DOI: 10.12737/article_5a0038bf1dc556.80354200

Дорошенко Ю.А., д-р экон. наук, проф.,
Ковтун Ю.А., канд. юр. наук, доц.,
Баранов В.М., канд. пед. наук, доц.,
Шевцов Р.М., канд. юр. наук, доц.
Белгородский государственный технологический университет им В.Г. Шухова

ИСПОЛЬЗОВАНИЕ ЗВУКОИЗОЛЯЦИОННЫХ МАТЕРИАЛОВ В ОБОРУДОВАНИИ ВЫДЕЛЕННЫХ ПОМЕЩЕНИЙ (В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ)

vladimirbaranov84@gmail.com

В статье анализируются актуальные проблемы защиты конфиденциальной информации предприятия как комплекса мер правового, организационного и технического характера, направленных на обеспечение его экономической безопасности. Рассматривается деятельность предприятия по предотвращению утечки конфиденциальных сведений путем оборудования выделенных, защищенных помещений для работы с конфиденциальной информацией, в том числе размещение в этих помещениях вычислительной техники, предназначенной для обработки и хранения конфиденциальной информации, средств связи предназначенных для ведения конфиденциальных разговоров и хранение в данных помещениях носителей конфиденциальной информации. Так же авторы отмечают, что важным элементом оборудования выделенного помещения выступают звукоизоляционные свойства, изолированность в плане возможности дистанционного перехвата информации по акустическим каналам (с помощью лазерных и направленных микрофонов и т.п.). Даются рекомендации по использованию при оборудовании выделенного помещения звукоизоляционных свойств материалов, которые усиливают звукоизоляцию выделенного защищенного помещения, для эффективного противодействия несанкционированному доступу к речевой информации, обеспечения безопасности переговоров, а также предотвращения утечки конфиденциальной информации.

Ключевые слова*: защита информации, безопасность информации, обеспечение экономической безопасности, выделенное помещение, звукоизоляция, звукопоглощение.*

В настоящее время проблема обеспечения экономической безопасности является приоритетом деятельности руководителей организаций, интегрированных в единое экономическое пространство. Должностные лица организаций в своей деятельности вынуждены иметь дело со сведениями, отнесенными не только к коммерческой, но и государственной тайне. Важнейшим направлением деятельности служб безопасности организаций является предотвращение утечки конфиденциальной информации. С помощью специальных технических средств, в настоящее время получил развитие так называемый «коммерческий шпионаж», зачастую наносящий непоправимый урон экономической безопасности организаций [1]. Появилось большое количество литературы и электронных ресурсов в сети Интернет, в которых содержатся конкретные рекомендации по тактике конспиративного прослушивания, видеозаписи и других форм негласного получения информации. Информация – один из главных ресурсов мирового сообщества, защита информации о деятельности организации, является неотъемлемой частью деятельности служб безопасности организаций. Их действия включают в себя комплекс мер, направленных, прежде всего, на защиту конфиденциальности информации [2].

Под защитой информации понимают комплекс мер – правового, организационного и технического характера; направленных на недопущение либо существенное затруднение хищения, разрушения, искажения или блокирования в процессе ее обработки (создания, сбора, хранению и т.д.).

Под мерами правового характера следует понимать использование принятых, разработку и принятие новых нормативных актов, направленных на противодействие угрозам и их нейтрализацию в информационной сфере.

Под мерами организационного характера понимают:

1. организацию мероприятий, направленных на минимизацию утечки информации через персонал, то есть подбор и расстановка кадров;
2. организацию специального порядка подготовки, использования, хранения, уничтожения и учета документированной информации на всех видах носителей;
3. выделение специальных защищенных помещений для работы с конфиденциальной информацией, в том числе размещение в этих помещениях вычислительной техники, предназначенной

для обработки и хранения конфиденциальной информации, средств связи предназначенных для ведения конфиденциальных разговоров и хранение в данных помещениях носителей конфиденциальной информации;

4. использование лицензированной (категорированной) техники и программного обеспечения отвечающих современным требованиям защиты информации;

5. проведение технического обслуживания и ремонт средств вычислительной техники, предназначенных для обработки информации ограниченного доступа, должен проводиться организациями, имеющими соответствующие лицензии;

6. запрет на передачу узлов и блоков с элементами накопления, и хранения информации при техническом обслуживании и ремонте средств вычислительной техники, на которых обрабатывается информация ограниченного распространения, а также замена вышедших из строя элементов и блоков только на элементы и блоки, прошедшие специальную проверку.

7. организация контролируемого посещения помещений, где ведется работа с конфиденциальной информацией;

8. разграничение прав на доступ к информации ограниченного пользования;

9. запрет ведения конфиденциальных разговоров по открытым каналам связи и использование открытых каналов связи для передачи конфиденциальной информации;

10. назначение сотрудников, ответственных за обеспечение защиты информации;

11. обучение, переподготовка и повышение квалификации специалистов в области защиты информации;

12. контроль за соблюдением установленных требований по защите конфиденциальной информации.

Заключительный элемент рассматриваемого нами понятия «защита информации» – меры технического характера. Под мерами технического характера понимают выявление технических каналов утечки информации и их блокирование при помощи специальных технических средств. Сюда же можно отнести оборудование защищенных помещений, установку различных запорных устройств и средств контроля, позволяющих ограничить доступ посторонних лиц на объекты где производится работа с конфиденциальной информацией [3].

Существует два направления утечки информации. Первое – через персонал, имеющий доступ к информации (например, сотрудники, обслуживающие вычислительную технику; сотрудники, работающие с закрытой информацией). Причем эти утечки могут возникнуть как в результате преднамеренных противоправных действий, так и в результате халатных действий и эксплутационных ошибок отдельных сотрудников. Перекрытие данного канала утечки информации организуется административными мерами.

Второе – путем съема информации с технических каналов связи. Съем информации с данных каналов связи может осуществляться следующими основными способами:

Контактное подключение к электронным устройствам – данный способ съема информации является простейшим, обычно реализуется непосредственным подключением к линии связи.

Бесконтактное подключение (т.е. дистанционное) может осуществляться за счет побочных электромагнитных излучений, производимых техническими средствами обработки информации, а также за счет использования различных приборов наблюдения, в том числе и использования приборов виброакустического контроля. Установка встроенных электронных устройств (различные видео- и аудиозакладки) [4].

Тщательно продуманная организация и тактика проведения мероприятий, направленных на защиту информации, обеспечивает эффективное достижение реальных результатов от посягательств иногда путем, не требующих больших финансовых затрат. В первую очередь это относиться к оборудованию выделенных, защищенных помещений для работы с конфиденциальной информацией, в том числе размещение в этих помещениях вычислительной техники, предназначенной для обработки и хранения конфиденциальной информации, средств связи предназначенных для ведения конфиденциальных разговоров и хранение в данных помещениях носителей конфиденциальной информации. [5] Его расположение целесообразно в пределах контролируемой зоны, в которой, как правило, используются специальные средства защиты. При организации выделенного помещения все технические средства, от которых можно отказаться (системы телевидения и времени, телефонная связь, бытовая техника и т.д.), должны демонтироваться, а несертифицированные технические средства должны отключаться от соединительных линий и источников электропитания при проведении конфиденциальных переговоров. Если же требуется наличие телефонной линии, в сеть электропитания устанавливаются сертифицированные защитные устройства.

Особенностью выбора такого помещения, как правило, обуславливается оптимальными с точки зрения соображениями безопасности и вы-

бирается так, чтобы оно, по возможности, не примыкало к границам контролируемой зоны, не находилось на первом и последнем этажах здания. При организации учитывается его звукоизоляционные свойства, изолированность в плане возможности дистанционного перехвата информации по акустическим каналам (с помощью лазерных и направленных микрофонов и т.п.).

С позиции пассивной безопасности в выделенном помещение должны отсутствовать окна, при необходимости окон они располагаются со стороны двора предприятия или организации. В процессе ведения переговоров окна должны быть закрыты, шторы или жалюзи. Дверь в выделенное помещение целесообразно оборудовать звукоизоляционным тамбуром, а также персоналу отвечающему за обеспечение безопасности организации следует принять меры по защите вентиляционных отверстий – как угрозе доступа к информации, содержащей государственную или коммерческую тайны по виброакустическому каналу.

Мы полагаем, что важным элементом обеспечения такой безопасности выступают так же звукопоглощающие материалы и конструкции. Они усиливают звукоизоляцию выделенного защищенного помещения. Добиться повышенной звукоизоляции можно, закрыв все поверхности звукопоглощающим материалом (поролон, пенопласт и т.п.). Естественно, что от толщины этого слоя будет зависеть степень поглощения звуковых колебаний.

Известно, что выделение акустического сигнала на фоне естественных шумов происходит при определенных соотношениях сигнал/шум. Поэтому, применением звукоизолирующих материалов достигается значительного снижения сигнала\шума до предела, затрудняющего процесс выделения речевых сигналов, проникающих за пределы контролируемой зоны по акустическому или виброакустическому каналам [6].

Средний уровень громкости разговора, происходящего в помещении, составляет 50...60 дБ, соответственно звукоизоляция и звукопоглощение выделенных помещений должно поглощать эти звуки [7].

В практическом плане сложность представляют окна, вентиляция, кабельные каналы и двери. Идеальный вариант – если окон нет вообще. Но по разным причинам руководители предприятий и организаций не могут этого допустить. Поэтому мы считаем, что на проблеме окон следует остановиться отдельно. Решая проблему безопасности информации, по нашему мнению, наиболее экономически обоснованным способом усиления звукоизоляции является возможность установки не двух, а трех стекол. Причем, между стеклом и рамой по периметру нужно проложить тонкую резину либо поролон. Физические принципы отражения и поглощения радиоволн в таком варианте защиты подразумевают установку среднего стекла не параллельно двум другим, а под небольшим углом. Имеющиеся и возможные щели окна в данном случае следует перекрыть звукопоглощающим уплотнителем.

Решить проблему усиления звукоизоляции дверей гораздо сложнее. Мы считаем, что для начала следует поставить дополнительную полую дверь (организовать тамбур), а свободное пространство заполнить звукопоглощающим материалом. Также необходимо обеспечить плотное закрытие дверей, например, установив на косяк все тот же уплотнитель, так щель в доли миллиметра снижает звукоизоляцию на порядок.

Не менее доступным и действенным способом, по нашему мнению, является решение – «комната в комнате», т.е. создание помещения (пол, стены, потолок, дверь) внутри уже существующего с зазором между перекрытиями первого и второго не менее полуметра. Перекрытия внутренней и внешней комнат снаружи и изнутри также необходимо покрыть звукопоглощающим материалом.

В помещениях с большой площадью поверхностей, хорошо отражающих звук и линейными размерами от 3–4 м, эхо-эффект проявляется весьма заметно. В связи с чем, мебель и аппаратуру внутри как первого, так и второго варианта помещений нужно сократить до минимума [8]. Использование штор из плотной ткани, ковров с длинным ворсом, предметов мягкой мебели, цветов и картин оптимальным образом снизят вероятность использования средств перехвата акустической информации. Рассматривая проблему обеспечения безопасности объекта переговоров, мы полагаем уделить дополнительное внимание системам вентиляции и технологических полостей и пустот, как в стенах, так и перекрытиях. Лучшим вариантом является заполнение их строительной пеной, однако, для вентиляции такой способ неприемлем. Вариантом решения в данной ситуации, по нашему мнению, является установка звукопоглощающего материала на прямом участке воздуховода (протяженностью не менее 3 м), либо организация «звукового лабиринта» с целью затухания звуковой волны.

Подводя итог, отметим, что абсолютно надежную, непреодолимую защиту создать невозможно. Поэтому при планировании мероприятий по организации информационной безопасности необходимо представлять, кого и какая именно информация может интересовать, какова

ее ценность и на какие финансовые затраты ради нее готов пойти злоумышленник. То есть система защиты информации должна быть адекватна и эффективна потенциальным угрозам. И использование звукоизоляционных материалов с учетом звукоизоляционных свойств, при оборудовании выделенного помещения, предлагает наилучшую эффективность предотвращения утечки конфиденциальной информации, защиты несанкционированного доступа к речевой информации, обеспечения безопасности переговоров при минимальных финансовых затратах.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Савельев И.А., Антипенко А.О Совершенствование процесса оценки защищённости выделенного помещения от технических каналов утечки информации // Вопросы кибербезопасности. 2017. № 3 (21). С. 35–42.

2. Лаврова А.А., Сабынин В.Н. Методика оценки безопасности переговоров в выделенном помещении организации // Известия СПбГЭТУ "ЛЭТИ". 2017. № 4. С. 20–25.

3. Хорев А.А. Способы защиты выделенных помещений от утечки речевой (акустической) информации по техническим каналам: звуко-и виброизоляция помещений // Специальная техника. 2013. № 2. С. 48–63.

4. Алексеев А.П., Макаров М.И. Принципы многоуровневой защиты информации. Инфокоммуникационные технологии. 2012. Т. 10. № 2. С. 88–93.

5. Сабынин В.Н. Защита информации в выделенных помещениях // «ИНФОРМОСТ» «Радиоэлектроника и Телекоммуникации». 2002. №1. С. 25–29.

6. Смирнов В.И. Оценки защищенности речевой информации в выделенном помещении с помощью инструментально-расчетного метода // Кибернетика и программирование. 2012. № 2. С. 18–24.

7. Шевцов В.В., Куприянов А.И. Оптимизация мер по защите с учетом ценности информации // Известия Института инженерной физики. 2012. Т. 3. № 25. С. 2–6.

8. Бандурина О.С. Способы защиты коммерческой информации // Патентное дело. 2012. № 6. С. 16–21.

Информация об авторах

Дорошенко Юрий Анатольевич, доктор экономических наук, профессор.
E-mail: 549709@mail.ru
Белгородский государственный технологический университет им В.Г. Шухова.
Адрес: 308012, Белгород, ул. Костюкова, д.46

Ковтун Юрий Анатольевич, кандидат юридических наук, доцент, доцент кафедры стратегического управления.
E-mail: belad@yandex.ru
Белгородский государственный технологический университет им В.Г. Шухова.
Адрес: 308012, Белгород, ул. Костюкова, д.46

Баранов Владимир Михайлович, кандидат педагогических наук, доцент, доцент кафедры стратегического управления.
E-mail: vladimirbaranov84@gmail.com
Белгородский государственный технологический университет им В.Г. Шухова.
Адрес: 308012, Белгород, ул. Костюкова, д.46

Шевцов Роман Михайлович, кандидат юридических наук, доцент, доцент кафедры стратегического управления.
E-mail: roman377@mail.ru
Белгородский государственный технологический университет им В.Г. Шухова.
Адрес: 308012, Белгород, ул. Костюкова, д.46

Поступила в сентябре 2017 г.

Doroshenko Y.A., Kovtun Y.A., Baranov V.M., Shevtsov R.M.

THE USE OF SOUND INSULATING MATERIALS IN EQUIPMENT DEDICATED SPACE (IN THE CONTEXT OF ENSURING ECONOMIC SECURITY OF ENTERPRISES)

The article analyzes the topical problems of protection of confidential information of the enterprise as a complex of measures of legal, organizational and technical nature aimed at ensuring its economic security. Discusses the activities of the company to prevent the leakage of confidential information by a dedicated hard-

ware-protected areas for confidential information, including the location of these premises computing technology for processing and storage of confidential information, communications intended to be confidential conversations and storage in these areas of the media of confidential information. The same authors note that an important piece of equipment dedicated spaces are sound-proof properties, isolation in terms of the possibility of remote interception of information over acoustic channels (using a laser and directional microphones, etc.). Recommendations for use of the equipment allocated space acoustic properties of materials, which increase the sound insulation of a dedicated protected space, to effectively deal with unauthorized access to speech information, security negotiation, as well as preventing the leakage of confidential information.

Keywords: *information security, information security, economic security, a dedicated room, soundproofing, sound absorption.*

Information about the authors
Doroshenko Yuri Anatolyevich, Ph.D., Professor.
E-mail: 549709@mail.ru
Belgorod State Technological University named after V.G. Shukhov.
Russia, 308012, Belgorod, st. Kostyukova, 46.

Kovtun Yuriy Anatolyevich, Ph.D., Assistant professor.
E-mail: belad@yandex.ru
Belgorod State Technological University named after V.G. Shukhov.
Russia, 308012, Belgorod, st. Kostyukova, 46.

Baranov Vladimir Mikhaylovich, Ph.D., Assistant professor.
E-mail: vladimirbaranov84@gmail.com
Belgorod State Technological University named after V.G. Shukhov.
Russia, 308012, Belgorod, st. Kostyukova, 46.

Shevtsov Roman Mikhaylovich, Ph.D., Assistant professor.
E-mail: roman377@mail.ru
Belgorod State Technological University named after V.G. Shukhov.
Russia, 308012, Belgorod, st. Kostyukova, 46.

Received in September 2017