МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности

УТВЕРЖДАЮ
Проректор по учебной работе
_____ О.Г. Локтионова
«__» _____ 2016 г.

ИЗУЧЕНИЕ МЕТОДИКИ ОБСЛЕДОВАНИЯ ПОМЕЩЕНИЯ С ПОМОЩЬЮ ОНЧ-ЗОНДА И ДОПОЛНИТЕЛЬНОГО ВХОДА

Методические указания по выполнению лабораторных и практических работ по дисциплине «Инженерно-техническая защита информации» для студентов специальностей 10.05.02, 10.05.03, 10.03.01, 10.04.01.

Курск 2016

УДК 004
Составители: И.В. Калуцкий, Рудак И.И, Тепикина А.В.

Рецензент
Кандидат технических наук, доцент кафедры
информационной безопасности *А.Г. Спеваков*

Изучение методики обследования помещения с помощью ОНЧ-зонда и дополнительного входа: Методические указания по выполнению лабораторных и практических работ по дисциплине «Инженерно-техническая защита информации» / Юго-Зап. гос. ун-т; сост.: И.В. Калуцкий, И.И. Рудак, А.В. Тепикина. Курск, 2016. 12 с., Библиогр.: с. 12.

Содержат сведения по вопросам методики обследования помещения при помощи ОНЧ-зонда и дополнительного входа. Указывается порядок выполнения лабораторной работы, правила оформления, содержание отчета.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Комплексная защита объектов информатизации», «Информационная безопасность», «Информационная безопасность автоматизированных систем».

Предназначены для студентов специальностей 10.05.02, 10.05.03, 10.03.01, 10.04.01. дневной формы обучения.

Текст печатается в авторской редакции
Подписано в печать. Формат 60x84 1/16.
Усл.печ.л. 1,51 .Уч. –изд.л. 1,37 .Тираж 30 экз. Заказ 594 Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Низкочастотный зонд (ОНЧ-зонд) обнаруживает устройства с очень низкими частотами излучения, также известные как передатчики несущего тока. Эти устройства используют линии АС питания как линию передачи, перемещая несущий сигнал по ней (беспроводные FM частотные сообщения, проходящие через электронные преобразователи, являются примером передатчика несущего тока). Устройства несущего тока могут также использовать смешанные провода, кабели или телефонные линии. ОНЧ-зонд обнаруживает подслушивающие устройства - "жучки", которые используют для передачи сигнала комнатную электропроводку. Он подключается к сетевым розеткам, и имеет входной полосовой фильтр диапазоне от 15 кГц до 1мгц

Некоторое оборудование с комплексными устройствами подачи питания, такие как компьютеры, копиры, факсы и т. д. могут создавать ОНЧ сигналы в линиях питания. Необходимо выборочно выключить эти устройства, чтобы определить источник этого явления. Если нет уверенности, что причина этого явления комплексное устройство подачи питания, необходимо проверить подозрительное оборудование.

ЦЕЛЬ РАБОТЫ

Целью работы является выработка практических навыков при обследовании помещения универсальным прибором для обнаружения устройств скрытого съема информации СРМ-700 при использовании ОНЧ-зонда.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

1. Изучить область применения прибора
2. Изучить подготовку ОНЧ-зонда к работе
3. Изучить понятие дополнительного входа
4. Ознакомиться с методикой проверок с помощью дополнительного входа
5. Выполнить обследование помещения
4. Написать вывод

СОДЕРЖАНИЕ ОТЧЕТА

1. Титульный лист
2. Задание
3. Ход работы или основная часть
4. Вывод

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

ОНЧ-зонд применяется для поиска низкочастотных устройств прослушивания, которые используют линии электропроводки в качестве путей передачи сигнала. (Бытовой FM-intercom являются примером такого устройства). ОНЧ-зонд подключается к сетевым розеткам, и имеет входной полосовой фильтр диапазоне от 15 кГц до 1мгц. Вы можете проверить и другие сети, кабели и телефонные линии на наличие ОНЧ-передатчиков, присоединив их входную пару проводов к вилке ОНЧ-зонда. Некоторое оборудование, питаемое от сети, может производить аналогичный низкочастотный шум (НЧ-шум) в сети, который может быть принят за искомый сигнал передатчика. По очереди отключите эти устройства, чтобы отделить производящее такой НЧ-шум. Если вы не уверены, что детектируемый шум от блока питания такого устройства, то проверьте его на наличие передатчика.

Подготовка ОНЧ-зонда к работе

1. Подключите наушники, установите регулятор громкости на минимум (против часовой стрелки). На дисплее будет изображено:[1]

2. Проверьте калибровку счетчика. На дисплее должно быть 2 или 3 сегмента при высокой мощности (HIGH GAIN).

3. Сначала подключите ОНЧ-зонд к источнику переменного тока в области высокого уровня безопасности. Выберите режим высокой или низкой мощности по необходимости. Нормальный уровень для переменного тока – 3 к 7 на дисплее. (Отметьте показание для сравнения.) Изолируется напряжение переменного тока, пока CPM -700 исследует диапазон от 15Гц до 1МГц.

4. Подключите ОНЧ-зонд к источнику питания в исследуемой области и сравните показания на дисплее с уровнем из безопасного источника.

5. Настройте громкость и слушайте, нет ли известного источника звука.

6. Проверьте остальные источники питания, подключая прибор и сравнивая показания дисплея и звуки. Если Вы обнаружите устройство уровень на дисплее возрастет. Слушайте, нет ли известного источника звука.

7. Чтобы проверить другие провода, кабели или телефонные линии на наличие ОНЧ сигналов, включая видео, соедините ТВНЧ адаптер с зондом и зажмите подозрительную пару проводов.

ПРИМЕЧАНИЕ: Регуляторы и неисправные флуоресцентные лампы могут быть причиной фонового шума. Эти эффекты могут быть уменьшены при удалении неисправных ламп или включением регуляторов на максимум. Использование звукового фильтра также поможет уменьшить шумы. Полное выключение шумовой среды может также отключить жучок. ОНЧ обычно не проходят через трансформатор; поэтому проверьте все розетки, т. к. они могут быть с разными фазами.

Проверка сети

А. Подключите ОНЧ-зонд к сетевой розетке в зоне контроля и сравните показания дисплея с показаниями в незащищенной зоне.

Б. Установите усиление звука до комфортного уровня и включите источник "известного звука".

В. Проверьте все розетки в зоне контроля таким образом.

При приближении к ОНЧ-передатчику уровень сигнала на дисплее возрастает. Ловите "известный звук" в наушниках.

ПРИМЕЧАНИЕ: ОНЧ-сигнал не проходит через трансформатор, поэтому проверяйте все розетки, поскольку они могут быть расположены с разных сторон обмоток.

Физический поиск

Следует провести тщательный физический поиск, так как жучки могут дистанционно отключаться или не обнаруживаются обычной поисковой аппаратурой.

Проверьте все сетевые розетки, настенные выключатели, осветительные приборы и питаемое от сети оборудование: компьютеры, ксероксы, радиоприемники и т.д. на наличие необычных элементов и проводников.

Дополнительный вход

Усилитель дополнительного входа используется для "прослушивания" сетей, подозрительных с точки зрения передачи звуковых и иных сигналов. Симметричный вход позволяет тестировать телефоны и телефонные цепи на вторжение извне или отслеживать такое вторжение в режиме мониторинга и записи на внешний магнитофон [2]. В зависимости от уровня входного сигнала выбирается high или low уровень усилителя.

ВНИМАНИЕ: Дополнительный вход не должен подключаться к цепям с напряжением более 52 вольт. Это может привести к повреждению прибора и даже электротравме!

Процедура включения:

Если это не оговорено специально, данная процедура используется для каждого включения дополнительного входа.

А. Отсоедините любой зонд, если он был подключен к зондовому входу и подключите специальный кабель к дополнительному входу на боковой стороне прибора.

Б. Подключите наушники и выставьте усиление звука на минимум, затем, выбор режимов работы и усиления поставьте на Search и High, т.е. в нажатое положение.

В. Включите дисплей и убедитесь в следующих установках дисплея:

ПРИМЕЧАНИЕ: Дополнительный вход не будет работать, если к зондовому входу подключен один из зондов.

ПРИМЕЧАНИЕ: В СРМ-700 используется автоматическая регулировка усиления звука в цепи звукового усилителя для

контроля громкости и предупреждения перегрузки. В этом режиме дисплей не работает при показаниях выше 2 - 3 сегментов.

Проверка телефонных линий:

Дополнительный вход позволяет проверять наличие на телефонных линиях наличие жучков, работающих при положенной трубке и слушающих комнату по возбуждаемым гармоникам.

А. Определите телефонные провода для питания и собственно звука (обычно красный и зеленый) и присоедините к ним кабель дополнительного входа.

Б. Прослушивайте через наушники сигнал от источника "известного звука", "чистый" телефон не транслирует звук при лежащей трубке. Если на линии есть "электронный триггер" или в телефоне перемычка для активизации микрофона при лежащей трубке, то вы услышите в наушниках ваш звук. В этом случае проверьте линию и телефонный аппарат на наличие жучков.

В. Повторите этот тест с каждой комбинацией проводов, соединенных с телефоном. При необходимости проверьте назначение каждого провода с помощью цифрового вольтметра.

Г. Вы можете выполнять эту проверку в режиме мониторинга, поскольку эти устройства могут быть дистанционно управляемы и не работать в данный момент.

ПРИМЕЧАНИЕ: Для проверки телефонных линий на наличие РЧ и ОНЧ можно использовать РЧ (радиочастотный) и ОНЧ-зонды, как это было описано в соответствующих главах данного описания.

Идентификация обнаруженной проводки:

Во время физического поиска вы можете обнаружить "неизвестные" кабели провода. С помощью дополнительного входа CPM-700 возможно прослушать эти линии, чтобы определить, используются они для легальных целей или для нелегальной передачи информации.

Даже если эта линия используется легально, то это не значит, что она безопасна с точки зрения утечки информации. Громкоговорители, интеркомы, компьютеры, настольные

радиоприемники и охранная сигнализация, реагирующая на звук могут быть использованы для нелегального прослушивания помещения. Когда громкоговоритель выдает звук, то обычно он не может работать как микрофон, но если он выключен, то определенно может. Чтобы обезопасить себя в этом отношении, отсоедините и вынесите все громкоговорители, не используемые в этой комнате. С оставшимися следует поступить следующим образом: модернизируйте цепь громкоговорителя с помощью переключателя и резистора, как показано на рисунке, с целью физической изоляции громкоговорителя. Нагрузочное сопротивление должно быть мощностью 1 Вт для громкоговорителей офисного оборудования или настольных и 5-10 Вт для более мощных музыкальных. Значение сопротивления должно быть такое же, как и у громкоговорителя.

Следует проявить осторожность при работе с компанией, которая устанавливает охранную сигнализацию в офисе, работающую с помощью прослушивания определенной линии, контролируя таким образом происходящее в помещении. Хотя большинство компаний заслуживают доверия, факт прослушивания линии является настораживающим. Даже если охранная система отключается в рабочее время, линия с микрофоном остается на месте и может быть использована для нелегального прослушивания. Использование переключателей, описанных выше с целью физической изоляции микрофона, может свести опасность к минимуму. В зависимости от требуемого уровня безопасности иногда имеет смысл не оборудовать помещения типа конференц-зала охранной сигнализацией, следящей за звуком в помещении.

ПРИМЕЧАНИЕ: Для графитовых или электретных усилителей может понадобиться источник постоянного тока. Обычно, если вы проводите поиск, а другая сторона об этом не знает, или отсутствует дистанционное управление питания линии с жучком, то звуковой сигнал, передаваемый жучком, будет вами засечен. Но если питание может быть отключено, то не будет и сигнала.

ВНИМАНИЕ! Перед тем как пытаться присоединить прибор к неизвестному проводу или кабелю, убедитесь, не находится ли он под опасным напряжением. Значение напряжения не должно превышать 50 В как для переменного, так и для постоянного тока.

Звуковое тестирование:

Дополнительный встроенный усилитель CPM используется с дополнительным кабелем, чтобы проверять подозрительное проводное обеспечение на наличие голосов или других сигналов.

Исследование телефонных линий осуществляется для разового тестирования, но не для тайного перехвата.

*ПРЕДУПРЕЖДЕНИЕ: Разъем кабеля нельзя соединять с линиями питания более 52 В. Возможно повреждение прибора и поражение током!

Настройка прибора для звукового тестирования:

Удалите все подключенные к передней панели зонды и подключите шнур к разъему на боковой панели. Дополнительный разъем не будет функционировать, если зонд подключен к своему разъему.

Проверка проводов/кабелей на наличие звуковых сигналов:

А. Выполните процедуру включения прибора с дополнительным входом, как это было описано в начале главы.

Б. Убедитесь, что проверяемый провод или кабель не находятся под опасным напряжением и присоедините к нему специальный кабель от дополнительного входа.

В. Настройте автоматическую регулировку усиления на комфортный уровень слышимости звука. Для уменьшения шума постоянного тока можно использовать фильтр (Filter).

Г. Пытайтесь услышать ваш источник "известного звука" или какие-либо необычные шумы.

Д. Если идет перегрузка по входному звуку, можно поменять усиление на Low (низкое).

Е. В многожильном кабеле следует проверить каждую пару проводов независимо от того, составляют они витую пару или нет. Должны быть проверены все парные комбинации проводов.

Ж. Проведите проверку всех подозрительных проводов в зоне контроля.

ПРИМЕЧАНИЕ: Для проверки телефонных линий на наличие РЧ и ОНЧ можно использовать РЧ и ОНЧ-зонды, как это было описано в соответствующих главах данного описания.

ЗАДАНИЕ

1. Подключить ОНЧ-зонд к сетевой розетке в проверяемом помещении и сравнить показания дисплея с показаниями в незащищенной зоне.
2. Сделать вывод, изменился ли уровень шума.
3. Определить, влияет ли на уровень сигнала наличие электродвигателя (электродвигатель, как источник помех, может играть роль закладного устройства).

КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Какого применение ОНЧ-зонда.
2. Как осуществляется подготовка ОНЧ-зонда к работе?
3. Для чего используется дополнительный усилитель?
4. Как осуществляется проверка телефонных линий?
5. Для чего и каким образом осуществляется звуковое тестирование?

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Руководство пользователя прибора для обнаружения устройств скрытого съема информации. Модель: СРМ -700.
2. Бузов Г.А., Калинин С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам – М.: Горячая линия-Телеком, 2005.