РЕАЛИЗАЦИЯ МЕХАНИЗМА ОБМЕНА ПОЧТОВЫМИ СООБЩЕНИЯМИ ПОЛЬЗОВАТЕЛЕЙ ЗАЩИЩЕННОЙ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ С ПОЛЬЗОВАТЕЛЯМИ СЕТИ «ИНТЕРНЕТ»

Ю. В. Зверьков, Ю. И. Корнилов, Е. В. Дмитриева, М. М. Захаров, И. Л. Бондарь

ФГУП «РФЯЦ-ВНИИЭФ», г. Саров Нижегородской обл.

Введение

Сегодня корпоративная электронная почта – неотъемлемая часть бизнес-культуры и бизнес-коммуникаций в любой компании. Невозможно даже представить себе современную жизнь и бизнес без электронной почты. Электронная почта служит средством связи и при внутрикорпоративном взаимодействии.

Но все усложняется, когда речь заходит об автоматизированных системах в защищенном исполнении (АСЗИ). В случаях, когда АСЗИ имеет выход в глобальную сеть ИНТЕРНЕТ, реализация почтового взаимодействия серьезно осложняется за счет необходимости применения в АСЗИ средств защиты информации (СрЗИ) от несанкционированного доступа, обнаружения вторжений, межсетевого экранирования, применения дополнительных мероприятий, компенсирующих угрозы из ИНТЕРНЕТ. В целях обеспечения безопасности информации большая часть АСЗИ не имеет непосредственного взаимодействия с глобальной сетью, что сильно ограничивает связь с внешними системами. Одним из возможных вариантов организации доступа к данным за пределами АСЗИ является использование съемных носителей и накопителей информации для обмена данными между системами, образуя «воздушный зазор» между ними.

Организации, использующие для обработки данных АСЗИ без непосредственного доступа к глобальной сети, также нуждаются в использовании системы электронной почты для связи с внешними (для данной системы) абонентами. Наиболее простое в плане реализации решение – использование внутри предприятия абонентских пунктов доступа в ИНТЕРНЕТ, которые представляют собой небольшую локальную сеть с группой компьютеров, подключенных к глобальной сети. Но данное решение вносит множество неудобств и ограничений в работе: отсутствие работника на рабочем месте во время работы с электронной почтой, отсутствие необходимых данных из электронной почты на рабочем месте и т. п.

В данном докладе будет представлен механизм, позволяющий устранить большую часть ограничений, связанных с работой почтовой системы, с сохранением требуемого уровня защищенности АСЗИ.

Архитектура почтовой системы

В состав предлагаемой почтовой системы входит 4 почтовых сервера/кластера:

- внутренний кластер для обработки почтовых сообщений АСЗИ на базе Microsoft Exchange Server;
  - группа серверов с ролью mailbox объединена в Database Availability Group;
  - группа серверов с комбинированной ролью HubTransport+ClientAcces, объединена в NLB-кластер с общим сетевым именем;
  - сервер с ролью Unified Messaging для взаимодействия с MS Lync;
- внутренний почтовый сервер в открытой локальной сети предприятия, не имеющей выхода в ИНТЕРНЕТ;
- внешний почтовый сервер в ДМЗ внешней сети предприятия, имеющей выход в ИНТЕРНЕТ.

Всю структуру предприятия можно разделить на 3 части:

- изолированная сеть – АСЗИ, где работает большинство пользователей и идет обработка конфиденциальной информации;
- внутренняя сеть – сеть, оборудование которой не имеет доступа к сети ИНТЕРНЕТ, но имеет подключение к сети, имеющей выход в ИНТЕРНЕТ;
- внешняя сеть – сеть, оборудование которой имеет выход в ИНТЕРНЕТ.

Такая организация сетевой инфраструктуры позволяет обеспечить требуемый уровень информационной безопасности на предприятии при работе с ИНТЕРНЕТ. Передача информации между АСЗИ и внутренней сетью осуществляется через подключаемые устройства хранения информации, такие как usb-диски. В такой системе почтовый кластер АСЗИ выступает как полноценная почтовая система, где и осуществляется основной контроль исходящей почты.

Почтовая система внутренней сети обеспечивает всю обработку приходящих извне писем. Здесь же производится и обработка входящей почтовой корреспонденции, предназначенной для последующего перемещения в АСЗИ.

Почтовая система внешней сети служит только для выполнения операций приема и отправки почтовой

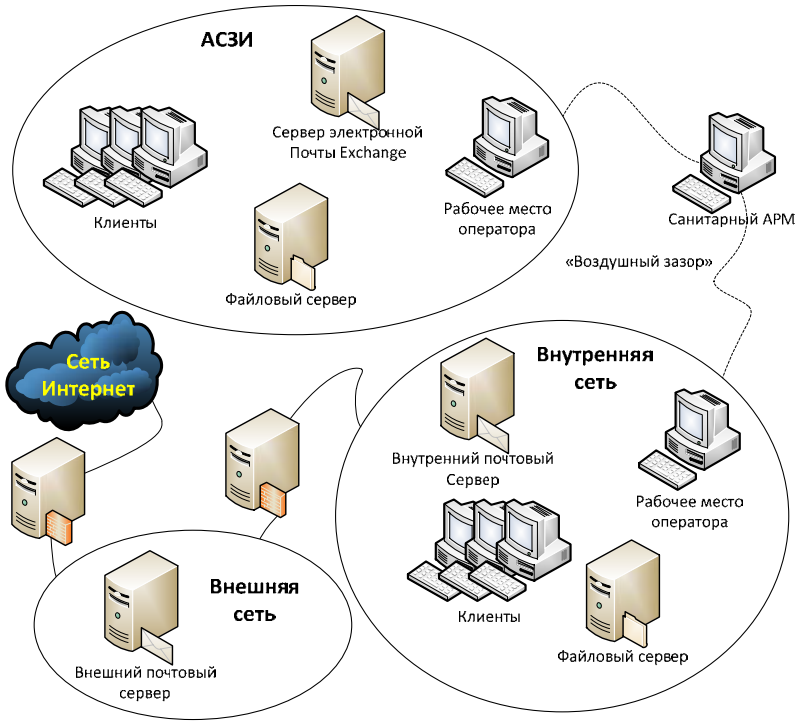

Рис. 1. Архитектура системы электронной почты предприятия

корреспонденции и первоначальной фильтрации входящих писем (фильтром спама отсеивается, как правило, 90 % нежелательной почты, приходящей на адреса пользователей АСЗИ).

Организация отправки-получения внешней электронной корреспонденции

Внутри АСЗИ электронная почта работает без видимых отличий от любой другой почтовой системы. При отправке на адреса АСЗИ на письма накладываются минимальные ограничения, определяемые ее руководящим составом. В случае, когда сервер Exchange сталкивается с незнакомым (внешним) адресом, письмо электронной почты проходит несколько уровней модерирования, прежде чем будет отправлено за пределы АСЗИ. Процесс модерирования имеет линейную структуру, позволяющую отсеивать некорректную корреспонденцию на различных этапах. В соответствии со штатной организацией было выбрано три ступени модерирования: непосредственный начальник отправителя, служба контроля подразделения отправителя, служба контроля предприятия.

После прохождения всех уровней модерирования письмо из АСЗИ передается для отправки на почтовый сервер внутренней сети предприятия путем сохранения копии письма в специальном формате. В связи с тем, что между АСЗИ и внутренней сетью, а соответственно, и между почтовыми серверами отсутствует прямой канал связи, перемещение информации осуществляется не стандартным почтовым протоколом, переносом файлов с письмами. При этом файлы переносятся операторами из выходного каталога почтового сервера АСЗИ во входной каталог почтового сервера внутренней сети, что и обеспечивает контролируемый ручной перенос данных – «воздушный зазор». Для реализации подобного механизма используются файловые серверы в каждой из сетей, между которыми осуществляется перемещение. Данные с сервера АСЗИ копируются на съемный носитель соответствующего уровня конфиденциальности с соблюдением требований информационной безопасности, далее, через санитарный АРМ, данные переносятся на открытый съемный носитель, после чего с него переносятся на файловый сервер внутренней сети. Аналогичным образом переносятся данные в обратном порядке. Для перемещения файлов между файловым и почтовым серверами внутри сети используются задачи по расписанию, что значительно сокращает затрачиваемое время и усилия, позволяя максимально автоматизировать этот процесс.

Внутренний почтовый сервер стандартным образом получает входящие письма от почтового сервера внешней сети, сохраняет их копии и осуществляет обработку: разбирает письма на составляющие и собирает их заново, чтобы исключить нестандартные внедренные данные. Допускается ввод в АСЗИ только некоторых типов изображений в качестве вложений (PNG, JPEG, TIFF, GIF), текст и вложения в формате PDF. Открытыми пакетами для ОС Linux производится попытка преобразования недопустимых вложений в формат PDF, если это не удается, вложение удаляется с соответствующим комментарием в письме. На абонентском пункте ИНТЕРНЕТ подразделения оригинал письма сохраняется – с ним можно работать вне АСЗИ.

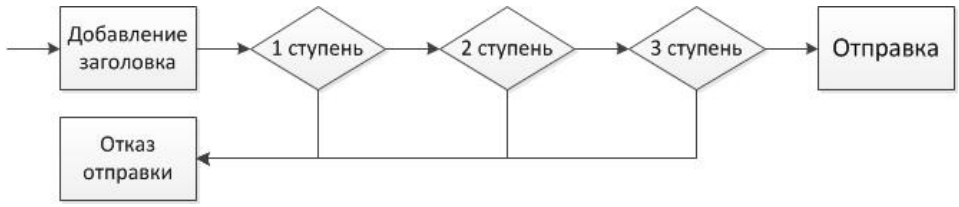

Рис. 2. Схема модерирования исходящей почты

Система согласования исходящей почты

Внешняя электронная почта, отправляемая из СВС РФЯЦ-ВНИИЭФ, подвергается трехступенчатому контролю при помощи разрешительной системы. Разрешительная система реализована с использованием механизма модерирования почтовых сообщений почтового сервера Microsoft Exchange Server. Для этого все пользователи делятся на группы, как правило динамические. Такое распределение пользователей позволяет определить ответственных сотрудников на каждом этапе модерирования, а также исключить один или все этапы модерирования. Таким образом существует два основных деления на динамические группы, для первых двух уровней. Первое включает в группы, в состав которых входят сотрудники одного отдела. Для каждого отдела существует собственная группа. По аналогии существуют группы, объединяющие в себе все отделы, одного подразделения. Для сложных случаев, когда нельзя точно определить принадлежность сотрудника к определенной группе, создаются статические группы. Так же создаются статические группы для исключения модерирования, для тех кому разрешено отправлять почтовые сообщения на внешние адреса.

Система модерирования имеет линейную структуру, где каждый след шаг начинается только при успешном окончании предыдущего. В первую очередь происходит формирование заголовка письма, после чего письмо поступает для проверки непосредственному руководителю. После получения разрешения на первом уровне, письмо поступает в службу контроля на уровне подразделения. И конечным уровнем является проверка службой безопасности.

При согласовании на всех трех уровнях, копия письма передается на файловый сервер, для дальнейшей отправки на внешний адрес. В случае отклонения на любом уровне, отправителю приходит уведомление об отказе в отправке данного сообщения. Таким образом, вся исходящая корреспонденция, за исключением доверенных отправителей, проходит 3 стадии контроля, что исключает отправку во вне информации, не предназначенной для внешних адресатов.

Статистическая информация по работе почтовой системы

Для более наглядного представления об исходящей почте, ежедневно формируются протоколы для службы контроля. Протоколы содержат сведения об отправленных за сутки сообщений на внешние адреса. Для простоты дальнейшего использования, протоколы формируются в формате HTML. Помимо этого, создается веб-ресурс, позволяющий отслеживать на какой стадии находится письмо. Таким образом, сотрудники могут посмотреть на какой ступени находится их письмо, и время прохождения очередной ступени. Пример реализации механизма отображения статистической информации представлен на рис. 3.

Информация об отправленных за пределы СВС ВНИИЭФ письмах

От кого	Кому	Согласование			Доставка	
		руководителем	службой контроля	службой безопасности	на внутренний сервер	на сервер получателя
[redacted]	[redacted]	-	01-07-2019 15:33:56	-	-	-
[redacted]	[redacted]	-	-	-	-	-
[redacted]	[redacted]	01-07-2019 14:53:42	01-07-2019 14:57:05	01-07-2019 15:18:28	-	-
[redacted]	[redacted]	-	01-07-2019 14:43:29	01-07-2019 15:18:06	-	-
[redacted]	[redacted]	-	-	-	-	-
[redacted]	[redacted]	-	01-07-2019 13:47:09	01-07-2019 14:10:00	-	-
[redacted]	[redacted]	01-07-2019 11:41:13	01-07-2019 11:42:44	01-07-2019 14:09:39	-	-
[redacted]	[redacted]	01-07-2019 07:54:42	01-07-2019 09:50:07	01-07-2019 14:03:41	-	-
[redacted]	[redacted]	-	-	-	-	-
[redacted]	[redacted]	01-07-2019 08:42:18	01-07-2019 09:05:50	01-07-2019 09:09:44	01-07-2019 11:56:17	01-07-2019 11:56:43

Рис. 3. Информация об исходящей корреспонденции

Заключение

Электронная почта, жизненно необходимая система для большинства компаний. Представленная реализация механизма электронной почты позволяет использовать полноценный обмен электронными почтовыми сообщениями в условиях автоматизированной системы в защищенном исполнении, что позволяет значительно экономить время сотрудников и своевременно получать информацию. При этом соблюдаются все необходимые требования информационной безопасности.

Литература

1. [Electronic resource] Mode of access: https://technet.microsoft.com