АНАЛИЗ ОСНОВНЫХ УЯЗВИМОСТЕЙ И УГРОЗ МУЛЬТИСЕРВИСНОЙ СЕТИ НА НИЖНИХ УРОВНЯХ МОДЕЛИ OSI

Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь

С. Н. Беликов

В. А. Богуш − д. ф.-м. н., профессор

Рассматривается особенность проектирования и эксплуатации современных мультисервисных сетей – обеспечение их информационной безопасности. Это обязывает к разработке соответствующей политики безопасности, для выработки и проведения которой необходимо провести анализ основных уязвимостей и угроз на сетевых уровнях модели OSI

В современных телекоммуникациях широкое применение нашла эталонная модель взаимодействия открытых систем OSI. Она предусматривает разделение процесса передачи данных на семь уровней: физический, канальный, сетевой, транспортный, сеансовый, представления и прикладной. Классификация элементов систем на основе данной модели упрощает рассмотрение вопрос взаимодействий и логических построений.

На рисунке 1 представлена семиуровневая модель OSI для мультисервисных сетей:

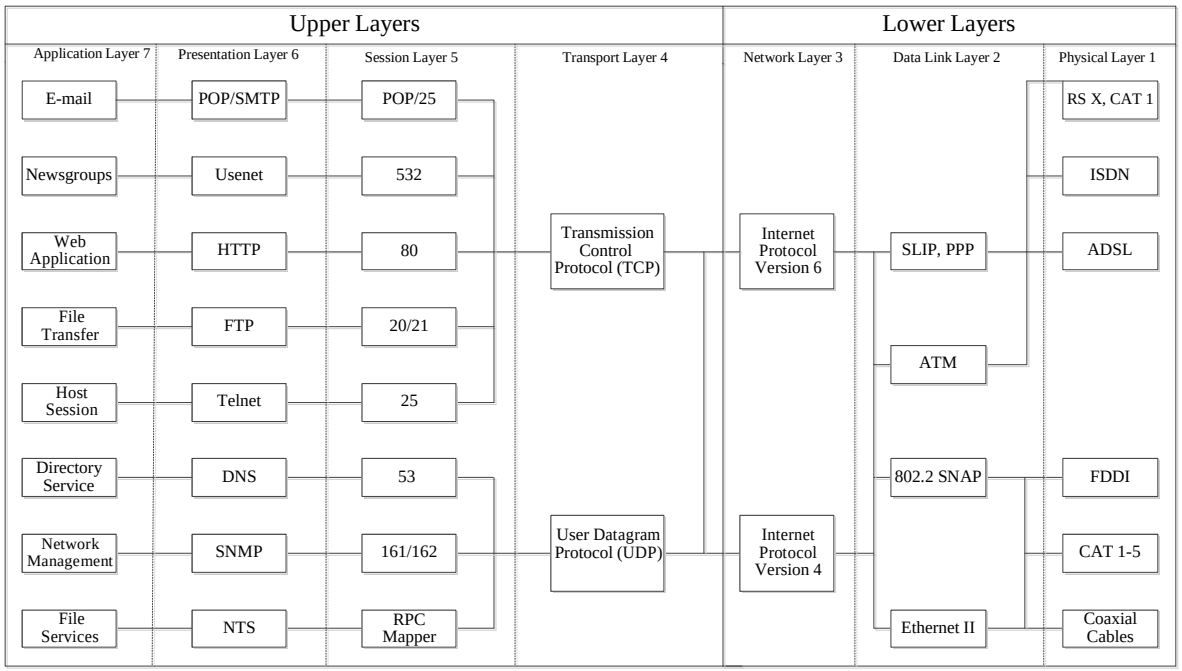

Рис. 1 – Семиуровневая модель OSI для мультисервисных сетей

Применение данной модели при разработке политики безопасности является эффективным решением, так как позволяет в полной мере провести анализ потенциальных угроз и существующих уязвимостей для всей сети в целом. Особое внимание уделяется анализу нижних уровней модели (физическому, канальному, сетевому), так как именно они отвечают за реализацию аппаратной части мультисервисной сети.

Физический уровень осуществляет физическое управление. Он определяет среду доставки сигналов и имеет дело с физическими, электрическими, функциональными и процедурными характеристиками для установления, поддержания и разрыва физического соединения на уровне битового потока. В таблице 1 представлен анализ уязвимостей и потенциальных угроз на данном уровне.

Канальный уровень относится к пересылке фреймов данных по физическому звену связи и отвечает за управление каналом. При этом необходима процедура управления физическим звеном связи, которая специфицирует головное и хвостовое обрамление передаваемых блоков и определяет протокол обмена этими блоками. На этом уровне присутствуют сообщения об ошибках, топология сети и команды управления прохождением пакетов, а также контроль Media Access Control (MAC) адресов портов физического звена, локализованный на уровне данного физического звена. В таблице 2 представлен анализ уязвимостей и потенциальных угроз на данном уровне.

Таблица 1 – Анализ уязвимостей и угроз на физическом уровне

Уязвимость	Угроза
– неадекватная физическая защита устройств и среды передачи; – передача незашифрованных данных по среде передачи; – создание техническими средствами побочных электромагнитных излучений.	– перехват, анализ и искажение передаваемого по линиям связи трафика путем применения активных и пассивных методов съема.

Таблица 2 – Анализ уязвимостей и угроз на канальном уровне

Уязвимость	Угроза
– большие эксплуатационные и накладные расходы при ведении баз данных MAC-адресов пользователей из-за использования различных терминалов; – передача трафика мультисервисной сети в открытом виде; – отсутствие механизма аутентификации или цифровой подписи сообщений.	Подмена трафика: – способность получать сообщение, маскируясь под легитимное место; – способность маскироваться под отправителя и посылать сообщения.

Сетевой уровень относится к виртуальной или логической цепи. Эта цепь не существует физически, но благодаря ей вышележащие уровни могут взаимодействовать друг с другом, так как она существует. В сетях передачи данных на этом уровне используются IP-пакеты, проводится логическая адресация всех узлов сети и определяются маршруты следования мультисервисного трафика. В таблице 3 представлен анализ уязвимостей и угроз на данном уровне.

Таблица 3 – Анализ уязвимостей и угроз на сетевом уровне

Уязвимость	Угроза
– возможность удаленного управления устройствами коммутации и маршрутизации трафика; – возможность получения физического доступа к сетевым устройствам	– внедрение ложного объекта путем навязывания ложного маршрута; – отключение и вывод из строя коммутационных и маршрутизирующих устройств; – дезорганизация функционирования системы путем реализаций атак «отказ в обслуживании».

Таким образом, был проведен анализ существующих уязвимостей и потенциальных угроз мультисервисной сети на нижних уровнях модели OSI, что позволяет оценить риски для безопасности информационных процессов внутри сети и разработать соответствующие меры.

Список использованных источников

1. Бакланов, И. Г. NGN : принципы построения и организации / И. Г. Бакланов ; под ред. Ю. Н. Чернышова. – Москва : Эко-Трендз, 2008. – 400 с.
2. Гургенидзе, А. Т. Мультисервисные сети и услуги широкополосного доступа/ А. Т. Гургенидзе, В. И. Кореш. – СПб. : Наука и техника, 2003. – 400 с.
3. Денисова, Т. Б. Мультисервисные АТМ-сети / Т. Б. Денисова [и др.]. – Москва: Эко-Трендз, 2005. – 317 с.