МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра Кибербезопасность, обработка и хранение информации

Қабдыкәрім Д.М.

Тема дипломного проекта
«Разработка сетевого фильтра в электросети 220В 50Гц от высокочастотного навязывания»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
к дипломному проекту

специальность 5В100200 – Системы информационной безопасности

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра Кибербезопасность, обработка и хранение информации

ДОПУЩЕН К ЗАЩИТЕ
Заведующий кафедрой
КБОиХИ
канд. техн. наук, доцент
_____ Н.А.Сейлова
«13» 05 2019 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к дипломному проекту

На тему: «Разработка сетевого фильтра в электросети 220В 50Гц от высокочастотного навязывания»

по специальности 5В100200 - Системы информационной безопасности

Выполнил Қабдыкәрім Д.М.

Рецензент
Председатель
КАИБ
_____ В.В. Покусов
«13» 05 2019 г.

Научный руководитель
сеньер-лектор
_____ С.А.Шалданбаев
«13» 05 2019 г.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

Казахский национальный исследовательский технический университет имени К.И.Сатпаева

Институт информационных и телекоммуникационных технологий

Кафедра Кибербезопасность, обработка и хранение информации

5В100200 - Системы информационной безопасности

УТВЕРЖДАЮ
Заведующий кафедрой КБОиХИ
канд. техн. наук, доцент
_____ Н.А.Сейлова
"_13_" _05_ 2019 г.

ЗАДАНИЕ
на выполнение дипломного проекта

Обучающемуся *Кабдыкәрім Диас Мержанұлы*
Тема: *Разработка сетевого фильтра в электросети 220В 50Гц от высокочастотного навязывания*
Утверждена *приказом Ректора Университета №1571-б от «20»102017 г.*
Срок сдачи законченной работы «___» _____ *2019 г.*
Исходные данные к дипломному проекту: *Заданная схема сетевого фильтра от высокочастотного навязывания от сети 220В*
Перечень подлежащих разработке в дипломном проекте вопросов:
а)изучение технических каналов утечки информации; б)исследование методов и средств защиты информации по цепям электропитания; в)разработка сетевого фильтра от высокочастотного навязывания от сети 220В;
Перечень графического материала (с точным указанием обязательных чертежей): *25 графических слайдов.*
Рекомендуемая основная литература: *1.Защита от утечки информации по техническим каналам», Бузов Г.А., Калинин С.В., Кондратьев А.В., Учебное пособие М.: Горячая линия – Телеком, 2005. 2. А.А.Хорев - "Технические средства и способы промышленного шпионажа", которое было впоследствии дополнено и вышло под названием "ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ. Часть 1. 3. Хорев А.А. Техническая защита информации/ учеб. пособие для студентов вузов/ в 3-х томах. – т. 1: Технические каналы утечки информации. - М.: НПЦ «Аналитика», 2008. - 436 с. 4. П.Хоровиц, У.Хилл Искусство схемотехники: Пер. с англ. – Изд.2-е. –М.: Издательство БИНОМ. – 2014 – 704 с.,*

ГРАФИК

подготовки дипломного проекта

Наименования разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Системы технической защиты	08.03.2019-15.03.2019	
Защита информации по цепям электропитания и заземления	16.03.2019-26.03.2019	
Разработка сетевого фильтра от сети 220В	07.04.2019-28.04.2019	

Подписи

консультантов и нормоконтролера на законченный дипломный проект с указанием относящихся к ним разделов проекта

Наименования разделов	Консультанты, И.О.Ф. (уч. степень, звание)	Дата подписания	Подпись
Нормоконтролер	А.А.Зиро	13.05.2019	

Научный руководитель _____ С.А.Шалданбаев

Задание принял к исполнению обучающийся _____ Д.М.Қабдыкәрім

Дата «13» мая 2019 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

ОТЗЫВ
НАУЧНОГО РУКОВОДИТЕЛЯ

на дипломный проект
(наименование вида работы)
Қабдыкәрім Д.М.
(Ф.И.О. обучающегося)
5В100200 - Системы информационной безопасности
(шифр и наименование специальности)

Тема: **«Разработка сетевого фильтра в электросети 220В 50Гц от высокочастотного навязывания»**

В современном мире безопасность IT-инфраструктуры отдельно взятого государства, предприятия, будь это обычные рабочие станции, сервера, локальные вычислительные сети, отдельные технические средства и т.д. становится актуальным. Будущим специалистам информационной безопасности необходимо знания и практические навыки обеспечения защиты информации в информационных системах.

Целью дипломного проекта является защита от высокочастотного навязывания по сети электропитания персонального компьютера, обрабатывающую конфиденциальную информацию, т.е. разработка и сборка макета сетевого фильтра 220В.

В работе студента Қабдыкәрім Д.М. полностью раскрыта классификация устройств съема информации от сети электропитания и средств защиты от них.. Разработана схемное решение и изготовлен макет сетевого фильтра 220В с мощностью до 10А тока. Цель достигнута, сетевой фильтр низких частот пропускает переменный ток до частоты 3,58 кГц, а все выше данного порога частоты понижаются до 30 дБ. Данное решение была взята за основу в изготовлении удлинителя с сетевым фильтром от 220В защищенного компьютера, разрабатываемой в настоящее время специалистами ТОО «Научно-производственное предприятие АСКБ Алатау».

Қабдыкәрім Д.М. показал хорошие теоретические и практические навыки в области информационной безопасности и схемотехники, разработал схемное решение, участвовал в монтаже и наладке устройства.

Дипломный проект на тему «Разработка сетевого фильтра на 220В от высокочастотного навязывания» выполнен Қабдыкәрім Д.М. на хорошем уровне и может быть допущен к защите.

Научный руководитель
Ведущий радиоинженер
ТОО «НПП АСКБ Алатау»
Сениор-лектор Шалданбаев С.А.

«13» 05 2019 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

РЕЦЕНЗИЯ

на дипломный проект
(наименование вида работы)
Қабдыкәрім Д.М.
(Ф.И.О. обучающегося)
5В100200 - Системы информационной безопасности
(шифр и наименование специальности)

На тему: **«Разработка сетевого фильтра в электросети 220В 50 Гц от высокочастотного навязывания»**

Выполнено:
а) графическая часть на 26 листах
б) пояснительная записка на 7 страницах

ЗАМЕЧАНИЯ К РАБОТЕ

Обеспечение технической защиты конфиденциальной информации, в частности защита от утечки по цепям электропитания является неотъемлемой частью системы обеспечения информационной безопасности коммерческих, частных и государственных учреждений. В условиях Республики Казахстан, данный аспект пользуется актуальностью, так как местному рынку информационной безопасности необходимы собственные разработки технических средств обеспечения защиты информации.

В данном проекте выявлена проблема и решена задача разработки устройства обеспечения защиты информации от утечки по цепям электропитания, которое защищает электрические цепи от высокочастотных и импульсных сигналов, посредством которых возможно перехватить критическую информацию. Для достижения этой цели, автором был рассмотрен собственно сам канал утечки информации, способы несанкционированного съема информации по этому каналу, меры защиты от них и виды технических средств, в частности, сетевые фильтры от сети 220В.

Важной особенностью дипломного проекта является, то что в нем рассматривается вопрос разработки устройства, а не использование уже существующих, которое фильтрует частотные составляющие выше частоты среза. Устройства собрано из недорогих элементов, что уменьшает экономические затраты и делает его простым в изготовлении, удобным в эксплуатации.

Все это повышает практическую ценность дипломной работы, которая выполнена качественно и технически грамотно. Пояснительная записка к работе, которая состоит из страниц и графические материалы выполнены в соответствии с требованиями ГОСТа.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
СӘТБАЕВ УНИВЕРСИТЕТІ

Оценка работы

Считаю, что Қабдыкәрім Д.М. выполнил дипломный проект на высоком инженерно-техническом уровне, заслуживает отличной оценки и присвоения ему степени Бакалавра военного дела и безопасности по специальности «Системы информационной безопасности».

Рецензент
Председатель
Казахстанской ассоциации
информационной безопасности _____ Покусов В.В

«13» 05 2019 г.

Краткий отчет

Университет:	Satbayev University
Название:	"Сетевой фильтр от высокочастотного навязывания от сети 220 В"
Автор:	Кабдукарим Диас
Координатор:	Саттар Шалданбаев
Дата отчета:	2019-05-02 10:58:18
Коэффициент подобия № 1:	**5,3%**
Коэффициент подобия № 2:	**0,0%**
Длина фразы для коэффициента подобия № 2:	**25**
Количество слов:	4 327
Число знаков:	34 101
Адреса пропущенные при проверке:	
Количество завершенных проверок:	5

К вашему сведению, некоторые слова в этом документе содержат буквы из других алфавитов. Возможно - это попытка скрыть позаимствованный текст. Документ был проверен путем замещения этих букв латинским эквивалентом. Пожалуйста, уделите особое внимание этим частям отчета. Они выделены соответственно.
Количество выделенных слов 2

Самые длинные фрагменты, определеные, как подобные

№	Название, имя автора или адрес гиперссылки *(Название базы данных)*	Количество Автородинаковых слов
1	URL_ https://studfiles.net/preview/4170603/page:3/	17
2	URL_ https://studfiles.net/preview/1669515/page:43/	15
3	URL_ http://it-security.admin-smolensk.ru/zinfo/info_or/	14
4	URL_ http://www.consultant.ru/document/cons_doc_LAW_2481/b6a297f676cd64a5eea867c45fb375fcb1dee3a5/	13

5	URL_ http://www.consultant.ru/document/cons_doc_LAW_2481/b6a297f676cd64a5eea867c45fb375fcb1dee3a5/	12
6	URL_ https://studfiles.net/preview/4170603/page:3/	11
7	URL_ https://studfiles.net/preview/4170603/page:3/	11
8	URL_ https://referat.bookap.info/work/133428/Zashhita-informacii-ot-utechki	11
9	URL_ https://studfiles.net/preview/4170603/page:3/	10
10	URL_ http://www.0zd.ru/gosudarstvo_i_pravo/dokumenty_i_tajna.html	10

Документы, в которых найдено подобные фрагменты: из RefBooks

Не обнаружено каких-либо заимствований

Документы,содержащие подобные фрагменты: Из домашней базы данных

Не обнаружено каких-либо заимствований

Документы,содержащие подобные фрагменты: Из внешних баз данных

Не обнаружено каких-либо заимствований

Документы,содержащие подобные фрагменты: Из интернета

Документы, выделенные жирным шрифтом, содержат фрагменты потенциального плагиата, то есть превышающие лимит в длине коэффициента подобия № 2

№	Источник гиперссылки	Количество одинаковых слов (количество фрагментов)
1	URL_ https://referat.bookap.info/work/133428/Zashhita-informacii-ot-utechki	69 (11)
2	URL_ https://studfiles.net/preview/4170603/page:3/	61 (6)
3	URL_ http://www.consultant.ru/document/cons_doc_LAW_2481/b6a297f676cd64a5eea867c45fb375fcb1dee3a5/	25 (2)
4	URL_ http://kzbydocs.com/docs/48/index-655617-4.html	16 (2)
5	URL_ https://studfiles.net/preview/1669515/page:43/	15 (1)
6	URL_ http://it-security.admin-smolensk.ru/zinfo/info_or/	14 (1)
7	URL_ http://nauchebe.net/2014/05/filtry-na-mikrosxemax-ou/	10 (2)
8	URL_ http://www.0zd.ru/gosudarstvo_i_pravo/dokumenty_i_tajna.html	10 (1)
9	URL_ https://rg.ru/2006/07/29/informacia-dok.html	6 (1)
10	URL_ https://online.zakon.kz/document/?doc_id=1009179	5 (1)

Протокол анализа Отчета подобия

заведующего кафедрой / начальника структурного подразделения

Заведующий кафедрой / начальник структурного подразделения заявляет, что ознакомился(-ась) с Полным отчетом подобия, который был сгенерирован Системой выявления и предотвращения плагиата в отношении работы:

Автор: Кабдукарим Диас

Название: "Сетевой фильтр от высокочастотного навязывания от сети 220 В"

Координатор: Саттар Шалданбаев

Коэффициент подобия 1:5,3

Коэффициент подобия 2:0

Тревога:2

После анализа отчета подобия заведующий кафедрой / начальник структурного подразделения констатирует следующее:

☑ обнаруженные в работе заимствования являются добросовестными и не обладают признаками плагиата. В связи с чем, работа признается самостоятельной и допускается к защите;
☐ обнаруженные в работе заимствования не обладают признаками плагиата, но их чрезмерное количество вызывает сомнения в отношении ценности работы по существу и отсутствием самостоятельности ее автора. В связи с чем, работа должна быть вновь отредактирована с целью ограничения заимствований;
☐ обнаруженные в работе заимствования являются недобросовестными и обладают признаками плагиата, или в ней содержатся преднамеренные искажения текста, указывающие на попытки сокрытия недобросовестных заимствований. В связи с чем, работа не допускается к защите.

Обоснование:

..... заимствования не обнаружено .....
.....
.....
.....
.....

....

Дата 13.05.22 *Подпись заведующего кафедрой /* КВДаки

начальника структурного подразделения

Окончательное решение в отношении допуска к защите, включая обоснование:

допущен к защите

Дата

Подпись заведующего кафедрой /

начальника структурного подразделения

АННОТАЦИЯ

В представленном дипломном проекте была рассмотрена тема разработки сетевого фильтра 220В 50Гц от высокочастотного навязывания.

В выполненном исследование представлен обзор и краткие характеристики существующих сетевых фильтров, объяснены физические принципы поиска, разработан сетевой фильтра 220В от высокочастотного навязывания, рассказано о возможностях дальнейшего совершенствования данного устройства.

АҢДАТПА

Берілген дипломдық жобада жоғары жиілікті байлаудан 220В 50Гц желілік сүзгіні әзірлеу тақырыбы қарастырылды.

Зерттеу барысында бар желілік сүзгілерге шолу және қысқаша сипаттама берілген, іздеудің физикалық принциптері түсіндірілген, жоғары жиілікті байлаудан 220В желілік сүзгісі әзірленген, осы құрылғыны одан әрі жетілдіру мүмкіндіктері туралы айтылды

ANNOTATION

In the presented thesis project was considered the theme of the development of a network filter 220V 50Hz from high-frequency imposing.

The study provides an overview and brief characteristics of the existing network filters, explains the physical principles of search, developed a network filter 220V from high-frequency imposing, describes the possibilities for further improvement of this device.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время пристальное внимание уделяется безопасности IT-инфраструктуры в целом, будь это обычные рабочие станции, сервера, локальные вычислительные сети, отдельные технические средства и др. Этому явлению есть простое объяснение, с развитием инфокоммуникационных технологий растет не только количество, но и качество атак злоумышленников, что неизбежно несет собой рост угроз информационной безопасности. Неэтичные действия со стороны недоброжелателей становятся все изощрённее и сложнее в предупреждении и далее в их расследование. Поэтому специалисты информационной безопасности должны перекрывать все возможные и невозможные пути обхода систем защиты критической информации.

Новые технологии таят в себе новые риски и угрозы для безопасности, как пользователей, так и мировых корпораций, и государств. Слова британского бизнесмена Натана Ротшильда «Кто владеет информацией, тот владеет миром», сказанные еще в первой половине XIX века, и сегодня не потеряли актуальность.

Защита информации по техническим каналам относится к развивающейся отрасти в области информационной безопасности. Вспомним историю, когда СССР восемь лет прослушивал рабочий кабинет посла США с помощью закладочного устройства. Это говорит о том, что это сфера начала свое развитие еще в начале XX века и продолжается по сей день. Основа физической сущности природы технической разведки, это процессы, связанные с обработкой, хранением, передачей возрастающих объемов информации, обусловливают побочные явления: поля рассеивания различной физической природы, наведение токов и напряжений на другие физические цепи. Указанные обстоятельства обусловливают повышение требований к показателям, а также методам и средствам, обеспечивающим защиту информации.

Данный дипломный проект посвящен разработке средства защиты информации по цепям электропитания, в частности сетевого фильтра 220В от высокочастотного навязывания для работы персонального компьютера, обрабатывающую конфиденциальную информацию.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Изучить методы и способы несанкционированного съема информации из сети электропитания;
2. Изучить теоретические аспекты источников питания;
3. Разработать принципиальную схему с применением САПР «Altium Designer»;
4. Выбрать радиоэлектронные компоненты и произвести монтаж макета сетевого фильтра;
5. Осуществить тестирования работоспособности сетевого фильтра.

1 Системы технической защиты

Концепция инженерно-технической защиты информации определяет основные положения, методы и средства обеспечения информационной безопасности объектов. Она представляет собой общий замысел и принципы обеспечения информационной безопасности объектов в условиях угроз и включает в себя:

- оценку угроз;
- систему защиты информации;
- принцип построения системы защиты информации.

Инженерно-техническая защита представляет собой совокупность людей, технических средств, политик по их использованию для защиты критической информации.

Эффективная техническая защита информационных активов есть неотъемлемая часть эшелонированной или комплексной системы управления информационной безопасностью и способствует повышению эффективности, с точки зрения экономических затрат для организации информационной безопасности. Техническая защита информации - это комплекс мероприятий по защите информации от несанкционированного доступа по различным каналам и для обеспечения трех главных принципов информационной безопасности, это конфиденциальность, целостность и доступность.

Утечка информации - это несанкционированный перенос информации от источника к злоумышленнику. Утечка информации может произойти посредством разглашения определенными индивидами, утерей людьми носителей конфиденциальной информации (флэш-карты, дисковые носители), переносом информации через физические поля, потоки частиц, веществ в агрегатных состояниях. Переносчиками информации возможны любые ее носители. В обычной жизни под понятием «утечка» понимают случайный процесс, например, как вытекание воды из сломанной системы водоснабжения. Данный подход является тривиальным. В профессиональной практике правоохранительных органов, есть факты организации утечки, к примеру, топлива с последующим списыванием его на якобы неработоспособность нефтепровода.

Утечка информационных активов в сравнении с утечкой материальных вещей имеет некоторые особенности, которыми не следует пренебрегать при организации защиты информации:

- факт утечки информации имеет место быть только при несанкционированном попадании ее к злоумышленнику, в сравнении, например, от утечки газа;
- при утечке, информация тиражируется, но не меняются характеристики носителя информации (не уменьшается количество листов, число пикселей изображения, размер и др. параметры);
- тиражирование во время утечки информации намного уменьшает стоимость информации;

– в случае неэффективной работы систем обеспечения безопасности, факт утечки информации, как правило, выясняется не сразу, а через некоторое время.

Первый пункт имеет немалое влияние для безопасности информации. Потому что, сама по себе утеря секретного документа, разглашения сведений, и другие действия не всегда приводят к утечке информации. К примеру, в случае ведения конфиденциальных переговоров во время брифинга или встреч в кабинете руководителя, разговор слышен в приемной из-за неплотно закрытой двери, а там нет посторонних людей, то факт утечки информации не наблюдается, хотя носитель информации (акустическая волна) выходит за пределы контролируемой зоны, то есть кабинета. Только в том случаем, когда в приемной будет находиться нежелательное лицо, воспользовавшейся услышанной информацией в неэтичных целях или поделиться, продаст заинтересованными людям и происходит утечка информации.

Исходя из этого, понятие «утечка информации» следует понимать правильно. То есть это не процесс распространения носителя информации за пределы определенной территории, а частный случай распространения, когда она попадает к злоумышленнику. Но вероятность выхода носителя информации за пределы заданной области создают условия для утечки информации и повышают угрозу информационной безопасности.

Физический путь переноса информации от источника к несанкционированному получателю, есть канал утечки. Канал, где утечка информации происходит с использованием технических средств, называется техническим каналом утечки. Несанкционированный перенос информации полями различной природы, макро- и микрочастицами происходит в технических каналах утечки информации.

1.1 Информация и ее классификация

Сегодня, есть много интерпретаций понятия «информация». В законе Республики Казахстан от 16 ноября 2015 года № 401 «О доступе к информации» дается следующая дефиниция: «Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах, полученные или созданные обладателем информации, зафиксированном на любом носителе и имеющие реквизиты, позволяющие ее идентифицировать» [8].

Информацию классифицируют по разным видам. С точки зрения категории доступа делится на общего пользования информацию и информацию ограниченного доступа, то есть на конфиденциальные данные и государственную тайну. В зависимости от распространения информация делится на:

– для всеобщего пользования;

– ограниченного пользования, предоставляемую по соглашению лиц, участвующих в определенных отношениях;

– в соответствии с законами РК, подлежащая предоставлению или распространению;

– ограниченную или же запрещенную на территории РК;

По назначению информация делится на:

– массовая информация – содержит простые сведения и оперирует данными, знакомыми большей части общества.

– специальная информация, которая содержит специфический набор понятий, непонятные основной доле общества, но необходимы и понятны в рамках какой-либо социальной группы, где эксплуатируется данная информация.

– секретная информация, доступ к которой, предоставлен ограниченному кругу лиц и по закрытым защищенным каналам.

– личная (персональная) – данные, об определенной личности, касающаяся социального положение, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных законами случаях.

Средства и системы защиты информации, необходимо применять конкретно к информации ограниченного доступа – это государственная тайна и конфиденциальные данные.

Согласно закону Республики Казахстан от 15 марта 1999 года N 349-1. «О государственных секретах» главе третьей.

«Перечень сведений, относимые к государственным секретам Республики Казахстан»:

1. Сведения в военной области;
2. Сведения в области экономики, науки и техники;
3. Сведения внешней политики и экономики;
4. Сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в зоне противодействия терроризму и обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной зашиты.

Перечень сведений, которые могут составлять конфиденциальную информацию, содержится в указе первого лица государства.

1.2 Канал утечки информации по цепям электропитания

Высока вероятность попадания критической информации, которая циркулирует в технических средствах (ТС) и вспомогательных технических средствах и системах (ВТСС) в цепи и сети электропитания, далее посредством их, выйти за пределы защищаемой зоны. К примеру, в линию электрического питания высокая частота имеет возможность передаваться через паразитные емкости трансформаторов блока питания.

Для их защиты, широкое применение получил метод развязки (разводки) цепей электропитания с помощью стабилизаторов, преобразователей, сетевых фильтров для определенных средств или помещений. В целях защиты и

локализации этого канала утечки информации, практикуют использование отдельных трансформаторных подстанций или узлов для снабжения электричеством объекта защиты, находящегося в зоне контролируемой территории. Правильное оборудование заземления - это одно из значительных требований защиты конфиденциальной информации по линиям заземления.

Заземление - это устройство, которое состоит из заземлителей проводников, соединяющих земли с электронными и электрическими устройствами, средствами, приборами. Они могут быть любой формы - в виде трубы, стержня, полосы, цилиндра и т.д., используются для защиты и соединения с землей средств защиты. Отношение напряжения заземлителя к току, который с него сходит, именуют сопротивлением заземления. Его величина прямо имеет зависимость от удельного сопротивления поверхности земли и площади соприкосновения заземления с землей. Линии заземления вне здания надо проводить примерно на глубине 1,5 - 2 м. Тогда как в здании - по стенам или определенным каналам так, чтобы их визуально осматривать на цельность и присутствие контактного присоединения. Исходя из лучших практик и опыта, необходимо отметить, что использование металлических конструкций здания, которые имеют соединение с землей, это могут быть системы отопления или водоснабжения, настоятельно не рекомендуется использовать как заземление.

Обстоятельства и возможные причины при которых образуется данный канал утечки информации (смотреть рисунок 1):

Рисунок 1 – Причины образования канала утечки информации по линиям электропитания

Кабели сетей электропитания соединяют различные рода технические средства и системы, которые размещены в разных местах, более того они как антенны, которые имеют особенность излучать или принимать электромагнитные поля.

Если используют сети электрического питания как соединяющие проводники, обычно имеет место использования сетевых закладных устройств. Этот тип «закладок» относят к устройствам, которые вставляют или же

встраивают в средства, питающиеся от сети 220В или в розетки, удлинители и т.д. Это устройство имеет в своем составе усилитель, микрофона и передатчик низкой частоты, данного рода частота используется в диапазоне от 10 до 350 (кГц). Передача и прием реализуется через одну фазу. А когда фазы разные, их объединяют по высокой частоте с помощью разделительной емкости. Приемник разрабатывают специально, но на практике в некоторых случаях используют доделанные узлы бытовых переговорных аппаратов. Такого рода закладные устройства имеют широкое применение в настоящее время, их не трудно маскировать под разные электроприборы, тяжело обнаружить специальными поисковыми средствами и не нуждаются в дополнительном источнике питания.

Когда сеть электропитания используют как линейные антенны, образуются два вида наводок: ассиметричные и симметричные.

Ассиметричные наводки (смотреть рисунок 1.2) имеют место быть, когда линии сети электрического питания источника и приемника наводки прокладываются совместно и имеют одинаковые емкости относительно источника и приемника наводки. Здесь наводятся единые напряжения по величине и по фазе касательно «земли» и корпуса технического средства.

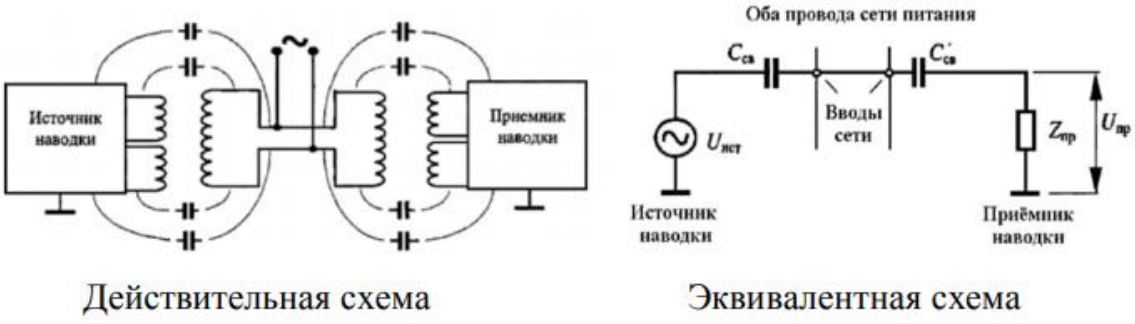

Рисунок 1.2 – Ассиметричная связь

Каждый из проводов сети электропитания, передают сигналы в одну сторону, обратным проводом будет «земля». Поэтому и называют их ассиметричными, либо однонаправленными.

Симметричное распространение наводки бывают, когда на проводах сети образуется разность потенциалов и токи по проводам текут в одну сторону, а в разные.

1.3 Высокочастотное навязывание

Высокочастотное навязывание (ВЧ-называние) – способ влияния на технические средства, посредством высокочастотных сигналов, эти сигналы подают специальным генератором ВЧ-сигналов.

Существует два способа ВЧ-навязывания:

1. Подключением контактов с высокочастотными сигналами в цепь электропитания, которая связана с техническим средством;
2. Посредством излучения ВЧ электромагнитного поля.

Вероятность снятия конфиденциальной информации высокочастотным навязыванием, обусловлена наличием в схемах технических средств нелинейных элементов. ВЧ сигналы действуют на эти элементы единовременно с низкими частотами, которые есть в работающих технических средствах, обрабатывающих критическую информацию.

2 Защита информации по цепям электропитания и заземления

Существуют активные, пассивные методы, так же организационные процессы и люди с соответствующим набором компетенций для обеспечения защиты конфиденциальной информации по линиям электрического питания. Пассивные методы это - сетевые фильтры и трансформаторы, экранирование и заземление, а к активным методам относят пространственное и линейное зашумление (смотреть рисунок 2). Рассмотрим более подробно данные методы.

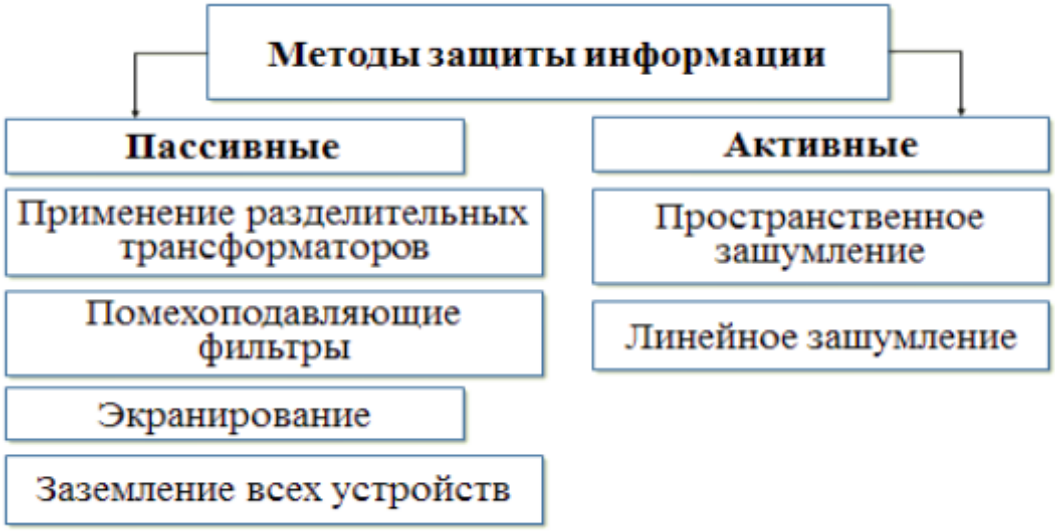

Рисунок 2 — Методы и средства защиты информации

2.1 Организационные меры

Одним из немаловажных моментов в организации системы управления информационной безопасностью, являются организационные меры.

На данном этапе необходимо:

– категорировать список информационных активов, подлежащих технической защите. Данная процедура определяется владельцем информации в согласно с законодательством Республики Казахстан;

– разработать обоснованный план по построению системы защиты информации, определить риски и угрозы, которые могут нанести ущерб защищаемой информации;

– выделить список помещений или зданий, где будет обрабатываться конфиденциальная информация;

– выделить список технических средств и систем, обрабатывающих критическую информацию;

– выделить список инженерных сооружений, технических средств, кабельных сетей, линий электропитания, заземления, которые не служат производственной необходимостью и демонтировать их;

– выделить используемые и неиспользуемые системы кабелей, электрических цепей и проводов, которые имеют выход за пределы контролируемой зоны;

По результатам обследования составляется произвольная форма отчета со списком выполненных действий:

– список технических средств, расположенных в защищаемых помещениях;

– подробный план защищаемого помещения, где указаны все места установок технических средств, схем кабельной системы и линий электрического питания;

– список технических средств и систем, кабельных сетей, электрических цепей и проводов, которые необходимо демонтировать.

Данный документ подписывается офицером безопасности или любым другим уполномоченным лицом, далее отдается на рассмотрение руководству организации.

2.2 Пассивные меры защиты

Технические меры делятся на активные и пассивные. К пассивным методам относят сетевые фильтры.

2.3 Сетевые фильтры.

Абсолютно каждый проводник, расположенный в выделенном помещении и выходящий за пределы контролируемого зоны, является своеобразной антенной. Эта антенна принимает и передает во вне, электромагнитные волны технических средств. С помощью специальных технических средств и систем можно перехватить информативный сигнал и прочитать информацию, находящуюся в ней. Эксплуатируя небезопасные линии и сети электрического питания, можно подвергнуться к высокочастотному навязыванию на свои компьютеры, тем самым поставить под угрозу утечки информационные активы своего бизнеса или государства. Сетевые фильтры уменьшают уровень информационного сигнала до безопасного состояния, то есть когда нельзя его перехватить и далее прочитать.

Фильтрацией называют преобразование сигнала, когда его полезные функции остаются, а небезопасные или нежелательные свойства подавляются. Существует много задач, которые решает фильтрация в практических условиях, в их число входят:

1) подавление шумов, которые скрывают полезный сигнал;

2) устранение искажения несущей частоты, вызванного низким качеством канала передачи или помехами;

3) разложение сигналов на частоты;

4) демодуляция сигналов;

5) преобразование дискретных сигналов в аналоговые;

Сетевой фильтр — техническое средство, которое фильтрует сигналы от импульсных и высокочастотных помех, содержит в себе два фильтрующих блока. Первый блок – это варисторный фильтр, который служит для фильтрации импульсных помех. Варисторы – полупроводниковые элементы, тоже самое что и резисторы, только их сопротивление прямо зависит от входящего напряжения: чем оно выше, тем ниже сопротивление. Второй блок – это LC – фильтр (где L – индуктивность, C - емкость). Состоит из конденсаторов, которые при скачке напряжения, заряжаются, а при падении наоборот отдают эту энергию, то есть разряжаются. Помехоподавляющие фильтры дают возможность ослаблять нелинейные сигналы в разных местах диапазона частот. Главная цель фильтра – пропускать сигналы в рабочей частоте и срезать после порога частоты среза.

Различают четыре вида фильтров, зависит от полосы пропускания фильтра от частоты среза (смотреть рисунок 2.1):

— фильтры нижних частот (ФНЧ) – идеальный ФНЧ пропускает все частоты $(0, \omega_{гр})$ до частоты среза, а далее подавляет $(\omega_{гр} ,\infty)$, (а);

— фильтры верхних частот (ФВЧ) – имеет обратные функции, пропускает частоты в диапазоне $(\omega_{гр},\infty)$ и режет их в диапазоне $(0, \omega_{гр})$, (б);

— полосовые (полосно-пропускающие)фильтры (ПФ) – пропускает только определенные частотные составляющие $(\omega_{гр1}, \omega_{гр2})$ и подавляет другие (в);

— заграждающие (режекторные) фильтры (ЗФ) – подавляет только определенный частотный диапазон $(\omega_{гр1}, \omega_{гр2})$, а другие частоты пропускать без изменений (г).

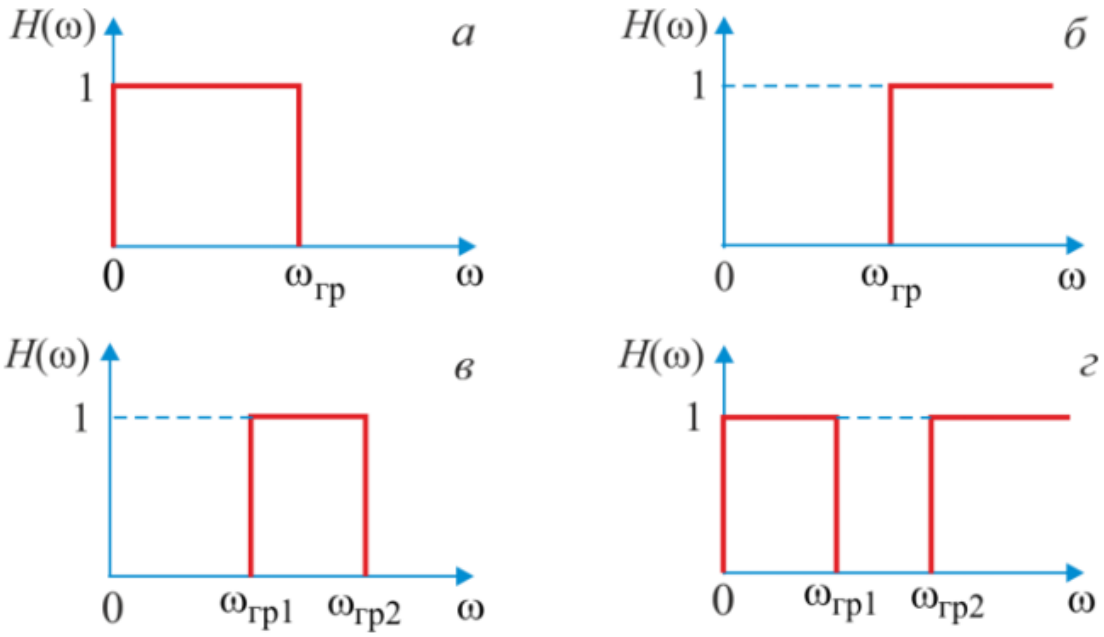

Рисунок 2.1 — Идеальные амплитудно- частотные характеристики (АЧХ) фильтров

Существуют фильтры разных структур, это Г, Т, П структуры. Самым простым является структура Г типа (смотреть рисунок 2.2), он состоит из двух элементов Z1 и Z2, которые являются сопротивлением току.

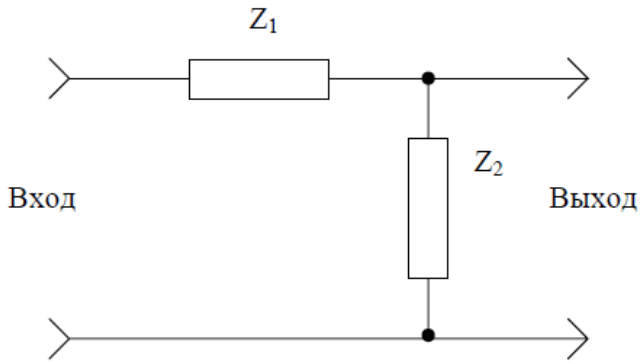

Рисунок 2.2 — Фильтр типа Г

На рисунке 2.3 показана структура сетевого фильтра Т- типа, состоящего из трех элементов, то есть добавляется дополнительный элемент.

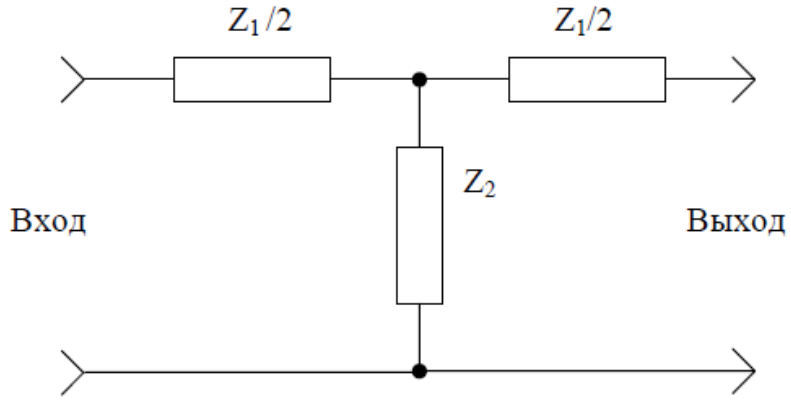

Рисунок 2.3 — Фильтр типа Т

В случае изменения соединения фильтра Т-типа, получается фильтр типа – П. Он показан на рисунке 2.4.

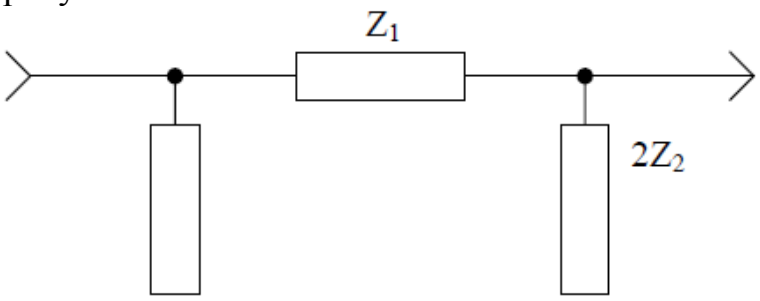

Рисунок 2.4 — Фильтр типа П

2.4 Принцип функционирования сетевых фильтров

Главная цель такого фильтра пропустить через себя ток с рабочей частотой сети электропитания, это 50-60 Гц, в зависимости от страны и континента и заодно отфильтровывая помехи (смотреть рисунок 2.5) и скачки напряжения, которых довольно много в сети.

Рисунок 2.5 — Импульсная помеха в сети электропитания

Так же амплитуда фазы выброса помехи бывают в сотни и тысячи вольт, которого достаточно, чтобы сгорело устройство. Их именуют импульсными либо быстрыми помехами. Существуют так же помехи, с относительно медленным изменением фазы в сети. Сетевой фильтр, не пропуская опасных скачков напряжения, защищает он них. Для медленных провалов напряжения, намного

лучше использовать стабилизаторы, в составе которых есть и фильтр, так как сетевой фильтр не может скомпенсировать медленные провалы. Для технических средств, более опасными будут импульсные помехи, рассмотрим подробнее концепцию построения сетевого фильтра. На рисунке 2.6 показана схема сетевого фильтра питания. Устройства промышленного типа имеют более сложную архитектуру, в зависимости от функционала и требований заказчиков.

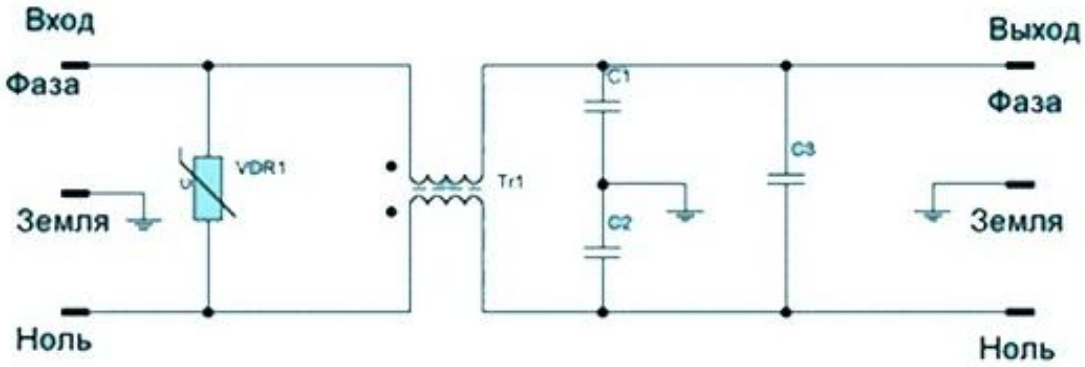

Рисунок 2.6 — Схема сетевого фильтра питания

Изучим схему подробнее. Смотря на схему видим, что на входе расположен элемент VDR1 — варистор. Его главной целью является подавление высоковольтных скачков напряжения электросети. При скачке напряжения сопротивление варистора падает, тем самым не позволяя пройти помехе дальше, замыкает ее. На практике варисторы, как правило, имплементируются в промышленных фильтрах. Среднее значение работы – 275-300 В, а максимальное значение сбрасывания – 350-385 В. Для помех, которые появляются при напряжении 230 – 300 В, используют так называемые LC-фильтры. В данной схеме это дроссель Tr1 и конденсаторы C1, C2, C3. В нашем случае, конденсаторы — «реактивные элементы», то есть, их сопротивление постоянному току или низким частотам другое, а к высокой частоте совершенно иное. Всем известно, что частота импульсной помехи во много превышает частоты сети питания (50-60 Гц), значит необходимо, чтобы ток беспрепятственно прошел через фильтр, а импульсные помехи были задержаны. С увеличением частоты тока, соответственно будет возрастать сопротивление LC-фильтра, и так будет происходит задержка помехи. В данном случае сеть питания имеет три провода: фазу, ноль и землю, а помехи возможны не только между 1 и 0, которые фильтрует конденсатор C3, но и между «1» и «землей». Чтобы эффективно бороться с такими помехами важна наличие физического заземления, а в сетевом фильтре — наличие фильтрующих конденсаторов C1 и C2. Эти емкости собирают помехи и не позволяют им пройти внутрь защищаемого устройства.

Необходимо отметить, что, если нет «земли», общая точка соединения конденсаторов C1 и C2 останется в «воздухе», что создаст емкостями и дросселем - паразитный колебательный контур, который будет излучать

высокочастотное электромагнитное поле, а наводки будут потенциальной опасностью для рядом стоящих технических средств.

2.4.1 Применение LC – фильтров

LC-фильтры имеют широкое применение в силовых электрических цепях. Они глушат помехи и сглаживают скачки напряжения после выпрямителя. В схемах радиоаппаратуры имеют место быть перестраиваемые LC-фильтры. К примеру, простой LC-контур, который включен на входе радиоприёмника дает возможность настраивать на конкретно радиостанцию.

Фильтры часто используются в звуковой аппаратуре, для коррекции амплитудно-частотной характеристики в эквалайзерах. В акустических системах делит сигналы низких, средних, высоких звуковых частот.

2.4.2 Выбор сетевого фильтра

Критериев выбора сетевых фильтров немало. Во-первых, важна электрическая характеристика системы, в которою фильтр устанавливается, способности эффективно подавлять помехи; частотные характеристики фильтруемой линии имеют огромную роль, это частота среза, предельная частота ослабления. Немаловажным являются условия эксплуатации.

Электронной промышленностью предлагаются:

- корпусные сетевые фильтры;
- помехоподавляющие изделия из феррита;
- соединители с экранированным фильтрами-контактами;

В Казахстане имеет место использование пассивных LC - фильтров Российского производства, такие как ФАЗА-1-10, ФАЗА-3Ф-10А (смотреть рисунок 2.7).

Сетевой фильтр ФАЗА-1-10 эксплуатируется для защиты информации по техническим каналам, в частности по цепям электрического питания, имеющими выход за пределы выделенной зоны, путем подавления наводок информативных сигналов.

Техническое средство выпускается с учетом требований безопасности военной аппаратуры. Имеет сертификат Гостехкомиссии РФ.

Рисунок 2.7 — Сетевой фильтр ФАЗА-1-10

Данный фильтр состоит из LC-фильтров. Работает при напряжении от 110 до 240 (В) с частотой 50-60 (Гц). Имеет возможность подключения трех потребителей. Ток утечки от 5 до 10 (мА), вес – 1,5 (кг).

2.5 Разделительный трансформатор

На рисунке 2.8 показано обозначение разделительного трансформатора электрической схеме.

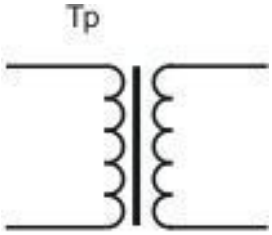

Рисунок 2.8 — Разделительный трансформатор

Разделительный трансформатор - это трансформатор, где первичная обмотка изолирована от вторичных обмоток, защитным электрическим разделением цепей с помощью двойной или усиленной изоляции. Другими словами, между обмотками есть заземленный металлический защитный экран, который выполняется как заземленная прокладка или обычная фольга. Если вторичная обмотка не заземлена, трансформатор будет считаться разделительным. Разделительный трансформатор с помощью средств экранирования и развязки, дают возможность ослабить информационный сигнал наводки на 126 дБ.

Разделительные трансформаторы используются для защиты электрических сетей, обеспечивают гальваническую развязку электрических цепей, дают возможность снизить токи короткого замыкания и подавляет

гармоники высокочастотного потенциала. Электрооборудование настоятельно рекомендуется подключать в сеть посредством такого трансформатора. Это обеспечит более длительную амортизацию продукта, надежность и электробезопасность.

К примеру, в ванных комнатах не должно быть источников питания на 220В. Потому что ванная комната опасна, из-за повышенной влажности, воды и т.д. Это прописано в «Правилах технической эксплуатации электроустановок». Но если есть такая необходимость в розетках, то их следует подключать через разделительный трансформатор.

2.6 Заземление

Заземление — это соединение нетоковедущих элементов устройства, то есть если изоляция испортится, они могут оказаться под напряжением. Состоит из заземлителя и заземляющего проводника, соединяющий заземляемое устройство с заземлителем. Заземлителем возможен быть обычный металлический стержень или непростой системой элементов специфического формата. Электрическое сопротивление линии земли – значение качества заземления, есть возможность его снижать, увеличивая площадь контакта или проводимость окружающей среды, посредством дополнительных стержней, повышением плотности соли в земле и др.

По линиям заземления может происходить утечка конфиденциальной информации (смотреть рисунок 2.9). Это бывает, когда общая «земля» является обратным проводом для других контуров.

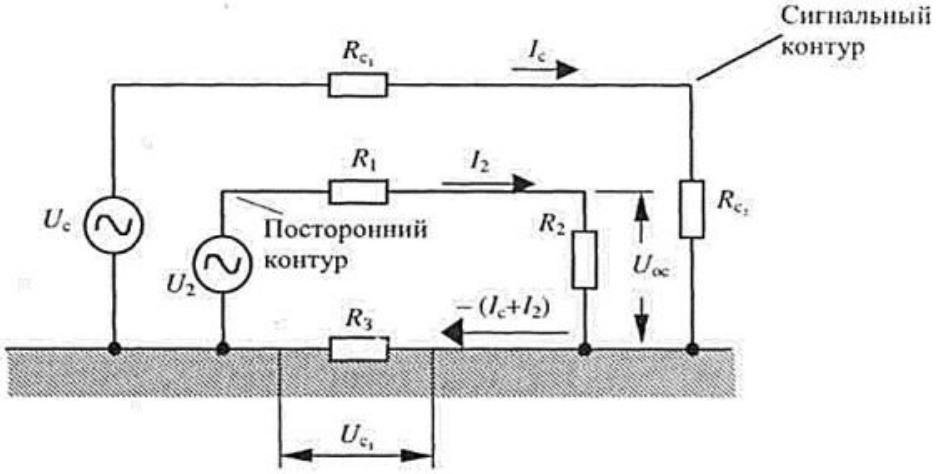

Рисунок 2.9 — Схема утечки информации по цепям заземления

Через «землю» проходит обратный ток полезного сигнала. В связи с конечным сопротивлением R3 падает напряжение, а фаза опасного сигнала увеличивается с увеличением сопротивления R3. Вероятность утечки есть из-за электромагнитного поля опасного сигнала в земле около заземлителя. Посредством существующих заземлителей можно перехватить полезный сигнал.

Два действия, на котором базируется защитное действие заземления:

1. Снижение разности напряжений до безопасного уровня между объектом заземления и иным проводящим средством, которое имеет естественную «землю».

2. При контакте «земли» устройства с проводом «фаза», происходит отвод тока. Обычно, при проектировании какой-либо системы, предусматривают срабатывание устройств защитного отключения (УЗО).

Это говорит о том, что заземление более эффективно функционирует с УЗО.

2.7 Экранирование

Экранирование — процесс локализации электромагнитных волн в пределах некой территории посредством преграждения ее пути определенными элементами (экранами). При экранировании конкретных элементов, к примеру, катушек индуктивности, проводов и др., как правило, есть необходимость в единовременном экранировании от электрического и магнитного составляющего тока.

Методы экранирования:

— электрическое;

— электромагнитное;

— магнитостатическое.

Такой способ является одним из эффективных средств обеспечения защиты информации по техническим каналам.

2.8 Активные меры защиты

Пассивные меры приводят к ослаблению уровня опасных сигналов, и тем самым уменьшают соотношение сигнал/шум. Однако, если пассивные методы защиты не удовлетворяет требованиям информационной безопасности, то в ход идут имплементация активных меры, которые основываются на линейном и пространственном зашумлении.

Пространственное зашумление исключает перехват информативного или полезного сигнала по электромагнитному каналу, посредством создания маскирующих помех в контролируемом пространстве, нерегулярную структуру помех. В устройствах обеспечения пространственного зашумления используется «белый шум», такие помехи имеют широкое применение в защите электронно-вычислительных машин. Там импульсы случайно амплитуды есть как помеховый сигнал, которые совпадают с по форме с полезным сигналом. Словом, происходит имитация помехи, который в спектральном плане соответствует сигналу.

Для предотвращения съема наведенных полезных сигналов с посторонних линий и проводников, имеющих выход за территорию контролируемого пространства, применяют линейное зашумление (смотреть рисунок 2.10).

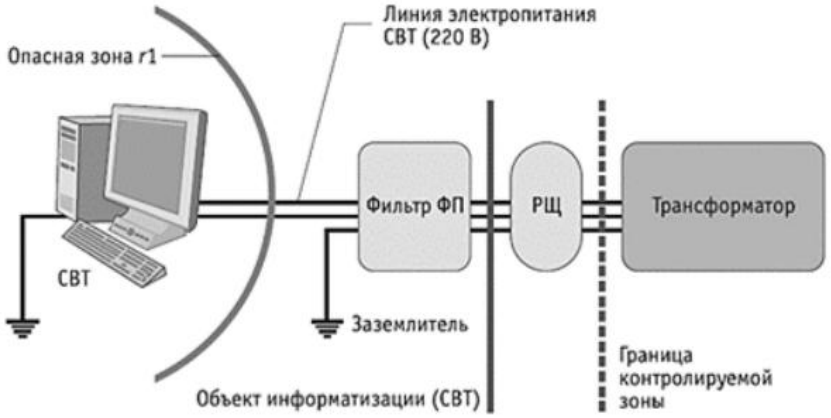

Рисунок 2.10 — Схема реализации генератора линейного зашумление линии электрического питания средств вычислительной техники

Система линейного зашумления – это генератор шума, который создает напряжение с определенными характеристиками, подключаемый гальванически м путем в линию зашумления. В практическом применении они в основном используются для защиты цепей электрического питания.

На рисунке 2.11 показан сетевой генератор шума «СОПЕРНИК», который в автоматическом режиме осуществляет обнаружение и подавление устройств несанкционированного съема конфиденциальной информации, которые передают информацию через сеть 220 В. Устройство работает в дежурном режиме, то есть постоянно осуществляет сканирование и анализ электросети 220 В.

Когда возникают высокочастотные сигналы в электросети, мгновенно загорается красная индикация, показывающий уровень информативного сигнала и одновременно с этим включается зеленая индикация, показывающая уровень зашумления, это, то самое противодействие от потенциальной угрозы. После понижения ВЧ-сигнала до определенного уровня, фильтр уходит в ждущий режим работы.

Рисунок 2.11 — ГШ «СОПЕРНИК»

3 Разработка сетевого фильтра от сети 220В

В практической части, необходимо разработать схему сетевого фильтра и собрать его.

3.1 Схема сетевого фильтра и принцип ее работы

Ниже приведенная схема сетевого фильтра от сети 220 В (смотреть рисунки 3, 3.1), которая была разработана в рамках данного дипломного проекта и начерчена в системе автоматизированного проектирования (САПР) Altium Designer.

Altium Designer – программное обеспечение для автоматизированного проетирования. Имеет удобный, современный интрефейс с огромными возможностями. В них входит: схемотехника устройства, 3D – дизайн печатных плат и много др.

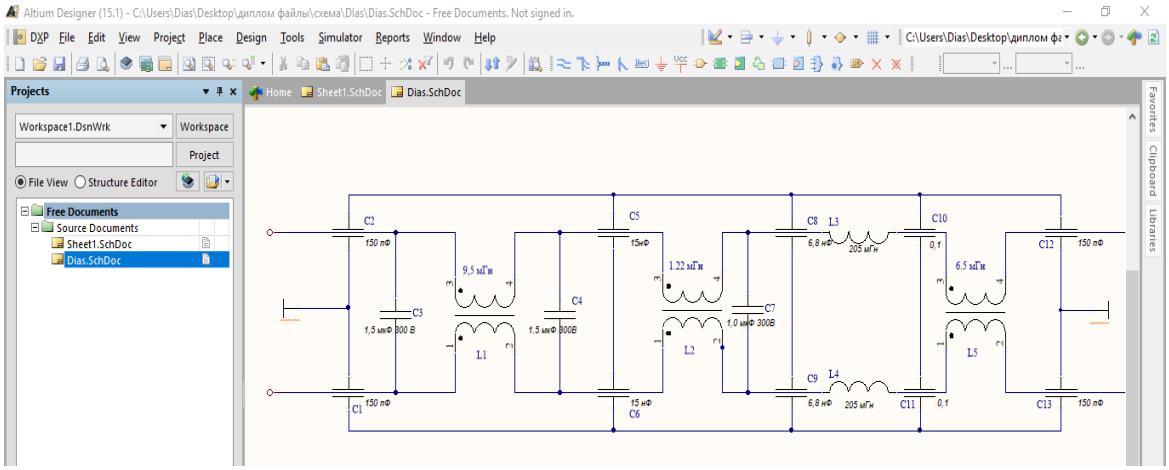

Рисунок 3 — Интерфейс САПР Altium Designer

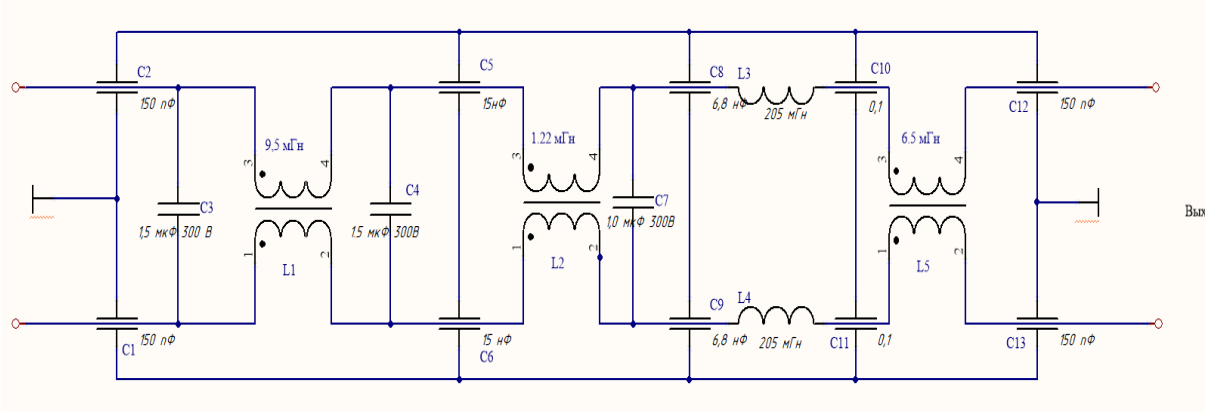

Рисунок 3.1 — Схема сетевого фильтра

В данном сетевом фильтре используются несколько LC – фильтров низких частот, это электрические цепи, которые состоят из индуктивностей (L) и емкостей (C). У нас на схеме это L1 - L5 – индуктивности и конденсаторы C1 – C13. Емкости C1, C2, C5, C6, C8, C9, C10, C11, C12, C13, тут используются в роли реактивных элементов, то есть, их сопротивление постоянному току или низким частотам другое, а к высокой частоте совершенно иное.

Всем известно, что частота импульсной помехи во много превышает частоты сети питания (50-60 Гц), значит необходимо, чтобы ток беспрепятственно прошел через фильтр, а импульсные помехи были задержаны. При увеличении частоты тока, сопротивление LC фильтров резко возрастает и данным образом происходит подавление помех, а реактивные элементы задерживают на себе высокочастотные помехи.

Чтобы добиться более лучшей помехоустойчивости, вставили устройство в металлический корпус и отделили LC – фильтры металлическими перегородками, в результате получился своеобразный экран.

3.2 Расчет LC – фильтра низких частот

Частота среза, относительно нулевой частоты вычисляется по формуле:

$$fc = \frac{1}{\pi\sqrt{LC}} \quad (1)$$

где π = 3,14, L - индуктивность, C – емкость;

Для начала, вычисляем общую индуктивность и емкость:

$$L = (9{,}5 + 1{,}22 + 6{,}5 + 205) = 222{,}22 \text{ мГн}$$
$$C = (1{,}5 + 1{,}5 + 1) = 4 \text{ мкФ}$$

Далее по формуле (1) рассчитываем частоту срезу:

$$fc = \frac{1}{\pi\sqrt{LC}} = \frac{1}{3{,}14\ \sqrt{222{,}22 * 4}} = \frac{1}{2791{,}08} = 3.58 \text{ кГц}$$

Характеристическое сопротивление фильтра к переменному току вычисляется по формуле:

$$R_x = \sqrt{\frac{L}{C}} \quad (2)$$

где L - индуктивность, С – емкость;

Расчет сопротивления по формуле (2):

$$R_x = \sqrt{\frac{L}{C}} = \sqrt{\frac{222{,}22}{4}} = \sqrt{55.555} = 7.45 \text{ Ом}$$

Индуктивность катушки фильра вычисляется по формуле (3):

$$L = \frac{C}{\pi f_c} \quad (3)$$

где, С – емкость, π = 3,14, f_c – частота среза;

Вычисляем по формуле (3):

$$L = \frac{C}{\pi f_c} = \frac{4}{3.14 * 3.58} = 0.355 \text{ мГн}$$

Емкость конденсатора ФНЧ, рассчитывается по формуле (4):

$$\text{C} = \frac{1}{\pi f_c \text{c}} \quad (4)$$

Вычисляем по формуле (4):

$$\text{C} = \frac{1}{\pi f_c \text{c}} = \frac{1}{3.14 * 3.58 * 4} = 0{,}0222 \text{ мкФ}$$

3.3 Тестирование фильтра в лаборатории

На рисунках 3.2, 3.3, 3.4 показан разработанный помехоподавляющий фильтр от сети 220В.

Рисунок 3.2 – Физическая реализация сетевого фильтра

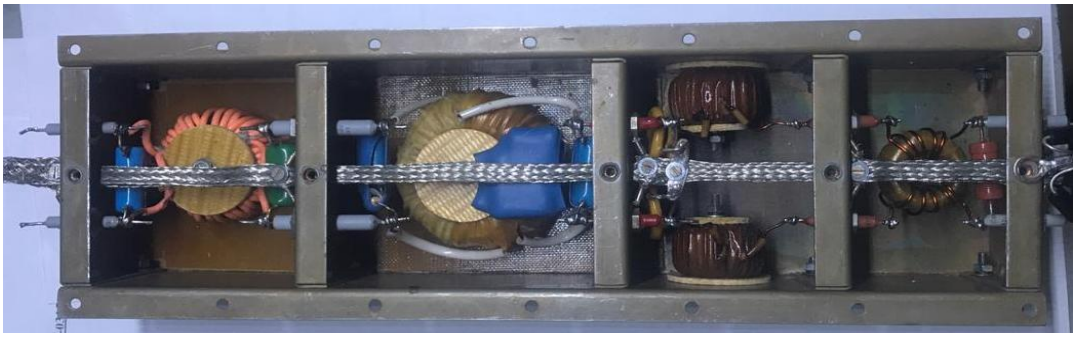

Рисунок 3.3 – Вид сверху на сетевой фильтр

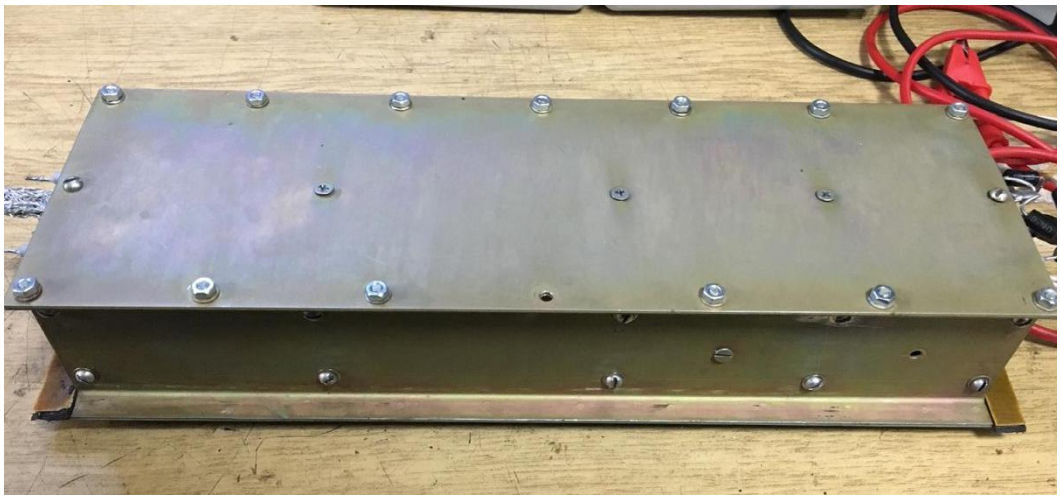

Рисунок 3.4 – Фильтр в закрытом корпусе

В процессе тестирования (смотреть рисунок 3.5) к сетевому фильтру подключили генератор сигналов, посредством которого на вход подавался

синусоидальный сигнал с разными частотными составляющими на входе, а на выходе измерили частоты пропускания и среза с помощью осциллографа. Подали частоты в диапазоне от 50 Гц до 3,58 кГц.

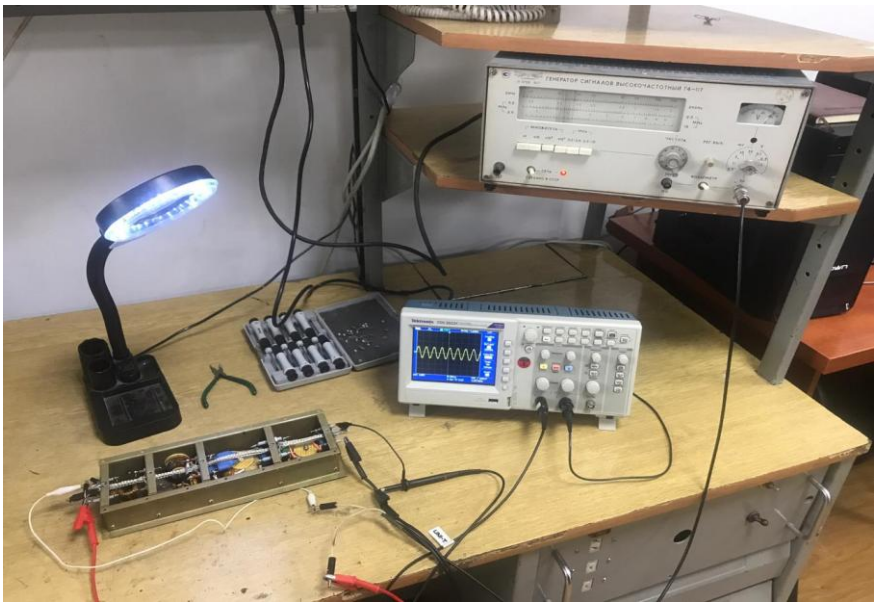

Рисунок 3.5 – Процесс тестирования

Тест показал следующий результат, пропускал все частоты (смотреть рисунок 3.6) до частоты 3,58 кГц. Расчеты сошлись на практике и сетевой фильтр соответствует рабочему диапазону.

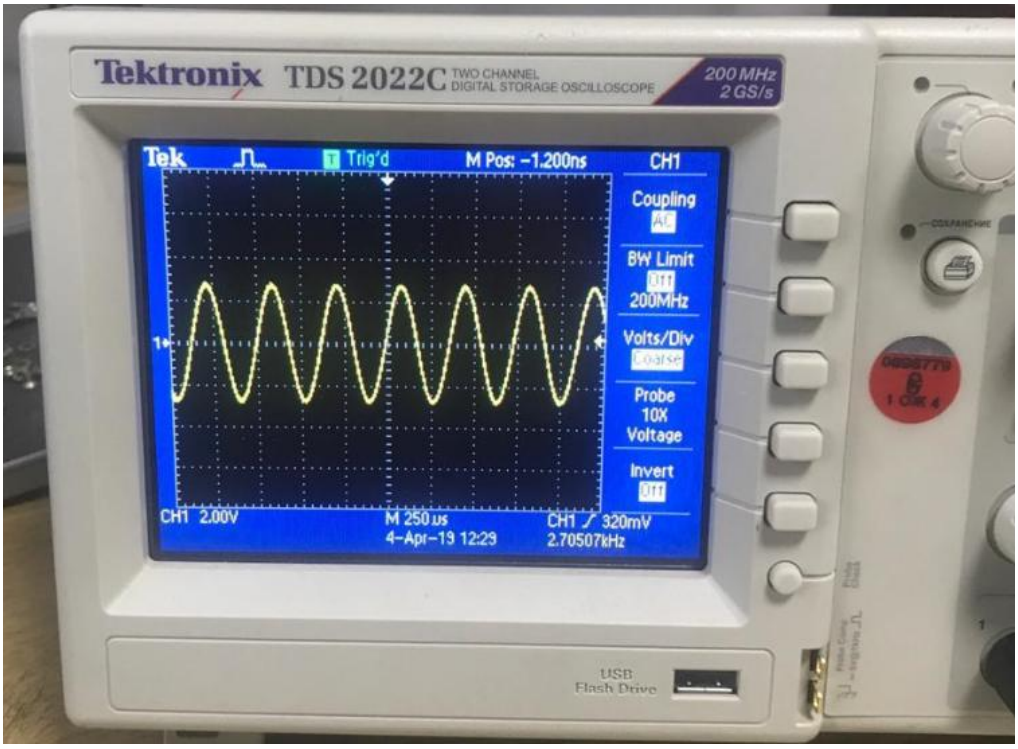

Рисунок 3.6 – Пропускание частот до частоты среза

Исходя из рисунка 3.7, видим, что фильтр с увеличением частоты подачи на вход, начал подавлять их.

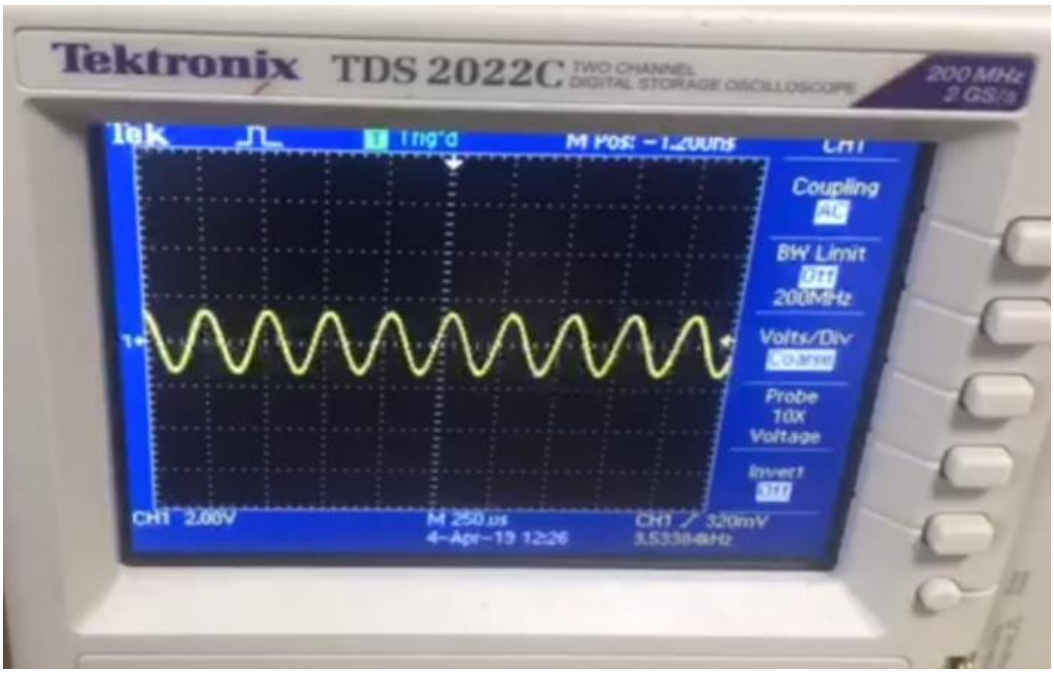

Рисунок 3.7 – Подавление частот после частоты среза

ЗАКЛЮЧЕНИЕ

В настоящее время вопросы информационной безопасности актуальны как никогда раньше. По последним данным, оборот рынка кибербезопасности составляет 167 миллиардов долларов, а к 2021 году он составит 202 миллиарда долларов. Такой быстрый рост, обуславливается все более растущей ролью информационной инфраструктуры.

В данной дипломной работе была рассмотрена тема разработки устройства сетевого фильтра от сети 220 вольт. Назначение, которого подавление высоких частот электросети частоты 50-60 Гц, что способствует пассивной защите технического канала утечки информации по линиям электропитания.

В процессе выполнения дипломной работы было достигнуто решение поставленных задач и данное решение была взята за основу в изготовлении удлинителя с сетевым фильтром от 220В защищенного компьютера, разрабатываемой в настоящее время специалистами ТОО «Научно-производственное предприятие АСКБ Алатау».

Практическая значимость данной разработки состоит в возможности применения данного устройства применение в разработках устройств для обработки конфиденциальной информации.

Исследование данного вопроса позволяет сделать следующие выводы:

- представлен обзор и краткие характеристики существующих сетевых фильтров;
- объяснен принцип работы этого технического средства;
- разработан сетевой фильтр от сети 220В с частотой среза от 3,58 кГц и выше;
- о возможностях дальнейшего совершенствования данного устройства.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1 А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков, С.В. Скрыль, И.В. Голубятников Технические средства и методы защиты информации Москва «Машиностроение» 2009 стр 105

2 Защиты информации от утечки по цепям питания//Электронная версия на сайте http://mirznanii.com/a/121257/zashchita-informatsii-ot-utechki-po-tsepyam-pitaniya

3 «Методы и средства инженерно-технической защиты информации», Аверченков В., Рытов М., Кувыклин А., Москва Издательство «ФЛИНТА», 2011г. Учебное пособие, 2-е издание.

4 П. Хоровиц, У. Хилл Искусство схемотехники: Пер. с англ. – Изд.2-е. – М.: Издательство БИНОМ. – 2014 – 704 с

5 А.А.Хорев - "Технические средства и способы промышленного шпионажа", которое было впоследствии дополнено и вышло под названием "ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ. Часть 1. Технические каналы утечки информации", 1997г

6 Защита информации от утечки по техническим каналам: учебное пособие / В.К.Железняк; ГУАП. - Спб., 2006. – 188 с.

7 Защита от утечки информации по техническим каналам», Бузов Г.А., Калинин С.В., Кондратьев А.В., Учебное пособие М.: Горячая линия – Телеком, 2005.

8 Высокочастотное навязывание//Электронная версия на сайте https://helpiks.org/5-8072.html

9 Закон Республики Казахстан от 16 ноября 2015 года № 401 «О доступе к информации»

10 Закон Республики Казахстан от 15 марта 1999 года N 349-1. «О государственных секретах»