КАК ЗАЩИТИТЬ СВОИ ПОЧТОВЫЕ СЕРВЕРА?

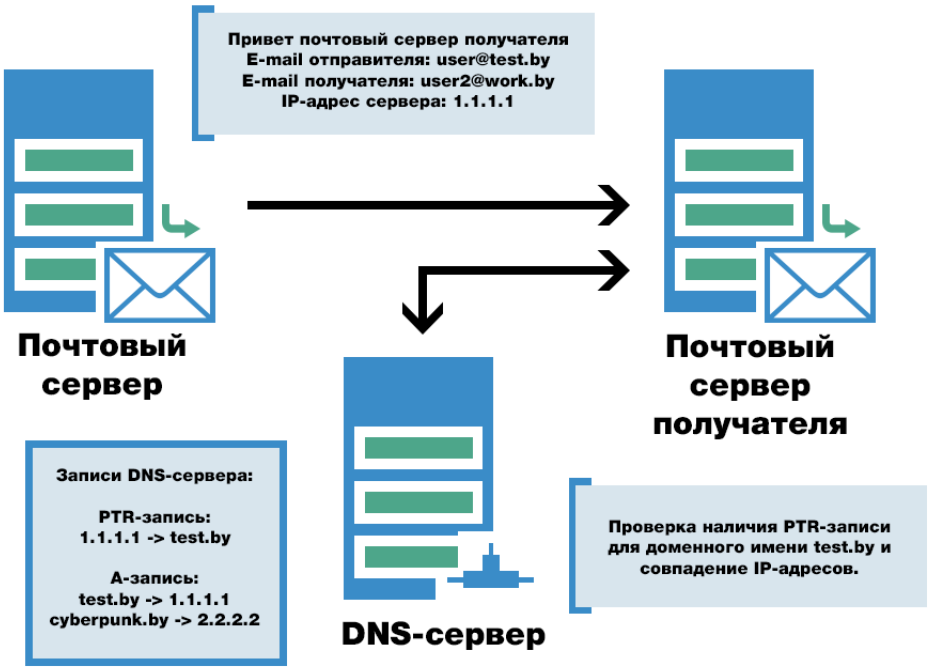
Защита почтовых серверов является важным элементом обеспечения информационной безопасности корпоративной сети и поддержания имиджа организации. Исторически сложилось, что электронная почта создавалась для личной переписки, а не для корпоративного использования, и, как следствие, не обладает механизмами защиты на архитектурном уровне. В данной связи понимание и корректная настройка электронной почты, дополнительное использование сторонних технологий и отказ от массовых рассылок электронных писем стали одними из основ защиты организации.

Для удобного обеспечения защиты почтовых серверов Оперативно-аналитическим центром при Президенте Республики Беларусь были разработаны рекомендации по корректной настройке указанных серверов. В свою очередь специалистами РУП «Белтелеком» был проведен анализ данных рекомендаций с целью пояснения работы технологий защиты и их рационального использования.

Рекомендация 1. Использовать механизмы проверки PTR-записи почтовых сервисов.

PTR-запись – это DNS запись, предназначенная для преобразования IP-адреса в доменное имя. Чаще всего PRT-запись представляются как обратную A-запись.

Данный механизм проверки является базовым, предназначен для защиты почтовых серверов организации от спама и фишинговых атак, использующих мошеннические домены, и работает следующим образом.



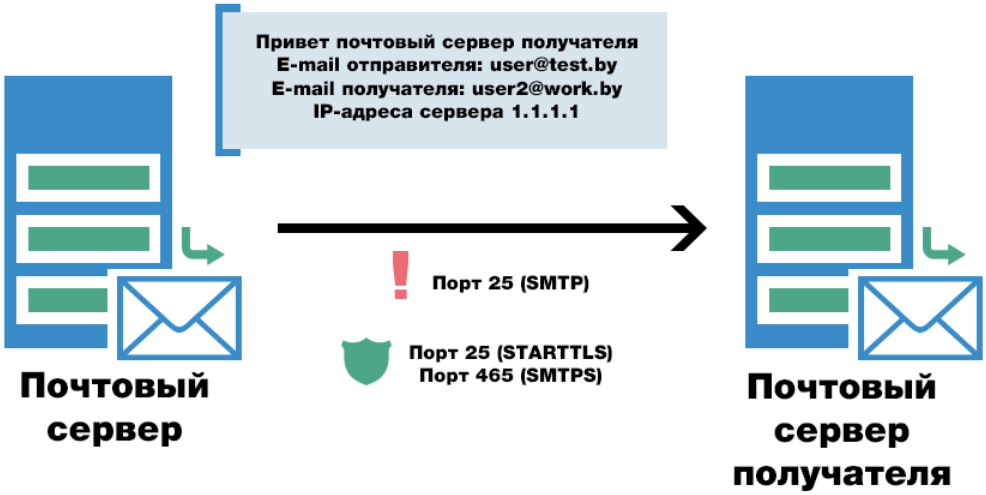
При получения заголовка любого электронного письма почтовый сервер получателя находит IP-адрес почтового сервера отправителя в заголовке и запрашивает доменное имя отправителя по указанному IP-адресу. Искомое доменное имя можно получить только в случае если для анализируемого

IP-адреса существует PTR-запись. Далее, полученное в результате запроса доменное имени сверяется с доменным именем из заголовка электронного письма. В случае если доменные имена совпадают, то считается, что проверка прошла успешно. Подробно указанная процедура описана в RFC 2505 и поддерживается всеми современными почтовыми серверами (Exim, Postfix, Sendmail, Microsoft Exchange Server, MDaemon Server и другие) .

Рекомендация 2. Использовать механизмы шифрования почтовых сообщений и (или) передачу почтовых сообщений с использованием криптографических протоколов передачи данных (SMTPS, STARTTLS).

SMTPS – это криптографический метод защиты протокола SMTP путем создания неявного TLS-соединения на 465 порту транспортного уровня. STARTTLS – это расширение протокола SMTP, позволяющее создать зашифрованное соединение прямо поверх обычного TCP-соединения на стандартном порту обмена почтовыми сообщениями (25 порт).

Указанные механизмы также являются базовыми, предназначены для обеспечения конфиденциальности и целостности передаваемых по каналам связи электронных почтовых сообщений и реализованы следующим образом.



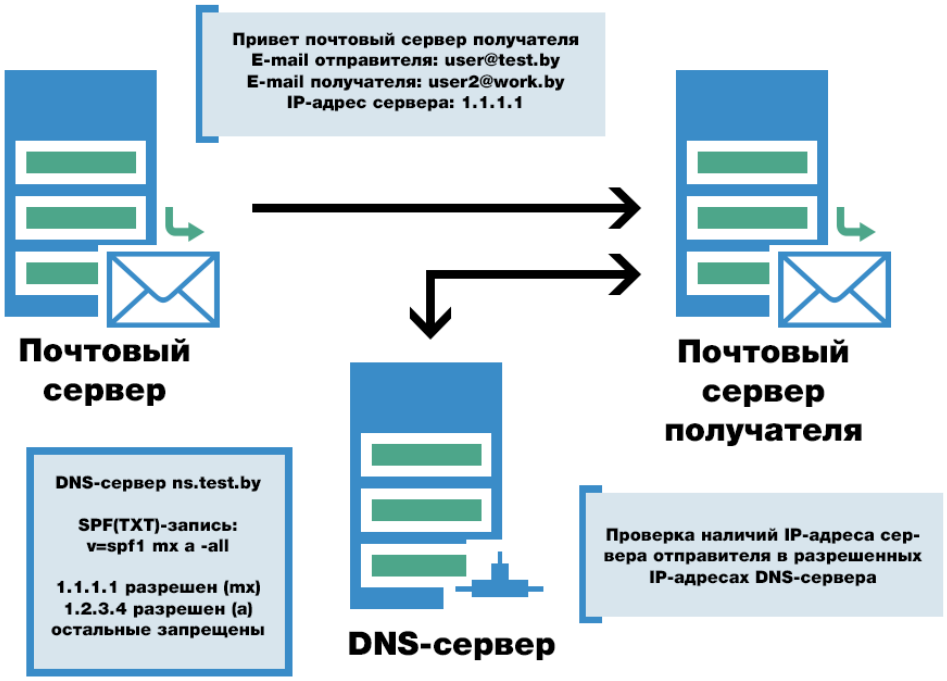
Если на почтовом сервере отправителе настроен SMTPS передача всей электронной почты проводится через отдельный транспортный порт с шифрованием всех данных на основе рукопожатий. В случае если на почтовом сервере отправителя настроен STARTTLS, проводится процедура согласования с почтовым сервером получателя криптографических протоколов по незащищенному протоколу SMTP после чего происходит шифрование и отправка исходного электронного письма. Стоит отметить, что при неправильной конфигурации STARTTLS процедура согласования криптографических протоколов не сможет быть проведена, а сами электронные сообщения будут передаваться в открытом виде. Подробно о работе SMTPS и STARTTLS можно узнать в RFC 8314 и в RFC 3207 соответственно.

Рекомендация 3. Использовать механизмы проверки SPF-записи почтовых сервисов.

SPF (Sender Policy Framework) – это расширение (дополнение) для протокола отправки почты через SMTP-сервер, реализующее механизм

подтверждения отправителя по IP-адресу. В настоящее время существует две версии расширения: SPFv1 и SPFv2.0/mfrom,pra. Версия расширения SPF2.0/mfrom,pra также называемая Sender ID не получила широкого распространения.

Данные механизм проверки предназначен для поддержания репутации организации путем защиты электронных писем от подмены поля «Отправитель» (From), требует соблюдения определенных условий и работает следующим образом.

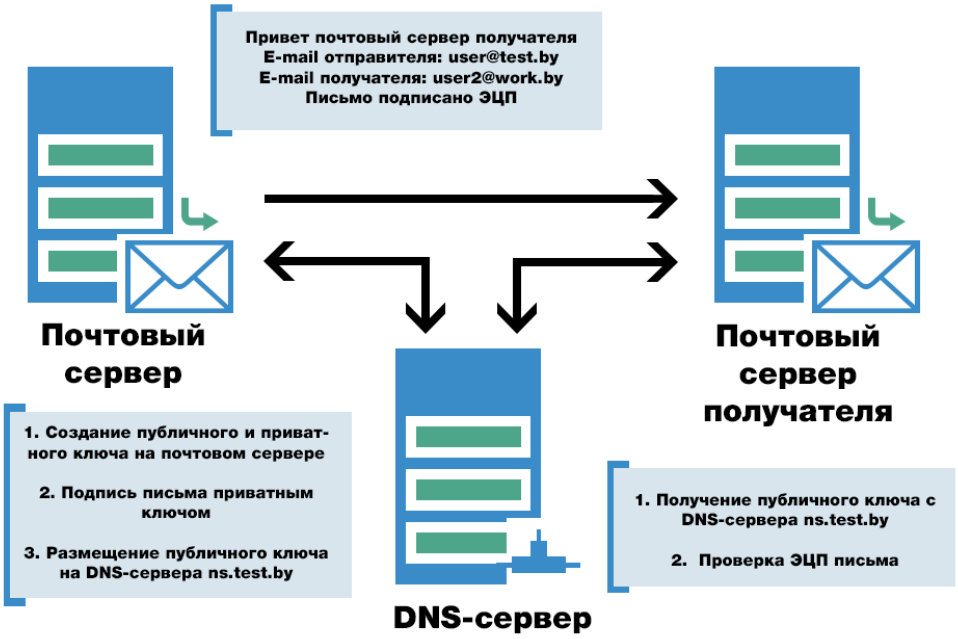


При получения любого электронного письма почтовый сервер получателя находит IP-адрес почтового сервера отправителя в заголовке электронного письма и запрашивает у DNS-сервера отправителя отдельную TXT- и/или SPF-запись, в которой указаны IP-адреса с которых могут отправляться электронные письма. Если IP-адрес полученные из заголовка существует в перечне разрешенных для отправки IP-адресов, то считается, что проверка прошла успешно. В случае, если IP-адрес отсутствует в перечне или TXT- и/или SPF-записи не существует электронные почтовые сообщения уходящие с данного почтового сервера будут блокироваться или относится к спам. Подробно указанная процедура описана в RFC 7208.

Рекомендация 4. Использовать механизмы почтовой аутентификации отправителя почтовых сообщений (DKIM).

DKIM (DomainKeys Identified Mail) – это расширение (дополнение) для протокола отправки почты через SMTP-сервер, реализующее механизм электронной цифровой подписи электронного письма.

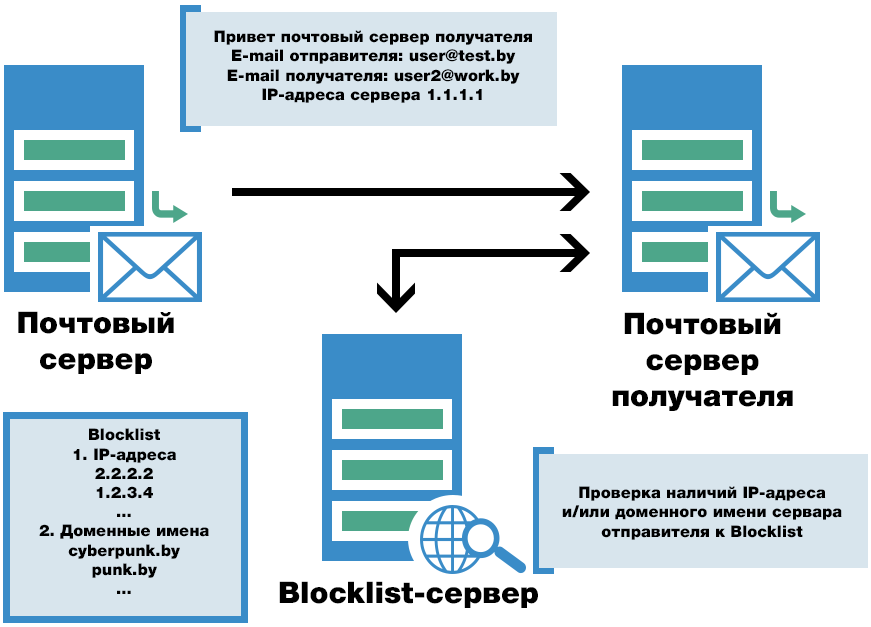
Указанный механизм проверки предназначен для поддержания репутации организации путем защиты электронных писем от подмены отправителя и работает следующим образом.



При начальной конфигурации почтового сервера отправителя создаются публичный и приватный ключи для последующего создания ЭЦП электронного почтового сообщения. Приватный ключ хранится в секрете на почтовом сервере отправителя, а публичный ключе размещается в TXT-записи на DNS-сервере отправителя. В момент отправки электронного письма почтовый сервер отправителя подписывает почтовое сообщение приватным ключом и направляет его почтовому серверу получателя. Почтовый сервер получателя проверяет валидность ЭЦП запрашивая с DNS-серверов отправителя TXT-запись с публичным ключом. Если ЭЦП верна, то считается, что проверка прошла успешно. В случае, если на принимающей стороне отключена функция проверки ЭЦП, то на прохождении электронного письма это никак не сказывается. Подробно указанная процедура описана в RFC 5585.

Рекомендация 5. Обеспечить фильтрацию почтовых сообщений с использованием списков нежелательных отправителей почтовых сообщений.

Указанная рекомендация предназначена для защиты от спама и фишинговых атак, использующих легитимные доменные имена или IP-адреса и реализована следующим образом.



При получения любого электронного письма почтовый сервер получателя находит IP-адрес и/или доменное имя почтового сервера отправителя в заголовке электронного письма и запрашивает у стороннего Blocklist-сервера их наличие в перечне подозрительных адресов. В случае если анализируемый IP-адрес и/или доменное имя отсутствует в указанном перечне, то считается, что проверка прошла успешно и электронное письмо принимается почтовым сервером получателя. Подробно указанная процедура описана в RFC 5782.

Дополнительно стоит отметить, что наиболее чаще всего в качестве Blocklist-сервера используют сервера некоммерческой компании Spamhaus.

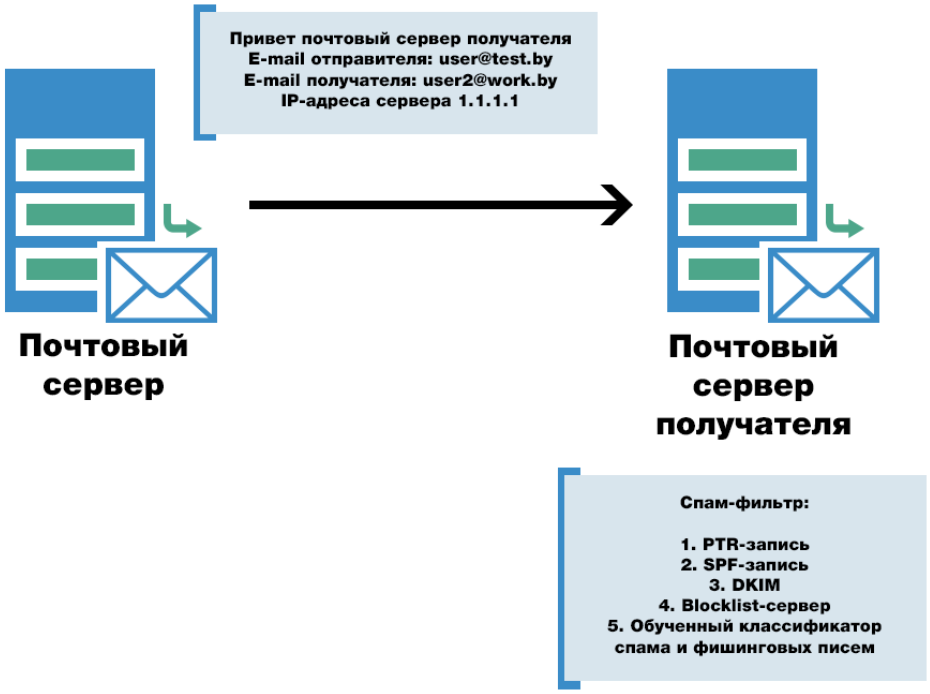
Рекомендация 6. Обеспечить в реальном масштабе времени автоматическую антивирусную проверку файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносного ПО.

Данная рекомендация предназначена для обнаружения, блокировки и удаления электронных писем с вложениями содержащими в себе вредоносное программное обеспечение и реализована следующим образом.

При начальной конфигурации почтового сервера получателя проводится установка и конфигурирование антивирусного программного обеспечения. В момент получения любого электронного письма почтовый сервер получателя инициализирует процедуру сигнатурного анализа электронного почтового сообщения на наличие вредоносного ПО. В случае отрицательного результата анализа считается, что проверка прошла успешно и электронное письмо передается почтовому клиенту получателя. Для указанной процедуры не существует нормативных документов, регламентирующих принцип работы.

Рекомендация 7. Обеспечить спам-фильтрацию почтовых сообщений.

Данная технология предназначена для защиты от спама и фишинговых атак, использующих легитимные доменные имена и/или IP-адреса и основывается на ранее описанных технологиях, а также Байесовских фильтрах (или нейронных сетях).



При начальной конфигурации почтового сервера получателя проводится установка и конфигурирование технологий проверки PTR-записи, SPF-записи, DKIM, подключение к Blocklist-серверу. Далее проводится установка и подключение к существующим технологиям спам-фильтра. Спам-фильтр проводит анализ полученных от почтового сервера отправителя электронных писем и на основе обученного классификатора, а также метрик других технологий выносит результат анализа (электронное письмо получает класс «Спам» или «Легитимное письмо»). Для указанной процедуры не существует нормативных документов, регламентирующих принцип работы.

Дополнительно стоит отметить, что наиболее чаще всего в качестве спам-фильтра используют средство фильтрации SpamAssassin.

Рекомендация 8. Блокировать массовую рассылку почтовых сообщений.

Указанная рекомендация предназначена для защиты защиты репутации организации, отправляющей большое количество почтовых сообщений, а также

обеспечения доступности почтового сервера организации (не попадания в Blocklist).

При начальной конфигурации почтового сервера отправителя необходимо задать разрешенное количество отправляемых электронных писем в единицу времени (чаще всего в 1 мин). При превышении данного параметра электронные почтовые сообщения будут помещаться в очередь до возможности отправки. Дополнительно, можно настроить спам-фильтра, что позволит не попасть в Blocklist при проведении массовых рассылок даже с включенным ограничением по количеству отправляемых писем.

Таким образом, специалисты РУП «Белтелеком» могут порекомендовать использовать все описанные выше технологии для обеспечения безопасности почтовых серверов. А в случае отсутствия возможности самостоятельной настройки безопасности почтового сервера воспользоваться услугой хостинга РУП «Белтелеком».