DOI: 10.17117/na.2016.01.01.366

<http://ucom.ru/doc/na.2016.01.01.366.pdf>

Поступила (Received): 29.01.2016

Арванова С.М., Ахкопек Ш.М., Настуева Л.С. Проведение конфиденциальных встреч на защищенном объекте

Arvanova S.M., Ahkopek Sh.M., Nastueva L.S.
Confidential meetings in the protected object

В работе проводится анализ и исследование необходимых мер по обеспечению информационной безопасности при проведении конфиденциальных встреч в компании

Ключевые слова: коммерческая тайна, акустическое зашумление, утечка информации, конфиденциальность, комплексный анализ

In work the analysis and research of necessary measures for ensuring information security when holding confidential meetings is carried out to the companies

Key words: trade secret, acoustic hindrance, information leakage, confidentiality, complex analysis

Арванова Саният Мухамедовна

Ассистент

Кабардино-Балкарский государственный университет им. Х.М. Бербокова

г. Нальчик, ул. Чернышевского, 173

Arvanova Saniyat Mukhamedovna

Assistant

Kabardino-Balkarian state university named Kh.M. Berbokova

Nalchik, Chernyshevskogo st., 173

Ахкопек Шаза Мухамад

Ассистент

Кабардино-Балкарский государственный университет им. Х.М. Бербокова

г. Нальчик, ул. Чернышевского, 173

Ahkopek Shaza Mukhamad

Assistant

Kabardino-Balkarian state university named Kh.M. Berbokova

Nalchik, Chernyshevskogo st., 173

Настуева Лейля Салиховна

Студент

Кабардино-Балкарский государственный университет им. Х.М. Бербокова

г. Нальчик, ул. Чернышевского, 173

Nastueva Leila Salihovna

Student

Kabardino-Balkarian state university named Kh.M. Berbokova

Nalchik, Chernyshevskogo st., 173

Реализация мер по обеспечению безопасности комнат в которых проводятся важные встречи по различным каналам всегда актуальна не только при выполнении необходимых требований по защите выделенных объектов, которая включает коммерческую тайну компании, но и прочих предприятий, в которых проводятся секретные переговоры. В основном применение активных средств обеспечения безопасности создает появление посторонних акустических звуков, которые снижают оптимальность работы в защищаемом и смежных комнатах. Очевидно, что только совместное применение активных и пассивных методов и средств может обеспечить полную безопасность встречи.

Активное обеспечение безопасности встреч непосредственно направляется на обеспечение сохранности информации лишь средствами аддитивного зашумления. Так при размещении точки сигнала и источника акустического зашумления в одном месте пространства по периметру комнаты и соответственно за ее границами будет осуществляться соотношения сигнал/помеха, устанавливаемые по мощности исходных источников звуковой информации. С точки зрения реализации защиты информации такое решение наиболее просто и эффективно, если не учитывать две особенности – возможность демаскировки факта закрытия речи за пределами комнаты наличием повышенного акустического шума и усложнения коммуникации для объектов переговоров.

Таким образом, если устройство для переговоров предназначено для обеспечения безопасности от средств негласного контроля, то уровень звукового давления источника акустической помехи должен выбираться из условия превышения над диффузной составляющей речевого сигнала.

При оценке защищенности комнаты и эффективности средств безопасности проводится инструментальный контроль допустимой утечки защищаемой информации по следующим каналам:

1. вторичные электромагнитные излучения;
2. наводки в цепях электропитания;
3. акустоэлектрические преобразования в элементах аппаратных средств;
4. акустический.

Рис. 1. Модель защищенной комнаты

Для контроля защищенности аппаратных средств от несанкционированного доступа используются сертифицированные в системе Сертификации РОСС RU.0001.01БИ00 программные продукты контроля защищенности информации от несанкционированного доступа в автоматизированных системах.

Не стоит надеяться на столь простые решения задачи, ведь средства атаки, как и методы обеспечения безопасности [1], всегда совершенствуются.

Встреча с участием представителей заинтересованных компаний должно проводиться с согласия руководителя предприятия, который, в свою очередь, назначает ответственного за проведение подобных встреч.

Участники встречи запускаются на встречу по спискам при предъявлении официальных документов, подтверждающих их личности и должности.

Средства обеспечения защиты информации при проведении встреч с участием представителей посторонних учреждений нужны для подготовки соответствующей комнаты (рис.1) и для предупреждения утечки защищаемых данных из нее, с учетом всех деталей встречи.

Рекомендуется применение следующих способов защиты:

1. до начала встречи необходимо произвести визуальный осмотр комнаты на предмет обнаружения подложных технических средств.

2. непосредственно перед началом встречи служба безопасности должна осмотреть прилегающие объекты к комнате для встреч.

3. количество лиц, участвующих в секретных переговорах должно быть максимально ограничено до минимума;

4. пропуск посторонних лиц во время секретного совещания должно быть ограничено;

5. должна быть четко разработана охрана выделенной комнаты во время проведения встречи, а также наблюдение за обстановкой на объекте в целом.

Для большей гарантии безопасности, у дверей комнаты должен стоять представитель службы охраны из постоянного штата компании, так как подобное присутствие создает возможность подслушивания непосредственно охранником.

6. по возможности проведение встречи переносить на нерабочее время;

7. любые работы в комнате, проводимые вне времени проведения конфиденциальных встреч, например: уборка, ремонт, должен проводиться в обязательном присутствии сотрудника службы безопасности.

8. после проведения встречи комната должна досконально осматриваться, закрываться и опечатываться.

9. между встречами комната должна быть закрыта и опечатана ответственным сотрудником принимающей компании.

Перечисленные меры организации информационной безопасности в комнате для встреч считаются весьма эффективными и не несут серьезных финансовых затрат или проблем с персоналом и могут применяться как отдельно, так и совместно, что позволит на порядок повысить уровень защиты информации рассматриваемого объекта.

Вывод.

В итоге хочется заметить, что при осуществлении защитных мер по обеспечению конфиденциальности от утечки речевой информации обязательно нужно провести комплексный анализ случая и наилучшим образом выбирать между пассивными и активными средствами защиты или их комплексом.

В отдельных ситуациях проведения встреч и переговоров с невыраженной периодичностью вполне достаточно предложить установить переговорное устройство.

Список используемых источников:

1. Арванова С.М. Криптографические механизмы безопасности // Научный альманах. 2015. №7(9). С. 578–580.

© 2016, Арванова С.М., Ахкопек Ш.М., Настуева Л.С.
Проведение конфиденциальных встреч на
защищенном объекте

© 2016, Arvanova S.M., Ahkopez Sh.M., Nastueva L.S.
Confidential meetings in the protected object