ГРНТИ 50.43.15

М. А. Чуприна[1], А. Д. Тастенов[2], О. А. Андреева[3]

[1]магистрант, Энергетический факультет, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;

[2]к.т.н., профессор, Энергетический факультет, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;

[3]ассоц. профессор (доцент), Энергетический факультет, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан

e-mail: [1]lyubeckaya.marin@mail.ru; [2]tastenov@mail.ru

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

В статье рассмотрены телекоммуникационные системы как транспортная среда автоматизированных систем управления и проблемы информационной безопасности.

Ключевые слова: телекоммуникационные системы, автоматизированные системы управления, информационная безопасность.

ВВЕДЕНИЕ

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

ОСНОВНАЯ ЧАСТЬ

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 диссертационной работы.

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.

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 access network) и техническая интеграция их единую систему дает более широкие возможности несанкционированного доступа.

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].

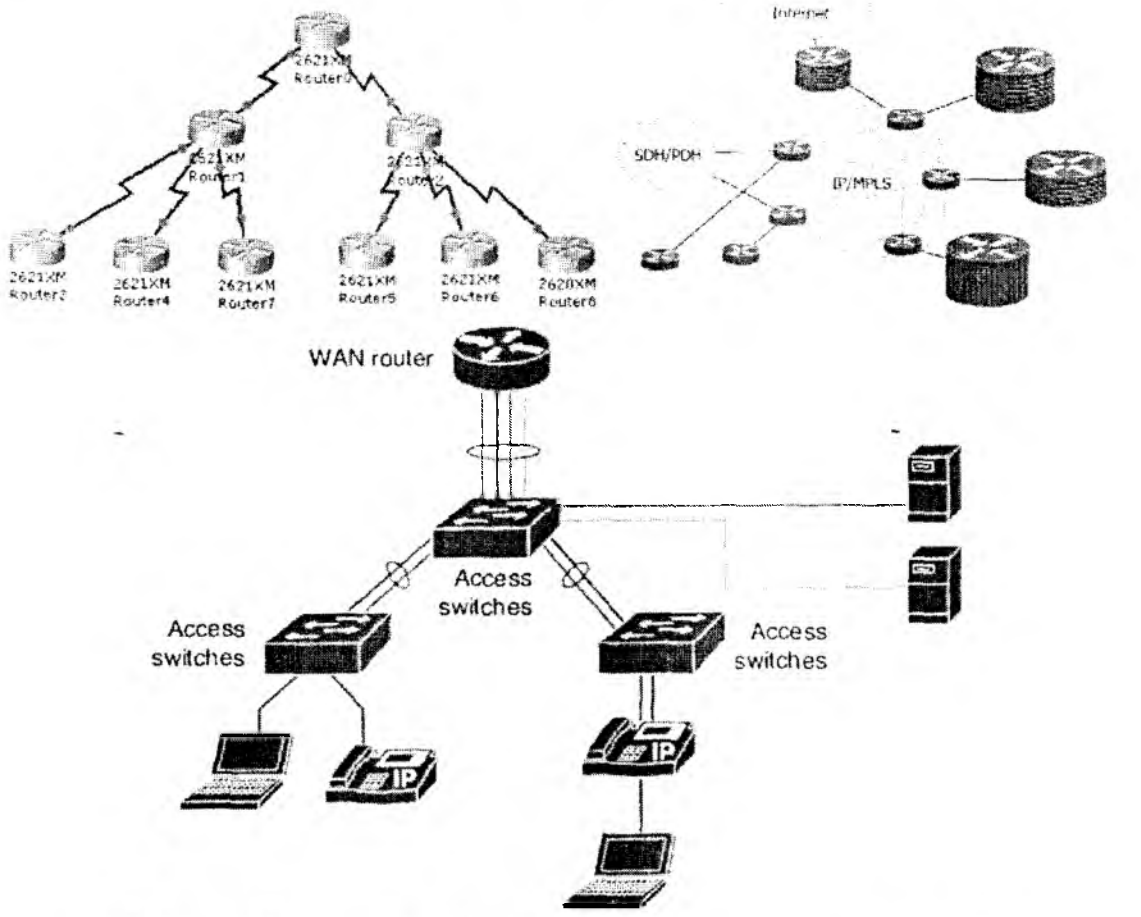

Рисунок 1 – Топологии телекоммуникационных систем

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).

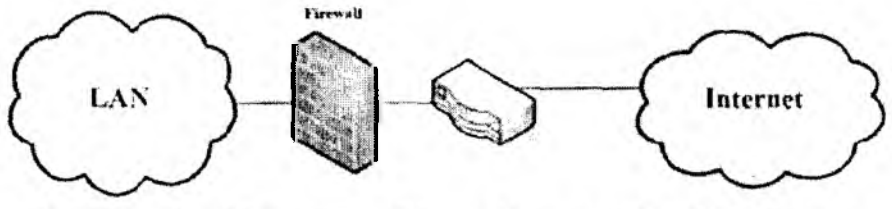

Рисунок 2 – Установка Firewall между LAN и Internet

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

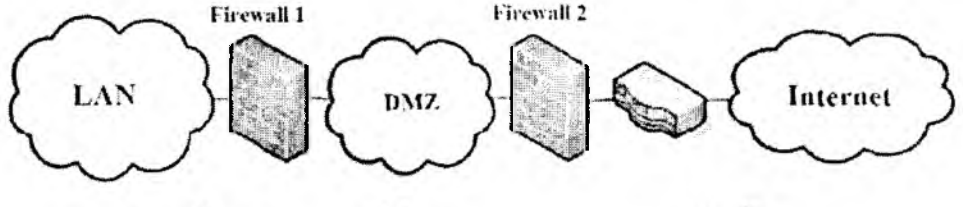

Рисунок 3 – Установка двух Firewall

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).

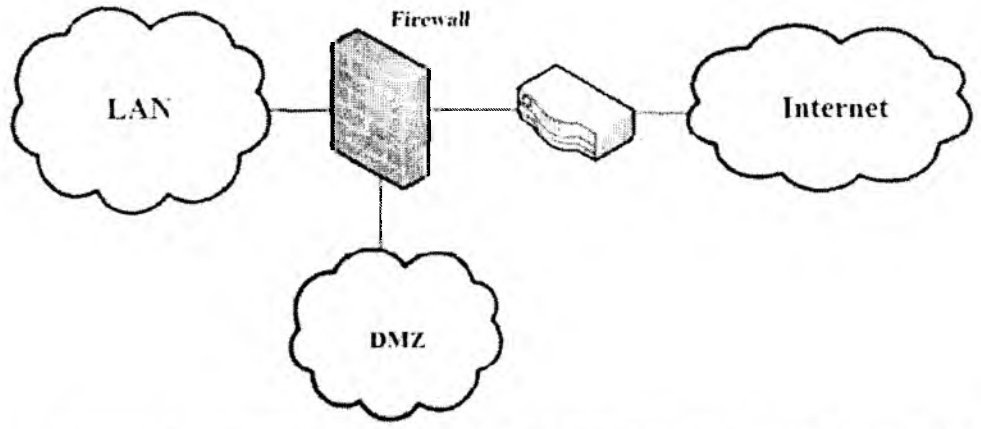

Рисунок 4 – Защита LAN и DMZ с помощью одного Firewall

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.

Материал поступил в редакцию 26.03.20.

М. А. Чуприна[1], А. Д. Тастенов[2], О. А. Андреева[3]

Телекоммуникациялық жүйелер автоматтандырылған басқару жүйесінің транспорттық ортасы ретінде және ақпараттық қауіпсіздік мәселелері

[1,2,3]Энергетика факультеті,
С. Торайғыров атындағы Павлодар мемлекеттік университеті,
Павлодар қ., 140008, Қазақстан Республикасы.
Материал 26.03.20 баспаға түсті.

M. Chuprina[1], A. Tastenov[2], O. Andreyeva[3]

Telecommunication systems as transport environment of automated control systems and problems of information security

[1,2,3]Faculty of Energy Engineering,
S. Toraighyrov Pavlodar State University,
Pavlodar, 140008, Republic of Kazakhstan.
Material received on 26.03.20.

Мақалада математикалық моделдеу әдісімен тік түсетін сыртқы сипаттамасы бар резонанстық ток көзінің өтпелі процестеріне зерттеу жүргізілді, резонанстық контур сыйымдылығының әртүрлі бірліктері мен мәндері кезінде токтың осциллограммалары алынды, модельдеу нәтижелеріне талдау жасалды.

The article deals with the study of transients of a resonant current source with a steeply falling external characteristic by the method of mathematical modeling, current waveforms are obtained at different q-values and capacitance values of the resonant circuit, the analysis of the simulation results is performed.

ГРНТИ 44.29.01

Б. К. Шапкенов[1], В. П. Марковский[2], А. П. Кислов[3], М. Б. Кайдар[4], А. Б. Кайдар[5], А. К. Жумадирова[6], О. Т. Кожанова[7], Р. М. Ирсымова[8], С. М. Иманбек[9]

[1]к.т.н., профессор, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;
[2]к.т.н., профессор, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;
[3]к.т.н., профессор, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;
[4]менеджер, ЗАО «Казтрансгаз», г. Нур-Султан, 010000, Республика Казахстан;
[5]м.т. и т., проектный менеджер, АО «Alageum Electric», г. Нур-Султан, Республика Казахстан;
[6]к.т.н., ассоц. профессор, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;
[7]магистрант, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;
[8]магистрант, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан;
[9]магистрант, Павлодарский государственный университет имени С. Торайгырова, г. Павлодар, 140008, Республика Казахстан
e-mail: [1]argin_intel@mail.ru; [2]wadim54@mail.ru; [4]m.kaidar@amangeldygas.kz; [5]argin_intel@mail.ru; [6]aliazk@mail.ru

МЕРЫ ОБЕСПЕЧЕНИЯ ЭЛЕКТРОБЕЗОПАСНОСТИ ПРИ КОСВЕННОМ ПРИКОСНОВЕНИИ

Применение малого напряжения, компенсации емкостных токов, защитного заземления, электрическое разделение сети, усиления рабочей изоляции, а также внедрения устройств защитного отключения и других средств позволяют повысить безопасность обслуживающего персонала.

Следует отметить, что все указанные средства уменьшают опасность поражения электрическим током, однако не обеспечивают полной безопасности работы.

Для научного обоснования объективных средств защиты от электропоражения необходимо исследовать условия возможного протекания тока через тело человека, определить закономерности