ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.05653
DOI: 10.21822/2073-6185-2022-49-3-52-60 Оригинальная статья /Original Paper

Аппаратно-программные методы защиты ресурсов информационной системы персональных данных от несанкционированного доступа путем «сниффинг-атак»

А.Р. Газизов
Донской государственный технический университет,
344002, г. Ростов-на-Дону, пл. Гагарина, 1, Россия

Резюме. Цель. В статье рассматриваются аппаратно-программные методы защиты ресурсов информационной системы персональных данных от несанкционированного доступа путем «сниффинг-атак», суть которого заключается в перехвате данных, которые доставляются в рамках наблюдаемой системы в виде пакетов**. Метод.** Анализ безопасности ресурсов ИСПДн относительно НСД путем «сниффинг-атак» включает пять условных этапов: сбор информации в ИСПДн, сканирование ИСПДн, получение доступа к ИСПДн, закрепление в ИСПДн, формирование отчета. При этом – анализ безопасности всегда сопряжен с несанкционированным доступом к данным (НСД). **Результат.** Для предотвращения НСД путем «сниффинг-атак» предлагаются следующие аппаратно-программные решения: применение протокола HTTPS – безопасной версии протокола HTTP; использование статической таблицы ARP, формируемой вручную; сканирование вычислительной сети ИСПДн программой AntiSniff; шифрование трафика вычислительной сети ИСПДн. **Вывод.** Представленные аппаратно-программные решения позволяют минимизировать последствия несанкционированного воздействия на информационные системы персональных данных.

Ключевые слова: анализ безопасности; активный перехват трафика; безопасность ресурсов; закрепление в системе; информационная система; пассивный перехват трафика; персональные данные; получение доступа; сбор информации; сниффинг-атака; сканирование; средства защиты ресурсов; формирование отчета; этапы анализа

Для цитирования: А.Р. Газизов. Аппаратно-программные методы защиты ресурсов информационной системы персональных данных от несанкционированного доступа путем «сниффинг-атак». Вестник Дагестанского государственного технического университета. Технические науки. 2022; 49(3):52-60. DOI:10.21822/2073-6185-2022-49-3-52-60

Hardware, software and organizational means of protecting the resources of the personal data information system from unauthorized access by means of "sniffing attacks"

A.R. Gazizov
Don State Technical University,
1 Gagarin Square, Rostov-on-Don 344000, Russia

Abstract. Objective. The article discusses hardware and software methods of protecting the resources of the personal data information system from unauthorized access by means of "sniffing attacks"; the essence of which is to intercept data that is delivered within the observed system in the form of packets. **Method.** The analysis of the security of resources by the personal data information system regarding unauthorized access to data by means of "sniffing attacks" includes five conditional stages: collecting information in the personal data information system, scanning the personal data information system, gaining access to the personal data information system, securing personal data in the information system, generating a report; at the same time, security analysis it is always associated with unauthorized access to data. **Result**. To prevent unauthorized access to data by means of "sniffing attacks", the following software and hardware solutions are proposed to minimize the consequences of

unauthorized exposure to the personal data information system: the use of the HTTPS protocol, a secure version of the HTTP protocol; the use of a static ARP table generated manually; scanning of the computer network of the personal data information system by the AntiSniff program; encryption of the computer network traffic networks of the personal data information system. **Conclusion.**The presented hardware and software solutions allow minimizing the consequences of unauthorized impact on personal data information systems.

Keywords: security analysis; active traffic interception; resource security; anchoring in the system; information system; passive traffic interception; personal data; access; information collection; sniffing attack; scanning; resource protection tools; report generation; analysis stages

For citation: A.R. Gazizov. Hardware, software and organizational means of protecting the resources of the personal data information system from unauthorized access by means of "sniffing attacks". Herald of the Daghestan State Technical University. Technical Science. 2022; 49 (3): 52-60. DOI: 10.21822 /2073-6185-2022-49-3-52-60

Введение. В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под информационной системой персональных данных (ИСПДн) будем понимать совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств [1, 18]. Анализ безопасности ресурсов ИСПДн относительно несанкционированного доступа (НСД) проводился в организации, осуществляющей торговую деятельность, после получения письменного разрешения руководителя организации на проведение работ по анализу безопасности ресурсов ИСПДн; при условии подписания соглашения о неразглашении информации, полученной в результате анализа.

Постановка задачи. Анализ безопасности ресурсов ИСПДн относительно НСД путем «сниффинг-атак» необходимо разделить на пять этапов: сбор информации в ИСПДн, сканирование ИСПДн, получение доступа к ИСПДн, закрепление в ИСПДн, формирование отчета.

Этапы анализа безопасности ресурсов ИСПДн.

1) Сбор информации в ИСПДн условно разделен на пассивную и активную фазы с целью получения её максимального количества относительно исследуемого объекта информатизации. Данный этап является наиболее важными и максимально трудоёмким.

Во время пассивной фазы ИСПДн «не знает» о том, что был начат сбор информации из открытых и общедоступных источников, таких как поисковые системы и базы данных NIC. Базы данных NIC – это ссылка на запись, которая размещена в базе данных той или иной организации, регулирующей деятельность во всемирной паутине [12]. Активная фаза предполагает непосредственное взаимодействие с самой ИСПДн; в том числе – сканирование портов, определение работающих сервисов и их версий, а также определение версий операционной системы, под управлением которой работают конечные пользователи и сервисы.

2) Сканирование ИСПДн осуществляется на основе информации, полученной на предыдущем этапе, с использованием следующего инструментария: ICMP-сканеры, SNMP-сканеры, сканеры открытых портов, сканеры уязвимостей.

Сканирование ИСПДн позволило получить следующую информацию: IP-адреса, версии операционных систем, запущенные сервисы и их версии, «имена компьютеров», учетные записи пользователей.

3) Получение доступа к ИСПДн. Используя данные, полученные после сканирования ИСПДн, выявляется уязвимость, позволяющая НСД к персональным данным.

4) Закрепление в ИСПДн предполагает закрепление в системе, к которой ранее был получен доступ, так называемые методы сохранения доступа к ИСПДн: установка троянских программ, backdoor или rootkit.

5) Формирование отчета относительно проделанной работы является последним этапом.

Подводя итог, следует отметить – анализ безопасности ресурсов ИСПДн всегда сопряжен с НСД; вопрос состоит исключительно в легитимности мероприятий анализа или её отсутствии [15,16].

Методы исследования. Анализ безопасности ресурсов ИСПДн путем «сниффинг-атак». «Сниффинг» – это один из простейших методов мониторинга трафика, проходящего через ИСПДн. Его суть заключается в перехвате данных, которые доставляются в рамках наблюдаемой системы в виде пакетов. Метод называют «сниффинг» потому, что он напоминает «обнюхивание» данных анализаторами сетевых протоколов, которые установил системный администратор. «Сниффинг» предполагает НСД к данным, передаваемым по проводам, оптоволокну, витой паре, радиоволнам или в любой другой среде [7].

Для целей анализа рассмотрим НСД к данным ИСПДн, передаваемым по проводам и радиоволнам вычислительной сети ИС. Применяемые в вычислительной сети ИСПДн сетевые карты принимают данные в виде сигналов, поступающие к ним по проводам, а также – радиосигналы. Далее – сигналы трансформируются в полезную информацию. Когда на одну из сетевых карт приходит пакет данных, в заголовке указывается – сетевой адрес интерфейса Media Access Control (MAC), а также – широковещательный адрес подсети broadcast или многоадресный пакет multicast; при этом – сетевая карта обрабатывает полученный сигнал, а информация передается в ИСПДн. Исходя из этого, чтобы осуществить перехват всего трафика, идущий по вычислительной сети ИСПДн, необходимо внести изменения в режим работы сетевой карты. Реализуется данный метод заменой драйвера или библиотеки, через которые операционная система (ОС) управляет сетевым интерфейсом.

Для ОС Windows – WinPcap; для ОС Linux – libpcap. Также, необходимо учесть среду передачи данных. При этом – для беспроводных сетей, чтобы перехватить трафик, необходимо заменить драйвер или библиотеку и установить специальное ПО; а для сетей, в которых для подключения используется кабель, необходимо получить доступ непосредственно к оборудованию [3,6].

Анализ безопасности ресурсов ИСПДн с использованием проводной сети предполагает использование кабеля типа витая пара; при этом – подключение реализуется с использованием топологии сети типа «звезда», изображенной на рис.1; когда интерфейсы в пределах такого сегмента вычислительной сети получают всю проходящую по ней информацию.

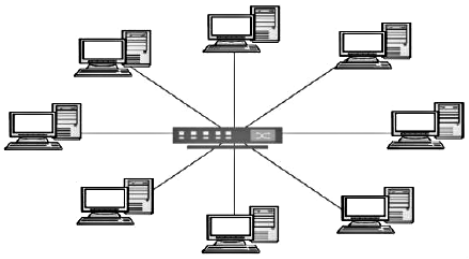

Рис. 1. Топология типа «звезда»
Fig. 1. Star topology

Концентратор (hub) функционирует по такому же принципу; когда подключенные к нему рабочие станции ИСПД, получают всю информацию, направленную в вычислительную сеть ИСПДн, несмотря на то, что для каждой из них используется для подключения отдельный кабель. Таким образом, передача данных по проводам и радиоволнам в вычислительной сети ИСПДн организации является достаточно шаблонной задачей.

В вычислительной сети ИСПДн организации используется коммутатор (switch); по этой причине перехват трафика незначительно усложняется в связи с тем, что коммутатор «знает» адреса рабочих станций, подключенных к его интерфейсу; передавая информацию от отправителя исключительно адресату. Для анализа безопасности ресурсов ИСПДн путем «сниффинг-атак» в аспекте возможного перехвата трафика необходимым элементом является соответству-

ющее программное обеспечение (ПО). С целью минимизации затрат на анализ был выбран бесплатный анализатор пакетов с открытым исходным Wireshark [2,4].

В анализируемой вычислительной сети ИСПДн применимы пассивный и активный методы перехвата трафика. Пассивный перехват трафика будет реализовываться с использованием анализатор пакетов Wireshark. Данное ПО способно работает как под управлением ОС Windows и Linux; позволяя при этом перехватывать, фильтровать, анализировать и сохранять сетевой трафик. Как правило, анализатор пакетов Wireshark используют специалисты по информационной безопасности организаций. По этой причине, обозначенное ПО будет рекомендовано администратору вычислительной сети ИСПДн организации, для выявления и устранения проблем, которые возникнут в ходе работы сетевых сервисов.

После запуска программы Wireshark, выбран интерфейс для мониторинга – eth0; в течение 60 минут было собрано порядка тридцати пяти тысяч пакетов. В данном конкретном случае трафик в вычислительной сети ИСПДН организации был ниже среднего.

Начиная с Domain Name System (DNS-запроса), необходимо отфильтровать запросы к сайту centr.expert.ru. После применения фильтра, появилась возможность увидеть полную, последовательную историю запросов и ответов браузера к DNS-серверу. Зная, по какому IP-адресу будет происходить дальнейшая коммутация, необходимо создать соответствующий фильтр (ip.addr==81.19.72.38), как изображено на рис. 2.

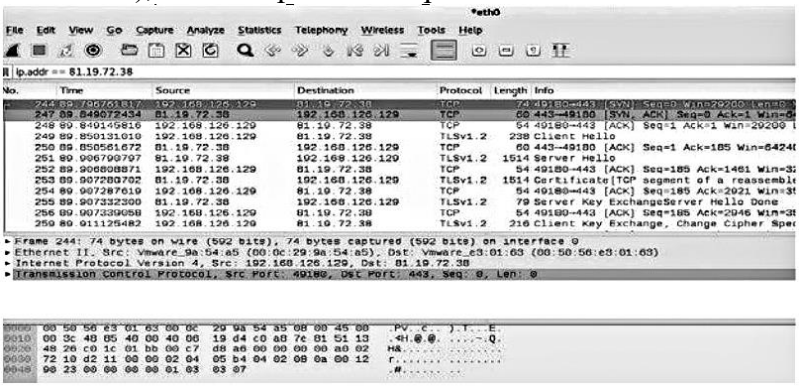

Рис. 2. Процесс коммутации с web-сервером
Fig. 2. The process of switching with a web server

Также можно отследить, поток данных для более детального анализа полученных пакетов, как изображено на рис. 3.

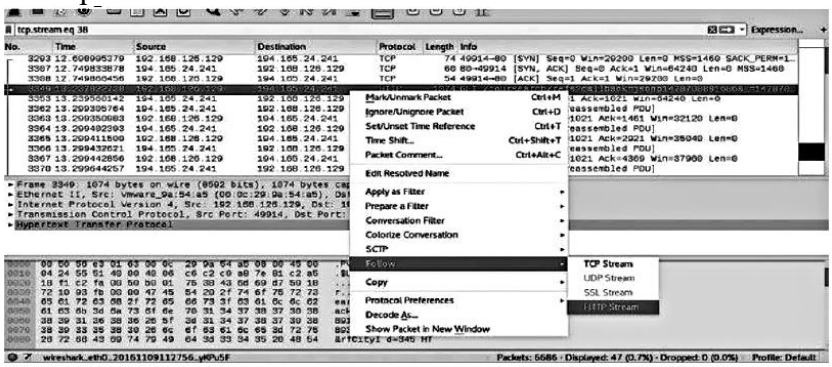

Рис. 3. Процесс отслеживания потока
Fig. 3. Flow tracking process

Для лучшего понимания результата анализа безопасности ресурсов ИСПДн, в Wireshark присутствует возможность отследить определенные потоки данных. В случае с HyperText Transfer Protocol (HTTP) была выбрана функция «follow HTTP stream»

В ходе анализа был применен графический доступ к интерфейсу; вместе с тем, существует иной метод анализа в терминальном исполнении – инструмент Tcpdump, представляю-

щий собой средство сетевого анализа, используемое специалистами в сфере информационной безопасности [2,4].

После запуска сканера было выявлено соединение ok.ru; при этом – количество данных для анализа избыточно. Для решения задачи анализа следует воспользоваться встроенным фильтром заголовков, акцентируя внимание на пакеты с флагами PSH и ACK по следующим причинам:

1) PSH-пакет делает этот пакет пакетом PUSH («проталкивания»). При нормальном потоке передачи данных, система получателя не будет подтверждать получение каждого пакета сразу же после его получения. Вместо этого система получателя в течение некоторого времени будет собирать и хранить полученные данные в буфере, пока не передаст их приложению пользователя. Пакет PUSH «инструктирует» систему получателя немедленно передать все полученные ранее данные из буфера в приложение пользователя и немедленно отправить сообщение с подтверждением получения.
2) ACK-пакет устанавливается в случае, если он содержит значение номера подтверждения в поле подтверждения. Все пакеты после стартового пакета SYN будут иметь установленный флаг ACK.

Структура прохождения пакетов представлена на рис. 4.

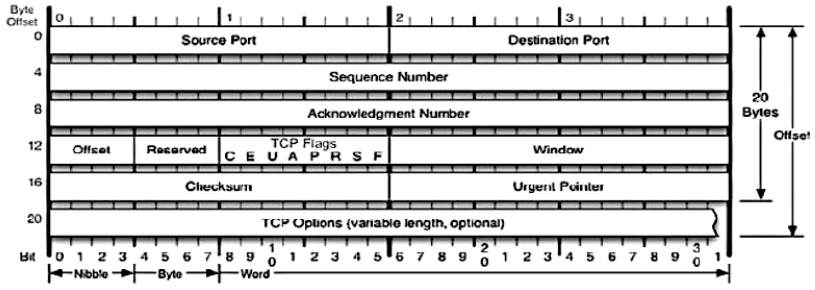

Рис. 4. Структура заголовка сегмента TCP
Fig. 4. The Structure of the TCP Segment Header

Представленная структура демонстрирует, что необходимые флаги A и P (как элемент кода, например: -p icmp …… или же -A OUTPUT…….) находятся в четвертой и пятой позиции; это обозначает, что в двоичном формате это будет иметь вид 00011000, а в десятичном – 24.

Активный перехват трафика. Этот сегмент анализа безопасности ресурсов вычислительной сети ИСПДн предполагает в качестве конечного результата получение доступа к одному из портов коммутатора. При этом – неважно, будет ли получен доступ к самому коммутатору или же это будет являться сетевой розеткой, имеющей подключение к сетевому оборудованию, расположенному в другом помещении. Главным является факт, что на сетевой интерфейс приходят исключительно те пакеты, которые должны приходить.

Для анализа безопасности ресурсов вычислительной сети ИСПДн предлагается применить один из самых известных способов – переполнение CAM-таблицы, чтобы обойти защиту сети и в принудительном порядке «заставить» коммутатор работать как концентратор; это позволит перехватить весь сетевой трафик. Как правило, все CAM-таблицы имеют конечную величину и определенные данные, которые направляют нужный трафик конкретному работнику организации, а именно MAC-адреса, номер порта и информацию о принадлежности к VLAN.

Переполнение такой таблицы приведет к тому, что коммутатор больше не сможет обрабатывать данные в штатном режиме, и для того, чтобы обеспечить работникам организации минимальный уровень сервиса, коммутатор перестает читать CAM-таблицу и переходит в режим работы концентратора [10,11]. Для проведения атаки, направленной на переполнение CAM-таблицы MAC-адресами, необходимо воспользоваться следующими командами в терминале Kali Linux: root@kali:~# macof.

Следующим шагом является захват ARP-таблицы на маршрутизаторах, которые используют для сопоставления IP и MAC-адресов, что делает возможным для коммутатора выбрать наиболее благоприятный путь для прохождения трафика. Важно то, что широковещательные пакеты, используемые для построения CAM-таблицы, никак не фильтруются; являясь по сути широковещательными. Данная уязвимость опасна тем, что злоумышленник может рассылать по вычислительной сети ИСПД организации недостоверные данные, а также трансформировать режим работы своего компьютера в режим работы концентратора. Во время анализа было использовано ПО Ettercap. При этом – был выбран режим сниффинга и интерфейс eth0, с которым будет осуществляться дальнейшая работа по анализу. После того, как список доступных хостов был получен и проанализирован, следует отметить роутер как первую цель, а случайный компьютер в сети как вторую цель [10,11].

Следующим шагом после определения целей, является непосредственно начало атаки. В ходе анализа был получен доступ к одному из сетевых портов, однако проникновения в вычислительную сеть не было, так как современные коммутаторы обладают способностью контроля доступа по MAC-адресам [1,2,7]. Для завершения анализа и успешного проникновения в вычислительную сеть ИСПДН организации необходимо сменить MAC-адрес компьютера, который используется для анализа следующим способом:

root@kali:~# ifconfig eth0 down
root@kali:~# macchanger -r eth0
root@kali:~# ifconfig eth0 up

После того, как MAC-адрес был заменен, доступ в вычислительную сеть ИСПДН организации был успешно получен.

Вторым способом анализа безопасности ресурсов вычислительной сети ИСПДн предлагается проверка на предмет уязвимости беспроводного соединения Wi-Fi в организации при помощи атаки Pixie Dust. Анализ проводится с помощью дистрибутива Kali Linux и встроенного в него терминала; а также, набора утилит – исходя из полученного результата, можно определить количество доступных Wi-Fi адаптеров, которые можно использовать для анализа. Информация о сканировании представлена на рис. 5.

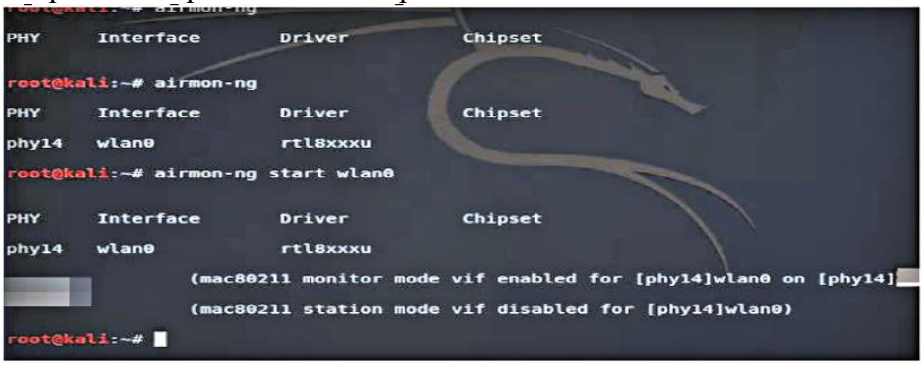

Рис. 5. Доступные Wi-Fi адаптеры
Fig. 5. Available Wi-Fi adapters

После выбора доступного интерфейса wlan0 необходимо включить мониторинг, используя следующую команду в консоли: root@kali:~# airmon-ng start wlan0.

После выполнения вышеописанной команды, адаптер с которого выполняется анализ, переходит в режим мониторинга и имеет название wlan0mon.

Следующая команда проверит доступ к WPS: root@kali:~# wash –I wlan0mon.

Для продолжения анализа была выбрана Pixie dust атака, дающая возможность получить WPS PIN, позволяющий получить пароль от сети. При помощи этой команды будет запущен reaver: root@kali:~# reaver –K –N – S –b (MAC-адрес интерфейса) –I wlan0mon. При этом – ключ i указывает интерфейс в режиме мониторинга, -K атака pixie dust, -b дает возможность

определить MAC-адрес анализируемой цели. В дальнейшем необходимо добавить ключ – A, для ассоциации с точкой доступа в aireplay-ng.

Обсуждение результатов. В итоге – удалось получить WPS PIN и для дальнейшего анализа необходимо получить пароль при помощи следующей команды: root@kali:~# reaver –A –p 54573895 –N –S –b (MAC-адрес) –I wlan0mon.

После получения доступа необходимо продолжить анализ безопасности ресурсов вычислительной сети ИСПДн для получения необходимых сведений относительно самой организации и персональных данных ее работников; что обеспечивает выполнение следующих команд:

– # sysctl –w net.ipv4.ip_forward=1 – функция подмены mac – адреса роутера субъекта на адрес Kali Linux злоумышленника;

– iptables –t nat –A PREROUTING -p tcp –destination-port 80 –j REDIRECT –to-port 65000 – по протоколу tcp с порта 80 переводит на порт 65000 тем самым будет осуществляться прослушивание трафика;

– arpspoof –i (название сетевой карты с которой будет осуществляться атака) ip – субъекта и ip роутера – начало атаки;

– sslstrip –k –l 65000 – подмена защищенного соединения https на небезопасное http в браузере субъекта;

– tail –f sslstrip.Log – выводит на экран злоумышленника только логин, пароль и на какой сайт был сделан вход субъектом.

В дальнейшем – злоумышленнику необходимо лишь ждать действий от субъекта атаки, на которого была совершена атака; т.е. после успешной атаки, злоумышленник получает допуск к ресурсам ИСПДн работников организации, в том числе – логин и пароль от учетных записей. Результат изображен на рис. 6 [10,16].

Рис. 6. Информация, вводимая сотрудником организации
Fig. 6. Information entered by an employee of the organization

Проанализирован НСД к данным ИСПДн, передаваемым по проводам и радиоволнам вычислительной сети ИС относительно двух типов сетей передачи данных:

1) Беспроводные вычислительные сети, а также сети, построенные с помощью концентраторов; в данном случае НСД к данным является незатруднительным для злоумышленника, т.к. данные относительно общедоступны при их передаче по сети.

2) Вычислительные сети, построенные с помощью коммутаторов; в данном случае НСД к данным является более затруднительным для злоумышленника, т.к. данные при их передаче по сети доступны исключительно адресату [16].

Вывод. Для предотвращения НСД к ИСПДн организации путем «сниффинг-атак» предлагаются следующие решения (аппаратно-программные и организационные средства защиты ресурсов), позволяющие минимизировать последствия несанкционированного воздействия на ИСПДн:

1) Применение протокола HTTPS – безопасной версии протокола HTTP, которая реализует протокол HTTP с использованием протокола TLS для защиты базового TCP-подключения. В этом случае пароль от учетных записей пользователей будет зашифрован и не виден.

2) Использование статической таблицы ARP, формируемой вручную; в итоге – неуязвимой к ARP – атакам. Для этого следует добавить необходимые MAC – адреса в таблицу. При этом – если отключить использование ARP на сетевых интерфейсах; то доступны будут исключительно те системы, MAC-адреса которых добавлены в ARP-таблицу «нашего» узла, а «наш» MAC-адрес добавлен в ARP-таблицы узлов, с которыми производится обмен трафиком. Если не отключать использование ARP на сетевых интерфейсах, статически заданный MAC-адрес имеет приоритет. Если MAC-адрес для какого-то IP-адреса не задан, используется ARP-запрос.

3) Сканирование вычислительной сети ИСПДн программой AntiSniff, позволяющей выявить рабочую станцию злоумышленника в сети; а также – собирающую и анализирующую не предназначенные для неё данные (пакеты).

4) Шифрование трафика вычислительной сети ИСПДн, для обеспечения конфиденциальности, целостности и доступности данных [16].

Библиографический список:

1. Geekkies: сайт. – 2022. – URL. https://geekkies.in.ua/crossplatform/chto-takoe-virtualbox-i-kak-ej-polzovatsja.html (дата обращения: 05.07.2022).
2. RU-center: сайт. – 2022. – URL. https://www.nic.ru/help/bazy-dannyh-1228/ (дата обращения: 05.07.2022).
3. Академик – информационная безопасность: сайт. – URL. https://dic.academic.ru/dic.nsf/dic_economic_law/5569/ (дата обращения: 05.07.2022).
4. Академик – официальная терминология: сайт. – 2022. – URL. https://official.academic.ru/7175 (дата обращения: 05.07.2022).
5. Академик – словарь чрезвычайных ситуаций: сайт. – 2022. – URL. https://dic.academic.ru/dic.nsf/emergency/777/ (дата обращения: 05.07.2022).
6. Астайкин, А. И. Методы и средства обеспечения программно-аппаратной защиты информации: научно-техническое издание / А. И. Астайкин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко. – Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. 224 с. Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/60959.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.
7. Башлы П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – Москва: РИОР, 2013. 222 с. Текст: электронный. – URL: https://znanium.com/catalog/product/405000 (дата обращения: 05.07.2022). – Режим доступа: по подписке.
8. Википедия – Kali Linux: сайт. – URL. https://ru.wikipedia.org/wiki/Kali_Linux (дата обращения: 05.07.2022).
9. Гатчин Ю. А. Основы информационной безопасности: учебное пособие / Ю. А. Гатчин, Е. В. Климова. – Санкт-Петербург: Университет ИТМО, 2009. – 84 с. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/67463.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.
10. Голембиовская О. М. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.]. – Саратов: Вузовское образование, 2021. – 265 с. – ISBN 978-5-4487-0791-9. – Текст: электронный//Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/109162.html (дата обращения: 05.07.2022). Режим доступа: для авторизир. пользователей.
11. Громов, Ю. Ю. Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017. – 193 с. – ISBN 978-5-8265-1737-6. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/85968.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.
12. Консультант плюс – Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ: сайт. – URL. http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 05.07.2022).
13. Основные проблемы защиты информации в сетях: сайт. – 2022. – URL. https://zen.yandex.com/media/id/5da8242eaad43600b1f1f9ed/osnovnye-problemy-zascity-informacii-v-setiah-5da82678c31e4900ae31ec07 (дата обращения: 05.07.2022).
14. Правительство России – Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: сайт. – URL. http://government.ru/docs/all/84743/ (дата обращения: 05.07.2022).
15. Ревнивых А.В. Информационная безопасность в организациях: учебное пособие. Москва: Ай Пи Ар Медиа, 2021. – 83 с. – ISBN 978-5-4497-1164-9. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/108227.html (дата обращения: 08.05.2022). – Режим доступа: для авторизир. пользователей.
16. Скабцов Н. Аудит безопасности информационных систем. СПб.: Питер, 2018. 72 с.
17. ФСТЭК России – Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в информационных системах персональных данных»: сайт. – URL. https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 05.07.2022).
18. ФСТЭК России – Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ»: сайт. – URL. https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/365-federalnyj-zakon-ot-27-iyulya-2006-g-n-152-fz?highlight=WyIxNTItXHUwNDQ0XHUwNDM3Il0= (дата обращения: 05.07.2022).
19. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 2-е изд. – Саратов: Профобразование, 2019. – 702 с. – ISBN 978-5-4488-0070-2. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/87995.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.
20. Шаньгин В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие. Москва: ФОРУМ: ИНФРА-М, 2020. – 592 с.

References:

1. Geekkies: сайт. – 2022. – URL. https://geekkies.in.ua/crossplatform/chto-takoe-virtualbox-i-kak-ej-polzovatsja.html (дата обращения: 05.07.2022).
2. RU-center: сайт. – 2022. – URL. https://www.nic.ru/help/bazy-dannyh-1228/ (дата обращения: 05.07.2022).
3. Академик – информационная безопасность: сайт. – URL. https://dic.academic.ru/dic.nsf/dic_economic_law/5569/ (дата обращения: 05.07.2022). (In Russ)
4. Академик – официальная терминология: сайт. – 2022. – URL. https://official.academic.ru/7175 (дата обращения: 05.07.2022). (In Russ)
5. Академик – словарь чрезвычайных ситуаций: сайт. – 2022. – URL. https://dic.academic.ru/dic.nsf/emergency/777/ (дата обращения: 05.07.2022). (In Russ)
6. Astaykin, A. I. Methods and means of providing software and hardware protection of information: scientific and technical edition / A. I. Astaykin, A. P. Martynov, D. B. Nikolaev, V. N. Fomchenko. – Sarov: Russian Federal Nuclear Center – VNIIEF, 2015; 224.Text: electronic // Digital educational resource IPR SMART: [website]. – URL: https://www.iprbookshop.ru/60959.html (accessed: 05.07.2022). – Access mode: for authorization. users. (In Russ)
7. Bashly P. N. Information security and information protection: textbook / P. N. Bashly, A.V. Babash, E. K. Baranova. – Moscow: RIOR, 2013; 222. Text: electronic. URL: https://znanium.com/catalog/product/405000 (accessed: 05.07.2022). (In Russ)
8. Wikipedia – Kali Linux: website. – URL. https://ru.wikipedia.org/wiki/Kali_Linux (accessed: 05.07.2022).
9. Gatchin Yu. A. Fundamentals of information security: a textbook / Yu. A. Gatchin, E. V. Klimova. – St. Petersburg: ITMO University, 2009;84. Text: electronic. Digital educational resource IPR SMART: [website]. – URL: https://www.iprbookshop.ru/67463.html (accessed: 05.07.2022). – Access mode: for authorization. users. (In Russ)
10. Golembiovskaya O. M. Stages of formation of the threat model and the information security violator model taking into account changes in the legislation of the Russian Federation: textbook / O. M. Golembiovskaya, M. Yu. Rytov, K. E. Shinakov [et al.]. Saratov: University Education, 202; 265. Text: electronic // IPR SMART Digital Educational Resource: [website]. URL: https://www.iprbookshop.ru/109162.html (accessed: 05.07.2022). Access mode: for authorization. users. (In Russ)
11. Gromov Yu. Yu. Software and hardware protection of information systems: a textbook / Yu. Yu. Gromov, O. G. Ivanova, K. V. Starodubov, A. A. Kadykov. – Tambov: Tambov State Technical University, EBS DIA, 2017. – 193 p. – ISBN 978-5-8265-1737-6. – Text: electronic. Digital educational resource IPR SMART: [website]. – URL: https://www.iprbookshop.ru/85968.html (accessed: 05.07.2022). – Access mode: for authorization. users. (In Russ)
12. Consultant Plus – Federal Law "On Information, Information Technologies and Information Protection" dated 27.07.2006 N 149-FZ: website. URL. http://www.consultant.ru/document/cons_doc_LAW_61798/(accessed: 05.07.2022). (In Russ)
13. The main problems of information protection in networks: site. 2022. URL. https://zen.yandex.com/media/id/5da8242eaad43600b1f1f9ed/osnovnye-problemy-zascity-informacii-v-setiah-5da82678c31e4900ae31ec07 (accessed: 05.07.2022). (In Russ)
14. The Government of Russia – Decree of the Government of the Russian Federation dated 01.11.2012 No. 1119 "On approval of requirements for the protection of personal data during their processing in personal data information systems": website. – URL. http://government.ru/docs/all/84743 / (accessed: 05.07.2022). (In Russ)
15. Jealous A.V. Information security in organizations: a textbook. Moscow: AI Pi Ar Media, 2021; 83 Text: electronic // Digital educational resource IPR SMART: [website]. – URL: https://www.iprbookshop.ru/108227.html (accessed: 08.05.2022). – Access mode: for authorization. users. (In Russ)
16. I will take it myself – The choice and justification of the methodology for calculating economic efficiency: website. – URL. http://zdamsam.ru (accessed: 05.07.2022).
17. Skabtsov N. Information systems security audit.St. Petersburg: St. Petersburg, 2018. 272 p.: (Series "Programmer's Library").(In Russ)
18. FSTEC of Russia – Order of the FSTEC of Russia dated February 18, 2013 No. 21 "On approval of the composition and content of organizational and technical measures to ensure the security of personal data when they are processed in personal data information systems": website. URL. https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (accessed: 05.07.2022). (In Russ)
19. FSTEC of Russia – Federal Law "On Personal Data" dated 27.07.2006 N 152-FZ": website. URL. https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/365-federalnyj-zakon-ot-27-iyulya-2006-g-n-152-fz?highlight=WyIxNTItXHUwNDQ0XHUwNDM3Il0 = (accessed: 05.07.2022). (In Russ)
20. Shangin V. F. Information security and information protection / V. F. Shangin. – 2nd ed. – Saratov: Vocational Education, 2019; 702. Text: electronic. Digital educational resource IPR SMART: [website]. URL: https://www.iprbookshop.ru/87995.html (accessed: 05.07.2022). Access mode: for authorization. users.Shangin, V. F. Complex information protection in corporate systems: a textbook. Moscow: FORUM: INFRA-M, 2020;592. (In Russ)

Сведения об авторе:

Газизов Андрей Равильевич, кандидат педагогических наук, доцент, кафедра «Вычислительные системы и информационная безопасность»; gazandre@yandex.ru

Information about author:

Andrey R. Gazizov, Cand. Sci. (Pedagogical), Assoc. Prof., Department of Computing Systems and Information Security; gazandre@yandex.ru

Конфликт интересов/Conflict of interest.

Автор заявляет об отсутствии конфликта интересов/The author declare no conflict of interest.

Поступила в редакцию/Received 21.07.2022.

Одобрена после рецензирования/ Reviced 30.08.2022.

Принята в печать/Accepted for publication 30.08.2022.