

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ

ІМЕНІ ІГОРЯ СІКОРСЬКО”

Факультет прикладної математики

Кафедра системного програмування і спеціальних комп’ютерних систем

**Розрахункова робота**

З дисципліни «Захист інформації»

«Налаштування системи захисту електронної пошти від спаму»

**Виконав:**

**студент III-го курсу**

**групи КВ-4**

**Горпинич-Радуженко Іван**

**Київ 2016**

**Теоретичні відомості**

В останні роки рішення проблеми спаму набуває все більшої актуальності. У минулому році частка спаму в світовому поштовому трафіку перевищила 55%. Згідно з узагальненими даними Асоціації документального електрозв'язку, співробітники, які отримують в день по 10-20 ділових листів, попутно знаходять в своїх електронних ящиках більше сотні спамерських повідомлень. Боротьба з рекламною та шкідливої ​​розсилкою зажадає близько 5-ї години в місяць, а це робочий час, оплачуване роботодавцем. Крім того, спам значно збільшує навантаження на комунікації, підвищує трафік, знижує ефективність роботи сервера.

Світовий лідер по розсилці спаму в 2015 році - США, їм належить більше 15% всіх небажаних повідомлень в світі. Слідом за Штатами, з 8-відсотковою часткою спаму, йде В'єтнам, а замикає трійку сумних лідерів Китай з 7% поштового «сміття». Російські спамери займають четверту сходинку за обсягом небажаної пошти, хоча не так давно вони були на другій позиції. А ось країни- «мішені» спамерів зовсім інші. Найбільше дістається Німеччини - на неї припадає понад 18% всього спаму, слідом - Бразилія з 11%, а потім вже наша країна з часткою в 7,5%. Найбільше з розвинених країн пощастило Саудівської Аравії, на неї припадає лише 1% спам-повідомлень.

Цікаво, що спамери не відстають від світових подій і актуальних потреб отримувачів. Так, в 2014 році основною темою підступних листів часто був Чемпіонат світу з футболу, а в 2015 році - події на Україні. Кожен туристичний сезон адресати бачать в своїх електронних ящиках несподівані листи від готелів, як справжніх, так і «фейковий».

Відповідь на подібні повідомлення заборонений в принципі, так як кожна реакція на отримане повідомлення призведе до того, що на ваш ящик буде приходити все більше і більше небажаної кореспонденції. Як «прибрати» спам, добре знає більшість фахівців: потрібно або змінити e-mail, або встановити додатковий захист.

Існують і більш небезпечні розсилки, які націлені на «зараження» комп'ютера або на отримання доступу до конфіденційної інформації, - так званий фішинг. Ці різновиди спаму - особливий вид інтернет-шахрайства, покликаний отримати ідентифікаційні дані користувача, такі як особисті та корпоративні паролі, номери кредитних карт, банківських рахунків і так далі.

Як правило, фішинг ми отримуємо у вигляді фальшивого повідомлення від провайдера, банку та інших організацій, які добре знайомі і можуть бути важливі для діяльності компанії. У темах таких листів нас попереджають про термінову інформації, загрозу, на яку потрібно зреагувати негайно. Фішери не гребують пропонувати боротьбу з «самими собою»: мовляв, варто тільки пройти по посиланню на рекомендований сайт, ввести свій логін і пароль - і про небезпеку фішингу можна забути назавжди. За допомогою введених даних шахраї отримують доступ до електронного ящика жертви та іншої особистої інформації. При цьому фішери самі рідко користуються отриманими даними, передаючи їх третім особам. І не можна забувати про небезпеку зараження комп'ютера шкідливою програмою, підхопленою на відкритій за посиланням сторінці або в прикріпленому до листа файлі. Адже коли вірус вражає один з комп'ютерів корпоративної мережі, є ризик паралізувати роботу всієї організації. Тепер розумієте, що значить для компанії захист від фішингу?

За даними фахівців, збитки від одного тільки інциденту, пов'язаного з інформаційною безпекою, для великих компаній складає в середньому 7 мільйонів гривень, а для невеликих організацій - трохи менше 200 тисяч гривень. Щоб ліквідувати проблему і убезпечити себе від подальших неприємностей, компанії великого розміру можуть витратити до 800 тисяч гривень, а менші фірми - приблизно 100 тисяч. Однак 90% світового бізнесу досить поблажливо ставиться до небезпеки шкідливих програм, іншими словами, не стежить за появою нових вірусів і оперативним оновленням програмного забезпечення для боротьби з ними. А починати слід з розуміння того, під якими темами листів найчастіше ховається спам.

Види спаму

За традицією однією з найпопулярніших тематик спам-повідомлень є інтернет-знайомства. Побачення, оголошення шлюбних агентств завжди були в лідерах тим небажаних листів, популярна і реклама сайтів «для дорослих». Далі за рейтингом йдуть освіту, подорожі (вони особливо активні в літній період), нерухомість і бухгалтерські послуги.

Залежно від змісту листа спам ділиться на «комерційний» і «некомерційний», чому відповідають абревіатури UCE - «unsolicited commercial e-mail» (комерційний) і UBE - «unsolicited bulk e-mail» (некомерційний).

Комерційний спам, в свою чергу, ділиться на санкціонований і несанкціонований, іншими словами, вам приходять комерційні пропозиції, на які ви погоджувалися або не погоджувалися. З такого роду спамом потрібно звертатися акуратно, так як можна упустити дійсно важливу інформацію.

Некомерційний спам, або анонімна масова розсилка, найчастіше представлений наступними його різновидами:

Політичний спам. Повідомлення політичного характеру найбільш популярні, природно, в період виборів. Мова в основному йде про «чорному PR» з метою компрометації певної особи. Цікаво, що така розсилка часто здійснюється нібито від імені конкурента. Користувачів обурює величезна кількість листів від кандидата, що змушує їх іти голосувати за іншого (істинного ініціатора розсилки).

«Благодійний» спам. Як вже говорилося вище, спамери вміло використовують відбуваються в світі події. Так, у 2008 році популярна було прохання перерахувати гроші в благодійний фонд для допомоги дітям з Південної Осетії. Пізніше «благодійники» збирали пожертви в Донецьк. Маса повідомлень надходить з кличем допомогти вмираючому від тяжкої недуги дитині, якій потрібна термінова дорога операція. Такий спам дуже небезпечний, так як оформлений досить грамотно. Небайдужим до чужих бід людям слід ретельно перевіряти викладену в подібних листах інформацію.

Шахрайський спам. У так званих нігерійських листах шахраї пропонують участь в грошових операціях, обіцяючи величезні доходи. У одержувача листа випрошується все більше грошей на сплату різних зборів, хабарів чиновникам і т.д. Популярний варіант - лист від нотаріуса, сповіщати про смерть людини з тим же прізвищем, що і адресат. Відправник пропонує отримати гроші з банківського рахунку «померлого». Спочатку такі повідомлення йшли з посиланням на загибель родича в Нігерії, чому спам і отримав свою назву. Цікаво, що, незважаючи на численні попередження про шкоду подібних листів, щорічно перебувають жертви, відправляють гроші на рахунки шахраїв.

Ланцюговий спам ( «листи щастя»). Завдання ланцюжка спаму - пересилання повідомлення всім родичам і знайомим адресата. Найчастіше це якесь «лист щастя», в якому користувачеві обіцяють повне благополуччя в житті, якщо він відправить лист певному числу інших користувачів. Інший варіант - «лист нещастя», в якому повідомляється про прийдешнє стихійне лихо, теракт або епідемії. Відправники листа настійно рекомендують перенаправити повідомлення всім знайомим, щоб попередити їх. Такі повідомлення особливо небезпечні можливої ​​панікою серед населення, а в деяких випадках містять і прохання про переведення невеликих сум грошей. Найчастіше «листи щастя» містять посилання на шкідливий сайт або заражений файл.

Спам «для дорослих». Цей вид спаму дещо здав свої позиції в порівнянні з початком 2000-х. Сталося це почасти завдяки введенню в деяких державах законодавчих обмежень на подібний контент. Але спад фіксується в західних країнах, а в Росії, навпаки, йде підйом. До тематики спаму для дорослих відносяться порносайти і матеріали, що містять порнографію, сайти знайомств, засоби для підвищення потенції. Найчастіше такі повідомлення приходять на англійській мові.

Вірусний спам. Самий проблемний вид спаму. Одне таке лист може пошкодити один комп'ютер або цілу мережу, знищити або викрасти інформацію, зупинити роботу організації, причому досить великою. Спамери призвичаїлися підробляти вірусні листи під повідомлення від поштових серверів (наприклад, звіт про нібито недоставлені листи) під важливі сповіщення, під документи, що вимагають термінового перегляду.

Згідно зі статистикою, найпопулярнішою на поточний момент вірусної програмою є Trojan-Spy.HTML.Fraud.gen. Це фішингова інтернет-сторінка, що маскуються під інтернет-магазин, банк, компанію, яка пропонує антивірусний захист. На другому за популярністю місці розташувався завантажувач Trojan-Downloader.JS.Agent.hhi, що представляє собою обфусцірований Java-скрипт. Завантажники використовують технологію ADODB.Stream, яка дозволяє їм завантажувати і запускати файли DLL, EXE і PDF. На третьому рядку розташувався Trojan-Downloader.VBS.Small.lj - це VBS-скрипти, які використовують ту ж ADODB.Stream, тільки скачують ZIP-архіви і запускають витягнуте з них шкідливе ПЗ.

Способи поширення спаму

Розглядаючи питання різноманіття спаму, було б дивно обійти стороною тему способів його поширення.

* прямі розсилки:

Спочатку повідомлення розсилалися спамерами з використанням власних поштових серверів і від власного імені. Але ці розсилки виявилися неефективні, так як їх досить просто блокувати: необхідно всього лише заборонити адреса відправника або поштового сервера. І як тільки подібні блокування стали поширеними, спамерам довелося шукати обхідні шляхи - наприклад, підробляти різну інформацію, включаючи адреси відправників.

* Відкриті сервіси (open relay, open proxy):

Існують поштові сервери, що дозволяють безпідставного відправнику послати будь-який лист на будь-який електронну адресу, - їх називають «відкриті релеї» (open relay). Все почалося ще в середині 90-х, коли абсолютно всі поштові сервери були якраз відкриті релеї (згодом конфігурації великих світових поштових серверів були змінені). Однак стежити за тим, щоб сервер був закритим, потрібно постійно, а фахівці з IT-безпеки не завжди приділяють цьому належну увагу, чим активно користуються створені інтернет-шахраями сервіси пошуку відкритих реле або відкритих проксі-серверів. І все ж більшість спамерів перестало застосовувати відкриті релеї, зрозумівши їх малу ефективність, і почало шукати інші способи впливу.

* Розсилка з модемних пулів:

Розсилка через dial-up підключення, що використовують модеми та телефонний зв'язок, відбувається наступним чином: пошта від клієнтів провайдера приходить на поштовий сервер, який її пересилає, а підключення «захоплює» динамічний IP-адресу, і спамер стає власником безлічі адрес, з яких розсилається пошта.

Як тільки провайдери дізналися про цю схему, вони стали використовувати обмеження на кількість повідомлень, відправлених від імені одного користувача, блокувати прийом пошти зі сторонніх модемних пулів і вводити чорні списки dial-up адрес.

* Зламані призначені для користувача ПК і інші способи:

Перераховані вище методи стають все менш ефективними, і зараз найбільшого поширення набула розсилка спаму за допомогою заражених комп'ютерів користувачів. Щоб отримати доступ до комп'ютера, шахраї використовують троянські програми (вони поширюються по мережі Інтернет або файлообмінними мережами разом з різним піратським програмним забезпеченням), уразливості в операційних системах і популярному софт, e-mail черви.

Методи захисту від спаму і фішингу

У міру того як спам стає все витонченішими, розробляються нові способи захисту пошти і ускладнюються «класичні» методи. Надійність антиспам-систем забезпечується використанням декількох методів в комплексі. При виборі способів захисту важливо також відштовхуватися від особливостей роботи організації і характеру спаму, який приходить найчастіше.

Основним і найпопулярнішим методом боротьби з небажаною кореспонденцією є фільтрація, тобто відсіювання спаму від дійсно важливих листів. Цей метод заснований на тому, що спам-листи значно відрізняються від звичайних. Фільтрація розділяється на автоматичну і неавтоматичного.

Автоматична фільтрація спаму. Для захисту від спаму використовуються спам-фільтри. Вони можуть бути встановлені на комп'ютерах користувачів або на серверах. Принципово різняться два способу роботи таких фільтрів. В одному випадку спам-фільтр пізнає відправника листа як спамера, не відкриваючи саме повідомлення. Особливість такого методу в тому, що ПО має бути встановлено на сервері, на який приходить небажана кореспонденція.

Іншим способом є аналіз «тіла» листа. Якщо воно оцінено як небажане, то відправляється в окрему папку або віддаляється. Спам-фільтр, який працює таким чином, може перебувати як на сервері, так і на комп'ютері користувача. Якщо фільтр знаходиться на комп'ютері, то одержувач бачить відфільтрований спам, однак дана опція пов'язана з витратами на його прийому. Якщо ж захист від спаму «організована» на сервері, то користувач не відчуває ніяких проблем, але може просто не отримати потрібний лист, яке було визначено як спам. Це, до речі, одна з основних труднощів автоматичної фільтрації, яка не дозволяє вважати систему захисту від спаму ідеальної.

Дуже популярна на даний момент байєсівська фільтрація спаму. Спосіб полягає в наступному: спам-фільтри попередньо «навчаються», тобто їм відправляються вже відсортовані листи, на основі яких фільтр аналізує статистичні особливості бажаної кореспонденції і небажаною. Якщо «навчання» відбувається нормально, то фільтр допомагає відсіяти до 97% спаму. На жаль, спамери зараз навчилися обходити і такі фільтри, вставляючи в «тіло» листи картинку, прибираючи при цьому текст повністю або частково. В такому випадку спам-фільтр не може грамотно впізнати лист і скласти статистику. Однак і для таких листів є протиотрута: якщо постійно «дообучать» антиспам, вказувати йому на недоліки, то автоматична фільтрація стає досить ефективною.

Неавтоматична фільтрація є більш трудомісткою і складно налаштовувальною. Але в кінцевому рахунку, якщо грамотно підійти до питання, вона може стати дуже результативною. При неавтоматичній фільтрації спам-фільтри задаються користувачем і, як правило, складаються з стоп-слів або виразів. Отже, користувач точно знатиме, чому відсіяні листи і які з них були відправлені в папку «Спам». Важливо пам'ятати, що для ефективності даної антиспам-перевірки потрібно постійно стежити за останніми тенденціями в поведінці спамерів і доповнювати фільтр новими установками.

Чорні списки

У чорні списки зазвичай вносяться:

IP-адреси тих комп'ютерів, з яких ведеться або велася розсилка небажаної кореспонденції;

* відкриті релеї;
* списки dial-up;
* локальні списки спамерів;

Чорні списки, складені службою DNS (комп'ютерної розподіленою системою для отримання інформації про домени).

Система чорних списків використовується вже давно, перевірена часом і підводить нечасто - в цьому її сильна сторона. Слабку сторону такого підходу становить безвідповідальність адміністрації в питанні складання списків, в які запросто потрапляють ні в чому не винні користувачі. Простий приклад: комп'ютери, з яких міг бути відправлений спам, включені в підмережу або належать поштової домену. А система включає в чорний список весь домен або всю мережу, і після цього тисячі користувачів деякий час не можуть відправляти пошту. Додамо до небажання вникати в деталі «нечистоплотне» поведінку деяких адміністраторів, які часом вимагають гроші за видалення IP-адрес з чорних списків.

Сірі списки

Принцип роботи даної методики заснований на тому, що функціонування програмного забезпечення, що відповідає за розсилку спаму, відрізняється від «поведінки» стандартних поштових серверів. Спамерське ПО, обходячи захист спам-фільтра, використовує різні релеї і інші зворотні адреси, приймаюча сторона розцінює це як спробу відправляти спам-листи. Тоді включається робота сірого списку. Спочатку все невідомі SMTP-сервери включені в дані списки, але при цьому пошта, яка надходить з такого сервера, не відхиляється. Сервери отримують код тимчасової помилки, і якщо пошта доброзичлива, то вона приходить знову з того ж адреси. Спамерське ж ПО повторно відправляє повідомлення вже з іншої адреси, і тоді спам знищується або відкладається в спеціальну папку. Так відсіюється значна (близько 90%) частина небажаної кореспонденції, а важливі листи доходять без втрат - це сильна сторона подібного методу, яка і принесла йому популярність.

Слабкою ж стороною є витрати часу (часом до 30-ти хвилин) на додаткову перевірку листів, а це неприйнятно при роботі зі строкової кореспонденцією. Однак затримка відбувається тільки при отриманні першого листа з невідомого сервера, так що метод може виявитися зручним для ряду організацій.

Аналіз заголовків

Для генерації своїх листів спамери застосовують спеціальне програмне забезпечення, яке автоматично створює і поширює повідомлення. У таких програм є серйозний недолік: вони припускаються помилок при оформленні заголовка, тому спам-повідомлення не відповідає поштової стандарту RFC. Завдяки цьому прорахунку антиспам-фільтри і виявляють небажану кореспонденцію. Такий захист дуже надійна і ефективна.

Аналіз вкладень

Спочатку фільтрація вкладень перевіряла тільки тему повідомлення і «тіло» листа, що містить текст. Однак зараз антиспам-перевірка проводиться по всьому повідомленням, навіть по вкладеним картинкам. Це одна з найбільш дієвих програм, яка швидко «вчиться», підлаштовується під нові види небажаної кореспонденції і діє практично безпомилково.

Захист від збору адрес

Часто спамери сканують сайти на предмет пошуку електронних адрес, вказаних в якості контактних, і потім на ці адреси йдуть десятки спам-повідомлень. Є кілька шляхів захисту e-mail від спам-ботів. Один з найпопулярніших способів - створення «лівого» адреси. На популярному поштовому ресурсі реєструється дублікат електронної пошти, який виставляється на сайті організації. Після оновлення сайту ви станете отримувати листи від реальних користувачів, а не від шахраїв.

Друге ефективний засіб захисту від збору адрес - перетворення адреси в картинку. Скріншот електронної адреси виставляється в розділ «Контакти» на сайті замість «словесного» еквівалента - користувач без проблем прочитає адреса, а ось спамерська програма не зможе його розпізнати. Схожим варіантом є «маскування» адреси. Наприклад, замість ivan.ivanov@com стає ivan (dot) ivanov (at) com, - в таких випадках спамерські програми теж безсилі. Недоліком підходів є те, що вони ускладнюють доступ до поштовою адресою реальним користувачам.

Визначення ознак масовості

Діє даний метод досить просто: у величезному потоці листів виявляються абсолютно ідентичні або незначно розрізняються повідомлення. Технологія призначена в основному для великих організацій, які володіють значними обсягами пошти.

Сучасні IT-компанії для захисту від спаму і фішингу використовують відразу декілька методів, формуючи комплексний захист. Загальні методи в спеціалізованому ПЗ - чорні і сірі списки, байєсівську фільтрація і аналіз листи. На практиці авторитетні антиспам-сканери - такі як GFI MailEssentials, Kaspersky Anti-spam, Kaspersky Security for Mailserver, McAfee Security, Symantec MailSecurity, ESET MailSecurity - утримують до 99% всіх небажаних повідомлень.

**Використання антиспам-сканеру GFI MailEssentials**

*Функції GFI MailEssentials:*

* GFI MailEssentials за допомогою багаторівневої фільтрації спаму захищає користувачів від марної трати часу на видалення непотрібних листів.
* Автоматичний білий список, в який відразу ж додаються всі адреси, на які ви відправляєте листи.
* Модуль захисту від фішингу виявляє і блокує фішингові повідомлення на основі щоденною бази фішингових адрес і ключових слів.
* Надбудова SpamTag addon дозволяє користувачам позначати повідомлення як «спам» і «не спам» безпосередньо з Outlook.
* Користувачі можуть керувати листами в карантині без допомоги адміністратора і налаштовувати свої власні білі і чорні списки.

**Етапи інсталяції та налаштування:**

* Завантажте збірку GFI MailEssentials, що відповідає типу використовуваного комп'ютера. Оберіть 32-біт (x86) для налаштування програми GFI MailEssentials в 32-бітних системах і 64-біт (X64) - в 64-бітних системах.
* Перед запуском майстра установки переконайтеся в наступному:
* Вхід в систему виконаний за допомогою облікового запису з правами адміністратора.
* Комп'ютер, на якому буде встановлено додаток GFI MailEssentials, відповідає указанним системним вимогам.
* Налаштуйте брандмауер так, щоб додаток GFI MailEssentials могло підключатися до серверів GFI.
* Вимкніть сторонні антивірусні програми і програми для резервного копіювання, скануючі папки, використовувані додатком GFI MailEssentials.
* Якщо Ви встановлюєте програму GFI MailEssentials на поштовий шлюз або сервер ретрансляції / зовнішній сервер необхідно налаштувати комп'ютер в якості шлюзу.

Запуск майстра інсталяції:

1. Запустіть програму інсталяції GFI MailEssentials.
2. Виберіть мову для роботи з цією установкою додатка GFI MailEssentials. Прийміть умови і положення і натисніть Далі.
3. Виберіть режим, в якому пріложеніеGFI MailEssentials буде витягувати список користувачів пошти.
4. Налаштуйте адресу електронної пошти адміністратора і конфігурацію SMTP-сервера.



Натисніть Далі.

1. Виберіть папку, в яку буде встановлюватися GFI MailEssentials, і натисніть Далі. Якщо установка виконується для переходу на нову версію, додаток GFI MailEssentials встановлюється в те ж місце, що і в попередній раз.
2. Натисніть Встановити для запуску інсталяції. Якщо на екрані з'явилося повідомлення про необхідність перезапуску служб SMTP, натисніть Так.
3. По завершенні натисніть Готово.

Майстер підготовки основних компонентів

Майстер підготовки основних компонентів завантажується автоматично після інсталяції GFI MailEssentials в перший раз. З його допомогою здійснюється налаштування найбільш важливих параметрів GFI MailEssentials.

1. Натисніть Далі на сторінці привітання.



Натисніть Перевірка для перевірки підключення до зазначеного DNS-сервера. Якщо перевірка була невдалою, вкажіть інший DNS-сервер. Натисніть Далі.



1. У вікні Налаштування проксі-сервера вкажіть спосіб підключення GFI MailEssentials до Інтернету. Якщо сервер підключається до Інтернету через проксі-сервер, натисніть Налаштування проксі-сервера ... і вкажіть налаштування проксі-сервера. Натисніть Далі.



1. У вікні Домени вхідних повідомлень електронної пошти вкажіть всі домени, які будуть скануватися на наявність спаму і вірусів. Локальні домени, які не вказані в цьому списку, скануватися не будуть. Натисніть Далі.



1. У вікні Сервери SMTP вкажіть спосіб отримання сервером зовнішніх повідомлень. Якщо, перш ніж потрапити в додаток GFI MailEssentials, повідомлення проходять через інші сервери, додайте IP-адреси цих серверів в список.



1. У вікні Дія для захисту від спаму, виберіть дію, яка виконуватиметься за замовчуванням при виявленні спам-повідомлень. Дана дія застосовується лише до спам-фільтрам. Фільтри шкідливих програм автоматично поміщають заблоковані повідомлення в карантин.

7. У разі інсталяції на сервері Microsoft® Exchange Server 2007/2010, відображається список

виявлених ролей сервера Microsoft ® Exchange і необхідних компонентів GFI

MailEssentials. Для інсталяції необхідних компонентів GFI MailEssentials натисніть Далі.

8. Для завершення інсталяції натисніть Готово.

Установка GFI MailEssentials завершена, і система захисту пошти ввімкнена.

**Налаштування GFI MailEssentials**

Персональний білий і чорний списки:

За допомогою функцій персонального білого і чорного списку можна вказати адреси або домени електронної пошти, повідомлення з яких завжди необхідно доставляти в поштову скриньку або блокувати:

*Персональний чорний список* - це окремий список адрес електронної пошти і

доменів, повідомлення з яких завжди будуть блокуватися.

*Персональний білий список* - це окремий список адрес електронної пошти і

доменів, повідомлення з яких завжди будуть доставлятися в поштову скриньку.

Щоб налаштувати персональний білий / чорний список, виконайте наступні дії:

1. Увійдіть в GFI MailEssentials.

2. Виберіть Персональний білий / чорний список.



3. Щоб створити персональний білий список, перейдіть на вкладку «Персональный белый список». Щоб створити персональний чорний список, виберіть «Персональный черный список».

4. Виконайте потрібну дію:

Щоб додати адресу електронної пошти, введіть його і натисніть Додати.

Щоб оновити наявну запис, виберіть адресу електронної пошти, внесіть потрібні зміни і натисніть Оновити. Щоб видалити запис, виділіть його та натисніть Видалити.

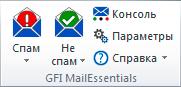
Модуль SpamTag:

*GFI MailEssentials SpamTag* - це модуль для додатка Microsoft Outlook,

дозволяє обробляти спам-повідомлення.

*Функції:*

* Класифікувати повідомлення як спам або не спам.
* Додавати відправників та / або домени в персональний чорний або білий список.
* Автоматично синхронізувати дозволених і заблокованих відправників в додатку Microsoft Outlook з персональним білим і чорним списками GFI MailEssentials відповідно.
* Автоматично додавати ваші контакти в персональний білий список.



*SpamTag в додатку Microsoft Outlook 2010*