РУКОВОДСТВО ПО РАЗРАБОТКЕ ПОЛИТИКИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ НА ПРЕДПРИЯТИИ

www.cybercontrol.ru

Руководство написано на основе рекомендаций корпорации SurfControl по внедрению политики управления потоками электронной корреспонденции.

Аналитическая компания 'The Meta Group' подсчитала, что ежедневно в сети Интернет рассылается 15 миллиардов электронных писем

По оценкам той же компании, к 2005 году количество ежедневно отправляемых писем возрастет до 35 миллиардов

Вопросы конфиденциальности

Вся информация, имеющая отношение к Вашим клиентам или бизнесу компании, является конфиденциальной. В новом веке информационных технологий электронная почта является таким же носителем информации, как и печатные материалы, поэтому разумно предъявлять те же требования к безопасности электронной информации, как и к бумажным материалам. Вот несколько рекомендаций по обеспечению безопасности информации в электронном виде:

- Уделяйте внимание сохранению конфиденциальности всякого рода паролей
- Если документ содержит строго конфиденциальную информацию, его следует хранить в особой папке компьютера
- Обеспечению безопасности может способствовать отказ от пересылки или разделения (даже внутри компании!) любой информации о клиентах
- Каждый раз, отправляя письмо, проверяйте список адресатов — все они должны обладать правами доступа к той информации, которую Вы посылаете

Злоупотребление

При написании электронных писем придерживайтесь общепринятых норм морали и этики; не делайте никаких заявлений от своего лица или от лица компании, которые изобличают компанию в чем-либо, портят деловую репутацию или могут быть неверно истолкованы получателем.

Вам не следует принимать участие ни в каких мероприятиях, которые являются противоправными или противоречат общепринятым нормам ведения дел, а также в тех случаях, когда Ваши действия могут тем или иным образом нанести компании ущерб. Вы не можете загружать, отправлять, использовать, распространять любые изображения, текст, иные материалы, программное обеспечение, которые:

- Могут быть признаны нелегальными или неэтичными
- Могут призывать к действиям, выполнение которых нанесет (или может нанести) ущерб компании
- Использование которых предполагает выполнение действий, не входящих в список Ваших должностных обязанностей — к примеру, неутвержденные продажи/продвижение продукции или услуг
- Могут отрицательно влиять на производительность информационной системы компании, включая локальную сеть и другие средства связи и обработки информации
- Могут привести к возникновению каких-либо судебных споров или конфликтов
- Являются предметом авторского права, защищенного законодательством, а разрешением на использование в том или ином виде Вы не располагаете

Следующие действия запрещены при любых обстоятельствах:

- Занесение в компьютерную сеть компании вирусов или любых иных вредоносных программных средств
- Поиск и обнаружение средств или методов для получения несанкционированного доступа к компьютерным системам, находящимся внутри компании или за ее пределами
- Попытки чтения почтовых сообщений других пользователей без их разрешения

Почтовые сообщения, которые были удалены, могут тем не менее быть отслежены и восстановлены. Таким образом, любой сотрудник, принимающий участие в создании или рассылке запрещенных сообщений, может быть идентифицирован. Почтовые сообщения, как в электронном, так и в бумажном виде, могут представлять собой вещественные доказательства для суда.

Мониторинг

Все ресурсы компании, включая компьютеры, электронную и голосовую почту, предоставляются для пользования сотрудниками исключительно в рабочих целях. Компания оставляет за собой право в любое время без предварительного предупреждения проверить состояние компьютерных систем, а также информацию, которая в них содержится. Любая информация, содержащаяся как на постоянных носителях (к коим можно отнести жесткие диски и оптические неперезаписываемые компакт-диски), так и на временных (дискетах, CD-R/RW и пр.) может быть проверена и изучена представителями компании.

В целях обеспечения выполнения пунктов настоящих Правил, компания может внедрять специализированное программное и аппаратное обеспечение для проверки и мониторинга использования компьютерных систем. Компания оставляет за собой право отслеживать, изучать, удалять или изменять любые почтовые сообщения, которые проходят через корпоративную почтовую систему.

Соглашение

Все сотрудники компании, включая работающих по контракту и временный персонал, имеющие доступ к почтовой системе компании, должны подписать настоящее соглашение, подтверждая тем самым понимание сути предъявляемых требований.

Подпись, дата

ВЫРАБОТКА СТАНДАРТОВ

Внутренние стандарты

После того, как Вы выработали определенные Правила пользования Вашей почтовой системой, Вы можете заняться выработкой стандартов, которые позволят эффективно применять Правила. Некоторые стандарты невозможно поддержать без применения специализированных технических средств, однако четкое планирование позволит Вам без труда разобраться, какое именно техническое решение Вам необходимо. Следующие стандарты, утвержденные представителями всех отделов Вашей компании, помогут Вам внедрить и успешно применять Правила пользования почтовой системой.

Официальные заявления

Официальные заявления в форме отказа от обязательств (disclaimer) предназначены для информирования получателей писем о том, что компания не отвечает за содержание корреспонденции, отосланной сотрудниками. Заявления обычно содержат три основных типа положений, которые:

- Уведомляют получателя письма о конфиденциальности переписки и просят перенаправить письмо в случае, если оно попало к получателю по ошибке
- Объясняют, что содержание письма может не отражать официальную точку зрения компании
- Показывают, что компания предприняла все возможные меры для того, чтобы защитить получателя письма. Одновременно с этим следует отказ от каких-либо обязательств в случае, если получателю был все же нанесен ущерб

Типичное заявление может выглядеть следующим образом:

Настоящее почтовое сообщение является конфиденциальным и предназначено исключительно для получателя письма. Если Вы не являетесь получателем, вероятнее всего Вы получили письмо по ошибке и в этом случае любое использование, перенаправление, вывод на печать или копирование данного сообщения запрещаются. Если Вы получили сообщение по ошибке, пожалуйста свяжитесь с отправителем письма. Любые взгляды или мнения, представленные в письме, могут не совпадать с точкой зрения компании и отражают только точку зрения отправителя. Однако настоящее почтовое сообщение и любые вложения в него не содержат вирусов или каких-либо других недостатков, которые могли бы причинить вред Вашей системе; тем не менее, компания не несет никакой ответственности за причинение ущерба в результате получения данного письма.

Мы рекомендуем согласовать текст заявления с Вашим юристом.

Файлы подписи

Подпись в электронном письме используется для идентификации отправителя и сообщения своих контактных данных. Возможно, Вы захотите стандартизировать подписи всех Ваших сотрудников, сделать так, чтобы они все содержали практически один и тот же текст.

Сохранение электронной корреспонденции

В компании стоит выработать определенные правила, согласно которым происходит сохранение электронной переписки в течение некоторого периода времени. Возможно, Вам понадобится установить ограничение на размер почтового ящика каждого из сотрудников. Говоря в целом, почтовые сообщения, не имеющие отношения к делу, могут удаляться незамедлительно, тогда как переписка с клиентами, партнерами и т.п. может сохраняться в течение относительно длительного периода времени. Часто разумным представляется создание дерева папок, в каждой из которых сохраняются сообщения, сходные по тематике. По прошествии нескольких месяцев новому сотруднику будет гораздо проще войти в курс дела, пользуясь архивом сообщений.

Стандарты фильтрации

Типы файлов

Обсудите с представителями отделов Вашей компании вопрос, какие типы файлов следует запретить пересылать через корпоративную почтовую систему. Вы можете выбрать такие типы файлов, как WAV, AVI, MPG, MP3 — они практически никогда не используются в работе, только если Вы не работаете в медиа-индустрии. Общепринятой практикой сегодня является проверка всех исполняемых (EXE) файлов на предмет наличия вирусов.

Упакованные файлы должны проверяться как на вирусы, так и на содержание исходных файлов. Для этого при выборе программного обеспечения для анализа следует обратить внимание, какие типы архивов поддерживает система. Самые распространенные типы архивов: ARJ, LZH, CAB, CMP, GZIP, RAR, TAR, ZIP.

Анализ содержания

Большая часть программных продуктов, предназначенных для анализа почтового трафика, исследуют почтовые сообщения на предмет наличия в них определенных ключевых слов. Некоторые продукты даже содержат в себе списки слов, обнаруживая которые, программа должна выполнять заданные администратором действия. Такими словами могут быть: password; vitae; horoscopes; confidential и прочие. Обратите внимание на возможность ввода ключевых слов в Вашей кодировке и на Вашем языке, а не только на английском.

Разработка Правил пользования почтовой системой

Перед тем, как окунуться в мир программных разработок для управления почтовым трафиком, рекомендуется разработать Правила пользования Вашей почтовой системой. Четкое определение, что можно, а что нельзя — это лучший аргумент, против обвинений в ограничении прав и свобод, а также скрытого неприятия нововведений. После разработки Правил рекомендуется согласовать окончательный текст с Вашим юристом.

Иногда случается так, что вопрос о контроле над электронными почтовыми сообщениями возникает после инцидента, когда нервы у всего персонала напряжены, а руководство спешно ищет способы избежать повторения неприятностей. Здесь очень важно не забывать то, что задача — не ликвидировать последствия, а разработать комплекс средств, призванный обеспечить эффективность и безопасность использования такого важного в бизнес-практике инструмента, как электронной почты. Не ожидайте, что выработка методик и стратегии пройдет легко и быстро. Возможно, что подготовительные мероприятия займут месяцы в зависимости от размера Вашей компании, а еще некоторое время уйдет на адаптацию сотрудников к изменившимся «правилам игры».

Консультации с отделами и руководством

Внедрение ограничений на пользование электронной почтой может быть воспринято персоналом очень остро и не в положительном смысле. Чтобы преодолеть сомнение и неприятие, чрезвычайно важно обеспечить прозрачность процесса разработки новых правил, показать сотрудникам, что новые решения не навязываются руководством, а предлагаются к совместному обсуждению и выработке компромисса. Значительно проще будет разрабатывать Правила путем формирования некоторой комиссии, состоящей из представителей всех отделов компании, включая высшее руководство.

Поощрение и объяснение реальных причин и мотивов для разработки Правил будет производить больший эффект, нежели Правила, основанные на запретах. С другой стороны Правила должны служить общему делу, поэтому вряд ли Вам удастся совсем обойтись без запретов. Помните, что разрабатывая новые Правила, Вы имеете дело прежде всего с человеческим фактором, а технологии лишь помогают Вам внедрить Правила и обеспечить контроль их исполнения.

Управляя ожиданиями

Держите всех менеджеров в курсе изменений, производимых в почтовой системе. Будьте реалистом, не переоценивайте значимость и положительный эффект от внедрения той или иной технологической системы. Не исключено, что сейчас разрабатываемые Вами Правила изменяться через некоторое время, следуя за изменениями в тактике и стратегии компании.

Сотрудники компаний часто считают, что пользование электронной почтой должно быть таким же свободным и не подверженным ограничениям, как разговор по телефону. В этом смысле важно разъяснить, до какого предела корпоративная почтовая система может быть использована в личных целях. Каждый сотрудник должен четко себе представлять, что почтовая система предоставляет минимум средств для сохранения приватности, а каждое поступающее или отправляемое сообщение может быть просмотрено и сохранено администрацией. Собственно Правила пользования электронной почты должны начинаться с обозначения общих принципов работы с электронной почтой. Далее следует указать условия, на которых компания предоставляет сотруднику право пользования электронной почтой, и те действия, которые считаются недопустимыми в компании. Закончить Правила имеет смысл разделом, поясняющим, какие последствия могут иметь нарушения положений документа, а также местом для подписи сотрудника.

По закону (западных стран – прим. ред.), сотрудники должны быть уведомлены о том, что компания производит перлюстрацию электронных писем. Впрочем, в обсуждениях с представителями отделов сделайте акцент на том, что мониторинг почтовых сообщений автоматизирован, и никто не собирается вручную просматривать каждое письмо. Применяя автоматизированные средства анализа, компания лишь желает оградить себя и своих сотрудников

от возможных нежелательных последствий, которые могут наступить в результате утечки конфиденциальной информации, рассылки спама, оскорбительных и неэтичных материалов и т.д.

Допустимо ли использование почты в личных целях?

В компании следует выработать общую точку зрения на то, в какой мере допустимо использование корпоративной почтовой системы в личных целях. Существует по сути три возможных варианта:

- Полностью запретить любое использование Интернет-ресурсов и электронной почты в личных целях. Согласие с этим сделать одним из условий работы в компании.
- Обеспечить наличие альтернативных компьютерных систем, не входящих в корпоративную информационную систему, с помощью которых сотрудники могли бы использовать службы Интернет в личных целях. Что же касается корпоративной почтовой системы, то отношение к ее частному использованию такое же негативное, как и в первом варианте.
- Разрешить до определенной степени использование электронной почты в личных целях, однако не гарантировать приватности этой переписки. При этом уровень безопасности, разумеется, снижается; в то же время, с точки зрения психологии такой вариант предпочтителен.

Конфиденциальность

Удостоверьтесь, что Ваши Правила содержат положения о том, как следует обращаться с информацией о клиентах. Сотрудники должны быть уведомлены об общепринятых в мировой бизнес-практике правилах работы с информацией о клиентах, а также об особенностях применения этих правил в компании.

Электронная почта через Web (Web-based Email)

В настоящее время существует масса почтовых веб-сервисов, наподобие Microsoft Hotmail. Безусловно, гораздо проще контролировать один канал передачи электронных сообщений через корпоративную почтовую систему, нежели отслеживать огромное количество бесплатных почтовых служб. Заметьте, что большая часть подобных почтовых служб не является безопасной. Они в принципе не могут удовлетворять всем требованиям по безопасности, которые предъявляются Вашей компанией, а потому представляют собой угрозу Вашей корпоративной системе.

Разумным путем может быть запрещение использования подобных веб-сервисов с тем, чтобы все электронные письма отсылались исключительно через центральный почтовый сервер предприятия. Для обеспечения безопасности и в то же время благоприятной психологической атмосферы Вы можете установить несколько дополнительных компьютеров, не являющихся частью Вашей системы, с которых сотрудники могли бы посетить любые веб-сайты и пользоваться веб-почтой.

Для ограничения доступа к почтовым веб-услугам Вы можете воспользоваться решением SuperScout Web Filter.

Пример Правил пользования электронной почтой

Пожалуйста внимательно ознакомьтесь с текстом Правил пользования корпоративной электронной почты; в дальнейшем предполагается, что Вы понимаете все положения настоящих Правил и обязуетесь их выполнять.

Цель

Цель настоящих Правил заключается в донесении до всех работников компании позиции компании относительно того, как должна использоваться корпоративная электронная почта. Конечной целью является гарантия того, что электронная почта используется эффективно для общего дела без создания дополнительного бизнес-риска или инцидентов.

Область применения

Все сотрудники компании, включая работающих по контракту и временный персонал, должны подчиняться положениям настоящих Правил. Нарушение Правил может привести к дисциплинарным взысканиям вплоть до увольнения. Кроме того, Ваши действия могут быть расценены как противозаконные, и в этом случае Вы несете личную полную ответственность перед законом за совершенные действия.

Общие принципы

Компания предоставляет почтовую систему в пользование сотрудникам для организации рабочего процесса и доступ к системе предоставляется только для этого. Почтовые сообщения полученные или отправленные через корпоративную почтовую систему не являются частной собственностью, а составляют часть внутреннего документооборота компании.

Эпизодическое или время от времени встречающееся использование корпоративной электронной почты в личных целях допустимо, однако ограничивается положениям настоящих Правил. Любое частное использование электронной почты должно выполняться в свободное от работы время и не может нарушать ход рабочего процесса. Личное использование электронной почты не должно каким-либо образом воздействовать на работу других сотрудников, нарушать работу электронных систем компании или портить репутацию компании.

Использование электронной почты

При использовании электронной почты обращайте внимание на содержание писем. Отношение многих людей к электронной почте можно назвать легкомысленным по сравнению с отношением к бумажной корреспонденции. Помните, что любые заявления, сделанные в ходе электронной переписки имеют точно такой же вес, как и письменные, и могут быть использованы против Вас и/или компании.

Доступ к почтовым веб-услугам (например, Hotmail, Mail.ru) запрещается с целью уменьшения риска попадания вирусов и других вредоносных программ в корпоративную сеть компании.

Обучение

Обучение сотрудников является одной из важнейших задач в ходе внедрения Правил доступа к электронной почте. В ходе обучения используйте плохие примеры пользования почтой и объясняйте, почему та или иная практика использования несет отрицательный заряд и недопустима в компании. Не стоит говорить только о том, что нужно делать; приводя отрицательные примеры, Вы тем самым четко проводите границу между тем, что хорошо, а что плохо.

Уведомления

Чтобы все те аспекты Правил, о которых Вы говорили в ходе внутренних семинаров, не забылись на вторую неделю, подумайте о том, как напоминать сотрудникам о всем вышесказанном. Вот несколько способов, как не дать забыть о том, что Правила все еще в силе:

- Когда исходящее сообщение не соответствует положениям Правил и задерживается почтовой системой, разумно отправлять уведомление об этом факте с подобным текстом: «Почтовое сообщение, которое Вы только что отправили на адрес vasya.pupkin@mail.ru было автоматически проверено, и установлено, что не соответствует Правилам использования почты в компании. Мы рекомендуем связаться с получателем сообщения и уведомить о задержке с отправкой письма. Вам следует связаться с системным администратором по внутреннему телефону 1234, если Вы считаете, что запрет на отправку сообщения является результатом ошибки. В случае, если от Вас не последует какой-либо реакции на задержку сообщения, последнее будет удалено в течение 72 часов».
- Задержанная входящая корреспонденция должна обрабатываться похожим образом. Уведомление высылается отправителю письма с просьбой связаться с получателем. Предпочтительно связываться именно с отправителем, поскольку сообщение потенциально может быть спамом.
- Вы можете вставлять в каждое входящее письмо несколько строк, в которых указываете, например, адрес на текст Правил. Вот пример подобного раздела: «Настоящее сообщение было проверено на предмет наличия вирусов и соответствия положениям Правил пользования электронной почты. Текст Правил может быть найден по адресу: f:/company/policies/email.doc».
- Предлагайте сотрудникам самим сделать выводы об эффективности применения тех или иных технических средств, которые Вы установили. Для этого регулярно представляйте цифры, отражающей количество входящих писем, содержащих вирусы или спам, которые были остановлены системой.

Поэтапное создание и внедрение Правил

Далее мы предлагаем Вам возможный вариант плана внедрения Ваших Правил использования электронной почты. План состоит из нескольких этапов, между которыми рекомендуется сделать хотя бы недельный перерыв для получения и анализа результатов выполненных ранее задач. Для Вашего удобства Вы можете распечатать эту таблицу

ЭТАП 1 – ОБСУЖДЕНИЕ БУДУЩИХ ПРАВИЛ

Можете ли Вы четко объяснить сами себе, какую проблему представляет собой неуправляемый доступ к корпоративной почтовой системе? Вполне вероятно, Вам придется не раз объяснять и доказывать очевидные для Вас вещи своим сотрудникам.	
Помогите понять высшему руководству компании, что проблема существует и на ее решение необходимо выделение людских и материальных ресурсов	
Организуйте комиссию по разработке Правил пользования корпоративной электронной почты. Вовлеките в работу сотрудников отдела кадров, поскольку Правила имеют большее отношение к персоналу, нежели к технологиям	
Решите, до какой степени возможно использование корпоративной электронной почты в личных целях	
Примите решение относительно запретов на пользование почтовых веб-услуг. Если Вы решаете полностью запретить подобные сервисы, следует сразу задаться вопросом, какими техническими средствами будет обеспечена реализация запрета	
Подготовьте черновик Правил и разошлите его всем участникам рабочей группы перед обсуждением. Возможно, имеет смысл разослать черновик документа всем сотрудникам компании для получения отзывов до принятия Правил	
Решите вопрос, следует ли требовать от сотрудников письменного согласия выполнять положения Правил при приеме на работу	
К черновику Правил приложите возможный вариант текста обязательной вставки во все исходящие электронные письма (Disclaimer). Посоветуйтесь с юристом относительно содержания текста	
Проконсультируйтесь у юристов и специалистов в области трудового права относительно содержания Правил использования почты.	
Обсудите с участниками рабочей группы вопрос, существуют ли в компании отделы или сотрудники, к которым положения Правил неприменимы или применимы лишь частично	
Заранее подумайте о том, как следует поступать с теми сотрудниками, которые откажутся выполнять положения Правил	

ЭТАП 2 – РАБОТА С ПРАВИЛАМИ

Распространите Правила среди всех сотрудников. Не забудьте про временный персонал и контрактников	
Составьте расписание учебных мероприятий для сотрудников, на которых разъясняются аспекты Правил	
Достигните соглашения со всеми заинтересованными лицами относительно того, кто будет осуществлять мониторинг почтовых сообщений и кому это лицо будет подчиняться	
Найдите ответ на вопрос: следует ли устанавливать предел по объему почтового ящика, и если да, то существуют ли исключения из правил?	
Решите, будет ли создаваться структура папок для хранения различных сообщений	
Собираетесь ли Вы вводить обязательный для выполнения стандарт на подписи писем? Если да, то Вам следует разработать общий шаблон подписи	
Если Вы собираетесь организовать свободную зону доступа к Интернет (Интернет-кафе), то позаботьтесь о решении вопроса, связанного с материально-техническим оснащением и выбором места будущего кафе	
Какой максимальный объем одного письма является допустимым?	
Какую политику обработки вложенных файлов Вы решите применить? Следует ли жестко утвердить отсылку документов, созданных в MS Word, в формате RTF?	
Установите стандартную процедуру обработки всех документов, содержащих определенные знаковые ключевые фразы, вроде «Для служебного пользования»	

ЭТАП 3 – ОБУЧЕНИЕ

Обучите сотрудников грамотной и безопасной работе с почтовой системой. Доведите до их сведения все аспекты Правил пользования электронной почты	
Концентрируйте внимание не на запретах, корпоративном контроле и пр; акцент делайте на общепринятых правилах бизнес-этики. Сканирование почтовых сообщений – процесс полностью автоматизированный, и никто не собирается читать все проходящие сообщения	
Приведите примеры напрасной траты ресурсов почтовой системы (расход пропускной способности, место на диске и пр.), которая может препятствовать прохождению действительно важных для компании сообщений	
Сообщите сотрудникам, как они могут высказывать свое мнение о нововведениях	

ЭТАП 4 – МОНИТОРИНГ

Удостоверьтесь в том, что антивирусные средства, которые Вы применяете в настоящий момент, смогут эффективно работать вместе с почтовой системой. Возможно, Вам потребуется закупить дополнительное программное обеспечение	
Установите программное обеспечение для фильтрации почтового трафика в режиме мониторинга и вывода отчетов	
Просмотрите все существующие инструкции относительно обеспечения сохранности клиентской информации. Проверьте, что они не противоречат Правилам работы с почтой	
Оцените важность документов, с которыми работают сотрудники. Допустимо ли их пересылка по электронной почте? Можете ли Вы создать правила обработки сообщений, которые смогут предотвратить утечку конфиденциальной информации?	
Составьте список значимых фраз, наличие которых в письмах или вложенных файлах, будет являться признаком передачи конфиденциальных данных	
Есть ли в компании сотрудники, деятельность которых предполагает использования шифровальных средств?	
Какие типы вложений имеет смысл запретить к прохождению через почтовую систему? Удостоверьтесь в том, что Вы блокируете прохождение ненужных файлов баз данных или мультимедиа-файлов. Какие типы архивов Вы считаете допустимыми к использованию в электронной почте?	
Продумайте методику борьбы со спамом. Возможно Вам имеет смысл установить	

специальное программное обеспечение или подписаться на спам-список	
Выведите отчеты об использовании почты и проанализируйте их. Вероятнее всего, уже на данном этапе из отчетов Вы сможете определить кто из пользователей пользуется корпоративной электронной почтой не по делу	

ЭТАП 5 – ВНЕДРИТЕ ПРАВИЛА ДОСТУПА

Во исполнение Правил введите специальные условия на фильтрующем программном обеспечении: • Ограничение размера письма • Запрет на пересылку писем, содержащих файлы форматов WAV, AVI, MPG и пр. – файлы этих форматов используются в бизнес-практике чрезвычайно редко • Добавляйте к каждому исходящему письму стандартный заголовок или окончание • Блокируйте и проверяйте исполняемые exe-файлы. Перед блокировкой узнайте, кто привык использовать самораспаковывающиеся архивы	
Регулярно отслеживайте работу правил программного обеспечения. Настройте их таким образом, чтобы количество неверных срабатываний было минимальным	

ЭТАП 6 – НАПОМИНАЙТЕ СОТРУДНИКАМ О НАЛИЧИИ ПРАВИЛ ПОЛЬЗОВАНИЯ

Напоминайте пользователям о наличии Правил пользования почтой автоматическими письмами в случае, если их письма задерживаются или блокируются. Будьте вежливы и помните, что ни одно техническое средство не дает 100% гарантии распознавания конфиденциальной информации	
Подумайте о том, чтобы добавлять во входящие письма специальное сообщение, говорящее о том, что сообщение было просканировано	

ЭТАП 7 – ПЕРЕСМАТРИВАЙТЕ И РАССТАВЛЯЙТЕ АКЦЕНТЫ

Создавайте отчеты, демонстрирующие текущий уровень почтового трафика	
Создавайте отчеты, которые показывают активность тех пользователей, которые были неоднократно замечены в нарушениях Правил	
Пересматривайте правила программного обеспечения и список ключевых слов	
Пересматривайте результаты обучения сотрудников. Возможно, следует провести еще несколько корпоративных мероприятий?	
Позвольте сотрудникам кадрового отдела заниматься непосредственной работой с сообщениями и нарушителями. Отделу ИТ оставьте обеспечение функционирования техники	

Как обеспечить фильтрацию? Следующая таблица поможет Вам составить список технических требований по обеспечению выполнения Правил. С этим списком следует обратиться в отдел ИТ, который реализует его в конкретные правила программного обеспечения.

Тип	Лимит на входящие сообщения	Лимит на выходящие сообщения	Исключения для пользователей/групп пользователей
Максимальный размер письма	10Мб	5Мб	-
Допустимы ли зашифрованные файлы?	Да -	- Нет	- Отдел разработок
Запрещенные вложенные файлы	Avi, qtm, mpg, mpeg, wav, exe, com	Avi, qtm, mpg, mpeg, wav, exe, com	Отдел маркетинга
	Exe, com, dll	Exe, com, dll	Отдел ИТ
	-	Ns3, nsf, ntf (Lotus Notes)	Отдел ИТ
Ключевые слова	-	Конфиденциально, для служебного пользования	Директора
	-	Username, id, password	Отдел ИТ
	Cv, vitae, resume, резюме	Cv, vitae, resume, recruitment, резюме, поиск работы	Отдел кадров
	Виагра, халява	-	-
	Гороскопы, для взрослых	-	-
Отправитель	Anonymous, no one, nobody, no-one, replay.com (действия направлены против спама)	-	-
Получатель	-	Список конкурентов	-
	-	Hotmail.com	-
Наибольшее число получателей	10	10	
Период сохранения письма в БД	2 года	2 года	Менеджеры проектов, директора, отдел кадров, бухгалтерия
Стандартный размер ящикв	120Мб	120Мб	-

Вы можете предотвратить утечку конфиденциальной информации путем просмотра сообщений в поиске ключевых слов и фраз. Например, если Вы находите номера клиентских договоров, то это может означать, что информация о клиенте пересылается лицу, которое не должно иметь к ней доступ.

Исключения

В любых правилах есть исключения. Например, отдел кадров наверняка должен иметь доступ к получению писем, содержащих в огромном количестве фразы вроде «резюме» или «вакансия», а отдел кадров регулярно рассылает информацию о продукции компании и прайс-листы

потенциальным клиентам. Поэтому выработка списка исключений является чрезвычайно важной задачей. Наверняка, для разработки такого списка Вам потребуется консультация со стороны представителей всех отделов Вашей компании.

Стандарты обеспечения безопасности

Внутренние стандарты

Как Вы уже поняли из настоящего документа, Вы можете фильтровать конфиденциальную информацию, основываясь на наличии или отсутствии специальных ключевых фраз. Однако, если никто и никогда такие фразы в компании не применяет, эффективность работы фильтрующего программного обеспечения будет равна нулю. Поэтому Вам следует подумать над тем, как утвердить хорошую практику установки на каждый конфиденциальный документ соответствующего «электронного штампа» и сохранения некоторых особо важных документов в шифрованном виде в закрытых разделах сервера.

Для передачи особо важных документов третьим лицам следует применять шифрацию. На сегодняшний момент на рынке работает огромное число компаний, предлагающих свои продукты в области криптозащиты. Перед выбором такого средства почитайте о стойкость шифров, а также оцените степень защищенности системы на основе результатов экспериментов ряда независимых экспертов.

Вложенные файлы

Вложенные файлы представляют собой реальную угрозу заражения вирусом. В свое время, когда вложенные файлы хранили в себе преимущественно текстовую информацию, возможности заразить их вирусом практически не существовало. Однако сегодня многие файлы данных по сложности не уступают небольшим программам. Вы не можете уверенно утверждать, что находится в файле до тех пор, пока не откроете его, однако если файл заражен – будет уже слишком поздно. Хорошей практикой является отсылка документов в формате RTF. Это позволяет отсылать текстовую информацию со всем необходимым оформлением, но без возможности внедрения макросов, а значит и без возможности «подцепить» и перенести заразу. Хотя мысль о полном запрете на пересылку вложенных файлов может выглядеть ужасной, стоит ее рассмотреть. Помимо обеспечения антивирусной безопасности Вы, таким образом, можете предотвратить использование почтовой системы в целях передачи порнографических материалов, игр, мультимедийных файлов и т.д.

Размер писем

Стоит решить вопрос относительно размера писем, которые приходят в корпоративную сеть и отсылаются в Интернет. Обычно достаточно 10Мб. Важно не только остановить передачу больших файлов, но также показать пользователям, что существует множество способов более эффективной передачи данных через сеть.

Антивирусная безопасность

Существует три возможных способа обеспечения антивирусной безопасности:

1. Антивирусное программное обеспечение устанавливается на каждый из клиентских ПК.
2. Антивирусное программное обеспечение производит сканирование всех входящих и выходящих сообщений. Чаще всего такое ПО является надстройкой для известных и популярных почтовых серверов. Однако, не всегда такое возможно: установка антивирусного ПО на почтовый сервер требует определенной квалификации и собственно наличия выделенного почтового сервера, что не всегда выполняется в небольших компаниях.
3. Пользование услуг по антивирусной проверке третьих фирм. Входящая почта перенаправляется на удаленный сервер, где проверяется и возвращается в сеть компании. Этот метод очень хорошо себя зарекомендовал тем, что не требует обслуживания системы – все эти действия производит сервисная компания.

Собственно еще всегда важно помнить, что антивирусное ПО обеспечивает требуемый уровень защиты только в том случае, если регулярно обновляется.

Защита от спама

Ограничение потока нежелательной рекламной информации (спам) — одна из задач, которую ставят перед собой ИТ-менеджеры при реализации Правил. Вот несколько советов по этому поводу:

1. Подумайте о том, чтобы заказать услуги третьих фирм, которые будут обеспечивать фильтрацию Вашей почты на основе собственных спам-списков
2. Подпишитесь на регулярную рассылку спам-листов. Организации вроде MAPS (http://mail-abuse.org) предлагает список спам-хостов. Большая часть средств фильтрации почтового трафика располагают средствами анализа подобных списков и использования их в работе.
3. Если Ваши пользователи регулярно получают спам, Вы можете рассмотреть возможность отключения вывода изображений в клиентском почтовом программном обеспечении. Это предотвратит возможность скрытого сообщения об открытии сообщения спамерам
4. Вы можете также использовать возможности клиентского программного обеспечения для отсеивания спам-сообщений. Однако следует иметь в виду, что существует опасность отсева действительно важных сообщений.

Мониторинг и оценка состояния

Мониторинг является критически важной процедурой. «Правила без мониторинга – это тоже самое, что закон без полиции». Результаты мониторинга Вас могут сильно удивить после внедрения Правил: в среднем фильтрующее ПО от SurfControl обнаруживает, что 35-40% почтовых сообщений переносят графические изображения, а 70-80% почтового трафика не имеет отношения к делу.

Регулярно оценивайте точность срабатывания правил обработки сообщений.

Поддерживайте связь с сотрудниками; прислушивайтесь к их мнению относительно Правил. Не переусердствовали ли Вы? Действительно нужно чувствовать меру и не нарушать нормальные бизнес-процессы; с другой стороны, однако, решения не должны носить половинчатого характера.

Будьте готовы подвергнуть Правила изменениям. Никакие правила или законы не могут носить абсолютного и неизменного во времени характера. По мере изменения Вашей компании должны меняться и Правила.

Дисциплинарные взыскания

Средства для анализа почтовых сообщений должны использоваться по назначению. Включайте мониторинг действий определенного сотрудника только в том случае, если есть существенные основания подозревать его в совершении действий, нарушающих Правила. Не ищите «плохих» сотрудников специально путем перлюстрации корреспонденции. Почтовые системы не смогут заменить хорошей практики управления в компании. И помните: любые Правила пользования почтой в компании должны быть ***внедрены*** – иначе они будут просто игнорироваться.