты установки:
 - SROA_x64.msi - для 64-разрядной версии Office
 - SROA_x86.msi - для 32-разрядной версии Office
- stopphish-sign.crt - сертификат подписи ПО
- Instruction.pdf - инструкция по установке
- EULA.txt - лицензионное соглашение
- Шаблоны для настройки групповых политик:
 - StopPhish-Report-Outlook-Addin.adml
 - StopPhish-Report-Outlook-Addin.admx

1.2 Системные требования

- ОС Windows
- .NET Framework 4.7.2 Runtime или выше (обычно уже установлена в новых версиях ОС Windows):
<https://dotnet.microsoft.com/en-us/download/dotnet-framework/net472>
- Visual Studio 2010 Tools for Office Runtime (не всегда устанавливается вместе с Office, может потребоваться установка):
<https://www.microsoft.com/en-us/download/details.aspx?id=105890>
- Плагин протестирован на Microsoft Outlook for Windows® версий:
 - 2013
 - 2016
 - 2019
 - 2021

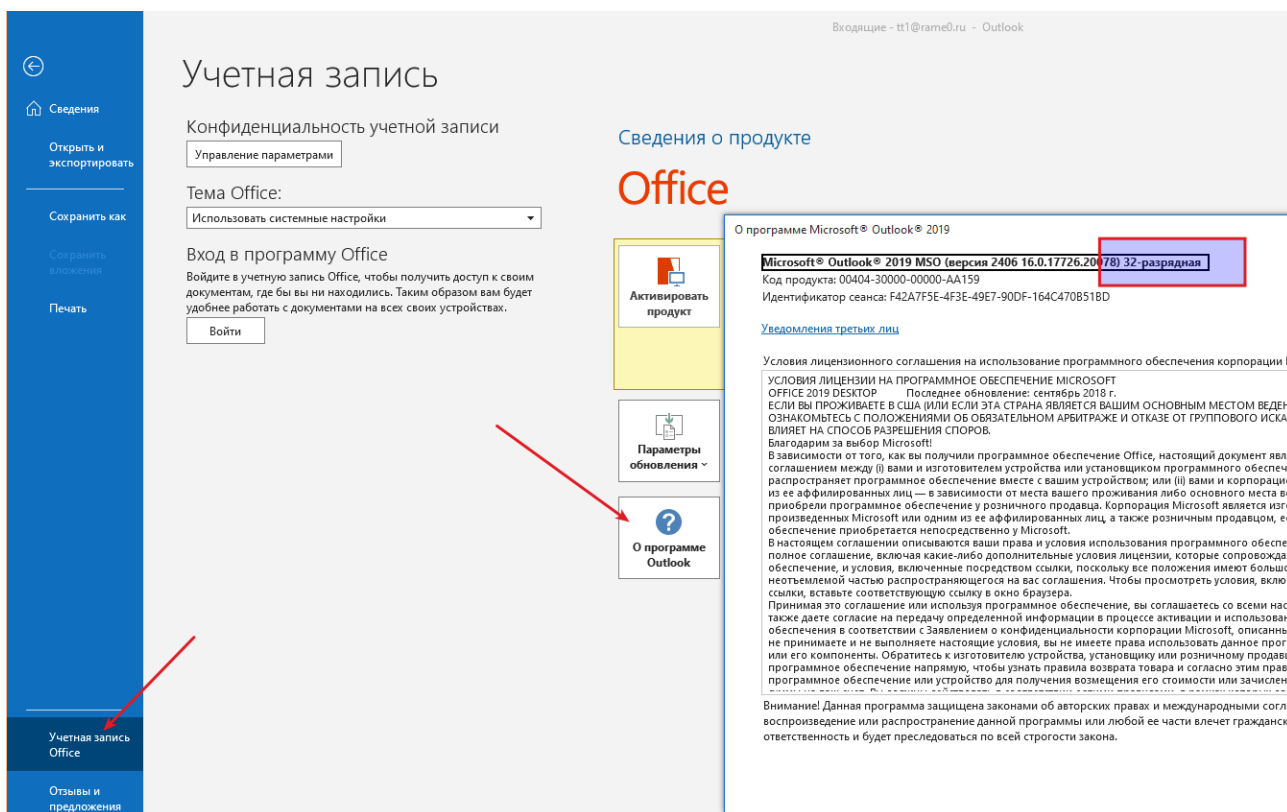
- Разрядность **Outlook**

Для корректной работы плагина, важно установить плагин той-же разрядности, что и Outlook (важно, не Windows, а именно Outlook).



Для 64-разрядной версии Outlook нужно использовать установщик SROA_x64.msi.
Для 32-разрядной - SROA_x86.msi.

Определить разрядность установленной версии можно здесь:



- **Сертификат подписи ПО**

В некоторых случаях плагин может не установиться, т.к. в текущей версии мы используем самоподписанный сертификат для подписи ПО.

Если у вас возникла такая проблема, добавьте сертификат **stopphish-sign.crt**, входящий в комплект поставки, в **Trusted Publishers**

1.3 Лицензионное соглашение

Лицензионное соглашение – это юридическое соглашение между вами и ООО "Си Кьюр", в котором указано, на каких условиях вы можете использовать программу.



Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с программой.

Если вы не согласны с условиями Лицензионного соглашения, не устанавливайте и не используйте Программное обеспечение.

Вы можете ознакомиться с условиями Лицензионного соглашения, прочитав документ **EULA.txt**, входящий в комплект поставки.

Установив данное Программное обеспечение вы соглашаетесь с условиями Лицензионного соглашения.

1.4 Предоставление/передача данных

Данное Программное обеспечение не собирает и не передает данные ООО "Си Кьюр" либо третьим лицам.

Когда пользователь отправляет отчет с подозрительным письмом, Программное обеспечение добавляет это письмо к отчету. Отчет отправляется на электронную почту указанную администратором системы на этапе установки.

Описание StopPhish Report Outlook Addin

VSTO надстройка (плагин) для MS Outlook, позволяющая направлять информацию о подозрительных электронных письмах (о фишинге) в подразделение информационной безопасности.

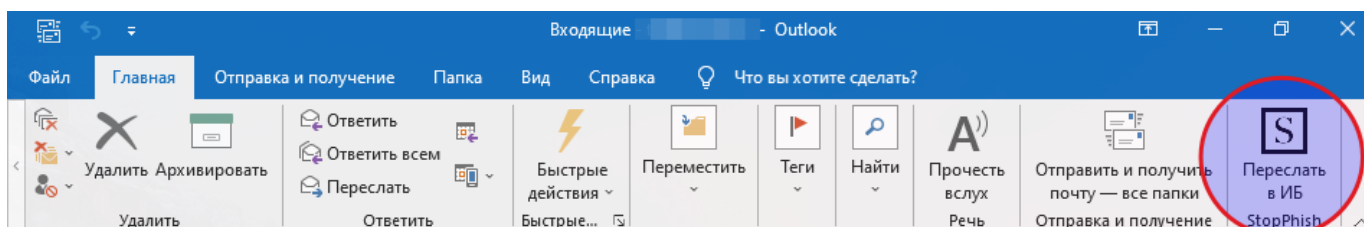
Когда пользователи щелкают по кнопке надстройки, они могут предупредить подразделение ИБ о потенциальных или реальных фишинговых атаках.

2.1 Предварительные требования

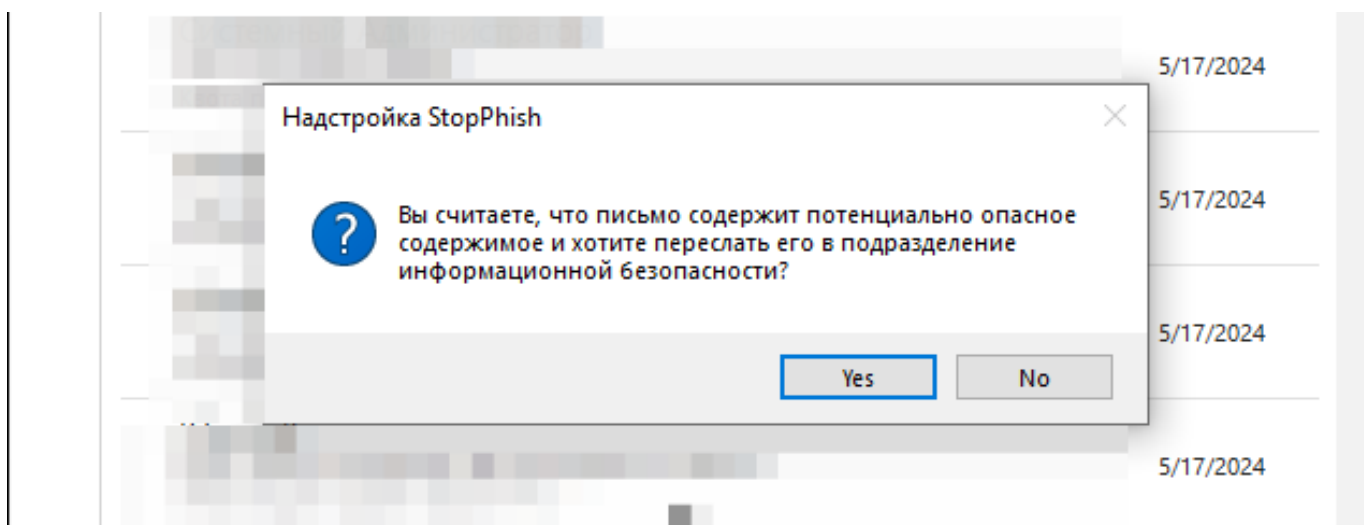
Если в вашей организации еще нет общей почты для сбора репортов пользователей, вам необходимо ее создать. Позже она понадобится в настройках плагина.

2.2 Порядок работы надстройки

После установки надстройка на ленте MS Outlook в группе TabMail ("Главная") появляется группа надстройки "StopPhish" с кнопкой "Переслать в ИБ". Иконка кнопки - логотип StopPhish (буква "S" в квадрате).



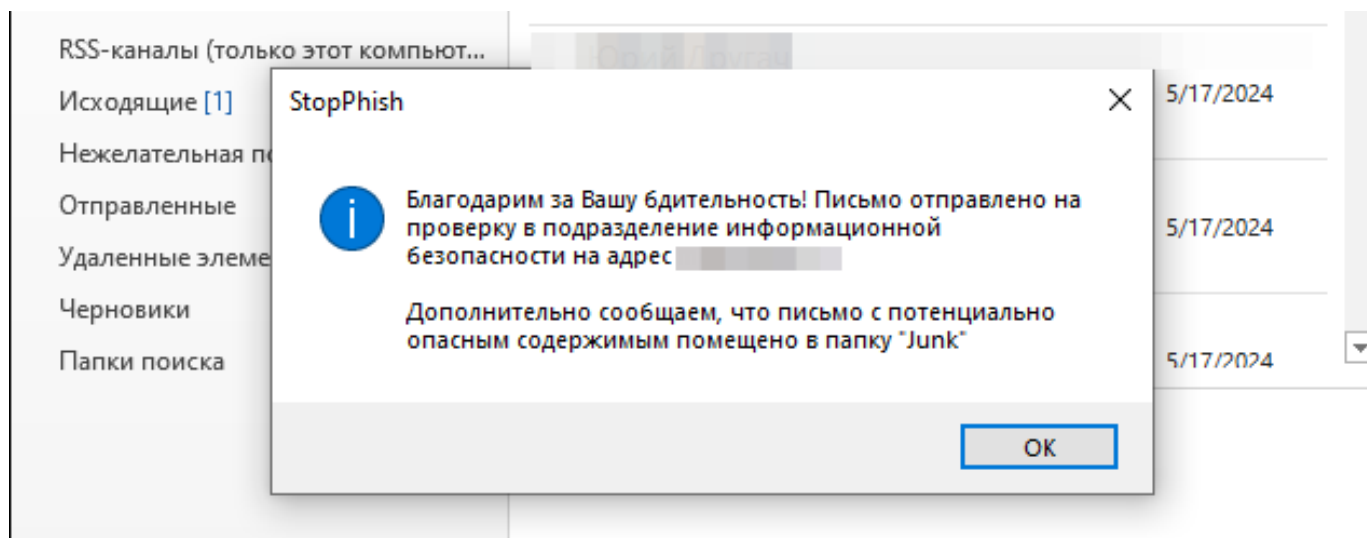
При нажатии на кнопку "Переслать в ИБ", всплывает окно для подтверждения отправки.



Когда пользователь подтвердит отправку, плагин благодарит его за бдительность, а в службу ИБ отправляется письмо с отчетом.

Письмо, в отношении которого был отправлен отчет, автоматически помещается в папку для нежелательной почты (спам) текущего аккаунта пользователя (того, на которое пришло

письмо с подозрительными признаками).



Письмо содержит:

- Тема сообщения: "Обнаружено подозрительное письмо!"
- Вложение: письмо, в отношении которого отправляется отчет, в eml формате.
- Важность сообщения: высокая.
- Текст в теле сообщения:



Во вложении письмо, которое сотрудник считает подозрительным. В нем либо действительно вредоносная нагрузка, либо сотрудник не до конца разобрался и перестраховывается. По возможности, поблагодарите его за бдительность

Установка

Плагин StopPhish Report Outlook Addin можно установить в операционной системе Windows® через групповые политики Active Directory® либо через командную строку с правами администратора.

3.1 Предварительная настройка

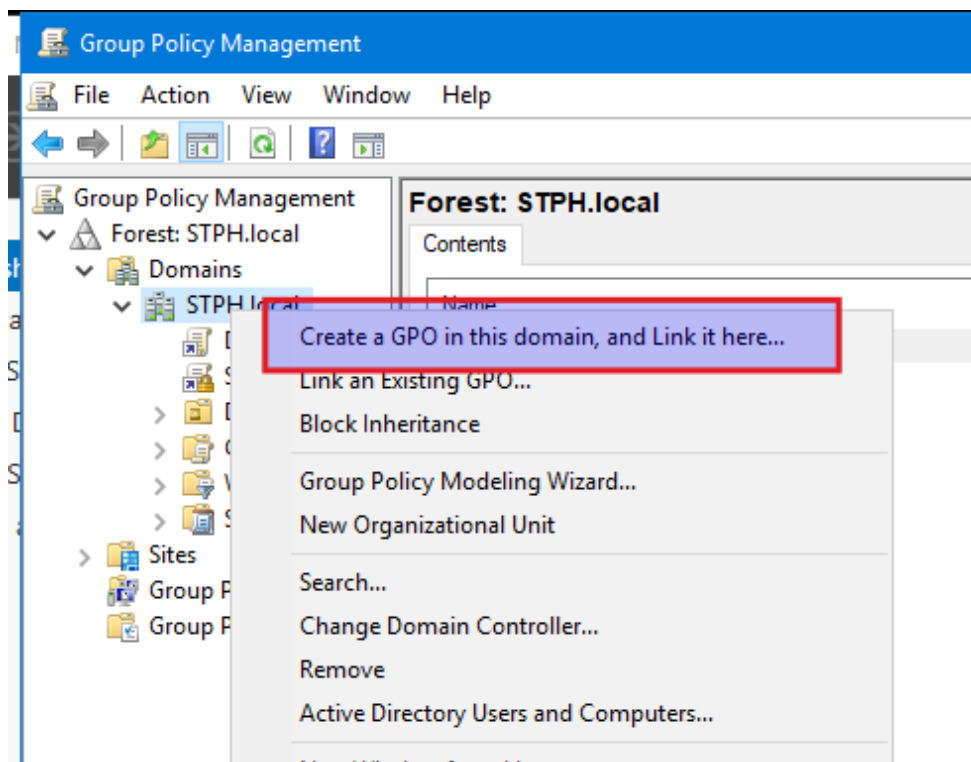
Для возможности установки плагина, с помощью групповых политик Active Directory в реестре на компьютерах пользователей должны быть созданы записи с настройками. Для того чтобы иметь возможность установить эти настройки, добавьте следующие файлы шаблонов групповых политик на сервере администратора домена:

1. Шаблон групповой политики `StopPhish-Report-Outlook-Addin.admx` в папке `C:/Windows/PolicyDefinitions`.
2. Локализация шаблона групповой политики `StopPhish-Report-Outlook-Addin.adml` в папке `C:/Windows/PolicyDefinitions/en-US`.

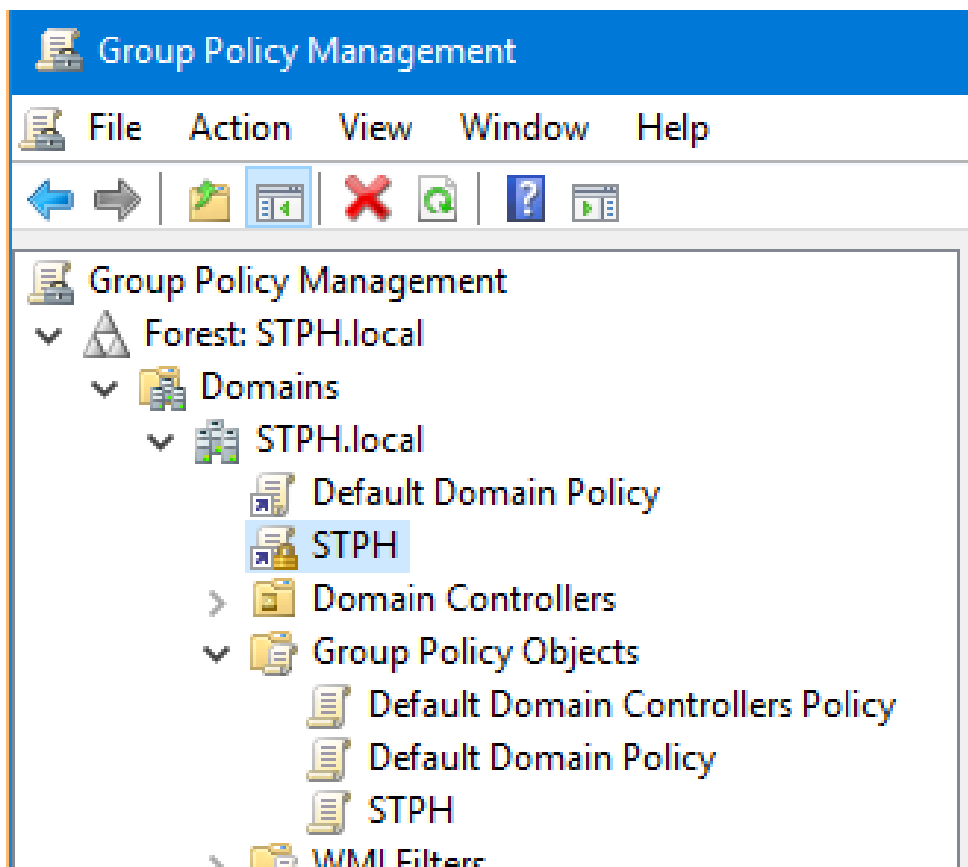
3.2 Установка через Групповые Политики Windows

Перед началом настройки групповых политик, разместите файл установщик ПО StopPhish Report Outlook Addin в общей сетевой папке (папка должна быть доступной для всех пользователей входящих в группу для которой настраивается политика).

1. Откройте консоль Group Policy Management, нажав комбинацию клавиш **WIN+R** и выполнив следующую команду: `gpmc.msc`
2. Создайте в консоли Group Policy Management объект групповой политики:
 - (a) В разделе **Domains** найдите домен, для которого необходимо добавить политику, нажмите на него правой кнопкой мыши и выберите **Create a GPO in this domain, and Link it here**.



- (b) В открывшемся окне создания объекта групповой политики введите название для объекта **OK**.
- (c) Созданная ссылка на объект групповой политики будет отображаться в разделе **Domain**, а сам объект будет в разделе **Group Policy Objects**.



- (d) Нажмите правой кнопкой мыши на созданной ссылке и во всплывающем меню выберите **Enforced**



Если в вашей организации используются версии Office различной разрядности, то нужно будет создать разные политики, чтобы установить плагин корректной разрядности.

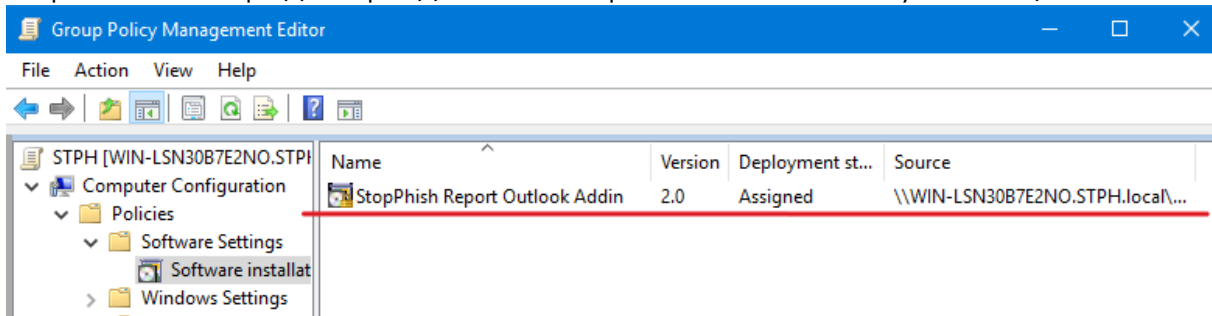
3. Нажмите правой кнопкой мыши на только что созданную ссылку на объект групповой политики и выберите **Edit**. Откроется окно редактирования объекта групповой политики.
4. Создайте политику для установки плагина:
 - (a) Перейдите в раздел **Computer Configuration \ Policies \ Software Settings \ Software Installation**.
 - (b) Нажмите правой кнопкой на **Software Installation**
 - (c) Выберите **New -> Package...**
 - (d) В открывшемся окне выберите UNC-путь до общей папки, в которой вы разместили файл установщика плагина.

Пример: `\\server\share\SOFT\SR0A_x86.msi` (для 32-разрядной версии Outlook)

Пример: `\\server\share\SOFT\SR0A_x64.msi` (для 64-разрядной версии Outlook)

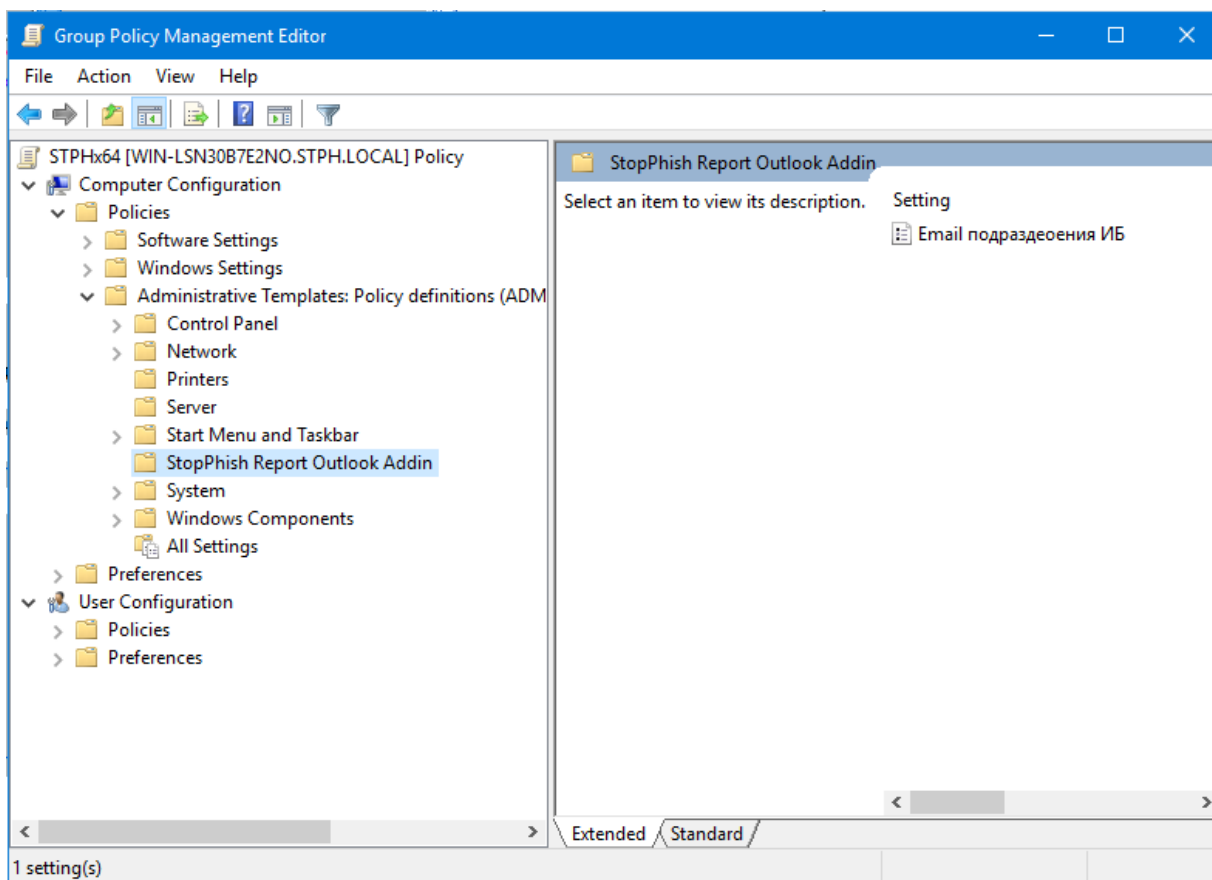
(е) В открывшемся окне **Deploy Software** выберите **Assigned** и нажмите **Ok**

(f) В правой части редактора должно отобразиться название установщика плагина:



5. Добавление почты службы ИБ на которую будут отправляться отчеты:

(а) Перейдите в раздел **Computer Configuration \ Preferences \ Administrative Templates:...**
\StopPhish Report Outlook Addin.

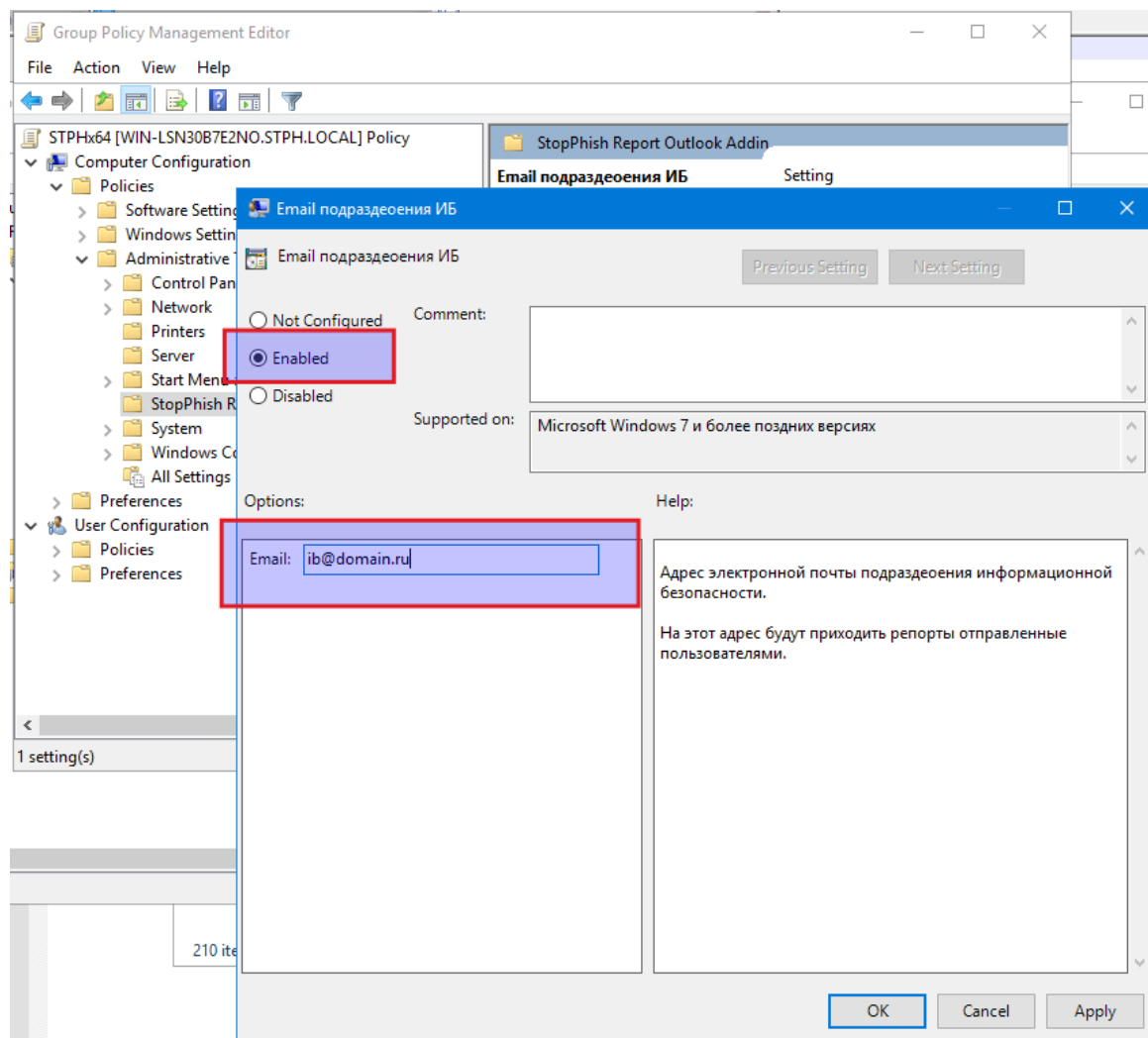


(b) Нажмите правой кнопкой на **Email подразделения ИБ**

(c) Выберите **Edit**

(d) В открывшемся окне укажите такие настройки:

- **Enabled**
- **Email:** email подразделения ИБ. На него будут приходить отчеты от пользователей



(е) Нажмите **Ok**

На экране Управление групповыми политиками щелкните правой кнопкой мыши новый объект групповой политики и убедитесь, что рядом с пунктами **Enforced** и **Link Enabled** установлен флажок.

Объект групповой политики создан, настроена. При следующем запуске указанных в политике компьютеров, на них будет установлен плагин.

Если между созданием политики и перезагрузкой прошло мало времени, политика может не примениться. В таком случае нужно перезагрузить компьютер повторно.

3.3 Установка через командную строку

1. Разместите на компьютере пользователя файл установщика из комплекта поставки: `SR0A_x86.msi` или `SR0A_x64.msi` (в зависимости от разрядности установленной на компьютере пользователя версии Outlook).
2. Запустите командную строку (`cmd.exe`) с правами администратора.
3. Перейдите в папку с в которую вы сохранили файл установщика

4. Запустите установку. Например, для 32-разрядной версии Outlook:

```
1 msixexec.exe /i "SR0A_x86.msi" EMAIL="ib@domain.ru" /qn /L*V "Setup.log"
```

* Обратите внимание, что команда должна быть написана в одну строку

Здесь:

- EMAIL - электронная почта на которую будут приходить отчеты отправляемые пользователями
- /qn (не обязательно) - запуск в тихом режиме без UI
- /L*V <filename> (не обязательно) - сохранить журнал установки в файл <filename>

После завершения установки плагин будет добавлен в Outlook.

Если кнопка  в Outlook не появилась, проверьте лог установки на ошибки.

Важно! Обратите внимание, если в реестре Windows уже был записано значение ISD_EMAIL по пути SOFTWARE\POLICIES\SE_CURE\OutlookAddins\StopPhishReport (например после предыдущей установки), то указанный в параметрах установки ключ EMAIL не будет иметь эффекта и плагин будет использовать ту почту, которая указана в реестре.

Настройки

Начиная с версии 2.1.0.0 надстройку можно настроить по своему усмотрению. Настройка осуществляется через групповые политики, либо через редактирование/создание записей в реестре напрямую.

Setting	State	Comment
Email подразделения ИБ	Enabled	No
Текст ошибки email ИБ	Enabled	No
Текст на кнопке	Enabled	No
Текст подтверждения	Enabled	No
Текст сообщения об ошибке при отправке	Enabled	No
Благодарность за бдительность	Enabled	No
Название группы	Enabled	No
Настройки письма в ИБ	Enabled	No

Рис. 4.1: Групповые политики

\Policies\SE_CURE\OutlookAddins\StopPhishReport		
Name	Type	Data
(Default)	REG_SZ	(value not set)
adminEmailNot...	REG_MULTI_SZ	Не найден адрес электронной почты подраздел...
buttonLabel	REG_SZ	Фишинг!
confirmMessage	REG_MULTI_SZ	Переслать в ИБ?
exceptionWhile...	REG_MULTI_SZ	Отправка не удалась.
gratitudeMessage	REG_MULTI_SZ	Спасибо.
groupLabel	REG_SZ	ИБ
ISD_EMAIL	REG_SZ	test@test.ru
reportEmailBody	REG_MULTI_SZ	Письмо во вложении.
reportEmailSubj...	REG_SZ	Это фишинг!

Рис. 4.2: Записи в реестре

Путь до ключа реестра:

```
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\SE_CURE\OutlookAddins\StopPhishReport
```

4.1 Описание настроек

ISD EMAIL

ГП: Email подразделения ИБ

Адрес электронной почты подразделения информационной безопасности. На этот адрес будут приходить репорты отправленные пользователями.

confirmMessage

ГП: Текст подтверждения

Текст окна запроса подтверждения показываемый пользователю, когда он нажимает кнопку "Переслать в ИБ".

Значение по умолчанию:



Вы считаете, что письмо содержит потенциально опасное содержимое и хотите переслать его в подразделение информационной безопасности?

adminEmailNotFoundMessage

ГП: Текст ошибки email ИБ

Сообщение об ошибке показываемое пользователю, если email службы ИБ не настроен.

Значение по умолчанию:



Не найден адрес электронной почты подразделения информационной безопасности. Для решения проблемы обратитесь к системному администратору.

gratitudeMessage

ГП: Благодарность за бдительность

Сообщение с благодарностью за бдительность, когда пользователь отправляет отчет в службу ИБ.

Вы можете использовать в тексте шаблон "{0}", вместо него будет подставлен email службы ИБ на который был отправлен отчет.

Значение по умолчанию:



Благодарим за Вашу бдительность! Письмо отправлено на проверку в подразделение информационной безопасности на адрес {0}.

exceptionWhileSendingReport

ГП: Текст сообщения об ошибке при отправке

Текст сообщения об ошибке при попытке отправить письмо в службу ИБ.

Значение по умолчанию:



Во время отправки сообщения возникла ошибка. Обратитесь к администратору системы.

reportEmailBody

ГП: Настройки письма в ИБ

Здесь вы можете изменить тело письма отправляемого в службу ИБ, когда пользователь нажимает кнопку "Переслать в ИБ".

Значение по умолчанию:



Во вложении письмо, которое я считаю подозрительным. Возможно, письмо содержит фишинговые ссылки или иное вредоносное содержимое.

reportEmailSubject

ГП: Настройки письма в ИБ

Здесь вы можете изменить тему письма отправляемого в службу ИБ, когда пользователь нажимает кнопку "Переслать в ИБ".

Значение по умолчанию:



Обнаружено подозрительное письмо!

buttonLabel

ГП: Текст на кнопке

Изменить текст на кнопке отправки отчета в службу ИБ.

Значение по умолчанию:



Переслать в ИБ

groupLabel

ГП: Название группы

Изменить название группы в которой находится кнопка отчета в службу ИБ.

Значение по умолчанию:



StopPhish

Удаление

5.1 Удаление групповой политики

1. Откройте консоль Group Policy Management, нажав комбинацию клавиш **WIN+R** и выполнив следующую команду: `gpmc.msc`
2. Нажмите правой кнопкой мыши на созданную на предыдущем шаге ссылку на объект групповой политики и выберите **Edit**. Откроется окно редактирования объекта групповой политики.
3. Удалите политику для установки плагина:
 - (a) Перейдите в раздел **Computer Configuration \ Policies \ Software Settings \ Software Installation**.
 - (b) В правой части нажмите правой кнопкой на **StopPhish Report Outlook Addin**
 - (c) Выберите **All Tasks -> Remove...**
 - (d) В открывшемся окне выберите выберите как должен удалиться плагин.
 - (e) Нажмите **Ok**

Плагин **StopPhish Report Outlook Addin** должен будет удалиться после следующей перезагрузки компьютера пользователя.

5.2 Удаление плагина установленного вручную

Удаление вручную выполняется стандартными средствами установки и удаления программ ОС Windows.