

A.P.Durakovskiy¹, I.V. Kunitcin², A.E. Bezuglenko¹, A.S. Trishkina¹

¹ National Research Nuclear University MEPhI, 115409, Moscow, Kashirskoe sh., 31, e-mail: apdurakovskiy@mephi.ru, ORCID iD is 0000-0002-8311-7735; e-mail: annoctka@mail.ru, ORCID iD is 0000-0002-0961-1575; e-mail: tonya_2006_95@mail.ru, ORCID iD is 0000-0002-1807-111X

² Non-profit educational institution "Educational center "MASCOM", 119421, Moscow, Novatorov str., 40, building 1, e-mail: kiv51@mail.ru, ORCID iD is 0000-0002-4242-5248

About the special investigations of the protection of the technical security systems against information leakage due to the acousto-electrical transformations

Keywords: acoustoelectric transformations, attestation test, special research, technical means of security, information leakage

None of the critically important facilities can operate without the engineered safety system. Functionally varied security networks or a fire alarm system can refer to this system as well as safety and reliability which are provided by secured energy, water and heating supply. In the process of attestation according to the requirements of information security of information objects with such technical means, it is necessary to conduct special investigations of protection against leakage of acoustic speech information through the channels of the acousto-electrical transformations (AET). There are major aspects in the data leak via AET, which currently include the following: lack of and /or obtaining legal and safety norms to regulate specified parameters; lack of the automated hardware and software system for some AET variations to carry out measurements; lack of specified safety equipment for some AET variations; lack of shelter security units; high costs of AET measurement and control units; and low measurement repeatability.

А.П. Дураковский¹, И.В. Куницын², А.Е. Безугленко¹, А.С. Тришкина¹

¹ Национальный исследовательский ядерный университет «МИФИ», 115409, г. Москва, Каширское ш., 31, e-mail: apdurakovskiy@mephi.ru, ORCID iD is 0000-0002-8311-7735; e-mail: annoctka@mail.ru, ORCID iD is 0000-0002-0961-1575; e-mail: tonya_2006_95@mail.ru, ORCID iD is 0000-0002-1807-111X

² НОУ «Учебный центр «МАСКОМ», 119421, Москва, ул. Новаторов, д.40, к.1, e-mail: kiv51@mail.ru, ORCID iD is 0000-0002-4242-5248

О СПЕЦИАЛЬНЫХ ИССЛЕДОВАНИЯХ ЗАЩИЩЕННОСТИ ТЕХНИЧЕСКИХ СРЕДСТВ ОХРАННЫХ СИСТЕМ ОТ УТЕЧКИ ИНФОРМАЦИИ ЗА СЧЕТ АКУСТОЭЛЕКТРИЧЕСКИХ ПРЕОБРАЗОВАНИЙ

Ключевые слова: акустоэлектрические преобразования, аттестационные испытания, технические средства охраны, специальные исследования, утечка информации

Критически важные объекты не могут существовать без технических систем обеспечения их безопасности. К таким техническим системам относят охранные системы различного функционального предназначения, системы пожарной безопасности и системы обеспечения безопасности жизнедеятельности, например, энергопитания, водоснабжения и теплоснабжения. В процессе аттестации по требованиям безопасности информации объектов информатизации, оснащенных техническими средствами охраны (ТСО), необходимо проводить специальные исследования защищенности ТСО от утечки акустической речевой информации по каналам акустоэлектрических преобразований (АЭП). В настоящее время можно выделить следующие основные проблемы защиты информации от утечки по каналам АЭП: отсутствуют нормативно-методические документы, регламентирующие нормируемые показатели и порядок их получения, для некоторых разновидностей каналов АЭП отсутствуют автоматические программно-аппаратные комплексы для проведения измерений а также для некоторых разновидностей каналов АЭП отсутствуют сертифицированные средства защиты, отсутствуют технические средства обеспечения безопасности в защищенном исполнении, высокая стоимость аппаратуры для проведения измерений в каналах АЭП, низкая повторяемость результатов измерений.

Отдельные технические средства охранных систем могут обладать так называемым "микрофонным эффектом", когда акустическая речевая информация из зон безопасности,

включая **выделенные помещения**¹, может быть перехвачена злоумышленником, находящимся за пределами **контролируемой зоны**². Акустическая речевая информация может быть перехвачена злоумышленником по техническим каналам акустоэлектрического преобразования (АЭП) [1]. В основе образования каналов АЭП лежат различные физические явления, сущность которых заключается в том, что при акустическом воздействии на какие-либо элементы ТС возникают электрические сигналы пропорциональные акустическому воздействию.

В настоящее время существуют следующие разновидности технических каналов утечки речевой информации, обусловленных АЭП (рис. 1):

В составе многих ТС могут штатно работать один или несколько разного рода генераторов. Воздействие на их элементы (конденсаторы, дроссели, системы заряженных проводников и т.д.) механическими колебаниями акустических сигналов, может привести к модуляции. Высокочастотные сигналы этих генераторов излучаются в окружающее пространство или распространяются по отходящим от ТС линиям. Такие сигналы могут быть перехвачены злоумышленником.

В некоторых ТС в результате старения элементов (или других причин) может возникнуть паразитная генерация высокочастотного сигнала. Этот сигнал может модулироваться информативным речевым сигналом и также может быть перехвачен злоумышленником. Особенностью этой разновидности канала АЭП является то, что паразитная генерация недопустима и при ее обнаружении использовать ТС на объекте информатизации нельзя.

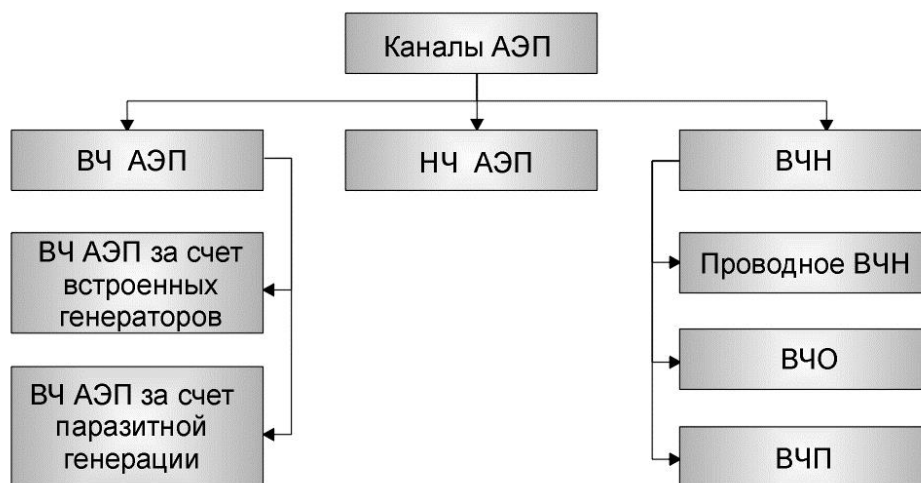


Рис. 1. Классификация каналов АЭП

- **канал высокочастотного акустоэлектрического преобразования (ВЧ АЭП).**
- **канал низкочастотного акустоэлектрического преобразования (НЧ АЭП).** Опыт проведения измерений в канале НЧ АЭП говорит, что все ТС в большей или меньшей степени являются "микрофонами" и информативный сигнал от таких "микрофонов" по проводам может выйти за пределы КЗ.

¹ Выделенное помещение это помещение, в котором присутствует защищаемая акустическая речевая информация.

² Контролируемая зона это пространство, в пределах которого осуществляется контроль за пребыванием и действиями лиц и транспортных средств.

- **канал высокочастотного навязывания (ВЧН)**. Злоумышленник, находясь за пределами контролируемой зоны, может подключить к проводной линии ТС генератор высокой частоты и воздействовать на него токами высокой частоты. Высокочастотный сигнал может отражаться от различных элементов этих ТС. Если элементы ТС обладают

эффектом акустоэлектрического преобразования, то отраженный сигнал может быть модулирован информативным акустическим сигналом. Злоумышленник осуществляет прием отраженного сигнала и это может привести к возникновению **канала проводного ВЧН**.

Злоумышленник, находясь за пределами КЗ, может облучать ТС, находящееся на объекте информатизации, высокочастотным сигналом. Высокочастотный сигнал может отражаться от различных элементов ТС. Если элементы ТС обладают эффектом акустоэлектрического преобразования, то отраженный сигнал может быть модулирован информативным акустическим сигналом. Злоумышленник осуществляет прием отраженного сигнала и это может привести к возникновению **канала высокочастотного облучения (ВЧО)**.

Злоумышленник, находясь за пределами КЗ, может также подключить к проводной линии ТС генератор высокой частоты и воздействовать на него токами высокой частоты. Высокочастотный сигнал может излучаться различными элементами ТС. Если элементы ТС обладают эффектом акустоэлектрического преобразования, то излученный сигнал может быть модулирован информативным акустическим сигналом. Злоумышленник осуществляет прием излученного ТС сигнала и это может привести к возникновению **канала высокочастотной прокачки (ВЧП)**.

В процессе аттестации охранных комплексов по требованиям безопасности информации в соответствии с действующим законодательством с целью выявления этих каналов утечки речевой информации и проведения измерений возникают следующие проблемы [2]:

- для некоторых разновидностей каналов АЭП отсутствуют нормативно-методические документы, регламентирующие нормируемые показатели и порядок их получения;
- для некоторых разновидностей каналов АЭП отсутствуют автоматические программно-аппаратные комплексы для проведения измерений;
- для некоторых разновидностей каналов АЭП отсутствуют сертифицированные средства защиты;
- отсутствуют ТС обеспечения безопасности в защищенном исполнении;
- высокая стоимость аппаратуры для проведения измерений в каналах АЭП;
- низкая повторяемость результатов измерений, обусловленная тем, что измеряются сверхмалые величины и поэтому на результат измерений влияет огромное количество факторов, учесть вклад которых невозможно.

Как в настоящее время решаются (или не решаются) эти проблемы.

От ФСТЭК России получена информация, что в ближайшее время организации - лицензиаты будут обеспечены новыми нормативно-методическими документами. И есть основания предполагать, что кроме кардинальной переработки существующих методик, появятся новые методики для выявления таких каналов утечки, как проводное ВЧН, ВЧО и ВЧП.

Проведение измерений без специализированных программно-аппаратных комплексов требует значительных временных затрат. В то же время, разработка новых программно-аппаратных комплексов в настоящее время практически прекращена, т.к. отсутствуют необходимые нормативно-методические документы. Таким образом, в лучшем случае новые программно-аппаратные комплексы могут появиться только через 2...3 года после выхода новых нормативно-методических документов.

Для защиты информации на критически важных объектах в соответствии с действующим законодательством могут применяться только сертифицированные средства защиты. Если, к примеру, для защиты телефонных линий связи существует достаточно большая номенклатура сертифицированных средств защиты, то для систем пожарной и охранной сигнализации пока что сертифицированные средства защиты информации не разрабатываются. Сейчас проблема может быть решена только путем применения ТС, удовлетворяющих нормам противодействия.

Останется и проблема высокой стоимости измерительной аппаратуры, и особенно программно-аппаратных комплексов. Стоимость современных программно-аппаратных комплексов составляет от одного до десятков миллионов рублей и будет только увеличиваться. С появлением новых нормативно-методических документов наверняка увеличится и номенклатура необходимой измерительной аппаратуры. Соответственно увеличится (по экспертным оценкам в два...три раза) и стоимость проведения аттестационных работ.

Насущной является проблема низкой повторяемости результатов измерений. Решение данной проблемы требует разработки и утверждения ФСТЭК России корректных методик проведения специальных исследований, а также жестких требований к измерительному стенду и помещениям, в которых проводятся измерения в каналах АЭП.

Вывод: Корректное проведение специальных исследований защищенности вспомогательных технических средств и систем, в частности технических средств охранных систем, от утечки акустической речевой информации по каналам АЭП, в процессе аттестации объектов информатизации (выделенных помещений) по требованиям безопасности информации, потребует значительных усилий государственного регулятора и значительных материальных затрат разработчиков и участников государственной системы защиты информации.

СПИСОК ЛИТЕРАТУРЫ:

1. Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации. Учебное пособие. – М.: НИЯУ МИФИ, 2015. - 152 с.:илл.
2. Куницын И.В., Лобашев А.К. Проблемы проведения измерений в канале низкочастотного акустоэлектрического преобразования. Информационно-методический журнал «Защита информации. Инсайд», № 3 (63), 2015 г., С. 67-72.

REFERENCES:

1. Durakovskiy A.P., Kunitcin I.V., Lavrukhin Y.N. Kontrol zashisthenosti retchevoy informacii v pomesthenijyh. Attestacionnye ispytaniya vspomogatelnyh tekhnicheskikh sredstv i sistem po trebovanijam bezpasnosti. Utchebnoe posobie. M.: NRNU MEPhI, 2015. 152 s.:ill
2. Kunitcin I.V., Lobashev A.K. Problemy provedeniya izmereniy v kanale nizkitchastotnogo akustoelektritcheskogo preobrazovaniya. Informatcionno-metoditcheskij jurnal "Zasthita informacii. Insaid" № 3 (63), 2015 г., С. 67-72.