Инструкция по обработке сообщений электронной почты

В целях уменьшения риска инфицирования вредоносным программным обеспечением при обработке сообщений электронной почты необходимо руководствоваться приведенным в данной инструкции комплексом мер.

Содержание инструкции

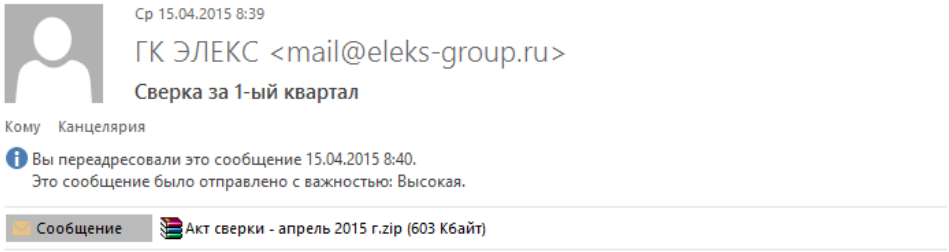
1. Характерные признаки вредоносных сообщений электронной почты

Вредоносное программное обеспечение, распространяющееся посредством электронной почты, в основном, содержится в следующих типах файлов:

- исполняемые файлы (*.exe, *.bat, *.cmd, *.pif, *.scr и др.);
- файлы формата Microsoft Office (*.doc, *.xls, *.ppt и др.). В данном случае вредоносный модуль может быть активирован следующими способами:
    - путем эксплуатации уязвимостей ПО MS Office;
    - путем запуска макросов и ActiveX-компонентов;
    - путем исполнения внедренного в документ объекта.
- файлы формата Adobe Acrobat (*.pdf). В данном случае вредоносный модуль может быть активирован следующими способами:
    - путем эксплуатации уязвимостей продуктов Adobe;
    - путем эксплуатации уязвимостей сторонних продуктов (например, Foxit Reader);
    - путем выполнения активного содержимого PDF (javascript, ActionScript, «событие» PDF формата;
- файлы, написанные на скриптовых языках (*.js, *.vbs, *.wsf и др.);
- архивы (*.rar, *.zip, *.7z), содержащие файлы представленных типов файлов.

Для выявления попыток заражения необходимо обращать внимание на следующие характерные признаки сообщений электронной почты, используемых для внедрения вредоносного программного обеспечения:

- **электронное сообщение оформлено таким образом, чтобы убедить получателя открыть вложение** (рисунок 1,2);

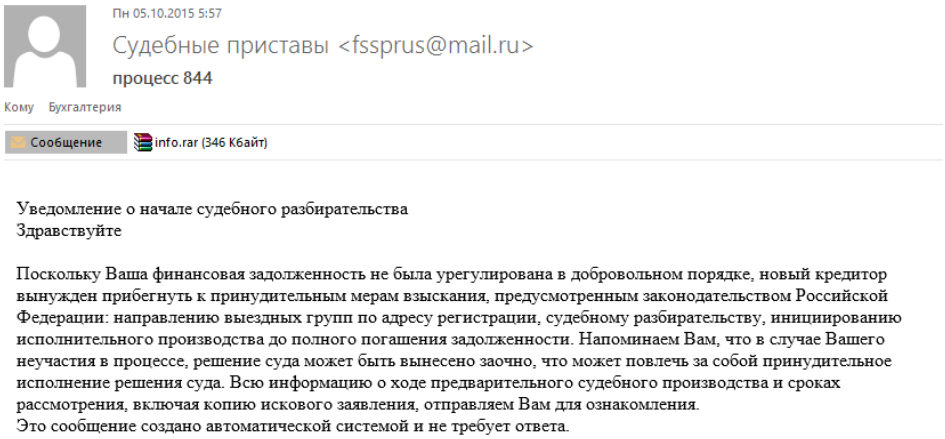


Ср 15.04.2015 8:39
ГК ЭЛЕКС <mail@eleks-group.ru>
Сверка за 1-ый квартал
Кому Канцелярия
Вы переадресовали это сообщение 15.04.2015 8:40.
Это сообщение было отправлено с важностью: Высокая.
Сообщение
Акт сверки - апрель 2015 г.zip (603 Кбайт)

День добрый,
Нами была проведена сверка (скан акта в аттаче).
Просим изучить документ и отправить завизированный экземпляр.
По нашей информации за Вашим предприятием имеется незначительная задолженность еще с января.

С уважением,
ООО "ГРУППА КОМПАНИЙ ЭЛЕКС"

Рисунок 1. Пример вредоносного сообщения электронной почты



Пн 05.10.2015 5:57
Судебные приставы <fssprus@mail.ru>
процесс 844
Кому Бухгалтерия
Сообщение
info.rar (346 Кбайт)

Уведомление о начале судебного разбирательства
Здравствуйте

Поскольку Ваша финансовая задолженность не была урегулирована в добровольном порядке, новый кредитор вынужден прибегнуть к принудительным мерам взыскания, предусмотренным законодательством Российской Федерации: направлению выездных групп по адресу регистрации, судебному разбирательству, инициированию исполнительного производства до полного погашения задолженности. Напоминаем Вам, что в случае Вашего неучастия в процессе, решение суда может быть вынесено заочно, что может повлечь за собой принудительное исполнение решения суда. Всю информацию о ходе предварительного судебного производства и сроках рассмотрения, включая копию искового заявления, отправляем Вам для ознакомления.
Это сообщение создано автоматической системой и не требует ответа.

Рисунок 2. Пример вредоносного сообщения электронной почты

При этом в качестве адресов отправителей могут быть использованы поддельные адреса компаний, Министерств и Ведомств, корпораций, например, Сбербанка, Ростелекома, Росатома, Пенсионного фонда, Роспотребнадзора, Высшего Арбитражного Суда, Федеральной службы судебных приставов и др.

- **вложение содержит двойной тип файла**, например (*.pdf.scr, *.doc.exe, *.xls.com, *.ppt.bat, *.odt.cmd, *.mdb.vbs, *.pdf.js, *.rar.hta и др.);
- **вложение содержит исполняемый файл или файл, созданный с использованием скриптового языка** (*.scr, *.exe, *.com, *.bat, *.cmd, *.vbs, *.js, *.hta, *.wsf и др.), прикрепленный к электронному письму, имитирует внешним видом файл распространенного формата данных (рисунок 3).

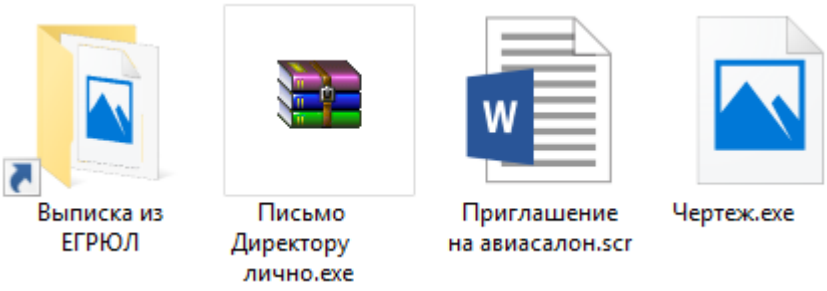


Рисунок 3 Пример исполняемых файлов, имитирующих внешним видом: ярлык, архивный файл, документ Microsoft Word, графический файл

– **прикрепленный к электронному письму архив (формат *.rar, *.zip, *.7z и др.) содержит исполняемый файл или файл, созданный с использованием скриптового языка;**

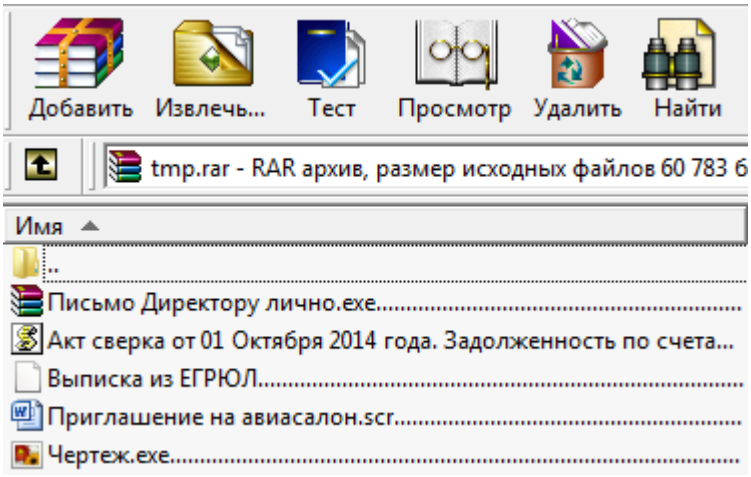


Рисунок 4 Пример исполняемых файлов, расположенных в архиве

- в электронном сообщении отсутствует вложение, но в тексте письма присутствует ссылка на файл, обладающий вышеуказанными признаками;
- во вложенный документ внедрённ объект (рисунок 5), который может быть активирован только с помощью действий пользователя (рисунок 6).

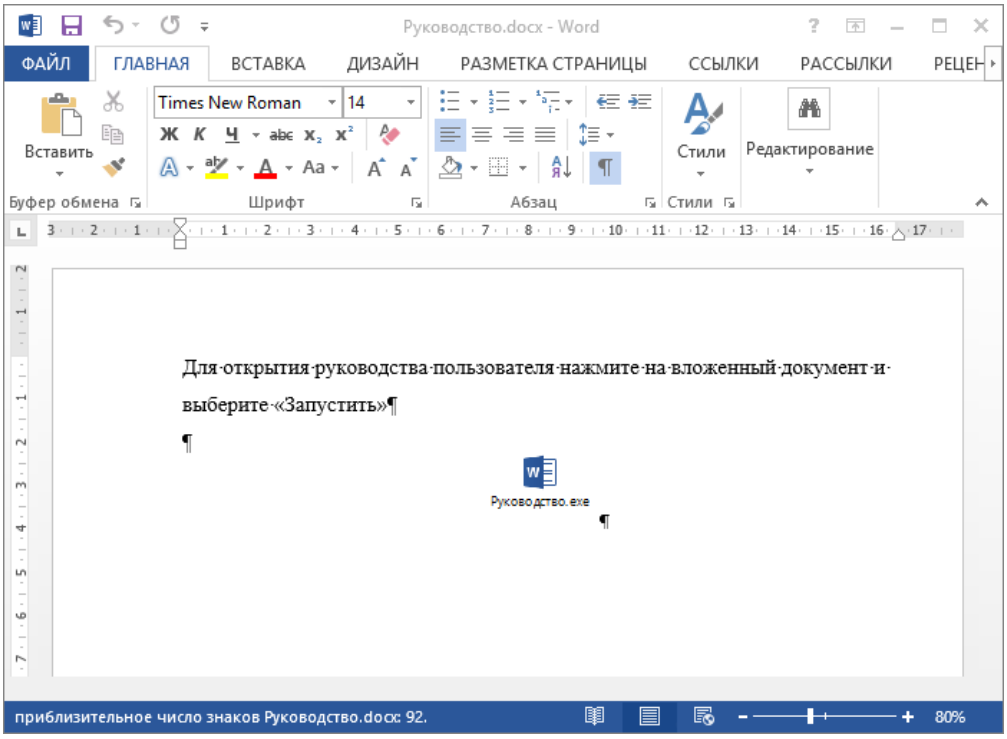


Рисунок 5 Пример вложенного в документ Microsoft Office объекта

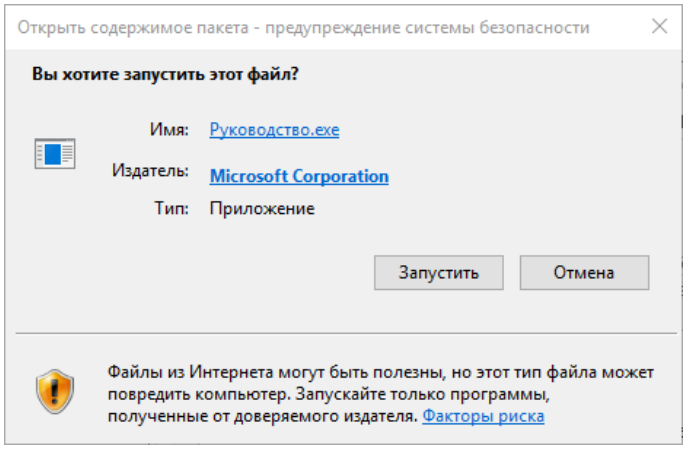


Рисунок 6 Запрос на открытие внедренного объекта

- при открытии файла формата Microsoft Office в программном пакете «LibreOffice» отображается ошибка (рисунок 7,8),

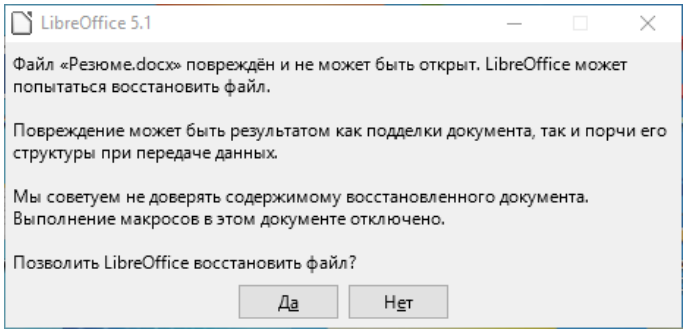


Рисунок 7 Диалоговое окно ошибки, возникающее при открытии инфицированного электронного документа в ПО LibreOffice

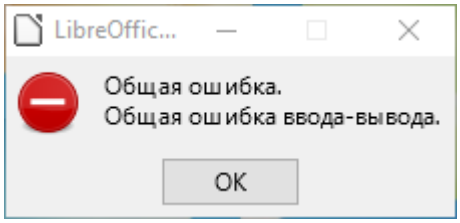


Рисунок 8 Диалоговое окно ошибки, возникающее при открытии инфицированного электронного документа в ПО LibreOffice

На рабочих станциях, где осуществляется работа с электронной почтой, для уменьшения возможностей эксплуатации уязвимостей ПО Microsoft Office рекомендуем провести установку альтернативного офисного программного обеспечения, например, «LibreOffice» и первоначальное открытие файлов формата Microsoft Office производить в нем;

– для маскировки расширения файла злоумышленники могут формировать длинные имена файлов, в результате чего в проводнике отображается часть имени файла (рисунок 9).

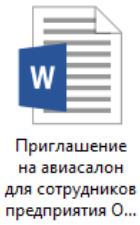


Рисунок 9 Пример маскировки расширения файла

В случае обнаружения одного из вышеперечисленных признаков дальнейшая работа с сообщением электронной почты должна быть прекращена, иначе велика вероятность заражения рабочей станции вредоносным программным обеспечением.

2. Технические меры

2.1. Настройка операционной системы

На рабочей станции, используемой для обработки сообщений электронной почты, необходимо провести следующие настройки:

- в настройках операционной системы включить отображение расширений известных типов файлов, отображение скрытых и системных файлов (рисунок 10).

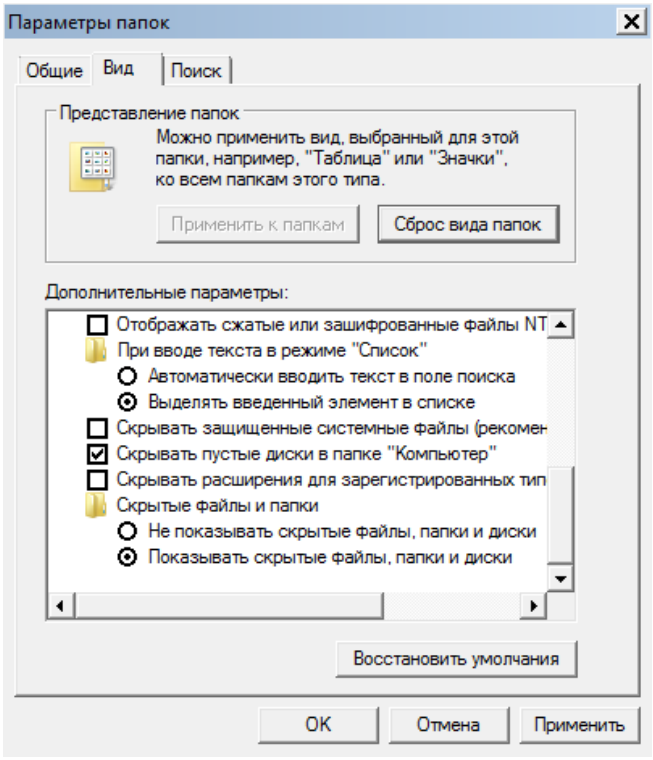


Рисунок 10 Настройка отображения расширений, скрытых и системных файлов

- для работы с файлами, имеющими длинные имена, необходимо в проводнике операционной системы установить вид просмотра каталогов «Таблица» (рисунок 11);

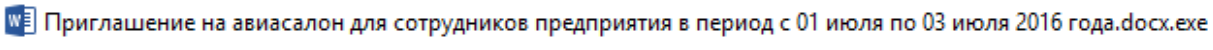


Рисунок 11 Отображение файлов в режиме «Таблица»

- изменить режим работы контроля учётных записей. Для этого в главном меню операционной системы (меню «Пуск») открыть *«Панель управления»* выбрать пункт *«Учётные записи пользователей»* и нажать *«Изменить параметры контроля учётных записей»* (или в поле поиска меню «Пуск»

ввести команду *«UserAccountControlSettings.exe»* и нажать клавишу «Enter») и установить вертикальный ползунок в верхнее положение «Всегда уведомлять» и нажать кнопку «ОК» (рисунок 12)

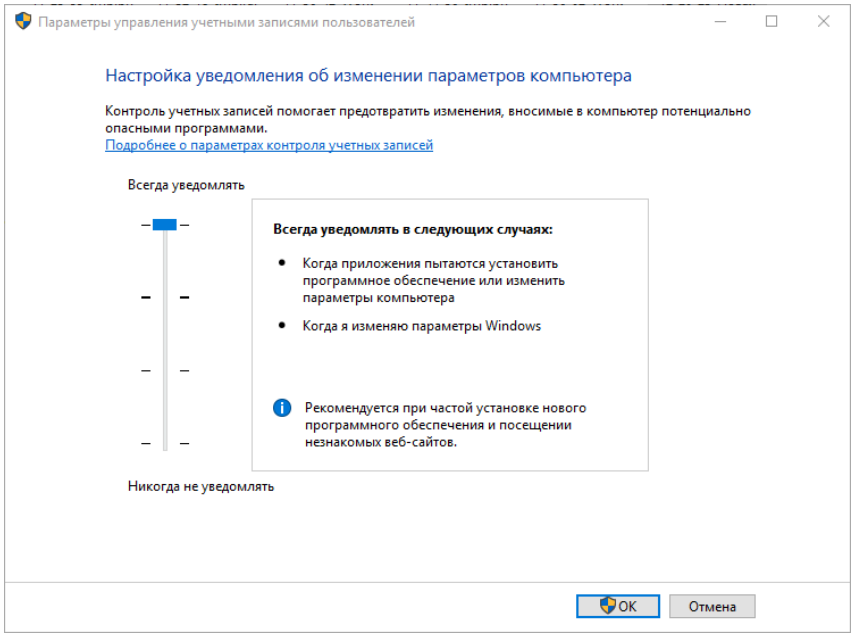


Рисунок 12 Изменение параметров контроля учётных записей

- запретить исполнение файлов, содержащих скриптовые языки («js», «vbs», «wsf» «hta»). Запрет может быть реализован с использованием настроек групповой политики операционной системы Windows;
- с целью блокирования взаимодействия с вредоносными ресурсами глобальной сети Интернет в настройках сетевого соединения использовать DNS-сервер **77.88.8.88** или **77.88.8.2**, предоставляемые бесплатным сервисом Yandex.DNS, http://dns.yandex.ru).

2.2. Настройка прикладных программ

2.2.1. Microsoft Office

В разделе «Параметры» – «Центр управления безопасностью» необходимо выполнить настройки (рисунок 13-15), использование которых предотвратить запуск активного содержимого. Рекомендуемые настройки представлены на примере Microsoft Office 2013.

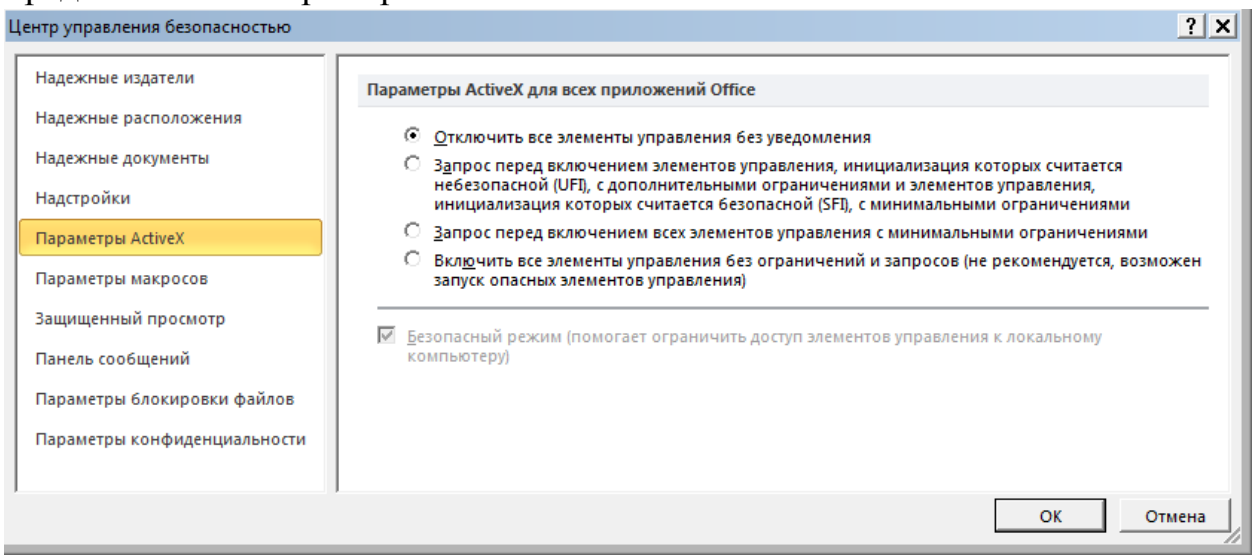


Рисунок 13 Отключение активного содержимого

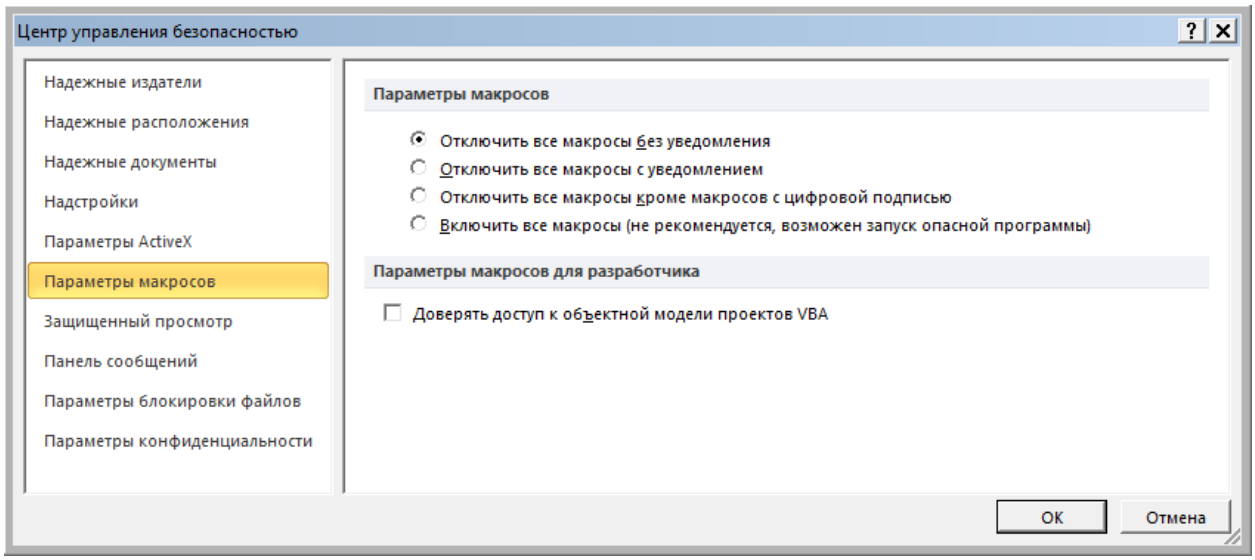


Рисунок 14 Отключение макросов

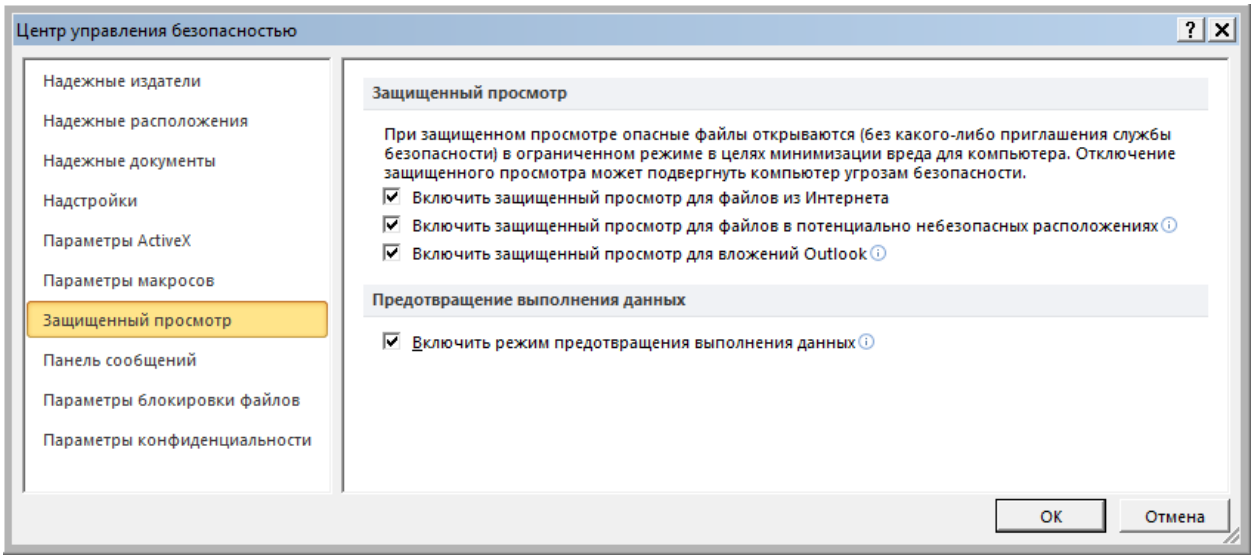


Рисунок 15 Включение защищённого просмотра

2.2.2. WinRar

В разделе «Установки» (рисунок 16) необходимо выбрать пункт «Типы файлов, исключаемых из распаковки» и указать следующие расширения: «*.com, *.pif, *.scr, *.bat, *.cmd, *.lnk, *.js, *.vbs, *.wsf».

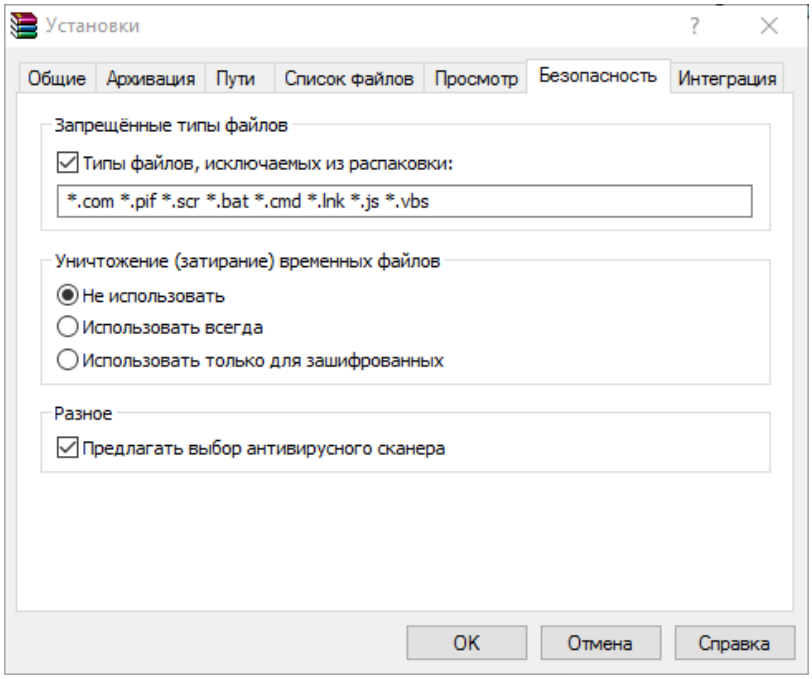


Рисунок 16 Настройка безопасности ПО «WinRar»

2.2.3. TheBat

В настройках почтового клиента TheBat включить проверку вложений антивирусными средствами (рисунок 17).

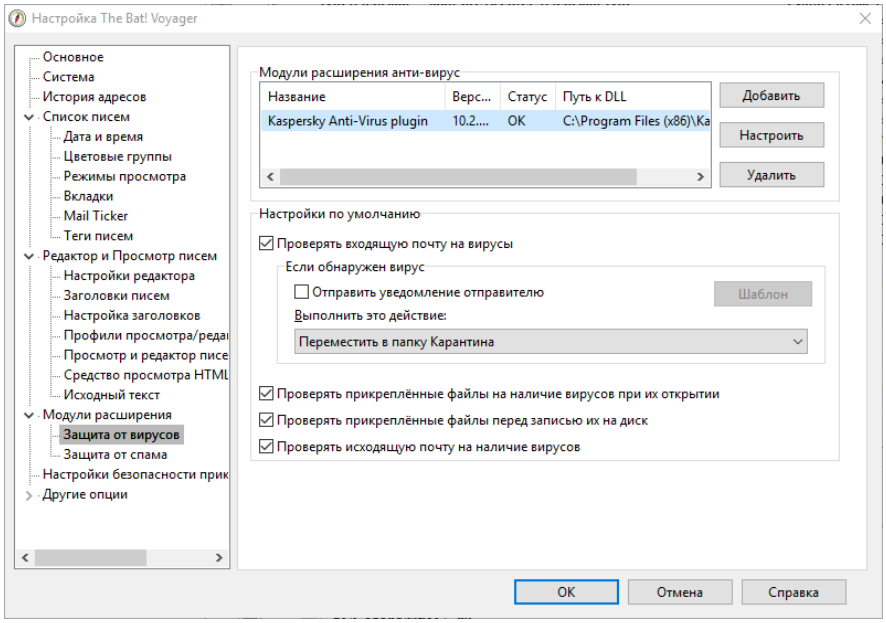


Рисунок 17 Настройка почтового клиента TheBat

2.2.4. Mozilla Thunderbird

В настройках почтового клиента Mozilla Thunderbird включить отображение тела сообщения в виде простого текста (рисунок 18), а также разрешить антивирусным средствам помещать в карантин инфицированные письма (рисунок 19).

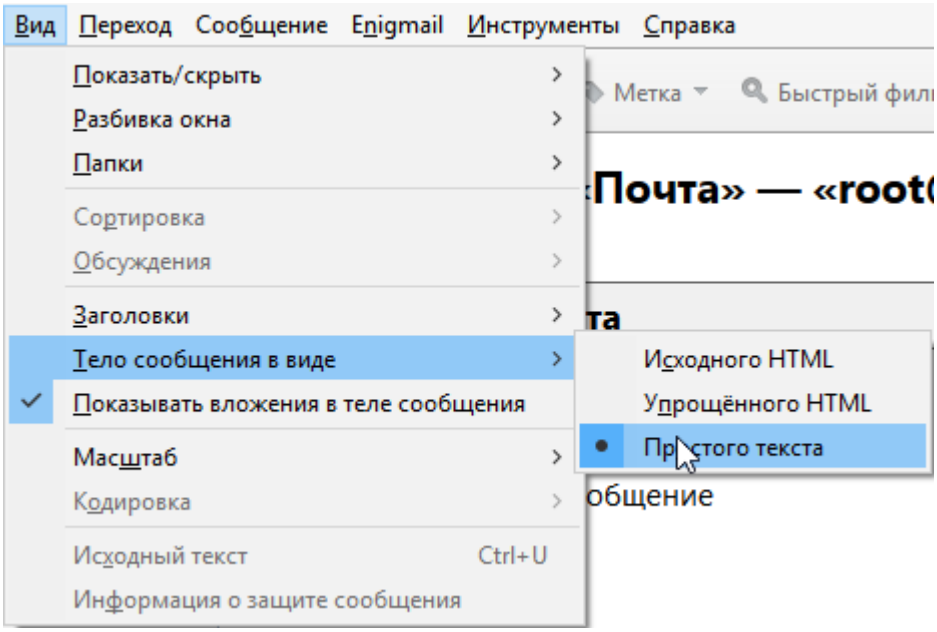


Рисунок 18 Настройки Mozilla Thunderbird

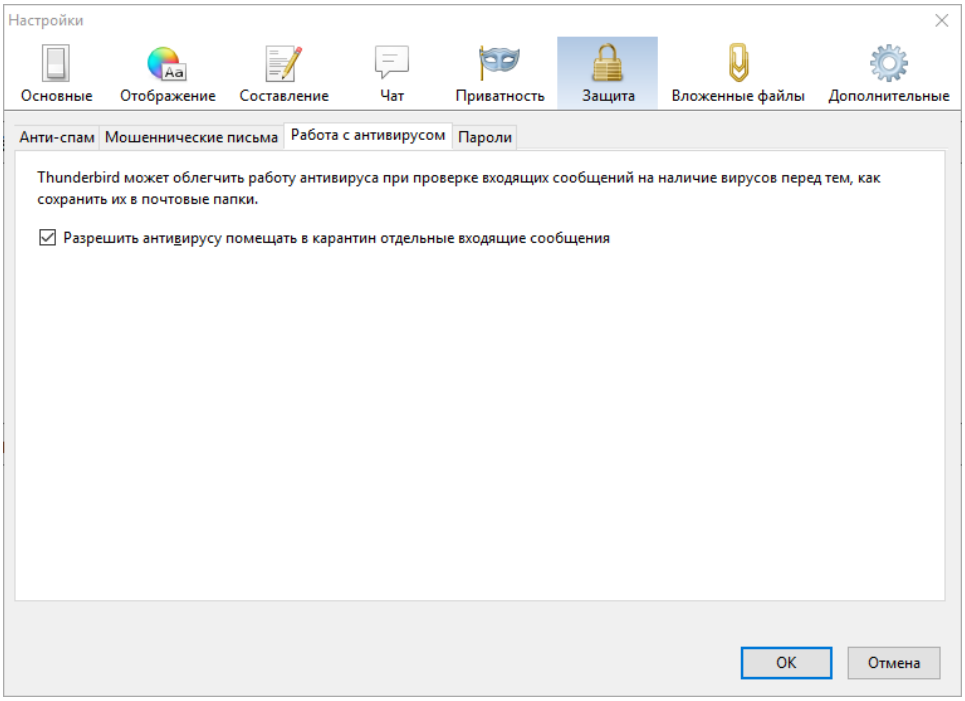


Рисунок 19 Настройки Mozilla Thunderbird

2.2.5. Microsoft «Enhanced Mitigation Experience Toolkit (EMET)»

Для уменьшения количества возможных фактов попыток эксплуатации уязвимостей прикладного программного обеспечения на рабочей станции необходимо установить программное обеспечение Microsoft «Enhanced Mitigation Experience Toolkit (EMET)[1]».

2.2.6. Настройка проверки почты в антивирусном ПО

Для детального анализа почтовых вложений необходимо в антивирусном программном обеспечении установить максимально высокий уровень безопасности (рисунок 20).

[1] Актуальная версия 5.5 для загрузки: https://www.microsoft.com/en-us/download/details.aspx?id=50766

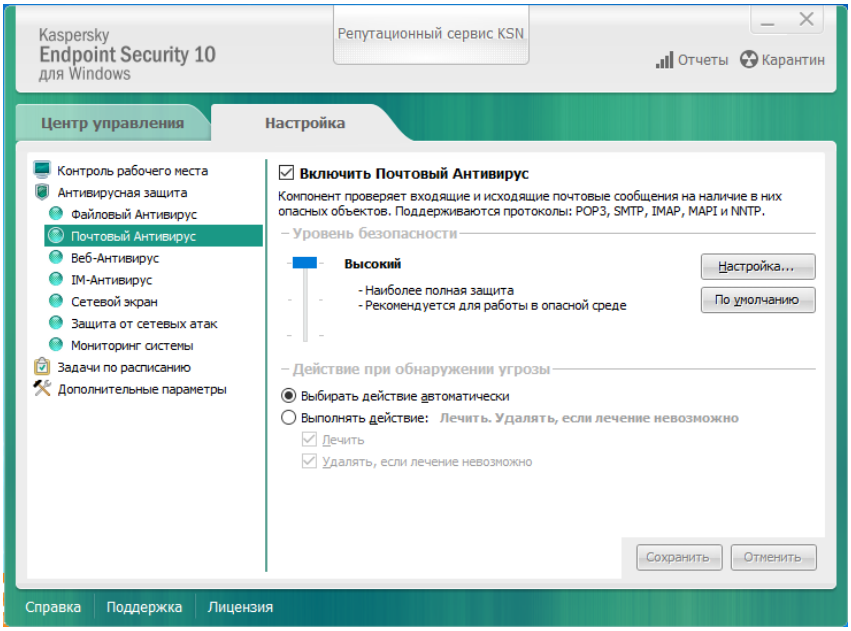


Рисунок 20. Настройка почтового модуля антивирусного ПО на примере антивируса лаборатории Касперского

2.3. Рекомендации антивирусных лабораторий по защите от действий программ-шифровальщиков

Лабораториями Касперского и Доктор Веб разработаны рекомендации, использование которых позволит предотвратить негативные последствия в случае заражения вредоносным программным обеспечением, обладающим функционалом шифрования пользовательских данных.

Актуальная версия рекомендаций расположена по адресу:

http://support.kaspersky.ru/10952

https://st.drweb.com/static/new-www/files/DWCERT-070-6_course_ru.doc

2.4. Список программного обеспечения для лечения рабочих станций от ВПО

Далее представлены ссылки на программное обеспечение и онлайн-сервисы, которые рекомендуется использовать при устранении последствий заражения вредоносным программным обеспечением.

Сканеры:

- **«Dr.Web CureIt!»** – антивирусный сканер;
  http://free.drweb.ru/cureit/
- **«Kaspersky Virus Removal Tool»**– антивирусный сканер
  http://devbuilds.kaspersky-labs.com/devbuilds/KVRT/latest/full/KVRT.exe

Загрузочные диски:

- **«Dr.Web LiveDisk»** – загрузочный диск, предназначенный для восстановления системы после вирусного заражения;
  http://www.freedrweb.ru/livedisk/
- **«Kaspersky Rescue Disk»** – загрузочный диск, предназначенный для восстановления системы после вирусного заражения;
  http://rescuedisk.kaspersky-labs.com/rescuedisk/updatable/kav_rescue_10.iso

Онлайн-сервисы:

- расшифровка файлов в Лаборатории Доктор Веб;
  https://support.drweb.ru/new/free_unlocker/
- разблокировка рабочих станций в случае действия ВПО семейства «WinLocker»
  https://www.drweb.com/xperf/unlocker/

3. Организационные меры

Необходимо ознакомить с разделом 1 данной инструкцией весь персонал, который производит обработку входящей электронной почты, а также персонал, ответственный за функционирование информационной системы.

Сотрудникам, ответственным за обеспечение информационной безопасности, необходимо:

- провести настройку рабочих станций с учетом изложенных в инструкции рекомендаций;
- ограничить круг лиц, обладающих на рабочих станциях правами «Администратора»;
- организовать антивирусную защиту каждой рабочей станции с автоматическим централизованным обновлением и журналированием;
- организовать централизованное обновление операционных систем и прикладного программного обеспечения на рабочих станциях;
- организовать централизованное получение и хранение входящей электронной почты, а также её централизованную антивирусную проверку;
- организовать резервное копирование пользовательской информации, в том числе подключаемых внешних накопителей;
- организовать контроль за подключаемыми к рабочим станциям внешними устройствами;
- организовать разграничение прав доступа к сетевым каталогам, запретить гостевой доступ;
- организовать периодические тренировки практических навыков персонала по выявлению вредоносных писем и действиям по локализации заражения, организовать проведение разбора допущенных в ходе тренировок нарушений.

4. Порядок действий в случае выявления активности ВПО

В случае заражения рабочей станции вредоносным программным обеспечением необходимо выполнить следующие действия:

- незамедлительно выключить рабочую станцию. Это может предотвратить потерю информации в случае, если вредоносное программное обеспечение инициировало процесс шифрования;
- проинформировать сотрудника, отвечающего за обеспечение информационной безопасности, о факте заражения;
- с использованием загрузочного диска с актуальной базой данных компьютерных вирусов провести проверку НЖМД;
- провести переустановку операционной системы в связи с тем, что в системе могут быть активны модули, не выявленные антивирусными средствами.
- установить причины, в результате которых произошло заражение ВПО;
- определить другие рабочие станции, которые могли быть подвержены заражению в результате установленных причин и провести профилактические работы на них.