Торайғыров университетінің хабаршысы
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Торайғыров университетінің ХАБАРШЫСЫ

Энергетикалық сериясы

1997 жылдан бастап шығады

ВЕСТНИК Торайгыров университета

Энергетическая серия

Издается с 1997 года

ISSN 2710-3420

№ 4 (2020)

Павлодар

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Энергетическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
№ 14310-Ж
выдано
Министерство информации и общественного развития
Республики Казахстан

Тематическая направленность
публикация материалов в области электроэнергетики,
электротехнологии, автоматизации, автоматизированных и
информационных систем, электромеханики и
теплоэнергетики

Подписной индекс – 76136

МРНТИ 81.93.29

https://doi.org/10.48081/WLGL3153

М. А. Чуприна, А. Д. Тастенов, А. А. Бектасова
Торайгыров университет, Республика Казахстан, г. Павлодар

ТЕЛЕКОММУНИКАЦИОННЫЕ СИСТЕМЫ КАК ТРАНСПОРТНАЯ СРЕДА АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ И ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Телекоммуникационные системы и устройства активно используются в промышленности, экономике, и других сферах деятельности. Безусловно то, что они подвержены угрозам различного характера и назначения.

В области информационной безопасности выделяются четыре вида угроза информационной безопасности, а именно, угрозы:

– правам гражданина в области информационной деятельности;

– информационному обеспечению государственной деятельности страны;

– развитию средств информатизации и телекоммуникации;

– сохранности и эффективному использованию информационных ресурсов;

– безопасности информационных и телекоммуникационных систем.

Последний вид угрозы и является предметом исследования и анализа данной статьи.

Ключевые слова: телекоммуникационные системы, информационная безопасность.

Введение

Общеизвестно, что автоматизированные системы имеют широкий спектр различного назначения, используются в различных системах. Не исключение и телекоммуникационные системы с использованием методов распределенной обработки и передачи информации различного типа.

Материалы и методы

Сложное построение телекоммуникационных сетей, использование множества вариантов сетевых протоколов, а в большей степени использование

стеков протоколов, приводит к большим возможностям несанкционированного доступа к обрабатываемой и передаваемой информации.

Например, использование в автоматизированной телекоммуникационной системе разнородных (например, проводных и беспроводных) локальных сетей (LAN – local accses network) и техническая интеграция их единую систему дает более широкие возможности несанкционированного доступа.

Результаты и обсуждения

Информационная безопасность, как неотъемлемая часть функционирования телекоммуникационной системы, это состояние данных, при котором невозможно их случайное или преднамеренное раскрытие, изменение или уничтожение.

В этих условиях обеспечить безопасность информации возможно только при условии использования специальных программных и технических мер, прежде всего на основе контроля доступа к передаваемым в телекоммуникационной системе данным.

Межсетевые экраны (Firewall – брандмауэры, дословный перевод с английского языка «пожарная стена») с использованием методов организации виртуальных сетей – это самые эффективные средства технического и системного обеспечения безопасности распределенной обработки и передачи данных.

Firewall представляет собой технически целое и однокомпонентное устройство. Вторым признаком межсетевого экрана является характеристика его программного обеспечения, которое является программно-аппаратным. Оба признака характеристики межсетевого экрана определяют его комплексность.

Общим признаком характеристики Firewall является его функция, а именно, контроль за данными, поступающими в автоматизированную систему и/или выходящей из автоматизированной системы. Реализуется эта функция на основе принципа фильтрации данных, содержащий:

– анализ по совокупности критериев межсетевых протоколов;

– принятия решения о ее распространении в (из) автоматизированной системы

– разграничение доступа пользователей из одной LAN к объектам другой автоматизированной системы.

В результате:

– первое: запрещается или разрешается передача данных между объектами автоматизированной системы;

– второе: разрешается доступ из других автоматизированных систем или объектам своей автоматизированной системы только к ограниченным (разрешенным) объектам, а, следовательно, и субъектам, эксплуатирующих автоматизированную систему.

Реализуется это последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

Первые теоретические исследования проблем обеспечения безопасности информации были выполнены 1980 и 1990-е годы [1, 2, 3, 4, 5]. В этих работах:

– разработаны концепция защиты информации: задачи, методология, принципы реализации процессов обеспечения безопасности информации;

– обоснована необходимость создания отдельной подсистемы управления безопасностью информации в виде иерархической системы автоматизированных рабочих мест;

– обоснованы принципы построения систем защиты информации объектов информатизации с использованием программно-аппаратных средств защиты информации;

– рассмотрены принципы построения систем защиты, методы обеспечения сохранности информации в замкнутых автоматизированных, не использующих для передачи информации сети общего пользования.

Исходя из вышеприведенного, можно констатировать, что анализ методов, моделей и алгоритмов, реализующие требования к Firewall для распределенных автоматизированных систем являются актуальными.

Появление разнообразных инфокоммуникационных технологий создало в последние 20–30 лет основу для разработки распределенных автоматизированных систем различной управления и назначения.

Автоматизированные системы, самых разных назначений и сфер применения строятся с применением топологий телекоммуникационных сетей распределенного характера. Вариантов таких топологий немного. Это объясняется тем, что телекоммуникационные системы состоят из распределенных сетей LAN различного назначения, структуры и программно-аппаратной реализации.

Классифицировать топологии телекоммуникационных сетей распределенного характера по множествам ее признаков нецелесообразно, так как, это только усложнит понятийный аппарат. Возникнет ситуации, которую можно охарактеризовать как «классификация ради классификации», без какой-либо практической целесообразности.

Исходя из вышеизложенного, телекоммуникационные сети автоматизированных систем по структуре топологии удобно классифицировать как иерархические, опорные и древовидные (рисунок 1.1). Последние включают в себя и звездообразные топологии [6].

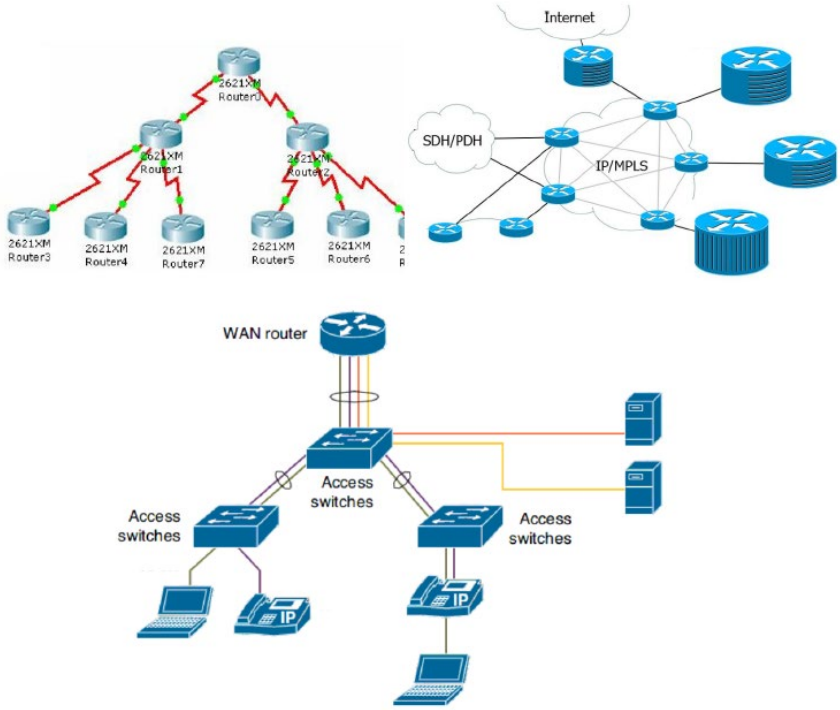

Рисунок 1 – Топологии телекоммуникационных систем

Сопрягающие устройство может соединять две или более отдельных сетей и называется межсетевым устройством или шлюзовой станцией. В настоящее время термины упрощаются используют термин шлюз.

Современные телекоммуникационные технологии разрабатываются на основе стандартов ISO, в числе основных принципов которых обеспечение пользователям сети быстрого доступа к телекоммуникационной системе. Однако это создает трудности в организации информационной безопасности в телекоммуникационных сетях и системах от несанкционированного доступа.

С 1986 года международными организациями стандартизации были приняты ряд документов [6, 7], требование обязательного обеспечения безопасности информации телекоммуникационных сетей и систем.

Телекоммуникационные системы – это объединенная совокупность распределенных корпоративных сетей, которые в свою очередь организуются сетями LAN филиалов, центральных офисов и т.п. с активным использованием глобальных сетей, прежде всего Internet.

Внешнее информационное взаимодействие между корпоративным сетями и даже сетями LAN реализуется через прямое подключение к Internet. При внутреннем информационном взаимодействии эти сети – это транспортная среда. Все это есть не что иное как виртуальная корпоративная сеть, построенную на базе сети общего пользования.

Как ясно из вышеизложенного, объединяющей структурой корпоративных сетей, включая и сети LAN стал Internet.

Использование Internet при кажущейся ее простоте и дешевизне далеко не оптимальное решение, прежде всего из-за ряда проблем, связанных с надежностью, доступностью и безопасностью.

Обеспечение надежности, доступности и безопасности, как факторов эффективной работы требуют тщательного анализа угроз безопасности информации и разработки оптимальной безопасности.

Наиболее простым решением является установка Firewall (межсетевого экрана) на границе LAN и Internet (рисунок 2).

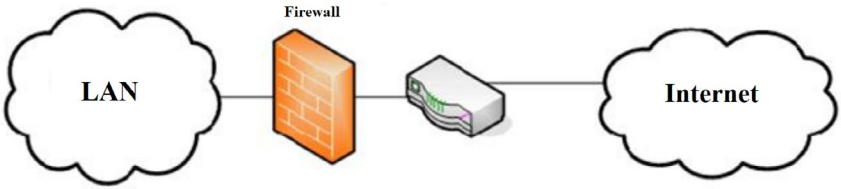

Рисунок 2 – Установка Firewall между LAN и Internet

Возможен также вариант с установкой двух Firewall, один из которых будет защищать LAN, а другой – DMZ (рисунок 3).

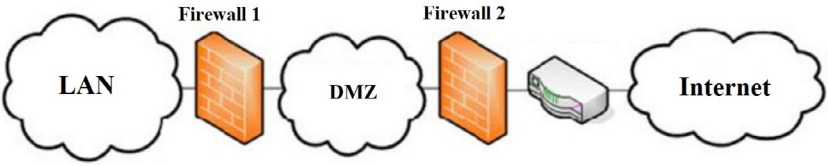

Рисунок 3 – Установка двух Firewall

DMZ – Demilitarized Zone – демилитаризованная зона – сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных.

Существует более простой вариант с защитой зоны DMZ с помощью одного Firewall (рисунок 4).

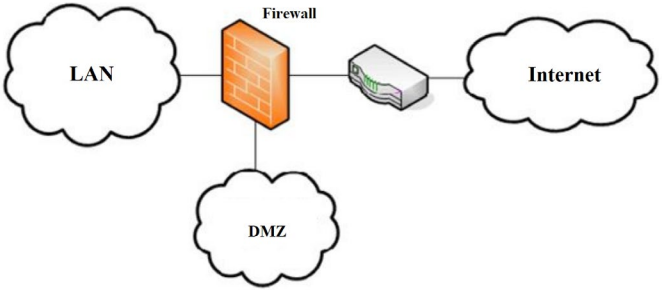

Рисунок 4 – Защита LAN и DMZ с помощью одного Firewall

Выводы

Firewall реализует политику сетевого доступа, пропуская через себя все соединения с сетью. Для каждого проходящего пакета Firewall принимает решение пропускать его или отбросить. Для этих целей необходимо определить набор правил фильтрации для Firewall.

Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но, не устраняет эту опасность совсем.

Более защищенная разновидность данного метода – это способ masquerading, когда весь исходящий из LAN трафик посылается от имени Firewall-сервера, делая LAN практически невидимой.

При реализации Firewall рекомендуется использовать отдельную станцию с соответствующими аппаратными требованиями.

Список использованных источников

1 **Хоффман, Л. Дж.** Современные методы защиты информации: пер. с англ. – М. : Сов. радио, 1980.

2 **Шураков, В. В.** Обеспечение сохранности информации в системах обработки данных. – М. : Финансы и статистика, 1985, С. 224.

3 **Ухлинов, Л. М.** Управление безопасностью информации в автоматизированных системах. – М. : МИФИ. 1996, С. 112.

4 **Ухлинов, Л. М., Казарин, О. В.** Методология защиты информации в условиях конверсии военного производства. М. : Вестник ВОИВТ. 1994, № 2.

5 **Конявский, В. А.** Управление защитой информации на базе СЗИ НСД «Аккорд». – М. : Радио и связь, 1999, С. 325.

6 International Standards Organization. Information Processing Systems – Basic Reference Model. – Part 2 : Security Architecture. ISO/DIS 7498-2. – 1984. – 64 p.

7 International Standards Organization. Information Processing Systems – OSI Reference Model. – Part 2 : Security Architecture. ISO 7498/PDAD-2. – 1986. – 65 p.

8 **Богатырев, В. А.** Информационные системы и технологии. Теория надежности. М. : Юрайт, 2016 – 126 с.

9 **Лукьянов, В. С.** Оценка показателей надежности сетей / В. С. Лукьянов, С. В. Гаевой, Ф. А. Х. Аль-Хаджа // Вестник компьютерных и информационных технологий. – 2013. – № 8. – с. 47 – 52.

10 **Любимов, А. К.** Введение в теорию надёжности : проектно-ориентированный подход : Учебно-методическое пособие. Нижний Новгород, 2014 – 164 с.

References

1 **Hoffman, L. Dj.** Sovremennye metody zaıty ınformatsıı: per. s angl. [Hoffman L. J. Modern methods of information security: trans. from English]. – M. : Sov. radio, 1980.

2 **Shýrakov, V. V.** Obespechenıe sohrannostı ınformatsıı v sıstemah obrabotkı dannyh. [Shurakov V. V. Ensuring the safety of information in data processing systems]. – M. : Finance and statistics, 1985, S. 224.

3 **Ýhlınov, L. M.** Ýpravlenıe bezopasnostıý ınformatsıı v avtomatızırovannyh sıstemah. [Ukhlinov L. M. Information security management in automated systems]. – M. : MEPhI. 1996, p. 112.

4 **Ýhlınov, L. M.**, Kazarın O. V. Metodologıa zaıty ınformatsıı v ýslovıah konversıı voennogo proızvodstva. [Ukhlinov L. M., Kazarin O. V. Methodology of information protection in the conditions of conversion of military production]. – M. : Bulletin VOIVT. 1994, no. 2.

5 **Konıavskıı, V. A.** Ýpravlenıe zaıtoı ınformatsıı na baze SZI NSD «Akkord». [Konyavskiy V. A. Information security management based on the information security system of the NSD «Akkord»]. – M. : Radio and communication, 1999, S. 325.

6 International Standards Organization. Information Processing Systems – Basic Reference Model. – Part 2 : Security Architecture. ISO/DIS 7498-2. – 1984. – 64 p.

7 International Standards Organization. Information Processing Systems – OSI Reference Model. – Part 2 : Security Architecture. ISO 7498/PDAD-2. – 1986. – 65 p

8 **Bogatyrev, V. A.** Informatsıonnye sıstemy ı tehnologıı. Teorııa nadejnostı. [Bogatyrev V. A. Information systems and technologies. Reliability theory]. – M. : Yurayt, 2016 – 126 p.

9 **Lýkıanov, V. S**. Otsenka pokazatelei nadejnostı seteı / V. S. Lýkıanov, S. V. Gaevoı, F. A. H. Al-Hadja // Vestnık kompıýternyh ı ınformatsıonnyh tehnologıı. [Lukyanov V. S. Assessment of network reliability indicators / V. S. Luk'yanov, S. V. Gayevoy, F. A. Kh. Al-Khadja // Bulletin of computer and information technologies]. – 2013. – No. 8. – p. 47 – 52.

10 **Lıýbımov, A. K.** Vvedenıe v teorııý nadëjnostı : proektno-orıentırovannyı podhod : Ýchebno-metodıcheskoe posobıe. Nıjnıı Novgorod. [Lyubimov A. K. Introduction to the theory of reliability: project-oriented approach: Study guide. Nizhny Novgorod]. – 2014 – 164 p.

Материал поступил в редакцию 11.12.20.

М. А. Чуприна, А. Д. Тастенов, А. А. Бектасова

Телекоммуникация жүйелері автоматтандырылған басқару жүйелеріне арналған көлік құралы ретінде және ақпарат қауіпсіздігінің мәселелері

Торайғыров университеті,
Қазақстан Республикасы, Павлодар қ.
Материал баспаға 11.12.20 түсті.

M. A. Chuprina, A. D. Tastenov, A. A. Bektasova

Telecommunication systems as a transport environment of automated control systemsand problems of information security

Toraighyrov University,
Republic of Kazakhstan, Pavlodar.
Material received on 11.12.20.

Телекоммуникация жүйелері мен құрылғылары өнеркәсіпте, экономикада және басқа қызмет салаларында белсенді қолданылады. Олар әр түрлі сипаттағы және мақсаттағы қатерлерге ұшырайтыны айтпаса да түсінікті.

Ақпараттық қауіпсіздік саласында ақпараттық қауіпсіздікке қатердің төрт түрі бар, атап айтқанда қатерлер:

– азаматтың ақпараттық қызмет саласындағы құқықтары;

– елдің мемлекеттік қызметін ақпараттық қамтамасыз ету;

– ақпараттандыру және телекоммуникация құралдарын дамыту;

– қауіпсіздік пен ақпараттық ресурстарды тиімді пайдалану;

– ақпараттық және телекоммуникациялық жүйелердің қауіпсіздігі.

Қауіптің соңғы түрі осы мақаланы зерттеу мен талдаудың тақырыбы болып табылады.

Кілтті сөздер: телекоммуникациялық жүйелер, ақпараттық қауіпсіздік.

Telecommunication systems and devices are actively used in industry, economy, and other areas of activity. It goes without saying that they are exposed to threats of various nature and purpose.

In the field of information security, four types of information security threat are distinguished, namely:

– the rights of a citizen in the field of information activities;

– information support of the state activities of the country;

– development of means of informatization and telecommunications;

– safety and efficient use of information resources;

– security of information and telecommunication systems.

The latter type of threat is the subject of research and analysis of this article.

Keywords: telecommunication systems, information security.

Теруге 11.12.2020 ж. жіберілді. Басуға 17.12.2020 ж. қол қойылды.
Электрондық баспа
3,99 Mb RAM
Шартты баспа табағы 26,6. Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген: А. К. Шукурбаева
Корректор: А. Р. Омарова
Тапсырыс № 3715

Сдано в набор 11.12.2020 г. Подписано в печать 17.12.2020 г.
Электронное издание
3,99 Mb RAM
Усл. печ. л. 26,6. Тираж 300 экз. Цена договорная.
Компьютерная верстка: А. К. Шукурбаева
Корректор: А. Р. Омарова
Заказ № 3715

«Toraighyrov University» баспасынан басылып шығарылған
«Торайғыров университет»
коммерциялық емес акционерлік қоғамы
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
«Торайғыров университет»
коммерциялық емес акционерлік қоғамы
140008, Павлодар қ., Ломов к., 64, 137 каб.
8 (7182) 67-36-69
e-mail: kereku@tou.edu.kz
www.vestnik.tou.edu.kz