Рекомендации
по обеспечению безопасности информации при работе с почтовыми сервисами в органах власти Смоленской области

При взаимодействии с почтовыми сервисами работники органов власти Смоленской области должны использовать рабочий почтовый адрес (ИМЯ@admin-smolensk.ru) только для служебной переписки, не указывать его в общедоступных источниках, не связанных с служебной деятельностью (регистрация на сайтах, форумах, при оформление подписок и т.д).

Для предотвращения заражения рабочих станций компьютерными вирусами необходимо руководствоваться следующими рекомендациями:

1. Своевременное обновление средств антивирусной защиты и операционной системы

Необходимо отслеживать состояние обновлений установленного антивируса и операционной системы на рабочей станции. Обновление антивирусных средств для рабочих станций, подключенных к распределенной мультисервисной сети связи и передачи данных органов исполнительной власти Смоленской области и органов местного самоуправления Смоленской области (далее – РМС), осуществляется в автоматическом режиме в соответствии с Положением об организации антивирусной защиты в органах власти Смоленской области и подведомственных им учреждениях, утвержденном приказом начальника Департамента Смоленской области от 10 сентября 2014 г № 50. В случае сбоя задачи обновления на рабочей станции следует уведомить о данном факте ответственного за обеспечение антивирусной защиты информации органа власти.

Обновления операционной системы также должно производиться в автоматическом режиме (параметры обновления Windows → Пуск / Настройка / Панель управления / Система / Автоматическое обновление). Для рабочих станций, входящих в доменную зоны admin-smolensk.ru, обновления происходят централизованно, в случае сбоя необходимо уведомить о возникшей проблеме системного администратора органа власти.

2. Отключение автоматического просмотра полученных электронных писем

В случае использования программы MS Outlook для работы с почтой необходимо отключить автопросмотр писем (MS Outlook → Вид /Текущее представление → Проверить снятие галочки с графы «Сообщения с автопросмотром»).

Если в полученном сообщении содержится вложение, содержимое которого нужно быстро просмотреть без его открытия, вложение можно просмотреть в области чтения (MS Outlook → Вид /Область чтения). Не рекомендуется осуществлять предварительный просмотр содержимого или открытие вложения, электронных писем, полученных из ненадежных или неизвестных источников. Для защиты от вредоносных программ внедренное содержимое вложений (включая сценарии, макросы и элементы управления ActiveX) отключается во время предварительного просмотра.

Средства просмотра вложений, которые поддерживает MS Outlook по умолчанию включены. Необходимо отключить их: MS Outlook → Сервис / Центр управления безопасностью / Обработка вложений / Отключить просмотр вложений.

3. Проверка ссылок на ресурсы сети «Интернет»

Так же обращаем Ваше внимание на необходимость предварительной проверки ссылок на страницы в сети Интернет, указанные в почтовых сообщениях (в средствах MS Outlook адрес появляется в окне над курсором при его наведении на ссылку). Адрес перехода может не совпадать с визуальным представлением ссылки в письме. В таком случае переходить по ссылке производить запрещено. О факте получения письма с подобными ссылками необходимо уведомить ответственного за обеспечение антивирусной защиты информации органа власти и

добавить отправителя в список нежелательных (порядок действий подробно описан в п.5 Рекомендаций).

4. Проверка вложенных файлов

По соображениям защиты рабочей станции в Microsoft Outlook запрещено получение файлов определенных типов (такие как BAT, EXE, VBS и JS) в виде вложений, поскольку они могут содержать вирусы, представляющие опасность для компьютера. По умолчанию почтовый клиент блокирует такие файлы. Такие вложения не отображаются, доступ к ним запрещен, но список заблокированных файлов вложений приводится в верхней части сообщения на информационной строке. Открывайте и просматривайте только те вложения, которые получены из надежных источников.

Проверка почтового контента должна осуществляться автоматически установленными средствами антивирусной защиты информации. Так же, в случае отсутствия уверенности в надежности отправителя и содержимого, в ручном режим:

- сохранить вложения на несистемном диске в отдельную папку.
- не открывая (не запуская) файлы вложений, произвести проверку файлов антивирусными средствами.

Microsoft Outlook не блокирует документы, имеющие расширения XLS, DOC, PPT и TXT. Большинство пользователей обычно работают с файлами именно этих форматов. Тем не менее, в них могут содержаться макросы, с помощью которых распространяться компьютерные вирусы. При попадании подобных файлов в папку «Входящие» их необходимо перед открытием проверить антивирусной программой.

При наличии необходимости в получении или отправке файлов, блокируемых почтовым клиентом необходимо руководствоваться следующими принципами:

- прежде чем присоединить файлы блокируемого типа к сообщению электронной почты, можно заархивировать их с помощью программы архивации;
- если возможность заархивировать вложение отсутствует, файл блокируемого типа необходимо переименовать, заменив расширение временным, отсутствующим в списке блокируемых типов файлов. Например, start.exe можно переименовать в start.exe_ok, а затем вложить в сообщение электронной почты. В тексте сообщения можно дать получателю указание сохранить файл с правильным именем start.exe.
- после получения и перед отправкой такие вложения подлежат обязательной проверке средствами антивирусной защиты;
- открывать и запускать можно только файлы, получение которых ожидались от доверенного отправителя.

5. Игнорирование писем рекламного характера

Запрещается реагировать на письма рекламного характера (СПАМ рассылки). В случае получения письма рекламного характера его необходимо удалить, предварительно добавив отправителя в «черный» список:

- Нажать правой клавишей мыши на нежелательное письмо.
- Выбрать графу «Нежелательная почта».
- Выбрать «Добавить отправителя в список заблокированных отправителей».

Такое действие позволит заблокировать получение писем от данного отправителя в дальнейшем.

Запрещается переходить по всем ссылкам в письмах, в случае отсутствии уверенности в надежности отправителя. Также, в случае наличия в письме ссылки «Отписаться от рассылки», запрещается переходить по ней, так как это ссылка также может оказаться фишинговой.