КОЖЕМЯКИН Н. В., БАЗАРОВА И. А. ПРИМЕНЕНИЕ INFOWATCH TRAFFIC MONITOR ДЛЯ ЗАЩИТЫ ОТ УТЕЧЕК ИНФОРМАЦИИ

УДК 004.056.52, ГРНТИ 81.93.29

Применение Infowatch Traffic Monitor для защиты от утечек информации

Н. В. Кожемякин[1], И. А. Базарова[2]

[1]ООО «Газинформсервис», г. Ухта;
[2]Ухтинский государственный технический университет, г. Ухта

Данная статья посвящена созданию концептуального макета сети небольшой компании. Для обеспечения информационной безопасности были использованы продукты Infowatch Traffic Monitor, предоставляющие возможность мониторинга imap4, pop3 и smtp трафика с целью выявления и анализа потенциальных угроз утечки конфиденциальной информации.

Ключевые слова: *infowatch Traffic Monitor, imap4, pop3, smtp, утечка информации, информационная безопасность, макетирование*

Using Infowatch Traffic Monitor to protect against information leaks

N. V. Kozhemyakin[1], I. A. Bazarova[2]

[1]Gazinformservice LLC in Ukhta;
[2]Ukhta State Technical University, Ukhta

This article is devoted to creating a conceptual layout of a small company's network. To ensure information security, Infowatch Traffic Monitor products were used, providing the ability to monitor imap4, pop3 and smtp traffic in order to identify and analyze potential threats to confidential information leakage.

Keywords: *infowatch Traffic Monitor, imap4, pop3, smtp, information leakage, information security, layout*

Введение

Для эффективного контроля и защиты конфиденциальной информации современные компании все чаще обращаются к решениям вроде DLP-систем (Data Loss Prevention). Эти системы представляют собой незаменимый инструмент в обеспечении безопасности при обработке и передаче данных.

DLP-системы позволяют автоматически определять, мониторить и управлять потоками данных в организации. Они обнаруживают и предотвращают несанкционированный доступ к конфиденциальной информации, отслеживают передачу данных за пределы предприятия и блокируют попытки утечки информации.

Использование DLP-систем важно не только для соблюдения требований по защите данных, но и для предотвращения утечек информации, которые могут привести к серьезным финансовым потерям и ущербу репутации компании.

Развертывание таких систем становится неотъемлемой частью стратегии информационной безопасности в современном бизнесе.

Рассмотрим применение DLP-системы на примере региональной компании из сферы медицины, предоставляющей услуги клинико-лабораторного центра, которая обратилась к ведущему исполнителю проектов в области информационной безопасности, ООО "Газинформсервис", с запросом на внедрение программно-аппаратного комплекса для предотвращения утечки информации.

Перед развертыванием системы защиты данных необходимо провести детальный анализ предоставленных входных данных.

Рассматривая характеристики клиники-заказчика, следует учитывать ее региональный масштаб, основные виды обрабатываемой информации (включая персональные данные и юридически значимые документы), а также особенности ее рабочих процессов, включающих в себя значительную часть коммуникации через электронную почту.

Особое внимание следует уделить количеству сотрудников, имеющих доступ к персональным данным, которое в данном случае ограничивается числом не более 100 человек.

Список персональных данных клиентов, хранимых и обрабатываемых в клинике, включает в себя такие критически важные элементы, как фамилии, имена и отчества, даты рождения, адреса проживания, номера телефонов, а также медицинские данные, включая результаты анализов и поставленные диагнозы. Важно отметить, что компания также хранит юридически значимые документы, включая медицинские карты, направления на анализы, справки и заключения врачей, а также копии личных документов клиентов, таких как паспорта, страховые полисы, СНИЛС и ИНН, а также чеки оплаты.

После тщательного ознакомления с предоставленными входными данными и анализа потребностей клинико-лабораторного центра, было принято решение об использовании передовых программных и аппаратных решений в области информационной безопасности.

Поскольку почтовый сервер компании уже функционирует и настроен, а на рабочих местах сотрудников не должно быть предустановлено ПО, выбор был остановлен на использовании DLP-системы.

На российском рынке существует множество отечественных DLP-систем, но фаворитом является решение от компании Infowatch – Traffic Monitor (IWTM) [3].

Infowatch Traffic Monitor представляет собой мощный инструмент, обеспечивающий комплексное управление и контроль за передачей данных в организации. Его использование обладает несколькими ключевыми преимуществами [2].

Во-первых, IWTM обеспечивает высокий уровень защиты конфиденциальной информации. Благодаря механизмам мониторинга и обнаружения утечек данных, он позволяет оперативно реагировать на любые попытки несанкционированного доступа к информации.

Во-вторых, данное программное обеспечение обладает гибкими настройками и возможностями кастомизации, что позволяет адаптировать его под уникальные потребности каждой организации. Это позволяет эффективно управлять и контролировать трафик данных в соответствии с внутренними политиками безопасности.

Кроме того, IWTM обеспечивает полный контроль за передачей данных через электронную почту, веб-сайты, облачные сервисы и другие каналы связи. Это позволяет предотвращать утечки конфиденциальной информации и обеспечивать соблюдение требований законодательства в области защиты данных.

Наконец, использование IWTM способствует повышению эффективности работы сотрудников, предоставляя им безопасные средства для обмена информацией и снижая риск утраты конфиденциальных данных.

Для реализации системы Infowatch Traffic Monitor будет развернуто два сервера, основанных на операционной системе RedOS – отечественной разработке.

Первый сервер, являющийся сервером базы данных и индексатором, предназначен для хранения всех перехваченных сообщений и их структурирования с целью оптимизации работы и повышения производительности системы.

Второй сервер, выполняющий функции перехватчика и веб-консоли, является ключевым инструментом для достижения поставленных целей. Он отвечает за перехват трафика и его анализ, а также предоставляет веб-консоль для настройки правил и реакции на события.

Операционная система RedOS обладает уникальной возможностью реализации схемы "В разрыв" (failover), что обеспечивает непрерывную работу системы в случае сбоя или отказа основного сервера. Это обеспечивает стабильность и надежность функционирования системы IWTM.

Операционная система RedOS обладает уникальной возможностью, только с помощью нее возможно настроить перехват трафика по схеме «В разрыв» для возможности полного блокирования сообщения.

Кроме того, RedOS представляет ряд других преимуществ, которые делают его привлекательным выбором для развертывания системы IWTM. Во-первых, это национальная разработка, что поддерживает отечественного производителя и способствует развитию отечественной ИТ-индустрии. Во-вторых, RedOS обладает высокой степенью надежности и безопасности, благодаря чему обеспечивается защита от внешних угроз и возможность бесперебойной работы системы. Наконец, гибкость и простота настройки RedOS делают его удобным выбором для реализации сложных системных конфигураций, таких как схема "В разрыв" для IWTM.

Postfix, в роли перехватчика сообщений в системе IWTM, обеспечивает эффективный контроль и анализ трафика данных. Его гибкость и надежность делают его идеальным выбором для обработки почтового трафика. Преимущества Postfix включают простую настройку, высокую производительность и поддержку различных протоколов. Кроме того, он

обладает широкими возможностями фильтрации и конфигурации, что позволяет эффективно реагировать на угрозы безопасности и соблюдать политики безопасности данных.

Реализация макета

Перед реализацией макета сети были построены схемы физического и сетевого уровней (Рисунок 1 и 2) [4].

Все сетевые узлы были связаны между собой сетевыми адаптерами виртуальных машин. Развертывание макета производилось при помощи гипервизора VMWare Workstation Pro.

Работы по развертыванию макета сети проводились в следующем порядке:

1. Создание виртуальной машины имитации почтового сервера, на базе Windows Server 2016. Включение ntp-сервера.

2. Развертывание кластера серверов InfoWatch, на базе RedOS Murom [1]:

2.1 Создание сервера «Database». Установка шаблонов «База данных» и «Индексер». Настройка связи с ntp-сервером.

2.2 Создание сервера «TM». Установка шаблонов «Перехватчик» и «Веб-консоль».

3. Настройка конфигурационных файлов службы «Postfix» на сервере «TM». Настройка конфигурационных файлов службы iwtm.

4. Развертывание 2 АРМ пользователей локальной корпоративной сети, на базе Windows 10. Установка почтовых клиентов и настройка связи с серверами.

5. Настройка технологий, объектов защиты и политик в веб-консоли. Настройка уведомлений и доступа.

6. Проверка перехвата, блокировки, разрешения и помещения в карантин почтового трафика.

Результаты разработки

Для проверки работоспособности созданного макета необходимо запустить виртуальные машины в следующем порядке:

1) Почтовый сервер «MailServer»;

2) Сервер базы данных «Database»;

3) Сервер перехватчика «TM»;

4) АРМы пользователей сети в любом порядке.

Данный порядок следует соблюдать для избежание возможных ошибок, поскольку кластер серверов InfoWatch обращается к ntp-серверу, его следует запускать в первую очередь. Сервер перехватчика не может работать без связи с базой данных, из-за этого сервер с БД запускается вторым.

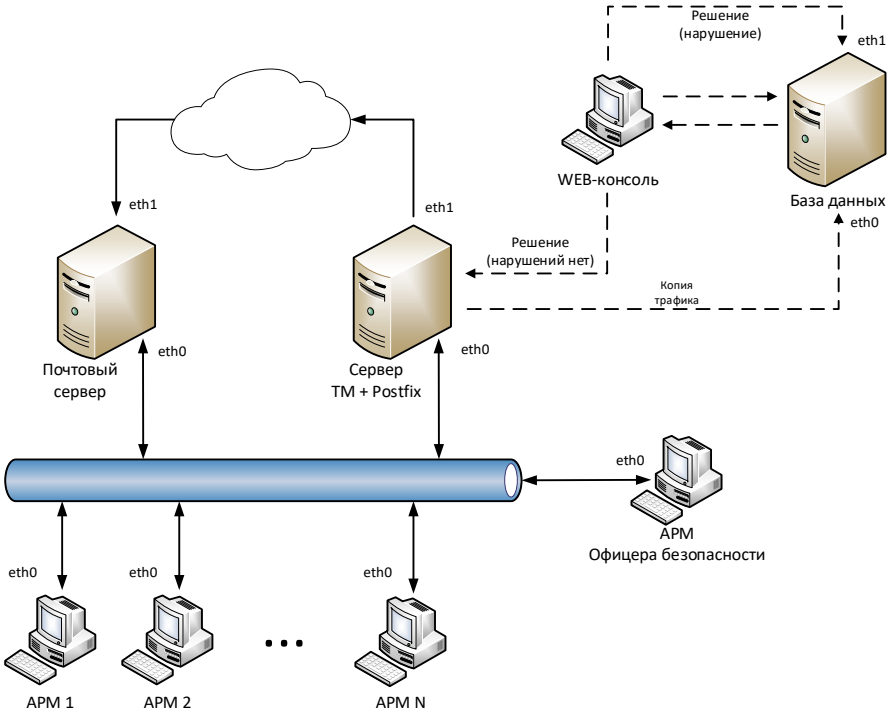

Рисунок 1. Физический уровень

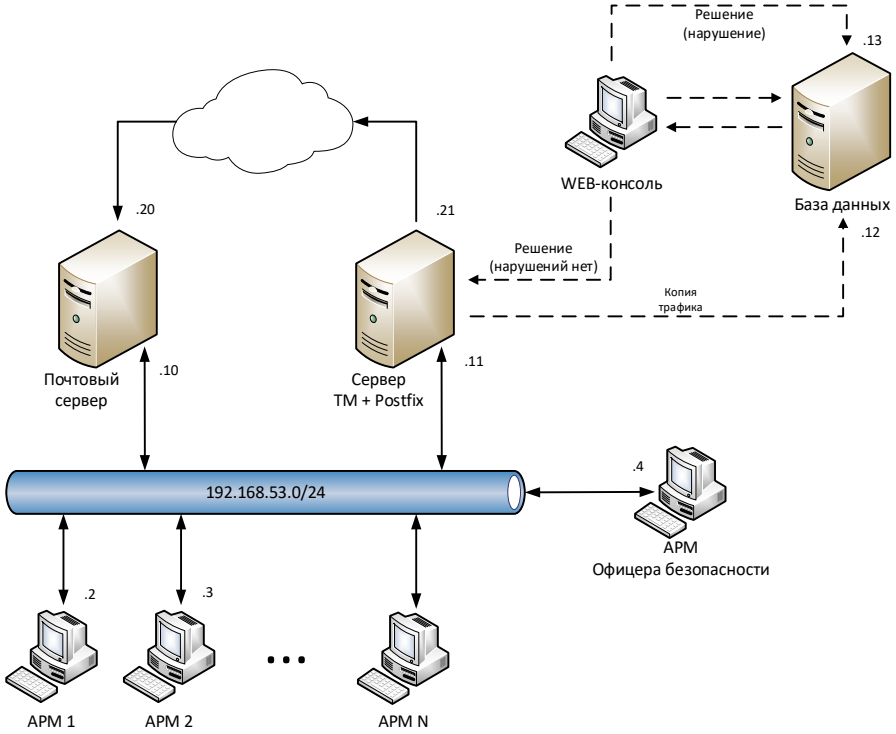

Рисунок 2. Сетевой уровень

После запуска всех виртуальных машин можно проверять работоспособность макета. Для этого зайдем на первое рабочее место сотрудника и отправим письмо, которое не попадет ни под одну из политик системы, это делается для проверки корректной доставки почтового трафика (Рисунок 3).

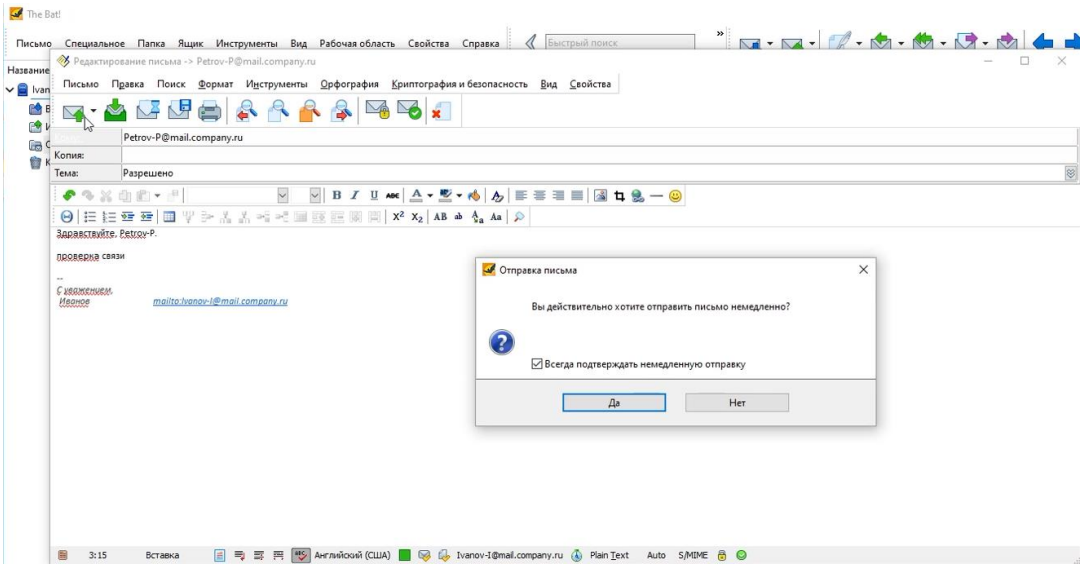

Рисунок 3. Отправка первого сообщения

Затем переходим на второе рабочее место, и проверяем наличие только что отправленного письма (Рисунок 4).

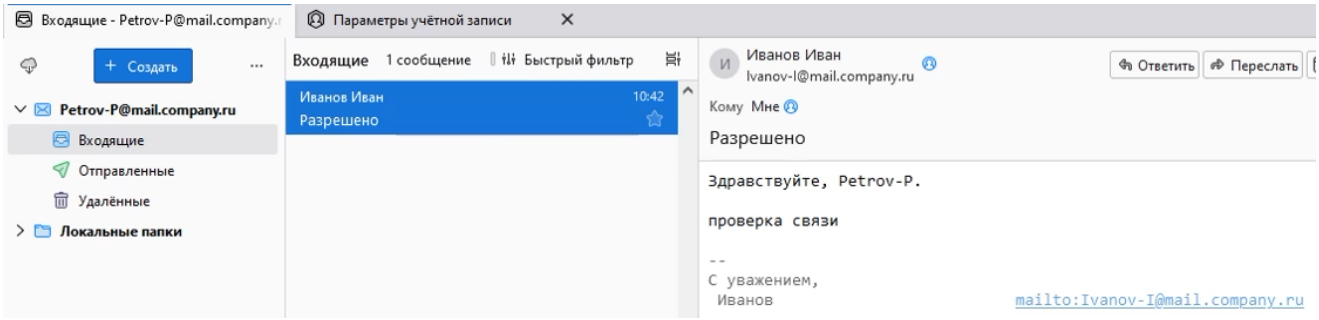

Рисунок 4. Первое письмо получено

Удостоверимся, что письмо действительно прошло через сервер перехватчика, для этого перейдем в веб-консоль, на вкладку «События» и загрузим отчет «События за последние 7 дней», там появилось событие, связанное с только что отправленным письмом (Рисунок 5).

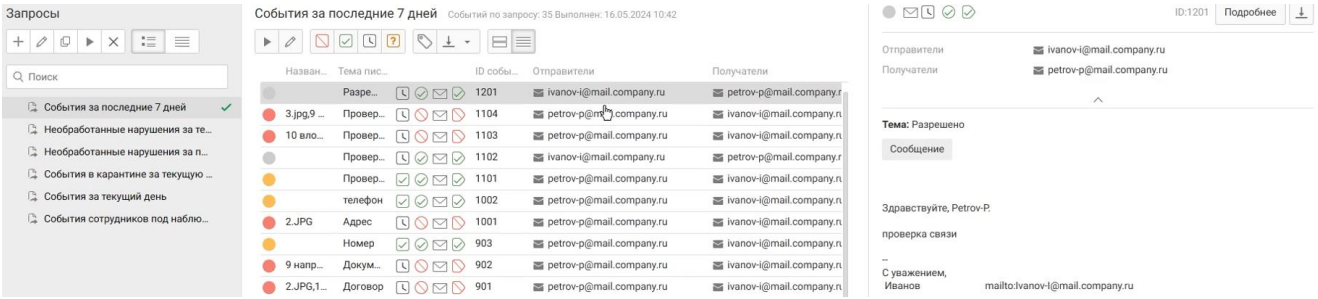

Рисунок 5. Первое письмо в веб-консоли

Следом отправим письмо содержащее персональные данные человека, загрузим в него фото паспорта, чек об оплате услуги лаборатории и документ направления на анализы, а также напишем в теле письма номер ИНН (Рисунок 6).

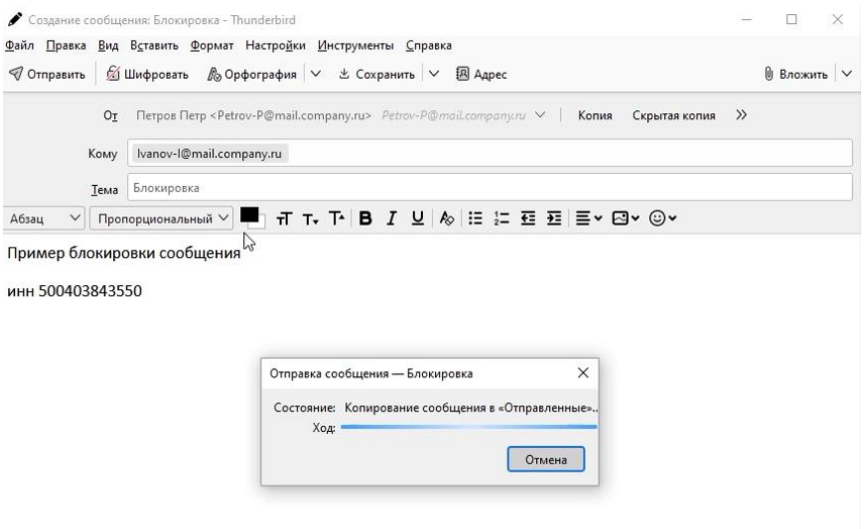

Рисунок 6. Отправка второго сообщения

Как можно увидеть, на компьютере получателя, письмо не дошло (Рисунок 7).

Перейдем на АРМ офицера безопасности и увидим сообщение о зафиксированном инциденте, созданное и отправленное системой в следствии попытки нарушения политик безопасности (Рисунок 8).

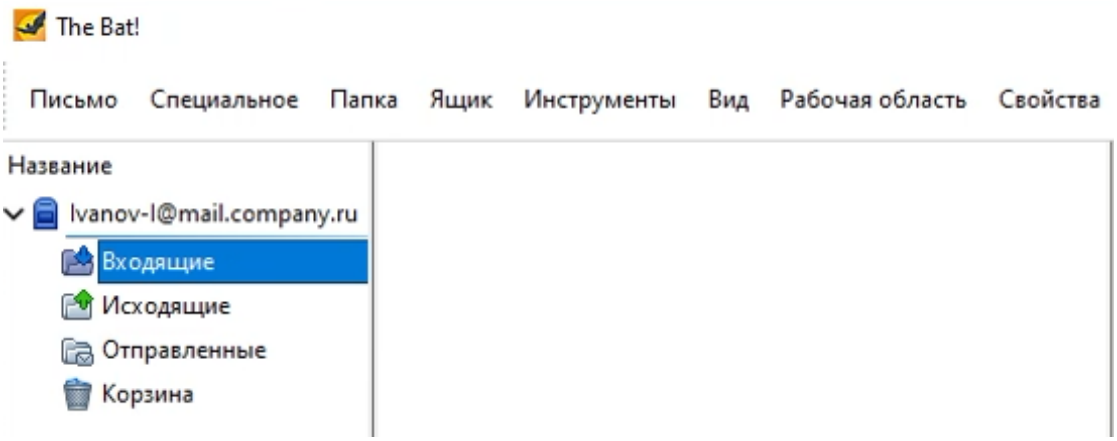

Рисунок 7. Второе письмо не дошло

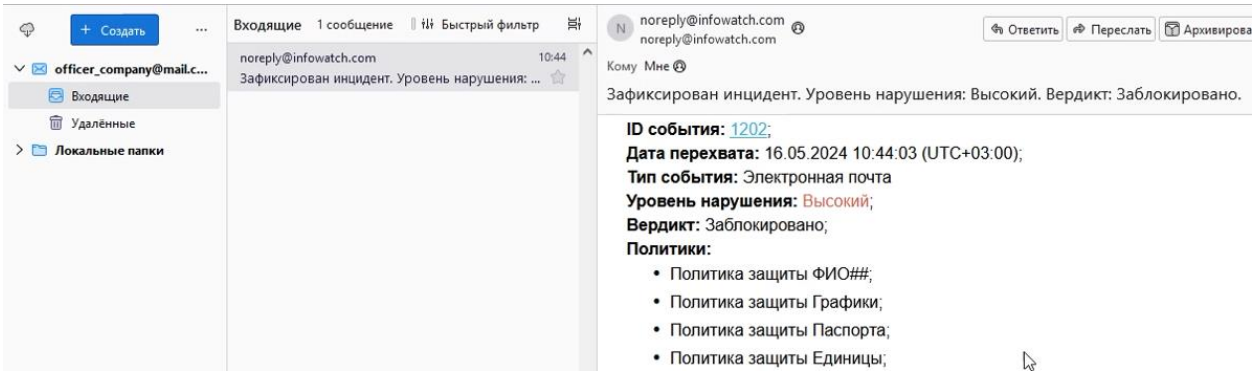

Рисунок 8. Сообщение об инциденте

Перейдем в веб-консоль и увидим зафиксированный инцидент, а также подробное описание какая часть письма и под какую политику попала (Рисунок 9).

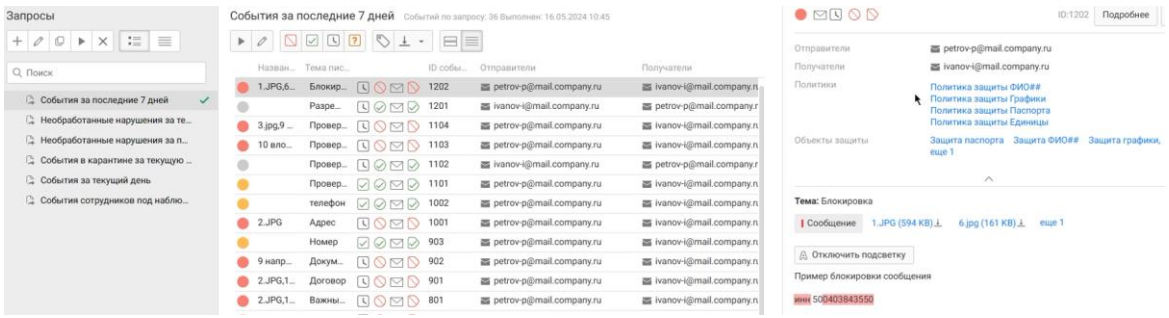

Рисунок 9. Инцидент зафиксирован в веб-консоли

С помощью последнего отправленного письма удостоверимся в работоспособности карантина. Отправим письмо, содержащее номер телефона (Рисунок 10).

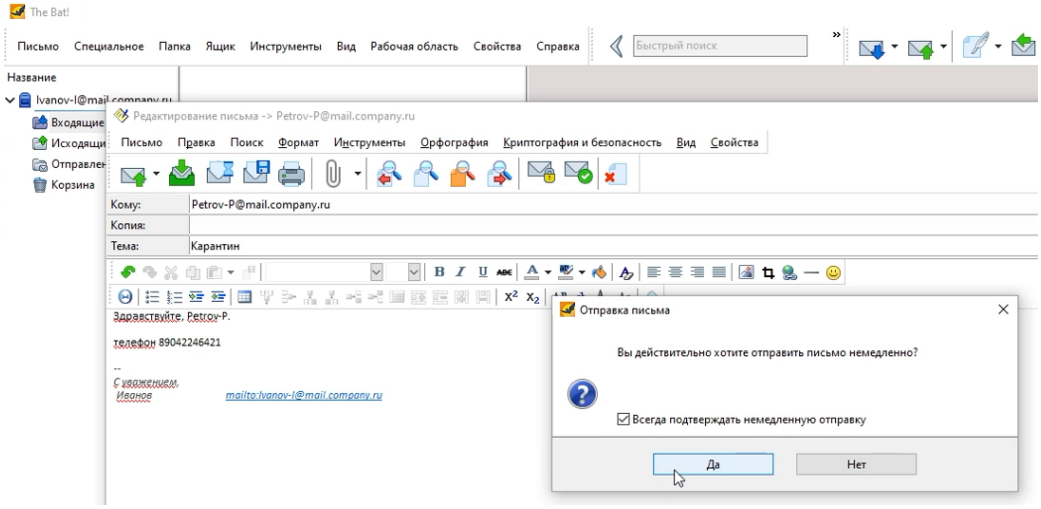

Рисунок 10. Отправка третьего сообщения

Перейдем на компьютер получателя и удостоверимся, что только что отправленное письмо до него не дошло, в папке «Входящие» находится только самое первое письмо, отправленное для проверки работоспособности почтового сервера (Рисунок 11).

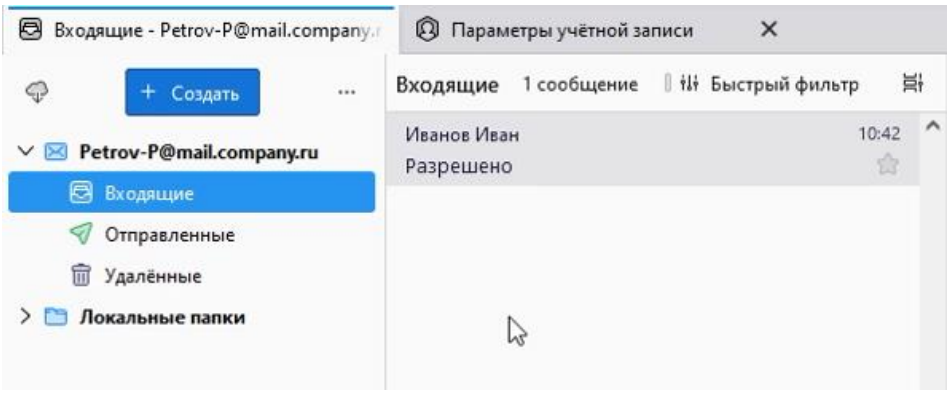

Рисунок 11. Третье сообщение не дошло

Перейдем на компьютер офицера безопасности и просмотрим письмо о новом нарушении (Рисунок 12).

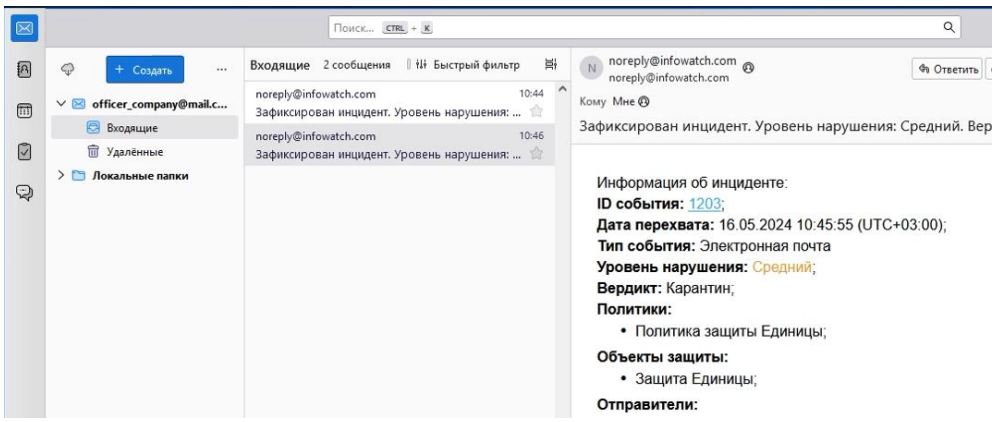

Рисунок 12. Зафиксировано нарушение

Просмотрим нарушение в веб-консоли и разрешим его. Это делается для того, чтобы проверить досылку почтовых сообщений после их нахождения в карантине (Рисунок 13).

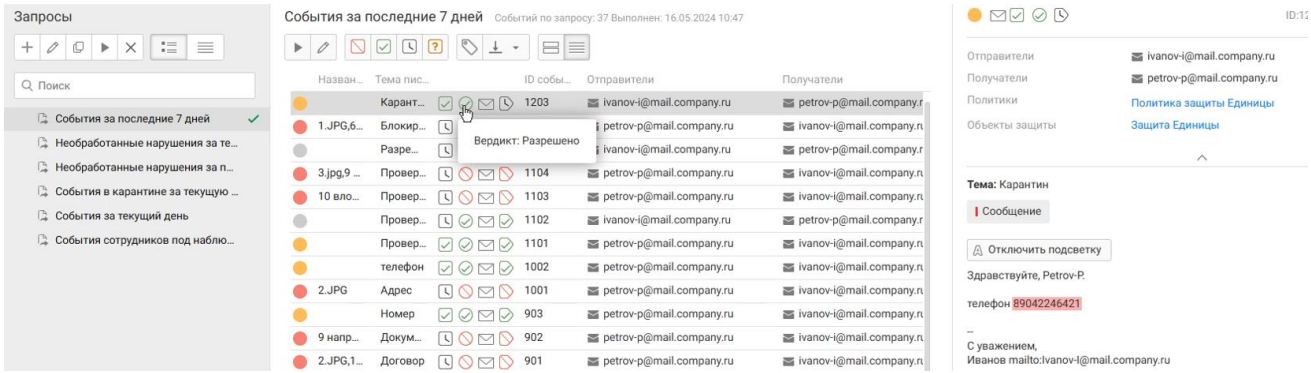

Рисунок 13. Разрешение третьего письма

Далее перейдем на АРМ получателя письма и удостоверимся в его доставке (Рисунок 14).

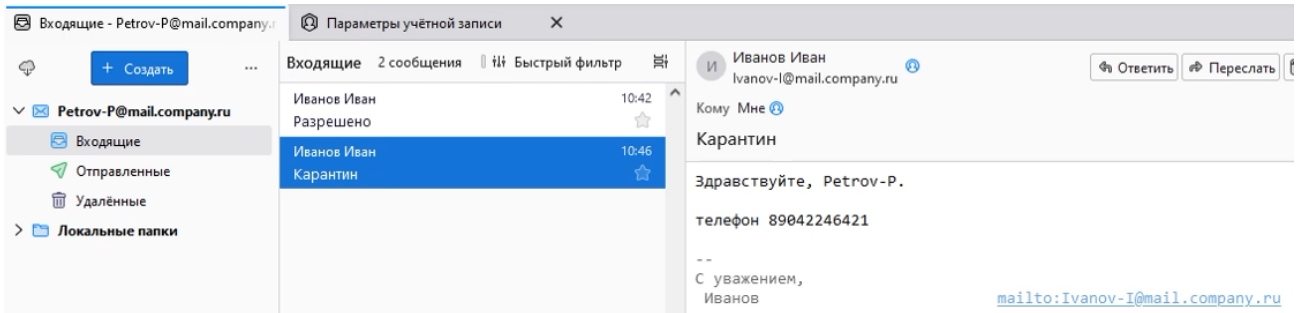

Рисунок 14. Третье письмо дошло

Заключение

В данной статье представлено краткое описание работ по разработке и проектированию макета системы защиты данных от утечки, построенного на основе продукта InfoWatch Traffic Monitor.

В рамках разработки был произведен анализ предметной области и выявлена необходимость во внедрении отечественного программно-аппаратного комплекса DLP-системы.

В ходе работ была произведена настройка программного обеспечения IWTM.

Результатом работы стал виртуальный стенд локальной сети компании. Для защиты данных от утечек был поднят кластер серверов, включающий в себя: сервер базы данных и индексера, сервер перехватчика и веб-консоли. Также была совершена проверка работоспособности макета сети путем отправки почтовых сообщений с одного почтового ящика на другой.

Список использованных источников и литературы

1. Комплект документации Traffic Monitor 7.8 для Системы, установленной на ОС Red Hat Enterprise Linux \ РЕД ОС \ Oracle Linux. – Режим доступа: https://kb.infowatch.com/display/TM78RHEL (дата обращения 22.05.2024). – Текст: электронный.

2. Официальный сайт InfoWatch. [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/ (дата обращения 22.05.2024).

3. Статья «Без права на утечку: обзор 10 российских DLP-систем». [Электронный ресурс]. – Режим доступа: https://servernews.ru/1102262 (дата обращения 22.05.2024).

4. Шабалин А. М., Калиберда Е. А. Построение виртуальной модели защиты корпоративной информации с использованием системы INFOWATCH TRAFFIC MONITOR // Вестник кибернетики. 2020. №1 (37). С. 35-42.

List of references

1. A set of documentation for Traffic Monitor 7.8 for a system installed on Red Hat Enterprise Linux \ RED OS \ Oracle Linux. – Access mode: https://kb.infowatch.com/display/TM78RHEL (accessed 05/22/2024). – Text: electronic.

2. The official InfoWatch website. [electronic resource]. – Access mode: https://www.infowatch.ru / (accessed 05/22/2024).

3. Article "Without the right to leak: an overview of 10 Russian DLP systems". [electronic resource]. – Access mode: https://servernews.ru/1102262 (accessed 05/22/2024).

4. Shabalin A.M., Kaliberda E.A. Building a virtual model of corporate information protection using the INFOWATCH TRAFFIC MONITOR SYSTEM // VK. 2020. NO.1 (37). URL: https://cyberleninka.ru/article/n/postroenie-virtualnoy-modeli-zaschity-korporativnoy-informatsii-s-ispolzovaniem-sistemy-infowatch-traffic-monitor (date of access: 05/30/2024).