



УДК 004.056.53

А. А. Лаврова, В. Н. Сабынин

Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» им. В. И. Ульянова (Ленина)

Методика оценки безопасности переговоров в выделенном помещении организации

Рассматривается описательная модель выделенного помещения, выбор и обоснование показателя оценки его защищенности при обработке конфиденциальной информации. Предложена методика оценки безопасности информации в выделенном помещении организации при угрозе внедрения в него радиозакладок.

Безопасность информации, радиозакладка, спецпроверка, вероятность

Утверждение Президентом Российской Федерации Доктрины информационной безопасности от 05.12.2016 указом № 646 еще раз подтверждает важность обеспечения безопасности информации, составляющей не только государственную, но и коммерческую тайну, или любой другой конфиденциальной информации. В организациях с различными видами собственности обработка конфиденциальной информации осуществляется не только в кабинетах, других помещениях организации, но и в так называемых выделенных помещениях. Здесь и далее под выделенными помещениями понимаются помещения (служебные кабинеты, актовые, конференц-залы и т. д.), специально предназначенные для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т. п.) [1]. Причем чаще всего на этих объектах конфиденциальная информация обсуждается руководством организации впервые. В связи с постоянным ростом роли Российской Федерации в международных отношениях растет и интерес к ее различным объектам и экономике в целом иностранных технических разведок, поэтому защита конфиденциальной информации на объектах информатизации, в том числе и в выделенных помещениях, является актуальной задачей, требующей к себе постоянного внимания и совершенствования защиты. Для обеспечения безопасности информации в выделенном помещении важно знать ее со-

стояние, что вызывает необходимость постоянного совершенствования методик ее оценки. В настоящее время существует достаточно большое количество методик оценки безопасности информации не только для корпоративного [2], но и для федерального уровня (корпоративные или ведомственные стандарты проведения аудита информационной безопасности; международные стандарты). Все они требуют большого количества исходных данных, которые не всегда известны. Приходится привлекать экспертов различного рода для их формирования, что в свою очередь вносит погрешности в интегральный показатель оценки. Также необходимо наличие подготовленных высококвалифицированных специалистов. Другими словами, для использования данных методик требуются большие силы и средства, в том числе и денежные средства, так как таким объемом работ могут заниматься только специализированные организации с высококвалифицированными специалистами, с современными техническими средствами, имеющие лицензию на право проведения аудита информационной безопасности. Средние и более мелкие компании по финансовым причинам часто лишены возможности нанимать подобные организации для оценки состояния безопасности информации. Поэтому, учитывая накопленный опыт по проведению аудитов информационной безопасности, анализируя существующие методики оценки состояния

безопасности, представляет интерес создание более простых методик оценки, позволяющих специалистам организации оценивать безопасность информации на объектах информатизации, в том числе и в выделенных помещениях при проведении внутреннего аудита. В данной статье предпринята попытка разработать такую методику.

Постановка задачи. Пусть для ведения переговоров имеется комната площадью примерно 16 м². Помещение расположено на втором этаже пятиэтажного здания, в комнате имеется одно окно, выходящее на улицу. Комната оснащена техническими средствами охраны и пожарной сигнализации. Стены здания кирпичные. Наружная стена толщиной порядка 50 см. Перегородки асбестоцементные толщиной 12 см. Дверь деревянная с обычным замком. В помещении находятся большой стол и стулья. При проведении совещания используется проектор с ноутбуком. В коридоре могут находиться не только персонал организации, но и посторонние лица. Необходимо оценить безопасность информации в данном выделенном помещении.

Решение задачи. В рамках настоящей методики будем говорить о защите информации в выделенном помещении, предназначенном для ведения конфиденциальных мероприятий. В связи с этим реальную угрозу будут представлять технические средства, предназначенные для негласного съема информации. Так как наиболее часто применяемым злоумышленниками техническим средством добывания информации (а значит, и наиболее опасным) является радиозакладка, то рассмотрим прежде всего методику оценки безопасности информации в выделенном помещении при возможности внедрения именно радиозакладки. Радиозакладка – это миниатюрное электронное устройство, состоящее из микрофона и радиопередатчика, способное передавать подслушанную информацию на большие расстояния с помощью электромагнитных волн. Структурная схема радиомикрофона представлена на рис. 1.



Рис. 1

Принцип работы радиозакладки очень прост: звуковые колебания (речь) с помощью микрофона преобразуются в электрические сигналы. Далее в

радиопередатчике эти сигналы модулируют колебания несущей частоты, которые в виде электромагнитных волн с помощью антенны излучаются в пространство. Радиус зоны акустической чувствительности радиозакладки определяет микрофон, а ее дальность действия зависит от мощности радиопередатчика и чувствительности применяемого радиоприемного устройства. Но самое интересное в радиозакладках то, куда они внедряются, как они выглядят и кто их внедряет. Внедрить радиозакладку может и уборщица, и сотрудник организации, и участник совещания, который незаметно пронес закладку и также незаметно ее внедрил в помещение. Однако участник может и не оставлять закладку в помещении, а держать ее все время у себя в кармане пиджака, например, или даже в пачке сигарет. Камуфляж радиозакладки иногда бывает настолько комичен и неприметен, что ни у кого не возникает даже подозрений о ее возможном наличии.

Рассматривая применяемые [3] злоумышленником маскировки радиозакладок можно сделать вывод, что «пронести» радиозакладку не составляет большого труда. Так, например, в качестве одного из организационных мероприятий защиты можно предложить сдавать все имеющиеся при себе вещи на хранение в сейф на время совещания. Конечно, никто не будет просить показывать обувь или раздеваться, так как это может подорвать доверительные отношения между участниками совещания. А вот у уборщицы или обслуживающего персонала больше возможностей внедрить радиозакладку в помещение. Например, в выделенном помещении вышел из строя удлинитель, требуется заменить его на новый. На тот самый, который с радиозакладкой. А если в помещении есть какие-то предметы интерьера, то не представляет никакого труда внедрить в них радиозакладку или же принести в это помещение новый предмет декора.

Приведенные примеры показывают, что существует множество способов внедрить радиозакладку, поэтому перед обладателями конфиденциальной информации встает вопрос: а как же защититься от этих маленьких и неприятных устройств? В реальной жизни перед проведением каждого совещания в помещении проводится специальная проверка. Специальная проверка – это проверка объекта информатизации в целях выявления и изъятия возможно внедренных закладочных устройств [4].

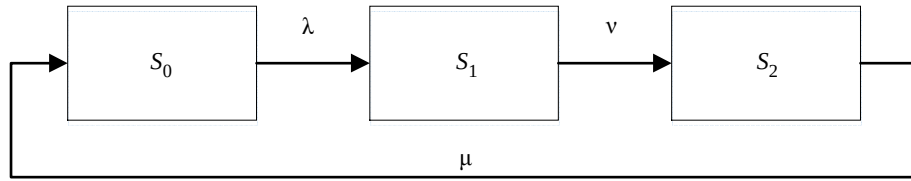


Рис. 2

Для определения вероятности состояния безопасности речевой информации в таком помещении используем теорию марковских процессов. Проанализировав ситуации, в которых может находиться помещение с точки зрения безопасности речевой информации, можно выделить следующие его состояния: S_0 – радиозакладка в помещение не внедрена; S_1 – радиозакладка в помещение внедрена за время $t_{\text{вн}}$, функционирует, но службой безопасности не обнаружена; S_2 – радиозакладка в помещение внедрена, функционирует, службой безопасности обнаружена за время $t_{\text{обн}}$, но местоположение ее неизвестно. При этом переход помещения в состояние S_0 произойдет после определения местоположения и изъятия радиозакладки службой безопасности за время $t_{\text{из}}$. Процесс перехода помещения из одного состояния в другое можно с достаточной для оценки точностью представить в виде графа (рис. 2).

Зная средние времена переходных процессов, можно найти их интенсивности: $\lambda = \frac{1}{t_{\text{вн}}}$ – интенсивность внедрения радиозакладки; $\nu = \frac{1}{t_{\text{обн}}}$ – интенсивность обнаружения радиозакладки; $\mu = \frac{1}{t_{\text{из}}}$ – интенсивность определения местоположения и изъятия радиозакладки.

Для вероятностей состояний помещения, показанных на рис. 2, можно составить уравнения Колмогорова:

$$\begin{cases} \frac{dP_0}{dt} = \mu P_2 - \lambda P_0, \\ \frac{dP_1}{dt} = \lambda P_0 - \nu P_1, \\ \frac{dP_2}{dt} = \nu P_1 - \mu P_2. \end{cases}$$

Решая данную систему уравнений, получим вероятность того, что радиозакладка в помещении отсутствует:

$$P_0 = \frac{\mu \nu}{\mu \nu + \lambda \nu + \lambda \mu}.$$

Вероятность того, что радиозакладка в помещение внедрена, функционирует, но службой безопасности не обнаружена:

$$P_1 = \frac{\mu \lambda}{\mu \nu + \lambda \nu + \lambda \mu}.$$

Вероятность того, что радиозакладка обнаружена службой безопасности:

$$P_2 = \frac{\lambda \nu}{\mu \nu + \lambda \nu + \lambda \mu}.$$

Из полученных выражений видно, что обсуждаемая информация будет безопасна тогда, когда радиозакладка в помещение не будет внедрена, а значит, вероятность безопасности информации будет определяться по следующей формуле:

$$P_{\text{б.и}} = P_0 = \frac{\mu \nu}{\mu \nu + \lambda \nu + \lambda \mu}.$$

Здесь среднее время внедрения и среднее время изъятия радиозакладки определяются экспертными оценками, а для определения среднего времени обнаружения радиозакладки можно использовать следующее аналитическое выражение [5]:

$$\bar{t}_{\text{обн}} = \frac{\frac{\bar{t}_{\text{прох}}}{\alpha_{\text{и}}} + \bar{t}_{\text{ан}}}{P_{\text{ЭМД}}},$$

где $P_{\text{ЭМД}} = P(Z > Z_{\text{тр}})$ – вероятность электромагнитной доступности (ЭМД) радиозакладки поисковому устройству. Здесь Z – отношение уровня сигнала к уровню помехи на входе поискового устройства, в дБ; $Z_{\text{тр}}$ – требуемое соотношение для качественного обнаружения. Для практических расчетов в выделенном помещении можно принять $P_{\text{ЭМД}} \sim 1$. Среднее время прохода поисковым приемником диапазона частот $\bar{t}_{\text{прох}}$ определяется по формуле [6]

$$\bar{t}_{\text{прох}} = \frac{\Phi_0}{\gamma_{\text{т}}} + \Phi_0 \lambda_f \frac{\bar{t}_{\text{ан}}}{K_f},$$

$$\alpha_{\text{и}} = \frac{\bar{t}_{\text{и}}}{\bar{t}_{\text{и}} + \bar{t}_{\text{ан}}},$$

где $\bar{t}_и$ – среднее время работы радиозакладки на излучение; $\bar{t}_{ан}$ – среднее время анализа обнаруженного излучения (согласно тактико-техническим характеристикам поисковых приемников оно составляет до 9 с); Φ_0 – диапазон частот, в котором может работать радиозакладка; γ_T – техническая скорость перестройки поискового приемника, определяемая из тактико-технических характеристик; λ_f – удельная нагрузка диапазона частот источниками излучения; K_f – коэффициент просеивания источников излучения по частоте. Частоты известных источников радиоизлучения записываются в память поискового приемника и автоматически им пропускаются, что ускоряет поиск радиозакладки. Данные выражения справедливы для поисковых приемников с последовательной перестройкой по диапазону частот. Для панорамных приемников время, затрачиваемое на перестройку по диапазону частот, будет отсутствовать. В этом случае среднее время прохода диапазона частот определяется только временем анализа обнаруженных излучений с целью опознавания радиозакладки.

На рис. 3 приведена зависимость вероятности безопасности информации в выделенном помещении от интенсивности внедрения радиозакладки λ при $\mu = 0.5$, $\nu = 0.5$, на рис. 4 – от интенсивности изъятия радиозакладки μ при $\lambda = 0.5$, $\nu = 0.5$.

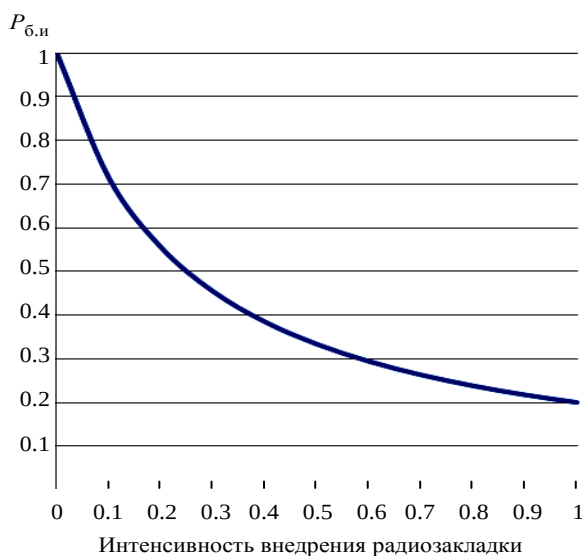


Рис. 3

Анализ полученных результатов. Анализ результатов показывает, что безопасность информации в выделенном помещении зависит от интенсивности внедрения радиозакладок и интенсивности

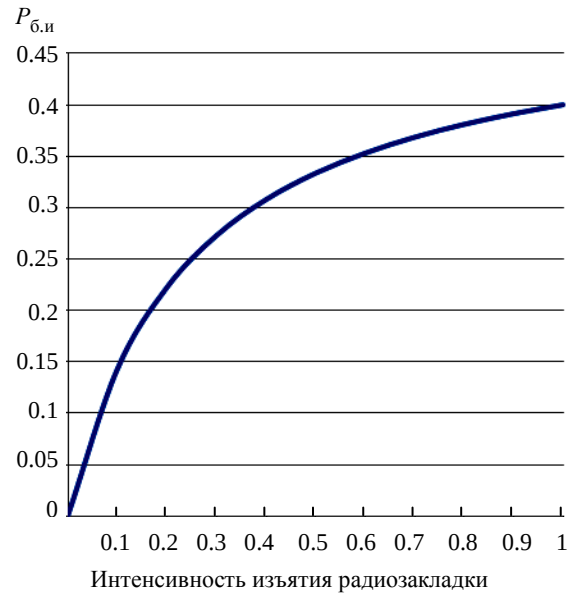


Рис. 4

проведения всех процессов спецпроверки помещения. Практически это означает, что безопасность в выделенном помещении должен обеспечивать особый режим его использования, заключающийся в надежной охране выделенного помещения, обеспечении безопасного пропускного режима и своевременного проведения профессиональными специалистами спецпроверки.

Как уже отмечалось, поиск радиозакладок имеет некоторые особенности. Мало понять, что радиозакладка в помещении присутствует, большую проблему представляет задача ее локализации. Аналитическое выражение для оценки вероятности безопасности информации получено в предположении, что вероятности опознавания радиозакладки и определения ее местоположения с учетом электромагнитной доступности равны 1. В реальной жизни это далеко не так, поэтому представляет теоретический и практический интерес учет этих особенностей.

Вероятность опознавания радиозакладки определяется по информативности ее демаскирующих признаков [7]:

$$P_{опоз} = 1.58 \left(1 - e^{-\frac{K_{ин}}{K_{ин.тр}}} \right),$$

где $K_{ин.тр}$ – требуемый коэффициент информативности, обычно принимаемый равным 0.8. Коэффициент информативности определяется по формуле

$$K_{ин} = \frac{M - M_a}{M},$$

где M – общее количество объектов; M_a – количество объектов, обладающих признаком «а».

Вероятность определения местоположения радиозакладки с учетом ее электромагнитной доступности учитывает особенности локализации месторасположения радиозакладки и определяется согласно выражению [6]

$$P_{\text{опр.мест}} = P \left[\left(\frac{P_{\text{сигн}}}{P_{\text{пом}}} \right)_{\text{вх}} > \left(\frac{P_{\text{сигн}}}{P_{\text{пом}}} \right)_{\text{вх. тр}} \right],$$

где $P_{\text{сигн}}$ и $P_{\text{пом}}$ – уровни сигнала и помехи соответственно.

Чем выше вероятность определения местоположения радиозакладки, тем меньше время на ее изъятие.

С учетом изложенного формула для определения вероятности безопасности речевой инфор-

мации в выделенном помещении будет выглядеть следующим образом:

$$P_{\text{б.и}} = \frac{P_{\text{опр.мест}} \mu P_{\text{опоз}} \nu}{P_{\text{опр.мест}} \mu P_{\text{опоз}} \nu + \lambda P_{\text{опоз}} \nu + \lambda P_{\text{опр.мест}} \mu}.$$

Таким образом, полученные аналитические выражения позволяют оценить не только безопасность переговоров в выделенном помещении, но и эффективность проводимых мероприятий защиты. Методика может использоваться специалистами организации при оценке состояния безопасности информации как в выделенном помещении, так и при проведении внутренних аудитов информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1. Приказ Гостехкомиссии России от 30.08.2002 № 282 «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТП-К)». URL: <http://cadastral-engineer.ru/wp-content/uploads/2015/01/str-k.pdf>.
2. Сабынин В. Н., Сущенко М. М. Методика комплексной оценки безопасности информации, обрабатываемой на объектах ТСОИ // Проблемы информационной безопасности. 1999. № 4.
3. Хорев А. А. Аналоговые акустические радиозакладки // Спецтехника и связь. 2011. URL: <http://www.bnti.ru/showart.asp?aid=941&lvl=05.01.01>.

4. ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения». URL: <http://docs.cntd.ru/document/gost-r-50922-2006>.

5. Сабынин В. Н., Беззатеев С. В. Безопасность информации: учеб. пособие / Департамент федеральной гос. службы, учеб.-метод. центр. СПб., 2001. Вып. 3. 64 с.

6. Сабынин В. Н. Разведзащищенность, радио-электронная защита и безопасности информации: учеб. пособие. 3-е изд. / ВАС. СПб., 1998. 32 с.

7. Справочник по информационной безопасности / под ред. Н. В. Нашивочникова; Газинформсервис. СПб., 2014. 424 с.

A. A. Lavrova, V. N. Sabyinin

Saint Petersburg Electrotechnical University «LETI»

METHODS SAFETY EVALUATION OF NEGOTIATIONS IN THE SELECTED ROOM OF THE ORGANIZATION

We consider a descriptive model of the special rooms, selection and justification of indicators evaluating it's security in the processing of confidential information. The technique of information security assessment in a special room of the organization under the threat of introduction in his embedded devices.

Information security, embedded device, special checks, the probability