Министерство образования Республики Беларусь

Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет заочного обучения

Специальность: Вычислительные машины системы и сети **1-40 02 01**

КОНТРОЛЬНАЯ РАБОТА

По курсу “Основы защиты информации”

Вариант № 5

Выполнил: Полховский А. Ф.
Студент группы 990541
Контакты: art.polhovsky@gmail.com
+375293465080

Проверил: Тимофеев А. М.
Преподаватель, кандидат технических наук,
доцент кафедры защиты информации

Минск 2022

СОДЕРЖАНИЕ

Тема 5: «Инженерно-технические методы защиты информации»

1. Классификация методов защиты информации.

2. Скрытие информации путем ее физической защиты, противодействия наблюдению, подслушиванию и утечке по вещественному каналу.

3. Экранирование побочных излучений и наводок.

ВВЕДЕНИЕ

Сегодня информацию считают основной ценностью. Ее относят к разряду важнейших ресурсов, сохранность которых является насущной задачей. Чем крупнее организация или сообщество, тем больше усилий прилагается для защиты информации. Попытки хищения или иные варианты враждебного использования сведений предпринимаются часто. Их цели различаются, но последствия всегда отрицательные.

Существует много способов хранения данных – от простых бумажных документов до электронных информационных массивов. Для обеспечения информационной безопасности нужны соответствующие организационные меры и технические средства. В этом направлении разработано множество мероприятий, протоколов защиты. Они реализуются в разных форматах и образуют комплексные системы.

Как было уже сказано, в целом, защита информации – это любая деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Наличие инженерно-технической защиты информации стало необходимым требованием для безопасной работы многих предприятий, бизнесов, сообществ, государств. Системы защиты приобрели ведущую роль в предотвращении утечек важных данных, поэтому ей выделяют значительную часть средств на постоянное совершенствование.

В данном реферате я постараюсь подробно рассмотреть классификации инженерно-технических методов зашиты информации, разобраться какие методы и почему являются самыми надежными, целесообразными, широко-используемыми.

1. ИНФОРМАЦИЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ПОНЯТИЕ ЗАЩИТЫ ИНФОРМАЦИИ, ЕЕ СУЩНОСТЬ

Информация, первоначально это сведения, передаваемые людьми устным, письменным или другим способом — с помощью условных сигналов, технических средств и т.д., включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передача признаков от клетки к клетке, от организма к организму и т.д.

Согласно традиционной философской точке зрения, информация существует независимо от человека и является свойством материи. Она рассматривается, как отражение объектов материального мира, в частности, отражение организованности или упорядоченности кибернетических объектов. Согласно нетрадиционной точке зрения информация трактуется как первооснова микро и макромира Вселенной (информация — первична, а материя — вторична). Она существует независимо от нас и проявляется в триедином процессе фундаментального взаимодействия энергии, движения и массы в пространстве и во времени.

Под информацией надо понимать сведения, являющиеся объектом сбора (накопления), хранения, обработки (преобразования), а также непосредственного использования и передачи.

Определению информации как сведений разного рода, представленных в любой форме и являющихся объектами различных процессов, наиболее соответствуют следующие трактовки понятий «безопасность информации», «защита информации».

Безопасность информации — это свойство (состояние) передаваемой, накапливаемой, обрабатываемой и хранимой информации, характеризующее ее степень защищенности от дестабилизирующего воздействия внешней среды (человека и природы) и внутренних угроз, то есть ее конфиденциальность (секретность, смысловая или информационная скрытность), сигнальная скрытность (энергетическая и структурная) и целостность — устойчивость к разрушающим, имитирующим и искажающим воздействиям и помехам (Рис.1.1)

Под защитой информации, в более широком смысле, понимают комплекс организационных, правовых и технических мер по предотвращению угроз информационной безопасности и устранению их последствий.

Сущность защиты информации состоит в выявлении, устранении или нейтрализации негативных источников, причин и условий воздействия на информацию. Эти источники составляют угрозу безопасности информации. Цели и методы защиты информации (гл. II.-1., II.-2.) отражают ее сущность.

В этом смысле защита информации отождествляется с процессом обеспечения информационной безопасности, как глобальной проблемы безопасного развития мировой цивилизации, государств, сообществ людей, отдельного человека, существования природы.

Рисунок 1.1 – Информация, информационная безопасность

При этом понятие информационная безопасность характеризует состояние (или свойство) информационной защищенности человека, общества, природы в условиях возможного действия угроз и достигается системой мер, направленных на:

- на предупреждение угроз. Предупреждение угроз — это превентивные меры по обеспечению информационной безопасности в интересах упреждения возможности их возникновения;
- на выявление угроз. Выявление угроз выражается в систематическом анализе и контроле возможности появления реальных или потенциальных угроз и своевременных мерах по их предупреждению;
- на обнаружение угроз. Обнаружение имеет целью определение реальных угроз и конкретных преступных действий;
- на локализацию преступных действий и принятие мер по ликвидации угрозы или конкретных преступных действий;
- на ликвидацию последствий угроз и преступных действий.

Предупреждение возможных угроз и противоправных действий может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами

Предупреждение угроз возможно и путем получения информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других элементах преступных деяний.

В предупреждении угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

Выявление имеет целью проведение мероприятий по сбору, накоплению и аналитической обработке сведений о возможной подготовке преступных действий со стороны криминальных структур или конкурентов на рынке производства и сбыта товаров и продукции.

Обнаружение угроз — это действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, а также фактов разглашения конфиденциальной информации или случаев несанкционированного доступа к источникам коммерческих секретов.

Пресечение или локализация угроз — это действия, направленные на устранение действующей угрозы и конкретных преступных действий. Например, пресечение подслушивания конфиденциальных переговоров за счет акустического канала утечки информации по вентиляционным системам.

Ликвидация последствий имеет целью восстановление состояния, предшествовавшего наступлению угрозы. Например, возврат долгов со стороны заемщиков. Это может быть и задержание преступника с украденным имуществом, и восстановление разрушенного здания от подрыва и др.

Все эти способы имеют целью защитить информационные ресурсы от противоправных посягательств и обеспечить:

- предотвращение разглашения и утечки конфиденциальной информации;
- воспрещение несанкционированного доступа к источникам конфиденциальной информации;
- сохранение целостности, полноты и доступности информации;
- соблюдение конфиденциальности информации;
- обеспечение авторских прав.

Учитывая вышесказанное про защиту информации, можно определить как совокупность методов, средств и мер направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов.

Защищаемая информация включает сведения, составляющие государственную, коммерческую, служебную и иные охраняемые законом тайны. Каждый вид защищаемой информации имеет свои особенности в области регламентации, организации и осуществления этой защиты.

Наиболее общими признаками защиты любого вида охраняемой информации являются следующие:

– защиту информации организует и проводит собственник или владелец информации или уполномоченные им на то лица (юридические или физические);
– защитой информации собственник охраняет свои права на владение и распоряжение информацией, стремится оградить ее от незаконного завладения и использования в ущерб его интересам;
– защита информации осуществляется путем проведения комплекса мер по ограничению доступа к защищаемой информации и созданию условий, исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям.

Таким образом, защита информации — есть комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям (рисунок 1.2)

Рис 1.2 – Иллюстрация мер по защите информации (в сети)

Защищаемая информация, являющаяся государственной или коммерческой тайной, как и любой другой вид информации, необходима для управленческой, научно-производственной и иной деятельности. В настоящее время перед защитой информации ставятся более широкие задачи: обеспечить безопасность информации. Это обусловлено рядом обстоятельств, и в первую очередь тем, что все более широкое распространение в накоплении и обработке защищаемой информации получают ЭВМ, в которых может происходить не только утечка информации, но и ее разрушение, искажение, подделка, блокирование и иные вмешательства в информацию и информационные системы.

Следовательно, под защитой информации следует также понимать обеспечение безопасности информации и средств информации, в которых накапливается, обрабатывается и хранится защищаемая информация.

- Таким образом, защита информации — это деятельность собственника информации или уполномоченных им лиц по:
- обеспечению своих прав на владение, распоряжение и управление защищаемой информацией;
- предотвращению утечки и утраты информации;
- · сохранению полноты, достоверности, целостности защищаемой информации, ее массивов и программ обработки;
- сохранению конфиденциальности или секретности защищаемой информации в соответствии с правилами, установленными законодательными и другими нормативными актами.

2. ВОЗМОЖНЫЕ УГРОЗЫ. СРЕДСТВА ЗАЩИТЫ. МЕРЫ ПО ЗАЩИТЕ ИНФОРМАЦИИ.

2.1 Источники угрозы

Независимо от способа хранения, основной угрозой для деловой или конфиденциальной информации является доступ посторонних пользователей. Данные могут существовать в разных формах, например: в виде баз данных, потоков сильно- и слабо-зашифрованных данных, физические текстовые документы; электронные файлы, хранящиеся в памяти компьютеров или на серверах; файлы, находящиеся на внешних носителях – жестких дисках, твердотельных накопителях, флешках и др.

Существуют разные виды несанкционированного доступа: целенаправленное обращение к базам данных, совершенное с целью их использования; случайный доступ, вызванный сбоем систем технической защиты информации.

Оба варианта одинаково недопустимы. В результате таких ситуаций возникает возможность несанкционированного изменения, копирования, тиражирования информационных ресурсов.

Различают несколько источников угроз:

- человеческий фактор;
- сбой компьютерных систем защиты;
- природные катаклизмы, стихийные бедствия, в результате которых штатные средства контроля оказались неэффективными.

Основную проблему представляет антропогенный фактор, и понятно почему.

В преступных же схемах могут быть задействованы как посторонние люди, так и недобросовестные сотрудники организации. Нередко в потере важных сведений оказываются виноваты доверенные лица компании, которые преследовали собственную выгоду. Известно немало примеров подобных действий, когда конфликтные ситуации или корысть побуждают людей использовать данные в собственных целях. Такие угрозы представляют собой наивысшую опасность, отследить враждебные намерения могут не все средства защиты информации. Поэтому, помимо обычных способов контроля и управления деятельностью информационных систем, важно учитывать психологию и мотивацию сотрудников.

2.2 Средства защиты. Классификация методов защиты информации

Средствами защиты информации называют совокупность организационных мер, технических устройств или программных продуктов, которые используются для предотвращения утечки или несанкционированного применения подконтрольных данных.

Средства защиты условно делят на следующие группы:

- *аппаратные, или технические*. Это все приборы или устройства, в том числе технические, механические или электронные, призванные обеспечить контроль доступа к защищенным массивам данных. Кроме этого, аппаратные средства способны маскировать, глушить или шифровать информационные потоки, отказывая в доступе к информации посторонним лицам;
- *программные средства*, способные работать только в компьютерной среде. Основными видами являются антивирусы, идентификаторы, приложения для текстового контроля и прочие программы. Максимальная опасность исходит из Сети, поэтому большинство программных средств ориентировано на отсечку несанкционированного внедрения в систему. Кроме этого, используются смешанные аппаратно-программные системы, одновременно выполняющие обе функции;
- *организационные методы защиты* представляют собой технические мероприятия по обеспечению безопасности информации. Сюда входит соблюдение технических норм при подготовке помещений, прокладке кабелей. Кроме этого, к организационным методам относятся нормы правового характера. Это рабочие правила, корпоративные регламенты, законодательные нормы Российской Федерации. Такие методы дают широкий охват всей деятельности организации (или всей отрасли), но в значительной степени зависят от человеческого фактора.

Рисунок 2.2.1 – Средства и методы защиты информации

Аппаратные методы преимущественно являются средствами контроля. Они ориентированы на идентификацию личности, шифрование данных и периодическую проверку подлинности адреса при передаче сведений.

К аппаратным средствам относят:

- провода и кабели специальной конструкции;
- комплекты оборудования для защиты периметра охраняемой территории;
- высокочастотные фильтры на линиях связи;

- ультразвуковые излучатели на стеклах окон кабинетов или переговорных комнат;
- специальные экраны для защиты помещений ограниченного доступа и т. д.

Помимо этого, также к техническим относятся охранные системы. Они обеспечивают комплексную защиту периметра, включают видеонаблюдение, контроль доступа людей, пожарную охрану объекта.

Программные средства являются наиболее обширной группой, способной обеспечить комплексную защиту информации от внешних воздействий. Они могут отсекать нежелательные действия:

- попытки соединиться с системой через Интернет;
- несанкционированный доступ к чужому ПК;
- возможность использования информации, прошедшей криптографическую обработку.

Организационные методы защиты. В пределах организации процесс охраны данных должен быть продуман так, чтобы не возникало препятствий для работы. Важно принять необходимые меры, но не создавать излишних сложностей. Для этого нужен тщательный анализ источников поступления информации, постоянный контроль каналов передачи и обработки данных. Необходимо определить уровень защиты, распределить нагрузку по техническим, организационным и программным средствам.

В первую очередь понадобится разработка общих правил хранения данных. Полезно рассортировать массивы по степени важности, определив уровень доступа к каждой группе, уточнить порядок пользования сведениями, принять меры, предотвращающие случайную или намеренную утечку сведений в Сеть или на внешние носители. Ограничить вынос текстовых или графических документов, установить ограничение на посещение ненадежных сетевых ресурсов. Такие мероприятия помогут поддерживать корпоративную дисциплину в отношении информации.

Для сохранности личной информации важны усилия самого владельца. Не следует раздавать данные кому попало, надеясь на порядочность и аккуратность людей. Пользователи, работающие с чужими данными, несут ответственность согласно действующему законодательству. Однако в процесс всегда могут вмешаться третьи лица. В Сети часто оказываются в свободном доступе базы данных, номера телефонов или другие личные сведения граждан. Это пример беспечного хранения или злонамеренной деятельности мошенников.

Итак, средства защиты информации смело можно делить на:

- Физические средства — механические, электрические, электро-механические, электронные, электронно-механические и т. п. устройства и системы, которые функционируют автономно, создавая различного рода препятствия на пути дестабилизирующих факторов.
- Аппаратные средства — различные электронные и электронно-механические и т.п. устройства, схемно-встраиваемые в аппаратуру

системы обработки данных или сопрягаемые с ней специально для решения задач защиты информации.

– Программные средства — специальные пакеты программ или отдельные программы, включаемые в состав программного обеспечения с целью решения задач защиты информации.

– Организационные средства — организационно-технические мероприятия, специально предусматриваемые в технологии функционирования системы с целью решения задач защиты информации.

– Законодательные средства — нормативно-правовые акты, с помощью которых регламентируются права и обязанности, а также устанавливается ответственность всех лиц и подразделений, имеющих отношение к функционированию системы, за нарушение правил обработки информации, следствием чего может быть нарушение ее защищенности.

– Психологические (морально-этические средства) — сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе.

2.3 Методы, меры и формы защиты информации

Основным объектом внимания являются компьютеры, работающие отдельно или объединенные в локальную сеть. Особенно уязвимы устройства, имеющие выход в Интернет. Для них необходимы комплексные меры защиты информации, ограничения постороннего доступа и прочие действия, в число которых входят:

– использование антивирусных средств, файрволов;

– меры защиты от случайного и постороннего вмешательства данных от шпионских или диверсионных атак;

– защита информации от электромагнитных воздействий, наводок;

– шифрование данных с целью предотвращения несанкционированного использования.

– В состав комплексных методик также входят правовые и организационные меры, действующие в постоянном режиме. В частности, в компаниях используются сложные пароли, созданные для предотвращения постороннего доступа к сведениям.

– Все мероприятия разрабатываются на этапе внедрения компьютерных систем. Во время эксплуатации они отрабатываются, способы защиты усиливаются и дополняются по мере появления новых угроз.

– К числу наиболее эффективных форм охраны данных относятся:

– общая надежность компьютерных или информационных систем;

– отсечка рискованных или ошибочных операций, исключение доступа неавторизованных пользователей;

– усиление безопасности пользования массивами данных, оптимизация методов передачи или обработки информации;

– резервное копирование сведений;

– профилактические меры безопасности при возникновении аварий, стихийных бедствий.

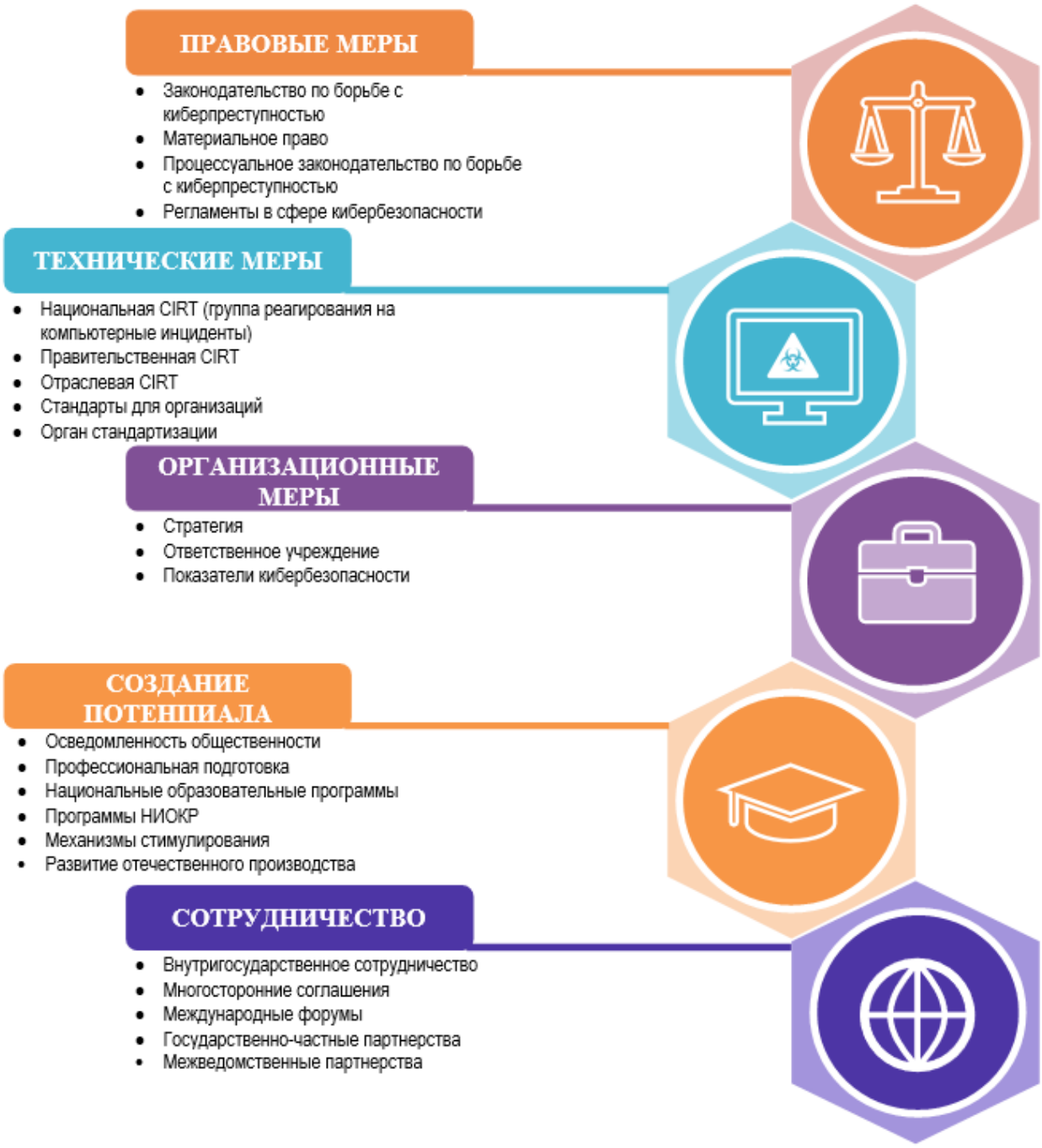

Рисунок 2.3.1 – Меры по защите информации

Важно понимать, что защита информации – не разовая мера, а постоянный и непрерывный процесс. В нем нет второстепенных деталей:

любая уязвимость рано или поздно станет каналом утечки данных. Поэтому относиться к мероприятиям по охране сведений надо с максимальной ответственностью и пониманием (рисунок 2.3.1).

3. ИНЖЕНЕРНО-ТЕХНИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

В современном мире на вооружении шпионов, недобросовестных конкурентов и просто злоумышленников находятся самые разные средства проникновения на объекты противоправных интересов и получения конфиденциальной информации. В этих условиях в интересах обеспечения информационной безопасности необходимы адекватные по назначению технические средства защиты.

Инженерно-техническая защита (ИТЗ) — это совокупность специальных органов, технических средств и мероприятий по их использованию в интересах защиты конфиденциальной информации.

В настоящее время сложилась некоторая система классификации средств по виду, ориентации и другим характеристикам. Например, средства инженерно-технической защиты можно рассматривать по объектам их воздействия. В этом плане они могут применяться для защиты людей, материальных средств, финансов, информации.

Многообразие классификационных характеристик позволяет классифицировать инженерно-технические средства (сокр. ИТЗ) по характеристикам (рисунок 3.1):

1) По объектам воздействия.
2) По характеру мероприятий.
3) По способу реализаций.
4) По масштабу охвата.
5) По классу технический средств защиты.
6) По классу средств злоумышленника.

Рисунок 3.1 – Классификация ИТЗ по характеристикам

Рисунок 3.2 – Классификация ИТЗ по используемым средствам

По используемым средствам ИТЗ классифицируется как:

1. **Физические** это — устройства, инженерные сооружения и организационные меры, затрудняющие или исключающие проникновения злоумышленников к конфиденциальной информации. К ним относятся механические, электромеханические, электронные, электронно-оптические и радиотехнические устройства для воспрещение несанкционированного доступа проноса средств и материалов и других возможна видов преступных действий.

Эти средства применяются для решения следующих задач, такие как охрана территории предприятия, зданий и внутренних помещений, а также наблюдение за ними, охрана оборудования, продукции, финансов и информации, осуществление контролируемого доступа в здания и помещения. Охранная сигнализация и охранное телевидение, например, относятся к средствам обнаружения угроз; заборы вокруг объектов — это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения, и от других преступных действий (подслушивание, обстрел, бросание гранат и взрывпакетов и т.д.) Средства пожаротушения относятся к системам ликвидации угроз.

В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы:

Охранные и *охранно-пожарные* системы (охранные системы и средства охранной сигнализации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты, в охраняемые зоны и помещения, попыток проноса (выноса) оружия, средств промышленного

шпионажа, краж материальных и финансовых ценностей и других действий; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения); *Охранное телевидение* (одно из распространенных средств охраны является охранное телевидение. Привлекательной особенностью охранного телевидения является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя); *Охранное освещение* (обязательной составной частью системы защиты любого объекта является охранное освещение. Различают два вида охранного освещения — дежурное и тревожное. Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри здания. Тревожное освещение включается при поступлении сигнала тревоги от средства охранной сигнализации. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и пр.)

Так же, физические средства можно разделить на три категории: *средства предупреждения средства обнаружения (сигнализация)* и *системы ликвидации угроз.*

2. Аппаратные — это механические, электрические, электронные и др. Устройств, предназначенные для защиты информации от утечки и разглашения и противодействия тех. средствам шпионажа. Особенности:

- Эти средства защиты информации применяются для решения следующих задач: проведение специальных исследований технических средств обеспечения на наличие каналов утечки информации; выявление каналов утечки информации на разных объектах, локализация каналов утечки информации, поиск и обнаружение средств шпионажа, противодействие несанкционированному доступу к источникам конфиденциальной информации.
- По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения средства поиска и детальных измерений, средства активного и пассивного противодействия.
- В качестве примера комплекс для обнаружения и пеленгования радио-закладок, предназначенный для автоматического обнаружения и определения местонахождения радиопередатчиков, радиомикрофонов, телефонных закладок и сетевых радиопередатчиков. Это уже сложный современный поисково-обнаружительный профессиональный комплекс. Таким является, например, комплекс «Дельта», который обеспечивает достоверное обнаружение практически любых из имеющихся в продаже радиомикрофонов, радио-стетоскопов, сетевых и телефонных передатчиков, в

том числе и с инверсией спектра; автоматическое определение места расположения микрофонов в объеме контролируемого помещения.

3. **Программные** – это система спец программ, реализующих функции защиты информации и сохранения целостности и конфиденциальности.

- Системы защиты компьютера от чужого вторжения классифицируются, как: а) средства собственной защиты(защита присущая самому ПО); б) средства защиты вычислительной системы(защита аппаратуры, дисков и штатных устройств); в) средства защиты с запросом информации (Они требуют для своей работы доп. информацию с целью определения полномочий пользователя); г) средства активной защиты(они включаются когда например не правильно вводишь пароль или при попытках доступа к инф без полномочий); д) средства пассивной защиты (они направлены на предостережения контроль улик с целью создания обстановки раскрытия преступления.
- Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации; а) защита информации от несанкционированного доступа; б) защита информации и программ от копирования; в) защита программ и информации от вирусов; г) программная защита каналов связи.
- По каждому из указанных направлений имеется достаточное количество качественных, разработанных профессиональными организациями и распространяемых на рынках программных продуктов

4. **Криптографические** – это технические и программные средства шифрования.

Если учесть, что сегодня по каналам шифрованной связи передаются сотни миллионов сообщений, телефонных переговоров, огромные объемы компьютерных и телеметрических данных, и все это, что называется, не для чужих глаз и ушей, становится ясным: сохранение тайны этой переписки крайне необходимо.

Задачи криптографии является преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных таким образом, что они становится совершенно непонятными для посторонних лиц.

Основные виды криптографии: *с симметричным ключом*, *с открытым ключом*.

Модель криптографической системы:

Вход – источник сообщения – шифратор – источник ключа – дешифратор – приемник сообщения – выход.

5. **Комбинированные** – это совокупная реализация аппаратных и программных средств и криптографических методов защиты информации.

Таким образом, можно сделать следующий вывод: деление средств защиты информации достаточно условно, так как на практике очень часто они взаимодействуют и реализуются в комплексах в виде программно-аппаратных модулей с широким использованием алгоритмов закрытия информации.

4. СКРЫТИЕ ИНФОРМАЦИИ ПУТЕМ ЕЕ ФИЗИЧЕСКОЙ ЗАЩИТЫ, ПРОТИВОДЕЙСТВИЯ НАБЛЮДЕНИЮ, ПОДСЛУШИВАНИЮ И УТЕЧКЕ ПО ВЕЩЕСТВЕННОМУ КАНАЛУ.

Подсистема инженерно-технической защиты информации от утечки предназначена для снижения до допустимых значений величины риска (вероятности) несанкционированного распространения информации от ее источника, расположенного внутри контролируемой зоны, к злоумышленнику. Для достижения этой цели система должна иметь механизмы (силы и средства) обнаружения и нейтрализации угроз подслушивания, наблюдения, перехвата и утечки информации по вещественному каналу.

В соответствии с рассмотренной во втором разделе классификацией методов инженерно-технической защиты информации основу функционирования системы инженерно-технической защиты информации от утечки составляют методы пространственного, временного, структурного и энергетического скрытия.

Для обеспечения пространственного скрытия система должна иметь скрытые места размещения источников информации, известные только людям, непосредственно с ней работающим. В помещения, в которых хранятся секретные документы, имеет допуск очень ограниченный круг лиц.

Руководители частных структур часто используют для хранения особо ценных документов тайники в виде вделанного в стенку и прикрытого картиной сейфа и даже отдельного помещения с замаскированной дверью.

Для реализации временного скрытия система защиты должна иметь механизм определения времени возникновения угрозы. В общем случае это время можно спрогнозировать, но с большой ошибкой. Но в отдельных случаях оно определяется с достаточной точностью. К таким случаям относится время:

– пролета над объектом защиты разведывательного космического аппарата;

– работы радиоэлектронного средства или электрического прибора как источника опасных сигналов;

– нахождения в выделенном помещении посетителя.

Возможность точного определения места нахождения в космическом пространстве разведывательного космического аппарата (КА) позволяет организовать эффективную временную скрытность объекту защиты. Это время рассчитывается по параметрам орбиты запущенного КА специальной службой, которая информирует заинтересованные организации о расписании его пролета. Включение не прошедшего специальную проверку радиоэлектронного средства и электрического прибора создает потенциальную угрозу речевой информации в помещении, в котором установлено это средство или прибор. Поэтому разговоры по закрытым вопросам при включенных непроверенных или незащищенных

радиоэлектронных средствах и приборах запрещаются. Также приход посетителя в выделенное помещение следует рассматривать как возникновение угрозы утечки информации. Поэтому в его присутствии исключаются разговоры и показ средств и материалов, не относящихся к тематике решаемых с посетителем вопросов. С целью исключения утечки информации через посетителей переговоры с ними за исключением случаев, когда в обсуждения возникает необходимость в демонстрации работы средств, проводятся в специальном выделенном помещении для переговоров, находящимся на минимальном расстоянии от КПП.

Средства структурного и энергетического скрытия существенно различаются в зависимости от угроз. Поэтому в общем случае подсистему инженерно-технической защиты от утечки информации целесообразно разделить на комплексы, каждый из которых объединяет силы и средства предотвращения одной из угроз утечки информации (рисунок 4.1).

Рисунок 4.1. Структура подсистемы защиты информации от утечки

Комплекс защиты информации от наблюдения должен обеспечивать:

– маскировку объектов наблюдения в видимом, инфракрасном и радиодиапазонах электромагнитных волн, а также объектов гидроакустического наблюдения;

– формирование и «внедрение» ложной информации об объектах наблюдения;

– уменьшение в случае необходимости прозрачности воздушной и водной среды;

– ослепление и засветку средств наблюдения в оптическом диапазоне длин волн;

– создание помех средствам гидроакустического и радиолокационного наблюдения.

Средства маскировки должны изменять видовые демаскирующие признаки поверхности защищаемого объекта под признаки других объектов фона или признаков фона под признаки защищаемого объекта. Так как характеристики объектов наблюдения существенно различаются в акустическом, оптическом и радиодиапазонах, то средства маскировки в этих диапазонах также различаются.

Изменить структуру изображения объекта или фона можно и активными средствами- генераторами помех. Активные средства создают помеху, которая в зависимости от расположения генератора помех может создавать ложную точку или их совокупность на изображении объекта или фона. Путем размещения источников помех на поверхности объекта защиты или между простыми объектами сложного объекта изменяется его структура.

С помощью средств, изменяющих статические и динамические признаки объекта под признаки ложного объекта (объекта прикрытия), обеспечивается дез-информирование органов разведки.

Комплекс защиты информации от подслушивания включает средства, предотвращающие утечку акустической информации в простом акустическом канале утечки информации. Так как структурное скрытие речевой информации возможно в исключительных случаях (кодирование речевых сигналов), то основу средств рассматриваемого комплекса составляют средства энергетического скрытия. Они должны обеспечить:

– звукоизоляцию и звукопоглощение речевой информации в помещениях;

– звукоизоляцию акустических сигналов работающих механизмов, по признакам которых можно выявить сведения, содержащие государственную или коммерческую тайну;

– акустическое зашумление помещения, в котором ведутся разговоры по закрытой тематике.

Учитывая, что основу защиты информации от подслушивания составляют энергетические методы скрытия, то средства защиты от подслушивания должны, прежде всего, обеспечивать звукоизоляцию защищаемых акустических сигналов в контролируемой зоне. Звукоизоляция достигается созданием вокруг источника акустических сигналов ограждений и экранов, отражающих и поглощающих эти сигналы.

Комплекс защиты информации от перехвата должен предотвращать перехват защищаемой информации, содержащейся в радио- и электрических

функциональных сигналах. С этой целью подсистема должна иметь средства, обеспечивающие:

– структурное скрытие сигналов и содержащейся в них информации;

– подавление до допустимых значений уровней опасных сигналов, распространяющихся по направляющим линиям связи (кабелям, волноводам);

– экранирование электрических, магнитных и электромагнитных полей с защищаемой информацией;

– линейное и пространственное зашумление опасных радио- и электрических сигналов.

Так как носителями информации в вещественном канале утечки информации являются отходы производства в твердом, жидком и газообразном виде, то средства комплекса защиты предотвращения утечки вещественных носителей должны обеспечивать:

– уничтожение информации, содержащейся в выбрасываемых или подлежащих дальнейшей переработке отходах;

– уничтожение неиспользуемых вещественных носителей;

– захоронение в специальных могильниках вещественных носителей, которые не могут быть уничтожены.

5. ЭКРАНИРОВАНИЕ ПОБОЧНЫХ ИЗЛУЧЕНИЙ И НАВОДОК

5.1 Проблема побочного излучения в защите информации

Технические средства, для которых характерна большая амплитуда напряжения опасного сигнала и малая амплитуда тока, относятся к электрическим излучателям. Технические средства с большой амплитудой тока и малой амплитудой напряжения рассматриваются, как магнитные излучатели.

Кроме того, электромагнитные излучения радиоэлектронного оборудования (РЭО) можно разделить на основные и нежелательные.
Основные радиоизлучения характеризуются:

- несущей частотой;
- мощностью (напряженностью) поля;
- широкой полосой излучаемых частот;
- параметрами модуляции.

Нежелательные излучения подразделяются на побочные, внеполосные и шумовые.

Наиболее опасными, с точки зрения образования каналов утечки информации, являются побочные излучения.

Известно, что побочные электромагнитные излучения и наводки (ПЭМИН) являются наиболее опасным техническим каналом утечки информации средств вычислительной техники (СВТ).

Отмечая многообразие форм электромагнитных излучений, следует подчеркнуть, что имеется и так называемое интермодуляционное излучение, возникающее в результате воздействия на нелинейный элемент высокочастотного (ВЧ) тракта радиоэлектронной системы (РЭС) генерируемых колебаний и внешнего электромагнитного поля.

5.2 Понятие и сущность побочных излучений и наводок

Побочные излучения — это радиоизлучения, возникающие в результате любых нелинейных процессов в радиоэлектронном устройстве, кроме процессов модуляции. Побочные излучения возникают как на основной частоте, так и на гармониках, а также в виде их взаимодействия. Радиоизлучение на гармонике — это излучение на частоте (частотах), в целое число раз большей частоты основного излучения. Радиоизлучение на субгармониках — это излучение на частотах, в целое число раз меньших частоты основного излучения. Комбинационное излучение — это излучение, возникающее в результате взаимодействия на линейных элементах радиоэлектронных устройств колебаний несущей (основной) частоты и их гармонических составляющих.

Как известно, любая передача электрического сигнала сопровождается электромагнитным излучением. Если электромагнитный сигнал сам не

используется как носитель информации (радиоволны), то подобное излучение оказывается крайне нежелательным с точки зрения безопасности. «В русскоязычной специализированной литературе используется определение «Побочные электромагнитные излучения и наводки» (ПЭМИН). За рубежом пользуются аббревиатурой TEMPEST (сокращение от Transient Electromagnetic Pulse Emanation Standard) или понятием «компрометирующие излучения» (compromising emanations)». Во всех случаях речь идет исключительно о таком явлении, как переходные электромагнитные импульсные излучения работающей радиоэлектронной аппаратуры.

По правде говоря, для пытливого исследователя изучение проблемы побочных излучений может превратиться в потрясающий детектив. Одна история чего стоит! На саму проблему ПЭМИН впервые обратили внимание еще в 20-х годах прошлого века, в ходе разработки армейских средств телефонной и радиосвязи. Полномасштабные (но закрытые) исследования побочных «компрометирующих» электромагнитных излучений начались только в конце 40-х - начале 50-х годов. Причем это тот самый случай, когда практические изыскания даже опережали теоретическую часть проблемы. Вот только несколько наиболее известных исторических примеров.

С конца 80-х годов охотники за чужими секретами часто перехватывают изображение прямиком с компьютерных мониторов при помощи весьма незамысловатого устройства - обычного бытового телевизора, в котором синхронизаторы заменены генераторами, перестраиваемыми вручную.

Осознание опасности побочных электромагнитных излучений привело к тому, что в наши дни правительственные службы используют дорогое металлическое экранирование отдельных устройств, помещений, а иногда и отдельных зданий. Однако даже для внутренних экранированных помещений существует принцип разделения оборудования на так называемое «красное» и «черное». «Красное» оборудование, используемое для обработки конфиденциальной информации (например, мониторы), должно быть изолировано фильтрами и экранами от «черного» (например, радиомодемов), которое передает данные без грифа «секретно».

«Оценочно, по каналу ПЭМИН (побочных электромагнитных излучений и наводок) может быть перехвачено не более 1-2 процентов данных, хранимых и обрабатываемых на персональных компьютерах и других технических средствах передачи информации (ТСПИ)». На первый взгляд может показаться, что этот канал действительно менее опасен, чем, например, акустический, по которому может произойти утечка до 100% речевой информации, циркулирующей в помещении. Однако, нельзя забывать, что в настоящее время практически вся информация, содержащая государственную тайну или коммерческие, технологические секреты, проходит этап обработки на персональных компьютерах. Специфика канала ПЭМИН такова, что те самые два процента информации, уязвимые для технических средств перехвата — это данные, вводимые с клавиатуры компьютера или отображаемые на дисплее, то есть, парадоксально, но весьма значительная

часть сведений, подлежащих защите, может оказаться доступна для чужих глаз.

Традиционно считается, что перехват ПЭМИН и выделение полезной информации - весьма трудоемкая и дорогостоящая задача, требующая применения сложной специальной техники. Методики контроля эффективности защиты объектов информатизации созданы в расчете на использование противником так называемых оптимальных приемников. Во времена, когда эти документы разрабатывались, приемные устройства, приближающиеся по своим характеристикам к оптимальным, были громоздкими, весили несколько тонн, охлаждались жидким азотом... Ясно, что позволить себе подобные средства могли лишь технические разведки высокоразвитых государств. Они же и рассматривались в качестве главного (и едва ли не единственного) противника.

5.3 Защита от побочных излучений и наводок

Известно два основных метода защиты: *активный* и *пассивный*.

Активный метод предполагает применение специальных широкополосных передатчиков помех. Метод хорош тем, что устраняется не только угроза утечки информации по каналам побочного излучения компьютера, но и многие другие угрозы. Как правило, становится невозможным также и применение закладных подслушивающих устройств. Становится невозможной разведка с использованием излучения всех других устройств, расположенных в защищаемом помещении. Но этот метод имеет и недостатки. Во-первых, достаточно мощный источник излучения никогда не считался полезным для здоровья. Во-вторых, наличие маскирующего излучения свидетельствует, что в данном помещении есть серьезные секреты. Это само по себе будет привлекать к этому помещению повышенный интерес ваших недоброжелателей. В-третьих, при определенных условиях метод не обеспечивает гарантированную защиту компьютерной информации.

Обоих этих недостатков лишен *пассивный метод*. Заключается он в экранировании источника излучения (доработка компьютера), размещении источника излучения (компьютера) в экранированном шкафу или в экранировании помещения целиком. В целом, конечно, для защиты информации пригодны оба метода. Но при одном условии: если у вас есть подтверждение того, что принятые меры действительно обеспечивают требуемую эффективность защиты.

Применяя активный метод, имеется в виду, что уровень создаваемого источником шума излучения никак не может быть рассчитан. В одной точке пространства уровень излучения источника помех превышает уровень излучения компьютера, а в другой точке пространства или на другой частоте это может и не обеспечиваться. Поэтому после установки источников шума необходимо проведение сложных измерений по всему периметру охраняемой зоны и для всех частот. Процедуру проверки необходимо повторять всякий

раз, когда вы просто изменили расположение компьютеров, не говоря уж об установке новых. Это может быть настолько дорого, что, наверное, стоит подумать и о других способах.

Если такие измерения не проводились, то это называется применить меры защиты «на всякий случай». Как правило, такое решение даже хуже, чем решение не предпринимать никаких мер. Ведь будут затрачены средства, все будут считать, что информация защищена, а реальная защита может вовсе и не обеспечиваться.

Каким бы путем вы ни шли, обязательным условием защиты является получение документального подтверждения эффективности принятых мер.
Если это специальное оборудование помещения (экранирование, установка генераторов шума), то детальному обследованию подлежит очень большая территория, что, конечно, недешево. В настоящее время на рынке средств защиты предлагают законченные изделия - экранированные комнаты и боксы. Они, безусловно, очень хорошо выполняют свои функции, но и стоят тоже очень хорошо.

Поэтому в наших условиях реальным остается только экранирование самого источника излучения - компьютера. Причем экранировать необходимо все. У некоторых сначала даже вызывает улыбку то, что мы экранируем, например, мышь вместе с ее хвостиком. Никто не верит, что из движения мыши можно выудить полезную информацию. А я тоже в это не верю. Мышь экранируется по той причине, что хотя она сама, может, и не является источником информации, но она своим хвостиком подключена к системному блоку. Этот хвостик является великолепной антенной, которая излучает все, что генерируется в системном блоке. Если хорошо заэкранировать монитор, то гармоники видеосигнала монитора будут излучаться системным блоком, в том числе и через хвостик мыши, поскольку видеосигналы вырабатываются видеокартой в системном блоке.

Десять лет назад экранированный компьютер выглядел настолько уродливо, что ни один современный руководитель не стал бы его покупать, даже если этот компьютер вообще ничего не излучает.

Современные же технологии основаны на нанесении (например, напылении) различных специальных материалов на внутреннюю поверхность существующего корпуса, поэтому внешний вид компьютера практически не изменяется.

Экранирование компьютера даже с применением современных технологий — сложный процесс. В излучении одного элемента преобладает электрическая составляющая, а в излучении другого — магнитная, следовательно необходимо применять разные материалы. У одного монитора экран плоский, у другого - цилиндрический, а у третьего с двумя радиусами кривизны. Поэтому реально доработка компьютера осуществляется в несколько этапов. Вначале осуществляется специсследование собранного компьютера. Определяются частоты и уровни излучения. После этого идут этапы анализа конструктивного исполнения компьютера, разработки

технических требований, выбора методов защиты, разработки технологических решений и разработки конструкторской документации для данного конкретного изделия (или партии однотипных изделий). После этого изделие поступает сообственно в производство, где и выполняются работы по защите всех элементов компьютера. После этого в обязательном порядке проводятся специспытания, позволяющие подтвердить эффективность принятых решений. Если специспытания прошли успешно, заказчику выдается документ, дающий уверенность, что компьютер защищен от утечки информации по каналам побочного радиоизлучения.

Комплектующие для сборки ПК поставляются из-за рубежа. С периодичностью 3-6 месяцев происходит изменение их конструкторских решений, технических характеристик, форм, габаритов и конфигураций. Следовательно, технология, ориентированная на защиту каждой новой модели ПК, требует высочайшей маневренности производства. При этом возможен вариант изготовления из металла набора универсальных корпусных изделий и размещения в них комплектующих ПК, а также периферийных устройств зарубежного производства. Недостатком этого подхода является то, что он приемлем только для полигонного или катастрофоустойчивого исполнения. Другой вариант — это выбор комплектующих для ПК из большого количества однотипных изделий по признаку минимальной излучательной способности. Этот вариант необходимо рассматривать как непрофессиональный подход к проблеме, так как он противоречит нормативной документации.

ЗАКЛЮЧЕНИЕ

Нужно четко представлять себе, что никакие аппаратные, программные и любые другие решения смогут или не смогут гарантировать абсолютную надежность и безопасность данных в любой организации. В то же время можно существенно уменьшить риск потерь при комплексном подходе к вопросам безопасности. Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ.

Анализ должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь и др.) и предоставить информацию для определения подходящих средств защиты – административных, аппаратных, программных и прочих.

Обеспечение безопасности информации – дорогое дело. Большая концентрация защитных средств в информационной системе может привести не только к тому, что система окажется очень дорогостоящей и потому нерентабельной и неконкурентоспособной, но и к тому, что у нее произойдет существенное снижение коэффициента готовности. Например, если такие ресурсы системы, как время центрального процессора будут постоянно тратиться на работу антивирусных программ, шифрование, резервное архивирование, протоколирование и тому подобное, скорость работы пользователей в такой системе может упасть до нуля.

Так же стоит большое внимание уделять и внутренним угрозам. Даже самый честный и преданный сотрудник может оказаться средством утечки информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Студенческий научный форум [Электронный ресурс]. – Режим доступа: https://scienceforum.ru/2017/article/2017036050 – Дата доступа: 09.03.2022

[2] Методы и средства инженерной защиты объектов информации – StudRef.com – Студенческие реферативные статьи и материалы [Электронный ресурс]. – Режим доступа: https://studref.com/334323/informatika/metody_sredstva_inzhenernoy_zaschity_obektov_informatizatsii – Дата доступа: 09.03.2022

[3] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД “ФОРУМ” ИНФРА-М, 2008 – 416 с.: ил. (Профессиональное образование).

[4] Опарина М.В. Защита информации. – М.: Смарт, 2001.

[5] Национальная библиотека им. Н.Э. Баумана [Электронный ресурс]. – Режим доступа: https://ru.bmstu.wiki/Классификация_инженерно-технической-защиты_информации – Дата доступа 10.03.2022

[6] Защита от побочных излучений и наводок – Статья на сайте works.doklad.ru [Электронный ресурс]. – Режим доступа: https://works.doklad.ru/view/lVI9p4ffrZY.html – Дата доступа: 12.03.2022

[7] Опарина М.В. Защита информации. – М.: Смарт, 2001.