УДК 004.056

ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ В ПУНКТАХ КОЛЛЕКТИВНОГО ДОСТУПА К УСЛУГАМ СВЯЗИ

Ажмухамедов И.М.[1], Зеленский С.В.[2]

[1]ФБГОУ ВПО Астраханский государственный технический университет, Астрахань, Россия (414056, г. Астрахань, ул. Татищева, 16), aim_agtu@mail.ru
[2]ФБГОУ ВПО Астраханский государственный университет, Астрахань, Россия (414056, г. Астрахань, ул. Татищева, 20А), spacetest@mail.ru

В последнее время, с одной стороны, наблюдается резкий рост объёма предоставления услуг связи в пунктах коллективного доступа (включая выход в интернет). С другой стороны, ужесточены требования законодательства по идентификации пользователей и используемого ими оконечного оборудования при предоставлении такого рода услуг. Типовые решения, позволяющие реализовать данные требования, отсутствуют. Поэтому целью работы стала разработка методики идентификации пользователей и используемого ими оконечного оборудования в пунктах коллективного доступа. Для этого была предложена общая схема идентификации, произведен подбор необходимых программно-аппаратных средств, разработаны и внедрены организационные меры, создающие условия безопасной эксплуатации предложенного технического решения. Предложенная методика прошла успешную апробацию в одном из вузов г. Астрахани и может быть легко адаптирована для различных организаций.

Ключевые слова: идентификация, услуги связи, пункт коллективного доступа.

IDENTIFY THE USER IN COMMUNITY ACCESS POINTS TO COMMUNICATION SERVICES

Azhmuhamedov I.M.[1], Zelensky S.V.[2]

[1]Astrakhan State Technical University, Astrakhan, Russia, (414056, Astrakhan, Tatischeva st., 16), aim_agtu@mail.ru
[2]Astrakhan State University, Astrakhan, Russia, (414056, Astrakhan, Tatischeva st., 20A), spacetest@mail.ru

Recently, on the one hand, there has been a sharp increase in the volume of communication services in the access points (including internet access). On the other hand, stricter legal requirements for the identification of users and their terminal equipment used in the provision of such services. Typical solutions to implement these requirements are lacking. Therefore, the aim of the work was to develop a technique used to identify users and their terminal equipment in the access points. For this was a general scheme for the identification, selection is made the necessary software and hardware are developed and implemented arrangements that create conditions for the safe operation of the proposed technical solutions. The proposed method has been successfully tested in one of the universities of Astrakhan and can be easily adapted for various organizations.

Keywords: identification, communication services, community access points.

В связи с резким ростом объёма предоставления услуг связи (включая выход в интернет) в пунктах коллективного доступа, сложность поиска злоумышленника и сбора доказательной базы в случае совершения преступлений с использованием компьютерных технологий многократно возрастает.

С июля 2014 года было принято несколько законодательных актов, обязывающих операторов связи осуществлять идентификацию пользователей и используемого ими оконечного оборудования в пунктах коллективного доступа (ПКД) [3,4,5,7]. Это важный шаг со стороны государства для поддержания и исполнения своих правовых функций. Однако готовых решений для реализации вводимых требований на данный момент не существует.

Постановка задачи

В связи с этим возникает необходимость разработки методики идентификации пользователей в пунктах коллективного доступа.

Решение задачи

В результате анализа законодательных актов [3,4,5,7] были выявлены основные требования, предъявляемые к операторам связи при оказании услуг в пунктах коллективного доступа:

- оказание услуг связи по передаче данных и предоставлению доступа к сети должно осуществляться только после идентификации пользователей;
- идентификация должна осуществляться путем установления фамилии, имени, отчества (при наличии) или достоверного установления абонентского номера, назначенного пользователю в соответствии с договором об оказании услуг подвижной радиотелефонной связи;
- идентификация должна обеспечивать достоверное установление указанных сведений;
- хранение сведений о пользователях, которым были оказаны услуги связи, а также об объеме и времени оказания им услуг связи должны храниться оператором универсального обслуживания не менее 6 месяцев.

Исходя из этого, разрабатываемая методика идентификации должна обеспечивать высокий уровень сервисов информационной безопасности (ИБ):

- доступность (обеспечение доступа к полученной информации по мере необходимости);
- целостность (обеспечение достоверности и полноты информации);
- конфиденциальность (обеспечение защиты от несанкционированного доступа);

Кроме того, необходимо учесть требования по экономичности и эргономичности предлагаемых решений.

При этом создание методики идентификации предусматривает решение двух задач:

1. Подбор программно-аппаратных средств для идентификации пользователя и хранения информации;
2. Разработку организационных регламентов, создающих условия безопасной эксплуатации предложенного технического решения.

Общая схема использования программно-аппаратных средств

Предлагаемый алгоритм идентификации пользователей в пунктах коллективного доступа представлен блок-схемой на рисунке 1. Алгоритм реализует:

1. Проверку доступности системы идентификации, а также её самодиагностику с помощью скриптов, выполняемых на устройстве оконечного оборудования оператора связи для проверки корректности работы системы идентификации пользователей.

2. Предоставление пользователю вариантов идентификации, приём данных и проверку их достоверности, которые осуществляются либо путем соответствующего конфигурирования оконечного оборудования оператора, либо с помощью использования дополнительного оборудования. В случае использования дополнительного оборудования необходимо обеспечить защищённый канал передачи данных между ним, пользователем и оконечным оборудованием оператора.

3. Идентификацию активных клиентов и перенаправление их трафика с оконечного оборудования оператора связи. Реализуется путем соответствующего конфигурирования оконечного оборудования оператора. Выполняется один раз при введении оборудования в эксплуатацию. При этом оконечное оборудование должно поддерживать функции распознавания идентифицированных пользователей и перенаправления данных о трафике.

4. Извлечение и хранение идентификационных данных пользователей. Применяется программное решение, выполняющее: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение данных, необходимых для идентификации пользователей. Реализуется средствами самого оконечного оборудования, либо путем использования дополнительного оборудования. В случае использования дополнительного оборудования необходимо обеспечить защищённый канал передачи данных между ним и оконечным оборудованием.

5. Извлечение и хранение данных о трафике идентифицированных пользователей. Осуществляется с помощью программного решения, позволяющего извлекать данные о трафике и сохранять их либо на оконечном оборудовании оператора, либо на дополнительном предварительно настроенном внешнем оборудовании. В случае использования дополнительного оборудования необходимо обеспечить защищённый канал передачи данных между ним и оборудованием оператора.

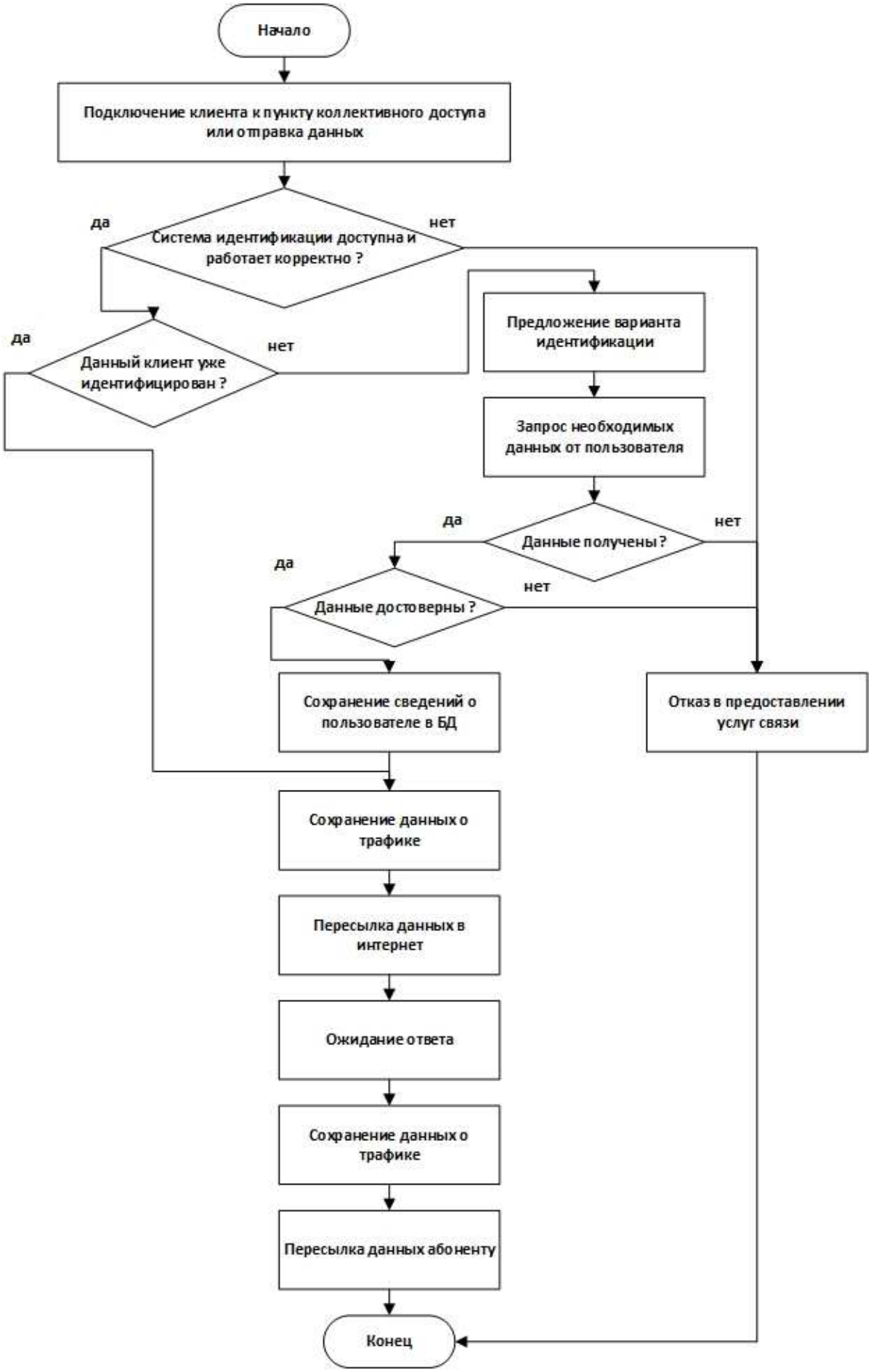

Рис.1. Алгоритм идентификации пользователей

Пример реализации предлагаемого решения

Рассмотрим пример реализации схемы идентификации пользователей в пунктах коллективного доступа одного из вузов г. Астрахани. Общая топология сети высшего учебного заведения, в ведении которого находится пункт коллективного доступа, и оператора связи *представлена на рисунке 2.*

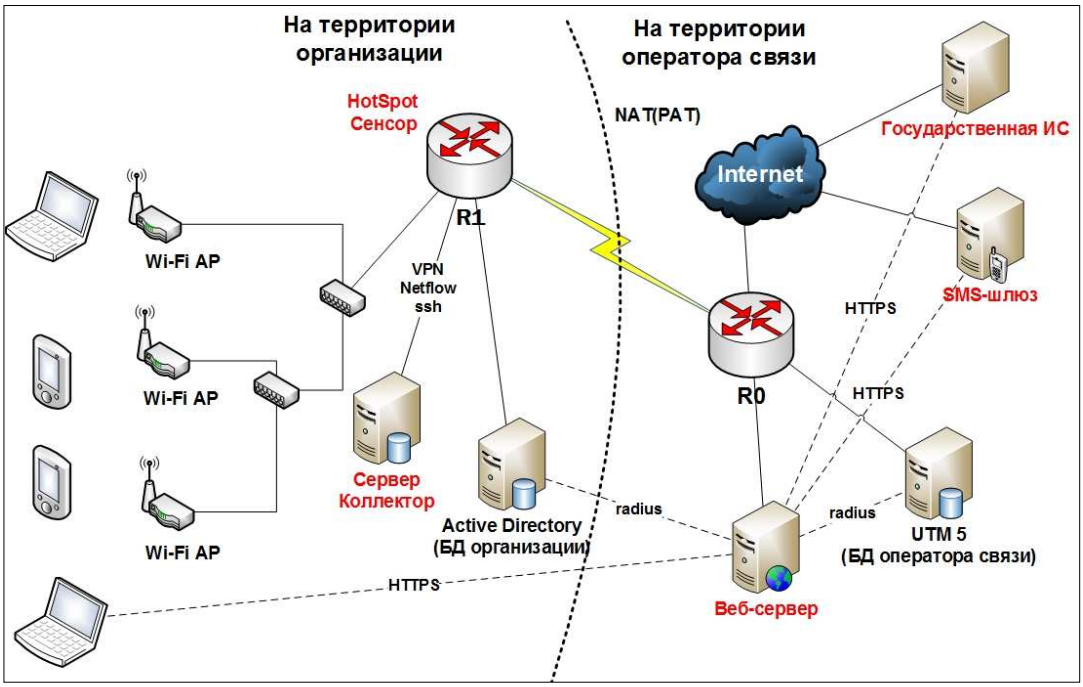

Рис. 2. Общая топология сети

В рассматриваемом примере в качестве оконечного оборудования (R1) был выбран программный маршрутизатор с операционной системой «RouterOS» фирмы «MikroTik». Данный маршрутизатор обладает широкими возможностями, включая исполнение пользовательских скриптов, что позволило осуществлять работу по предоставлению услуг связи только при проверке доступности системы идентификации и успешного результата самодиагностики [1].

Устройство R1 было запущено в режиме «HotSpot». Данный режим позволяет идентифицировать пользователей, как в самом устройстве, так и с помощью перенаправления запроса на внешние ресурсы. Маршрутизатор также дает возможность считывать данные о трафике с помощью протоколов NetFlow версий 5 и 9 [6].

Для предоставления пользователю возможности выбора вариантов идентификации используется внешний сервер с операционной системой FreeBSD 9.2 и установленным веб-сервером Apache 2.4. С помощью языка программирования общего назначения PHP 5.3 были реализованы скрипты, позволяющие пользователю выбрать в веб-форме на сайте следующие варианты идентификации:

- с помощью достоверного установления абонентского номера, назначенного пользователю в соответствии с договором об оказании услуг подвижной радиотелефонной

связи, заключенным с оператором связи посредством отправки SMS с уникальным ключом на указанный номер;

- с помощью базы данных оператора связи;
- с помощью базы данных организации;
- с помощью государственной информационной системы «Единая система идентификации и аутентификации в инфраструктуре, обеспечивающей информационно-технологическое взаимодействие информационных систем, используемых для предоставления государственных и муниципальных услуг в электронной форме».

Перечень вариантов идентификации может быть легко расширен.

Обработка полученных от пользователя данных и проверка их достоверности также была реализована скриптами на PHP 5.3. При этом взаимодействие веб-сервера с пользователем, sms-шлюзом и государственной информационной системой, осуществляется через защищённый протокол HTTPS, а взаимодействие веб-сервера с базами данных организации и оператора связи через RADIUS-протокол.

В качестве способа обработки данных о трафике был задействован протокол NetFlow 9, как один из самых популярных протоколов с поддержкой современных технологий (в частности, с поддержкой IPv6).

NetFlow – это проприетарный открытый протокол, разработанный Cisco для мониторинга трафика в сети. Netflow предоставляет возможность анализа сетевого трафика на уровне сеансов, делая запись о каждой транзакции TCP/IP. Для сбора информации о трафике по данному протоколу требуются следующие компоненты:

- сенсор (отправляет данные о транзакциях TCP/IP на коллектор);
- коллектор (собирает получаемые от сенсора данные и помещает их в хранилище).

На маршрутизаторе R1 был установлен сенсор. А в качестве коллектора используется внешний сервер с операционной системой FreeBSD 9.2 и установленными программами для обработки NetFlow протокола: nfdump и nfsen. Данные программы являются одними из самых стабильных среди открытого программного обеспечения с поддержкой IPv6 [2].

Взаимодействие маршрутизатора с сервером-коллектором осуществляется через защищённый VPN-канал, который поддерживается операционной системой маршрутизатора и коллектора.

Дополнительно на сервере производится обработка сведений об идентификации клиентского оборудования посредством определения уникального идентификатора оборудования сетей передачи данных и сохраняется информация о соответствии IP и MAC адресов с учётом времени выдачи IP.

Извлечение информации для последующего хранения производится скриптом PHP с роутера R1 через ssh-канал и заносится в базу данных MySQL, расположенную на сервере. При сборе сведений для обработки данных о трафике и клиентском оборудовании сетевые адреса преобразуются по механизму NAT. Сведения об идентификации пользователей также хранятся в базе данных MYSQL на сервере-коллекторе.

Примеры данных, собранных в пункте коллективного доступа

Пример собранных данных о транзакциях TCP/IP на коллекторе NetFlow приведен в таблице 1. Данные об идентификации клиентского оборудования приведены в таблице 2, данные об идентификации клиентов – в таблице 3.

Таблица 1

Данные о транзакциях TCP/IP на коллекторе NetFlow

Date first seen	Durtaion Proto	Src IP Addr:Port	Dst IP Addr:Port	Packets	Bytes	Flows
2014-10-25 01:34:13.890	2.400 UDP	192.168.1.1	8.123.34.23	7	458	1
2014-10-25 01:35:09.080	2.200 UDP	fe80::a..1a:22b6	ff02::1	3	274	1
2014-10-25 01:35:09.080	1.200 UDP	192.168.1.28	192.168.1.82	8	987	1

Таблица 2

Данные об идентификации клиентского оборудования

IP-address	MAC-address	Time INIT
192.168.1.1	D4:5C:61:66:56:B3	2014-10-25 01:00:30.260
fe80::a..1a:22b6	48:5D:61:68:16:B3	2014-10-25 01:13:50.460
192.168.1.28	D4:5C:61:58:58:A1	2014-10-25 01:15:40.560

Таблица 3

Данные об идентификации клиентов

Ф.И.О./Номер телефона	IP	Time INIT
Снежин Игорь Викторович	192.168.1.1	2014-10-25 01:00:10.260
79275774488	fe80::a..1a:22b6	2014-10-25 01:13:30.460
boy88test	192.168.1.28	2014-10-25 01:15:20.560

На основании совокупности таких данных можно получить исчерпывающую информацию о действиях пользователя, осуществленных через пункт коллективного доступа.

Перечень организационных мер

Для безопасного функционирования предложенного технического решения были предприняты следующие организационные меры:

- разработана и введена в действие инструкция по эксплуатации системы идентификации; назначен ответственный по контролю за соблюдение данной инструкции;
- реализована физическая защита сервера идентификации, путём расположения его в контролируемой зоне организации, в ведении которой находится ПКД.

Заключение

Предложенная методика идентификации пользователей в пунктах коллективного доступа позволяет выполнить основные требования законодательства и может быть легко адаптирована для различных организаций.

Список литературы

1. Документация сетевой операционной системы RouterOS http://wiki.mikrotik.com/wiki/Manual:TOC (дата обращения: 25.04.2015).
2. Официальный сайт Nfsen (Netflow Sensor) http://nfsen.sourceforge.net/ (дата обращения: 25.04.2015).
3. Письмо Министерства связи и массовых коммуникаций Российской Федерации от 19 ноября 2014 г. № ДА-П12-20690.
4. Постановление Правительства РФ от 12.08.2014 N 801 «О внесении изменений в некоторые акты Правительства Российской Федерации».
5. Постановление Правительства РФ от 31.07.2014 № 758 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей».
6. Разбор пакетов NetFlow http://habrahabr.ru/post/187820/ (дата обращения: 25.04.2015).
7. Разъяснения Министерства связи и массовых коммуникаций Российской Федерации от 8 августа 2014 года http://old.minsvyaz.ru/ru/news/ printable.php?print=1&id_4=44762 (дата обращения: 25.04.2015).

Рецензенты:

Лихтер А.М., д.т.н., профессор, зав. кафедрой «Общая физика» ФГБОУ ВПО АГУ, г. Астрахань;

Попов Г.А., д.т.н., профессор, заведующий кафедрой «Информационная безопасность», ФГБОУ ВПО АГТУ, г. Астрахань.