Система управления телекоммуникационным трафиком на базе точек оконечного подключения

Покусов Виктор Владимирович – председатель Казахстанской ассоциации информационной безопасности; аспирант кафедры Прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России.

Голубева Татьяна Викторовна – доцент кафедры Электроники и робототехники Алматинского университета энергетики и связи.

Аннотация: В статье рассматривается задача повышения безопасности телекоммуникационной сети. Предлагается схема анализа и контроля сетевого трафика на базе устройств в точках оконечного подключения. Приводятся базовые сценарии использования схемы в интересах информационной безопасности. Обосновываются некоторые аспекты возможности реализации предложенной схемы и ее аппаратной составляющей.

Ключевые слова: Телекоммуникационная система, управление сетью, информационная безопасность.

Введение

Стремительное развитие сетевых технологий неизменно ведет к вовлечению в информационный обмен еще большего количества телекоммуникационных устройств, даже в рамках одной организации. При этом, несмотря на очевидные преимущества такого обмена, существуют и определенные недостатки, связанные с информационной безопасностью, циркулирующей в сети информации. Так, недостаточный контроль за исходящими за периметр организации сетевыми потоками может приводить к нарушению конфиденциальности информации, бесконтрольное подключение устройств внутри организации – к нарушению целостности, а открытость сети организации в условиях проведения DoS-атак извне – к нарушению доступности. Одна из причин этого заключается в недостаточном контроле телекоммуникационного трафика современными средствами, а точнее отсутствие полноценного контроля за ним. Существующие же решения, такие как DLP-системы, антивирусное обеспечение или маршрутизирующее оборудование часто не работают в комплексе, сами подвержены атакам и не способны

противодействовать угрозам на более низком уровне, чем они сами. При этом, все существующие средства практически не подходят для реализации экстренных сценариев защиты от атак, таких, как мгновенное отключение всех сетевых устройств и/или обеспечение абсолютно доверенного маршрута для сверхконфиденциальной информации в организации. Таким образом, задача управления телекоммуникационным трафиком является крайне актуальной, а ее гипотетическое решение в виде целой системы и будет рассмотрено в статье.

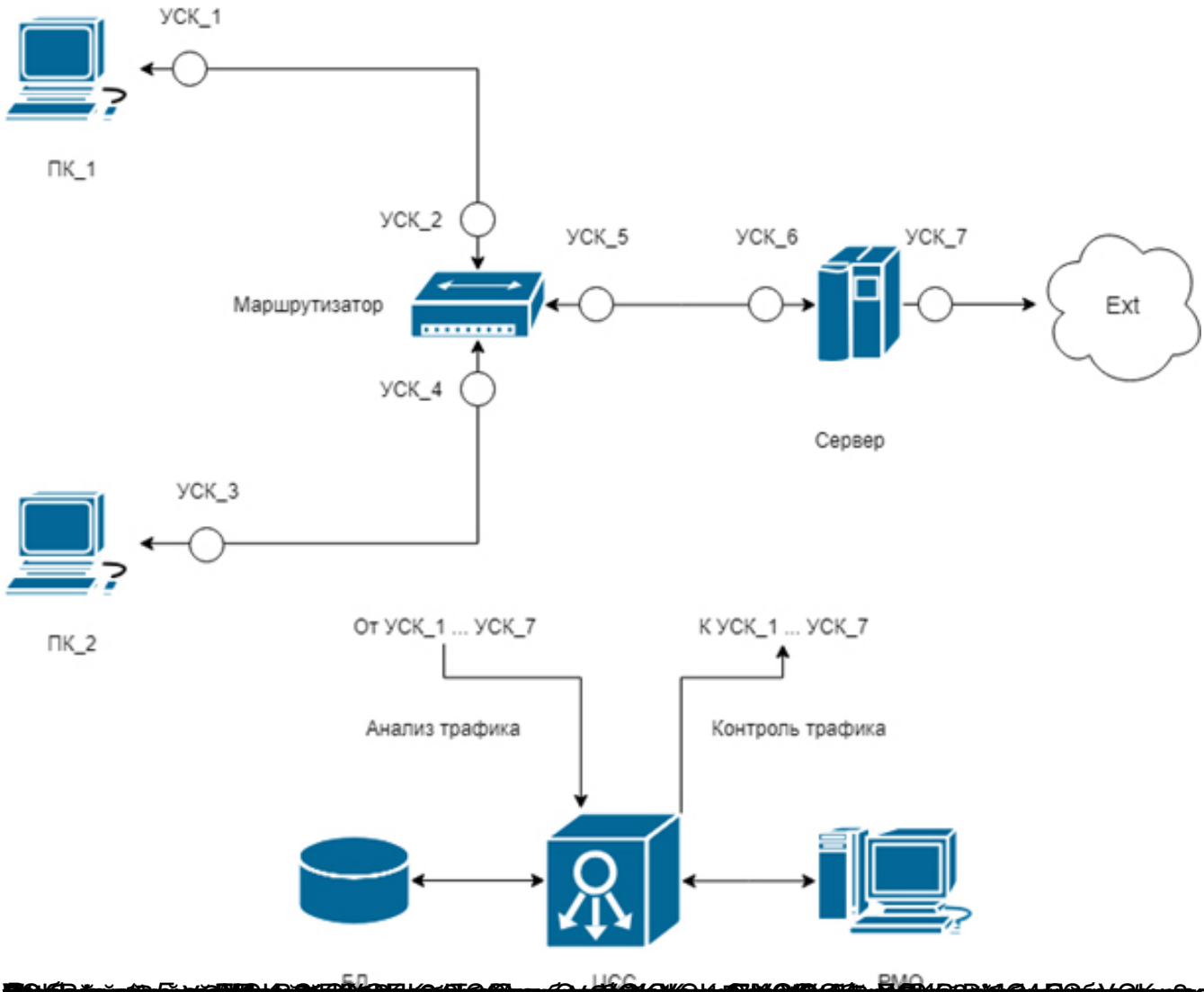
Схема системы

Опишем требования к гипотетической системе управления телекоммуникационным трафиком (далее – Системы) в интересах решения поставленной задачи. Во-первых, Система должна отслеживать все сетевые пакеты, и в особенности те, которые идут за рамки организации, где она функционирует; при этом должна иметься возможность их контроля. Во-вторых, Система должна определять факт появления в сети новых устройств, позволяя блокировать получение и передачу информации в случае несанкционированного подключения. В-третьих, в Системе должна иметься возможность отключения некоторых сетевых каналов; например, всех во внешнюю сеть или кроме выделенного пути.

Исходя из описанных требований, в качестве подходящего решения может быть выбрана следующая схема работы системы.

Принцип работы Системы основан на внедрение в сетевую инфраструктуру специальных сетевых устройств, контролирующих проходящий через них трафик – устройств сетевого контроля (УСК). При этом местами внедрения целесообразно использовать точки оконечного подключения всех рабочих устройств сети – сетевые разъемы для персональных компьютеров, точки присоединения маршрутизирующего оборудования, все выходы во внешнюю сеть, точки подсоединения IP-телефонии и т.п.

Пример такой Системы показан на Рисунке 1.



Возможности реализации

Анализ современного уровня развития науки и техники позволяет обоснованно утверждать о возможности реализации УСК. Также, в случае физически скрытых устройств, задача их питания решается использованием питания сетевых кабелей или встроенным аккумулятором. Для снижения нагрузки возможен перенос функционала УСК на ЦСС.

Заключение

Предложенная система управления телекоммуникационным трафиком на базе точек оконечного подключения представляет альтернативное решение обеспечения информационной безопасности для сетей организации. При этом оно гипотетически обладает существенными достоинствами, включающими высокую скорость изменения логической сетевой инфраструктуры, скрытность, контроль и управление сетевым

трафиком для всех устройств, независимо от их программного и аппаратного обеспечения. Для доказательства всех указанных преимуществ и проверки работоспособности сценариев необходима разработка соответствующего прототипа, включающего как сами устройства сетевого контроля, так и все программное обеспечение. Оценка эффективности системы может быть осуществлена на базе научно-исследовательской лаборатории (например, для исследования защиты от инсайдерских атак [4]). Практическим вопросам системы, а также исследованию других ее применений и будут посвящены дальнейшие работы авторов.

Список литературы

1. Буйневич М.В., Израилов К.Е., Покусов В.В. Способ визуализации модулей системы обеспечения информационной безопасности // Научно-аналитический журнал Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России. 2018. № 3. С. 81-91.
2. Буйневич М.В., Покусов В.В., Израилов К.Е. Гипотетическая схема информационно-технического взаимодействия модулей системы обеспечения информационной безопасности // III Международная научно-практическая конференция «Информатика и прикладная математика». 2018. С. 179-192.
3. Буйневич М.В., Тиамийу О.А. Программная архитектура системы управления доверенной маршрутизацией в глобальных телекоммуникационных сетях // Информатизация и связь. 2014. № 3. С. 40-43.
4. Дешевых Е.А., Конюхов В.М., Крылов К.Ю., Ушаков И.А. Исследование методов защиты от инсайдерских атак // Актуальные проблемы инфотелекоммуникаций в науке и образовании: сборник научных статей IV Международной научно-технической и научно-методической конференции. 2015. С. 310-313.
5. Израилов К.Е., Покусов В.В. Актуальные вопросы взаимодействия элементов комплексных систем защиты информации // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2017): сборник научных статей VI Международной научно-технической и научно-методической конференции. 2017. С. 255-260.
6. Израилов К.Е., Покусов В.В., Столярова Е.С. Информационные объекты в системе обеспечения информационной безопасности // Теоретические и прикладные вопросы комплексной безопасности: материалы I Международной научно-практической конференции. 2018. С 166-169.
7. Красов А.В., Сахаров Д.В., Ушаков И.А., Лосин Е.П. Обеспечение безопасности передачи Multicast-трафика в IP-сетях // Защита информации. Инсайд. 2017. № 3 (75). С. 34-42.
8. Пальчевский Е.В. Автоматизированная система блокировки протоколов для защиты доступности информации // Вектор развития современной науки: материалы международной (заочной) научно-практической конференции. 2016. С. 33-36.
9. Филиппов М.В., Рязанова Н.Ю., Рязанцев Б.И. Метод перехвата исходящих и входящих сетевых пакетов // Машиностроение и компьютерные технологии. 2017. № 12.

С. 45-56.

{social}