Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

На правах рукописи

УДК 004.056.5

КАШАЛЕВИЧ
Светлана Юрьевна

МЕТОДЫ И АЛГОРИТМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО КАНАЛАМ ПОБОЧНЫХ ЭЛЕКТРОМАГНИТНЫХ ИЗЛУЧЕНИЙ

АВТОРЕФЕРАТ
диссертации на соискание степени
магистра техники и технологий

по специальности 1-39 81 01 – Компьютерные технологии
проектирования электронных систем

Минск 2017

Работа выполнена на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Научный руководитель: **ЦЫРЕЛЬЧУК Игорь Николаевич,**
кандидат технических наук, доцент, заведующий кафедрой проектирования информационно-компьютерных систем, декан факультета непрерывного и дистанционного образования учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»

Рецензент: **ТОНКОВИЧ Ирина Николаевна,**
кандидат химических наук, доцент, заведующая кафедрой информационных технологий учреждения образования «Минский инновационный университет»

Защита диссертации состоится «22» июня 2017 г. года в $10^{\underline{00}}$ часов на заседании Государственной комиссии по защите магистерских диссертаций в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники» по адресу: 220013, Минск, ул. П.Бровки, 6, копр. 1, ауд. 415, тел. 293-20-80, e-mail: kafpiks@bsuir.by

С диссертацией можно ознакомиться в библиотеке учреждения образования «Белорусский государственный университет информатики и радиоэлектроники».

ВВЕДЕНИЕ

Представить жизнь человека без электронных вычислительных средств достаточно сложно, но в тоже время растет и количество преступлений, связанных с хищением конфиденциальной информации, в том числе персональный данных и информации, представляющей коммерческую тайну.

Преступления в сфере хищения информации совершаются с использованием технических каналов утечки информации. Одним из таких каналов является канал побочных электромагнитных излучений, источниками которых могут являться элементы электронных устройств различного назначения. Перехватывая и декодируя эти излучения, можно получить сведения об информации, обрабатываемой электронным вычислительным средством. Различные способы криптографической защиты не позволяют в полной мере обеспечить конфиденциальность данных, так как данные выводятся на периферийные устройства в незашифрованном виде, что позволяет получить доступ к ним с использованием канала побочных электромагнитных излучений.

На сегодняшний день существует большое число работ в области защиты информации от утечки по каналам побочных электромагнитных излучений. Значимые результаты в этой области были получены такими российскими и белорусскими учеными, как Хорев А.А., Бузов Г.А., Калинин С.В., Кондратьев А.В, Зайцев А.П., Киреева Н.В., Семенов А.В., Цырельчук И.Н., Алефиренко В.М. Среди зарубежных исследователей можно выделить *Daniel Genkin*, *Lev Pachmanov, Itamar Pipman*, которые продемонстрировали возможность извлечения ключа дешифрования с использованием побочных электромагнитных излучений с компьютера, расположенного на некотором удалении.

Основываясь на вышесказанном, актуальным является формирование алгоритма защиты информации от утечки по каналам побочных электромагнитных излучений с использованием активных и пассивных методов защиты.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Количество электронной техники, применяемой для обработки, хранения и передачи информации, с каждым днем растет. Всевозможные элементы электронных устройств различного назначения могут являться источниками побочных электромагнитных излучений, перехватывая и декодируя которые, можно получить сведения об информации, обрабатываемой компьютером.

При этом различные способы криптографической защиты не позволяют в полной мере обеспечить конфиденциальность данных, так как данные выводятся на периферийные устройства в незашифрованном виде, что позволяет получить доступ к ним с использованием канала побочных электромагнитных излучений.

Рассмотрение вопросов защиты информации от утечки по каналам побочных электромагнитных излучений является актуальным на сегодняшний день.

Степень разработанности проблемы

Алгоритм защиты информации от утечки по каналам побочных электромагнитных излучений сформирован на основе активных и пассивных методов защиты информации, описанных в работах Хорева А.А., Бузова Г.А., Калинина С.В., Кондратьева А.В, Зайцева А.П., Киреевой Н.В., Семенова А.В., а также на результатах исследований *Daniel Genkin, Lev Pachmanov, Itamar Pipman*.

Одним из недостатков рассмотренных источников является отсутствие четко сформулированного алгоритма защиты информации от утечки по каналам побочных электромагнитных излучений.

Цель и задачи исследования

Целью диссертации является разработка алгоритма защиты информации от утечки по каналам побочных электромагнитных излучений.

Поставленная цель работы определяет следующие основные задачи:

1. Провести анализ каналов утечки информации.
2. Изучить существующие методы защиты информации от утечки по каналам побочных электромагнитных излучений.
3. Разработать алгоритм защиты информации от утечки по каналам побочных электромагнитных излучений.

Область исследования

Содержание диссертации соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-39 81 01 «Компьютерные технологии проектирования электронных систем».

Теоретическая и методологическая основа исследования

В основу диссертации легли работы белорусских и зарубежных ученых в области защиты информации от утечки по техническим каналам.

Информационная база исследования сформирована на основе литературы, открытой информации, технических нормативно-правовых актов, сведений из электронных ресурсов, а также материалов научных конференций и семинаров.

Научная новизна

Научная новизна и значимость полученных результатов работы заключается в формировании алгоритма защиты информации от утечки по каналам побочных электромагнитных излучений.

Теоретическая значимость работы заключается в детальном анализе способов утечки информации по каналам побочных электромагнитных излучений и методов ее защиты.

Практическая значимость диссертации состоит в предложенном алгоритме защиты информации от утечки по каналам побочных электромагнитных излучений.

Основные положения, выносимые на защиту

1. Принцип построения пассивных и активных методов защиты информации, основанный на анализе электромагнитного канала утечки информации, позволяющий рекомендовать программно-аппаратные комплексы измерения побочных электромагнитных излучений, технические средства пространственного и линейного зашумления, фильтрацию опасных сигналов, а также заземление и экранирование электронных вычислительных средств для защиты информации от ее перехвата по каналам побочных электромагнитных излучений.

2. Алгоритм организационно-технических мероприятий, позволяющий защитить информацию от утечки по каналам побочных электромагнитных излучений.

Апробация диссертации и информация об использовании ее результатов

Результаты исследований, вошедшие в диссертацию, докладывались на 12-ой Международной молодежной научно-технической конференции «Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2016» (Севастополь, Российская Федерация, 2016 г.) и XXI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов «Новые информационные технологии в научных исследованиях» (НИТ-2016) (Рязань, Российская Федерация, 2016 г.).

Публикации

Изложенные в диссертации основные положения и выводы опубликованы в 4 печатных работах. В их числе 4 статьи в сборниках материалов научных конференций.

Общий объем публикаций по теме диссертационной работы составляет 0,53 авторских листа.

Структура и объем работы

Диссертация состоит из введения, общей характеристики работы, трех глав с краткими выводами по каждой главе, заключения, библиографического списка и приложений.

В первой главе приведена классификация технических каналов утечки информации, рассмотрен электромагнитный канал утечки информации и способы утечки информации по этому каналу. **Во второй главе** представлены существующие методы и средства защиты информации от утечки по каналам побочных электромагнитных излучений. **В третьей главе** предложен алгоритм защиты информации от утечки по каналам побочных электромагнитных излучений. **В приложении** представлены публикации соискателя, акт внедрения и графический материал.

Общий объем диссертационной работы составляет 93 страницы. Из них 48 страниц основного текста, 31 иллюстрация на 13 страницах, 3 таблицы на 3 страницах, библиографический список из 35 наименований на 3 страницах, список собственных публикаций соискателя из 4 наименований на 1 странице, 3 приложений на 23 страницах.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы защиты информации от утечки по каналам побочных электромагнитных излучений (ПЭМИ), указаны основные направления исследований, проводимых по данной тематике, а также описано обоснование актуальности темы.

В **общей характеристике работы** показана актуальность проводимых исследований, степень разработанности проблемы, сформулированы цель и задачи диссертации, обозначена область исследований, научная (теоретическая и практическая) значимость исследований, а также апробация работы.

В первой главе представлены определения информации в области защиты и технического канала утечки информации, проведена классификация

технических каналов утечки информации. Рассмотрены такие причины возникновения электромагнитного канала утечки информации, как случайные акустоэлектрические преобразователи, паразитные связи и наводки, побочные низкочастотные и высокочастотные излучения.

Произведен анализ утечек информации по каналам ПЭМИ. Из анализа следует, что наиболее характерные ПЭМИ, вызванные работой генераторов тактовой частоты, можно наблюдать у средств вычислительной техники. Побочные электромагнитные излучения возникают при следующих режимах обработки информации средствами вычислительной техники: выводе информации на экран монитора; вводе данных с клавиатуры; записи информации на накопители; чтении информации с накопителей; передаче данных в каналы связи; выводе данных на периферийные печатные устройства – принтеры, плоттеры; записи данных от сканера на магнитный носитель.

Наиболее опасным (с точки зрения утечки информации) режимом работы средств вычислительной техники является вывод информации на экран монитора. Текст передается на экран в виде цифровых импульсов различной длительности. При прохождении по проводникам импульсных сигналов возникают побочные электромагнитные излучения.

Перехват информации осуществляется путем приема и детектирования средством разведки побочных электромагнитных излучений, возникающих при работе технических средств приема информации. Для перехвата ПЭМИ используются специальные портативные средства разведки.

Во второй главе представлены существующие методы защиты информации от утечки по каналам побочных электромагнитных излучений, среди которых выделяют два основных метода: активный и пассивный.

Активный метод основан на применении специальных передатчиков помех. Метод позволяет устранить не только угрозы утечки информации по каналам побочного излучения компьютера, но и многие другие угрозы.

Активный метод защиты информации направлен на создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях, а также в пространстве с целью уменьшения отношения сигнал/шум на границе контролируемой зоны до величин, обеспечивающих невозможность выделения средством разведки информационного сигнала.

Для исключения перехвата ПЭМИ по электромагнитному каналу используется пространственное зашумление, а для исключения съема наводок информационных сигналов с посторонних проводников и соединительных линий вспомогательных технических средств обработки, передачи и хранения информации – линейное зашумление.

Пространственное зашумление считается успешным, если отношение сигнал/шум на границе контролируемой зоны не превышает установленного значения, которое рассчитывается по специальным методикам для каждой частоты ПЭМИ средства обработки, передачи и хранения защищаемой информации.

В системах пространственного зашумления наиболее широко используются «синфазные помехи», в которых в качестве сигнала зашумления используются импульсы со случайной амплитудой, синхронизированные с импульсами защищаемого информационного сигнала. Таким образом генерируются, так называемые, имитационные помехи, по спектральному составу похожие на защищаемые сигналы.

В простейшем случае система линейного зашумления представляет собой генератор шумового сигнала, формирующий шумовое маскирующее напряжение с заданными спектральными, временными и энергетическими характеристиками, который гальванически подключается в зашумляемую линию (посторонний проводник).

Пассивный метод заключается в экранировании источника излучения, заземлении технических средств и фильтрации опасных сигналов.

Различают три вида экранирования:

– электростатическое;

– магнитостатическое;

– электромагнитное.

Электростатическое экранирование заключается в замыкании электростатического поля на поверхность металлического экрана и отводе электрических зарядов на землю (на корпус прибора) с помощью контура заземления.

Магнитостатическое экранирование осуществляется от постоянных и медленно меняющихся магнитных полей. Экраны изготавливают в основном из ферромагнитных материалов с большой магнитной проницаемостью. При наличии такого экрана силовые линии магнитного поля проходят в основном по его стенкам.

Упрощенная физическая сущность электромагнитного экранирования сводится к тому, что под действием источника электромагнитной энергии на стороне экрана, обращенной к источнику, возникают заряды, а в его стенках – токи, поля которых во внешнем пространстве противоположны полям источника и примерно равны ему по интенсивности. Два поля компенсируют друг друга.

Защитное действие заземления основано на двух принципах:

1) уменьшение до безопасного значения разности потенциалов между заземляемым проводящим предметом и другими проводящими предметами, имеющими естественное заземление;

2) отвод тока утечки при контакте заземляемого проводящего предмета с фазным проводом.

Фильтрация применяется к источникам электромагнитных полей и наводок с целью предотвращения распространения опасных сигналов за пределы контролируемой зоны. Для фильтрации в цепях питания технических средств применяются разделительные трансформаторы и помехоподавляющие фильтры.

В третьей главе представлен алгоритм измерения побочных электромагнитных излучений от средств вычислительной техники на основе специализированного программно-аппаратного комплекса «Навигатор-П5М».

Для обнаружения сигнала ПЭМИ описан экспертным методом, который реализует следующий алгоритм работы. Панорамы электромагнитной обстановки (с выключенным и включенным тестом) измеряются при использовании широких полос пропускания (10-100 кГц, на что расходуется 30-40 секунд). Находится любой информативный сигнал ПЭМИ и по нему максимально точно определяется частота первой гармоники. Далее производится сканирование частот всех гармоник с более узкой полосой пропускания с периодической подстройкой частоты первой гармоники по уточненной частоте более высших гармоник. Данный способ позволяет использовать максимальную чувствительность измерительного прибора и очень точно настраиваться на прогнозируемую частоту следующей гармоники.

После обнаружения сигналов ПЭМИ и коррекции их уровня необходимо перейти к расчетам требуемых значений. Для этого в программе существует соответствующий режим работы. В данном режиме могут решаться следующие задачи: расчет зон разведдоступности (*R*2, *R*1, *R*1'); расчет отношения сигнал/шум на границе контролируемой зоны; расчет требуемой защищенности цепей электропитания и заземления.

Результаты расчета соответствуют действующим нормативно-методическим документам. Протокол расчета выводится в *Microsoft Word* (из состава *Office* 2000) и во внутренний редактор программы.

В протоколе расчета кроме результатов расчета фиксируются те исходные данные и параметры, которые влияют на результаты расчета.

Проанализировав открытые источники был предложен алгоритм защиты информации от утечки по каналам ПЭМИ, представленный на рисунке 1.

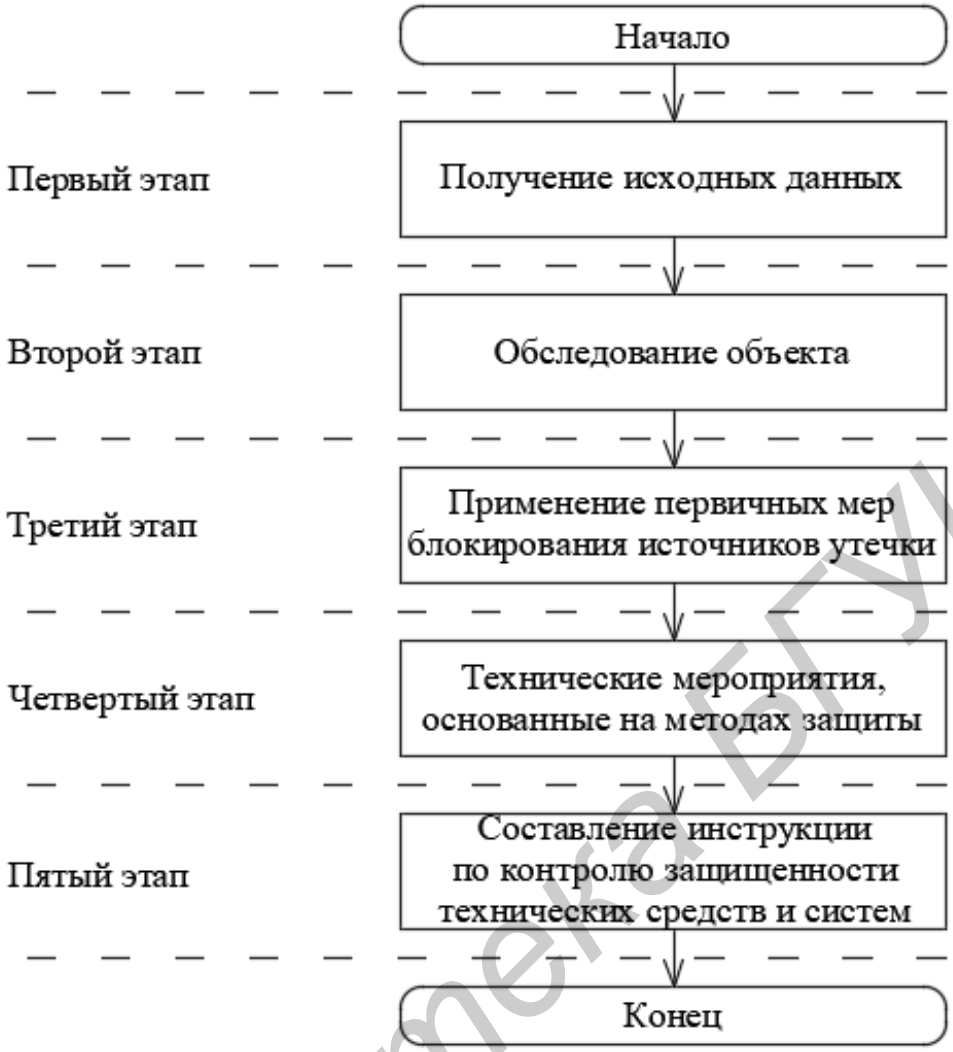

Рисунок 1 – Алгоритм защиты информации от утечки по ПЭМИ

Первым этапом является получение исходных данных об объекте.

Второй этап построения защиты объекта состоит в его обследовании по определенному алгоритму.

Третьим этапом построения защиты является применение первичных мер блокирования источников утечки информации по каналам ПЭМИ. Источниками утечки могут быть технические средства, описанные во второй главе, и кабельные линии, выходящие за пределы защищаемого объекта

Четвертым и основным этапом построения защиты являются технические мероприятия, основанные на методах защиты информации от утечки по каналам ПЭМИ, которые описаны во второй главе.

Оборудование для проведения описанных мероприятий подробно рассмотрено во второй главе.

Пятым и последним этапом построения защиты является составление инструкции по контролю защищенности технических средств и систем, смонтированных на объекте в соответствии с требованиями нормативно-правовых актов.

Требования к уровню защищенности объекта зависят от грифа секретности обрабатываемой и хранимой на объекте информации и его расположении.

ЗАКЛЮЧЕНИЕ

Основные научные результаты диссертации

1. Проведен анализ электромагнитного канала утечки информации, в результате которого выявлено, что с помощью лабораторного оборудования возможен перехват информации через побочное электромагнитное излучение с отображением перехваченных данных на приемном устройстве.

2. Изучены существующие методы защиты информации от утечки по каналам побочных электромагнитных излучений, которые позволяют рекомендовать программно-аппаратные комплексы измерения побочных электромагнитных излучений, технические средства пространственного и линейного зашумления, фильтрацию опасных сигналов, а также заземление и экранирование электронных вычислительных средств для защиты информации от ее перехвата по каналам побочных электромагнитных излучений.

3. Предложен алгоритм защиты информации от утечки по каналам побочных электромагнитных излучений.

Рекомендации по практическому использованию результатов

Полученные результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники» в учебный курс «Методы и технические средства обеспечения безопасности».

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1. Кашалевич, С.Ю. Методы защиты информации от утечки по каналам побочных электромагнитных излучений/ С.Ю. Кашалевич// Новые информационные технологии в научных исследованиях: материалы XXI Всероссийской научно-технической конференции студентов, молодых ученых и

специалистов, Рязань, Российская Федерация / ФГБОУ ВО «РГРТУ». – Рязань. 2016. – С. 222−224.

2. Кашалевич, С.Ю. Технические средства пространственного и линейного зашумления/ С.Ю. Кашалевич // Новые информационные технологии в научных исследованиях: материалы XXI Всероссийской научно-технической конференции студентов, молодых ученых и специалистов, Рязань, Российская Федерация / ФГБОУ ВО «РГРТУ». – Рязань. 2016. – С. 224−226.

3. Кашалевич, С.Ю. Методы защиты информации от утечки по техническим каналам/ С.Ю. Кашалевич// Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2016: материалы 12-я Международной молодежной научно-технической конференции, Севастополь, Российская Федерация / ФГБОУ ВО «СевГУ». – Севастополь. 2016. – С. 163.

4. Козлов, П. О. Средства защиты информации от утечки по техническим каналам/ П.О. Козлов, С.Ю. Кашалевич // Современные проблемы радиоэлектроники и телекоммуникаций, РТ-2016: материалы 12-я Международной молодежной научно-технической конференции, Севастополь, Российская Федерация / ФГБОУ ВО «СевГУ». – Севастополь. 2016. – С. 164.

РЭЗЮМЭ

Кашалевіч Святлана Юр'еўна

Метады і алгарытмы абароны інфармацыі ад уцечкі па каналах пабочных электрамагнітных выпраменьванняў

Ключавыя словы: абарона інфармацыі, пабочныя электрамагнітныя выпраменьванні.

Мэта працы: распрацоўка алгарытму абароны інфармацыі ад уцечкі па каналах пабочных электрамагнітных выпраменьванняў.

Атрыманыя вынікі і іх навізна: праведзены аналіз электрамагнітнага канала уцечкі інфармацыі. Выяўлена, што з дапамогай лабараторнага абсталявання, магчым з'ем інфармацыі праз пабочнае электрамагнітнае выпраменьванне з адлюстраваннем перахопленых дадзеных на прыёмным прыборы. Вывучаны існуючыя метады абароны інфармацыі ад уцечкі па каналах пабочных электрамагнітных выпраменьванняў, якія дазваляюць рэкамендаваць праграмна-апаратныя комплексы вымярэння пабочных электрамагнітных выпраменьванняў, тэхнічныя сродкі прасторавага і лінейнага зашумлення, фільтраванне небяспечных сігналаў, а таксама зазямленне і экранаванне электронных вылічальных сродкаў для абароны інфармацыі ад яе перахопу па каналах пабочных электрамагнітных выпраменьванняў. Прапанаваны алгарытм абароны інфармацыі ад уцечкі па каналах пабочных электрамагнітных выпраменьванняў.

Ступень выкарыстання: вынікі ўкаранёны ў навучальны працэс на кафедры праектавання інфармацыйна-камп'ютэрных сістэм ўстановы адукацыі «Беларускі дзяржаўны універсітэт інфарматыкі і радыёэлектронікі» ў навучальны курс «Метады і тэхнічныя сродкі забеспячэння бяспекі».

Вобласць ужывання: абарона інфармацыі.

РЕЗЮМЕ

Кашалевич Светлана Юрьевна

Методы и алгоритмы защиты информации от утечки по каналам побочных электромагнитных излучений

***Ключевые слова*:** защита информации, побочные электромагнитные излучения.

***Цель работы*:** разработка алгоритма защиты информации от утечки по каналам побочных электромагнитных излучений.

***Полученные результаты и их новизна*:** произведен анализ электромагнитного канала утечки информации. Выявлено, что с помощью лабораторного оборудования, возможен съем информации через побочное электромагнитное излучение с отображением перехваченных данных на приемном устройстве. Изучены существующие методы защиты информации от утечки по каналам побочных электромагнитных излучений, которые позволяют рекомендовать программно-аппаратные комплексы измерения побочных электромагнитных излучений, технические средства пространственного и линейного зашумления, фильтрацию опасных сигналов, а также заземление и экранирование электронных вычислительных средств для защиты информации от ее перехвата по каналам побочных электромагнитных излучений. Предложен алгоритм защиты информации от утечки по каналам побочных электромагнитных излучений.

***Степень использования*:** результаты внедрены в учебный процесс на кафедре проектирования информационно-компьютерных систем учреждения образования «Белорусский государственный университет информатики и радиоэлектроники в учебный курс «Методы и технические средства обеспечения безопасности».

***Область применения*:** защита информации.

SUMMARY

Kashalevich Svetlana Yuryevna

Methods and algorithms for protection of information from leakage through the channels of secondary electromagnetic emissions

***Keywords*:** protection of information, secondary electromagnetic emissions.

***The object of study*:** development of algorithm of protection of information from leakage through the channels of secondary electromagnetic radiations.

***The results and novelty*:** the analysis of electromagnetic channels of information leakage. It is revealed that with the help of laboratory equipment, possible removal of information through the secondary electromagnetic radiation, displaying the captured data in the receiving device. Studied the existing methods of information protection from leakage through the channels of secondary electromagnetic radiation, which allow us to recommend hardware and software packages measuring side electromagnetic radiation, means for spatial and linear noise filtering hazardous signals as well as grounding and shielding of electronic computers to protect information from being intercepted through the channels of secondary electromagnetic radiations. Proposed algorithm of information protection from leakage through the channels of secondary electromagnetic radiations.

***Degree of use*:** the results implemented in the educational process at the department of design information and computer systems educational institution «Belarusian State University of Informatics and Radio Electronics» in the training course «Methods and technical means of ensuring safety»

Sphere of application: protection of information.