ARTICLE HISTORY: Received: October 05, 2021 Accepted: November 27, 2021 Published: December 04, 2021

ПОСТРОЕНИЕ БЕЗОПАСНОГО ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ КРИТИЧЕСКОЙ ИНФРАСТРУКТУРЫ ЧЕРЕЗ ОТКРЫТУЮ СЕТЬ INTERNET

Франгиз Гильфанетдинович Хисамов, Татьяна Витальевна Вовк
Кубанский государственный технологический университет,
профессор кафедры «Информатики и вычислительной техники».
Кубанский государственный технологический университет, студентка третьего курса

BUILDING SECURE INFORMATIONAL COMMUNICATION BETWEEN AUTOMATED CRITICAL INFRASTRUCTURE SYSTEMS THROUGH AN OPEN INTERNET NETWORK

Frangiz Gilfanetdinovich Khisamov, Tatyana Vitalevna Vovk
Kuban State Technological University,
Professor of the Department of Informatics and Computer Engineering.
Kuban State Technological University, third-year student

Аннотация. В статье приведены основные принципы построения безопасного сетевого взаимодействия автоматизированных систем критической инфраструктуры (АСКИ) в защищенном исполнении и решены задачи безопасного информационного взаимодействия локальных сетей через открытую сеть Internet по технологии Intranet.

Abstract. The article provides the basic principles of building a secure network interaction of automated critical infrastructure systems (ACSIs) in a secure execution and solving the problem of safe communication of local networks through the open Internet network via Intranet technology.

Ключевые слова: автоматизированные системы критической инфраструктуры, межсетевой экран, брандмауэр, сегмент сети, локальная сеть, внешняя сеть, эталонная модель.

Keywords: automated critical infrastructure systems, firewall, firewall, network segment, local network, external network, reference model

В Стратегии национальной безопасности Российской Федерации [1] указано, что «…основными угрозами государственной и общественной безопасности являются нарушения безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации». Особенно остро проблема защиты информации стоит в автоматизированных системах критической инфраструктуры, обеспечивающих нормальное функционирование городских систем жизнеобеспечения граждан. Ужесточение требований к надежности, скрытности и оперативности передачи управляющей конфиденциальной информации в АСКИ обусловлены появлением новейших средств радиоэлектронного подавления (РЭП), которые могут быть использованы в злоумышленных целях. Поэтому противоборствующая сторона может не только дезорганизовать или снизить эффективность управления, но и полностью заблокировать АСКИ. Поэтому разработка основных принципов построения безопасного информационного взаимодействия автоматизированных систем критической инфраструктуры через открытую сеть internet в условиях злоумышленных противодействий является актуальной задачей.

Автоматизированная система критической инфраструктуры в защищенном исполнении должна удовлетворять всем требованиям Главного научно-технического управления при Федеральной службе по техническому и экспертному контролю (ФСТЭК), предъявляемым к автоматизированным системам, а также ГОСТ Р 51853-2014. «Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении» [2,3,4].

Заданный уровень защищенности сетей АСКИ обеспечивается размещением между сегментами сети или между сетью и внешней средой межсетевых экранов (Брандмауэров или так называемых систем Fire Wall). Наиболее эффективными являются комплексные брандмауэры, которые обеспечивают многопротокольный режим преобразования уровней модели OSI объединяемых сетей в полном объеме. Чаще всего возникает необходимость в совместной поддержке стеков протоколов SPX\IPX и TCP\IP [3,4,5].

Комплексный межсетевой экран удобно представить в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI. Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно различают такие неделимые брандмауэры, как экранирующий маршрутизатор, экранирующий транспорт (шлюз сеансового уровня), а также экранирующий шлюз (шлюз прикладного уровня).

Рассмотрим основные сетевые протоколы взаимодействия в автоматизированных системах критической инфраструктуры. Известно, что используемые в сетях протоколы (TCP\IP, SPX\IPX) не однозначно соответствуют модели OSI. Поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели. Поэтому при использовании межсетевых экранов важное значение придается схеме подключения. Среди всего множества возможных схем подключения брандмауэров типовыми являются следующие:

- схема единой защиты локальной сети;
- схема с защищаемой закрытой и не защищаемой открытой подсетями;
- схема с раздельной защитой закрытой и открытой подсетей.

Последняя схема может быть рекомендована для автоматизированной системы (АС) критической инфраструктуры, так как обеспечивает наибольшую безопасность межсетевых взаимодействий. Она содержит два брандмауэра, каждый из которых образует отдельный эшелон защиты закрытой подсети. Защищаемая открытая подсеть здесь выступает в качестве экранирующей подсети. Обычно экранирующая подсеть конфигурируется таким образом, чтобы обеспечить доступ к компьютерам подсети как из потенциально враждебной внешней сети, так и из закрытой подсети локальной сети. Однако прямой обмен информационными пакетами между внешней сетью и закрытой подсетью невозможен.

Настройка параметров функционирования брандмауэра должна удовлетворять ряду требований:

- иметь средства разграничения доступа к ресурсам системы;
- блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;
- запрещать привилегированный доступ к своим ресурсам из локальной сети;
- содержать средства мониторинга\аудита любых административных действий.

Приведенным требованиям удовлетворяют различные разновидности ОС UNIX, а также Microsoft Windows NT.

После установки на компьютер брандмауэра выбранной операционной системы, ее конфигурирования, а также инсталляции специального программного обеспечения можно приступать к настройке параметров функционирования всего межсетевого экрана. Этот процесс включает следующие этапы:

- выработку правил работы межсетевого экрана в соответствии с разработанной политикой межсетевого взаимодействия и описание правил в интерфейс брандмауэра;
- проверку заданных правил на непротиворечивость;
- проверку соответствия параметров настройки брандмауэра разработанной политике межсетевого взаимодействия.

Для надежной защиты АСКИ целесообразнее строить из полностью закрытых подсетей, что намного упростит защиту всей сети и существенно снизит стоимость проводимых работ.

Безопасность информационного взаимодействия локальных сетей через открытую сеть Internet требует качественного решения двух базовых задач:

-защиты подключенных к публичным каналам связи локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды;

-защиты информации в процессе передачи по открытым каналам связи.

Решение первой задачи основано на использовании рассмотренных выше брандмауэров, поддерживающих безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене информацией.

Защита информации в процессе ее передачи по открытым каналам основана на построении защищенных виртуальных каналов связи, называемых криптозащищенными туннелями или туннелями VPN. Каждый такой туннель представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети.

Для защиты от повтора, удаления и задержек пакетов сообщений, передаваемых по туннелю VPN, используются встроенные возможности стека протоколов TCP\IP.

Вариант, когда конечные точки защищенного туннеля совпадают с конечными точками защищаемого потока сообщений, является с точки зрения безопасности лучшим. В этом случае обеспечивается полная защищенность канала вдоль всего пути следования пакетов сообщений.

С целью защиты от отказа получения сообщений подсистемой защиты прикладного уровня должна предусматривать при приеме каждого сообщения передачу отправителю уведомления о получении сообщения. Такое уведомление должно криптографически подписываться получателем сообщения.

Компоненты виртуальной сети АСКИ, создающие защищенный туннель называются инициатором и терминатором туннеля. Для возможности расшифрования данных и проверки цифровой подписи при приеме инициатор и терминатор туннеля должны поддерживать функции безопасного обмена ключами.

Выводы. Таким образом, современные сетевые информационные технологии Intranet позволяют строить надежные защищенные высокоскоростные защищенные сети АСКИ, способных противостоять злоумышленному преднамеренному радиоэлектронному противодействию.

Список литературы

1. Доктрина информационной безопасности Российской Федерации [Текст]: [Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646] // Российская газ. – 2016. – 6 декабря.

2. Гостехкомиссия России. Руководящий документ. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. - М.: Военное издательство. - 1997.

3. ГОСТ Р 51853-2014. «Национальный стандарт Российской Федерации. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении» [Тескт]. Приказ Федерального агентства по техническому регулированию и метрологии от 27 декабря 2014 г. №374-ст.

4. Коржик В.И., Яковлев В.А. Основы криптографии: учебное пособие / В.И.Коржик, В.А.Яковлев. – СПб., ИЦ Интермедия, 2016. – 312 с. : илл.

5. Системы связи: Учебное пособие / под общей редакцией С.И.Макаренко, В.И.Сапожников, Г.И.Захаренко, В.Е.Федосеев. – Воронеж: Издание ВАИУ, 2011 – 287 с.

References

1. Doctrine of information security of the Russian Federation [Text]: [Approved by the Decree of the President of the Russian Federation of December 5, 2016 No. 646] // Russian Gas. – 2016. - December 6.

2. State Committee of Russia. Guidance document. Means of computer technology. Firewalls. Protection against unauthorized access to information. - M.: Voennoe izdatelstvo. - 1997.

3. GOST R 51853-2014. "National Standard of the Russian Federation. Data protection. The procedure for creating automated systems in a protected performance" [Techt].Order of the Federal Agency for Technical Regulation and Metrology of December 27, 2014 No. 374-art.

4. Korzhik V.I., Yakovlev V.A. Fundamentals of cryptography: a textbook / V.I.Korzhik, V.A.Yakovlev. – SPb., IC Intermedia, 2016. – 312 p. : ill.

5. Communication systems: Textbook / under the general editorship of S.I.Makarenko, V.I.Sapozhnikov, G.I.Zakharenko, V.E.Fedoseev. – Voronezh: Edition of VAIU, 2011 – 287 p.