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
«15» 12 2017 г.

Модификация тонального сигнала набора номера

Методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» для студентов укрупненной группы специальностей 10.05.02

Курск 2017

УДК 621.3.014.22 (076.5)

Составители: В.Л. Лысенко, М.А. Ефремов.

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

Модификация тонального сигнала набора номера: методические указания по выполнению практической работы по дисциплине «Информационная безопасность телекоммуникационных систем» / Юго-Зап. гос. ун-т; сост.: В.Л. Лысенко, М.А. Ефремов. Курск, 2017. 11 с. Библиогр.: с. 11.

Методические указания соответствуют требованиям программы, утвержденной учебно-методическим объединением по специальностям и направлениям подготовки «Информационная безопасность телекоммуникационных систем».

Предназначены для студентов укрупненной группы специальностей 10.05.02 дневной формы обучения.

Текст печатается в авторской редакции

Подписано в печать. 15.12.17. Формат 60x84 1/16.
Усл. печ. л. 0,7 Уч. –изд.л. 0,6 Тираж 30 экз. Заказ 2967. Бесплатно.
Юго-Западный государственный университет.
305040, г. Курск, ул. 50 лет Октября, 94.

Содержание

1 Цель практической работы

Ознакомление с одним из методов злонамеренной модификации двухчастотного тонального сигнала набора номера при несанкционированном доступе к системе телефонной связи.

Перед выполнением практического задания студенты должны ориентироваться в основных аспектах информатики, а также иметь начальные знания по программе **Adobe Audition**.

В результате выполнения практического задания студенты должны получить знания по возможным злонамеренным действиям с сигналами набора номера на основе использования специальных программных средств.

2 Задание

1. При подготовке к практическому занятию изучить следующие вопросы: методы сигнализации в телефонных сетях, методы генерации сигналов тонального набора номера (DTMF-signals) и шума, методы их редактирования (временного перемещения) в программе **Adobe Audition**.

2. Запустить программу **Adobe Audition**, кликнув ее значок на ***Рабочем столе*** (если он имеется), либо запустив ее из меню ***Пуск*** или с помощью ***Проводника***.

3. Сгенерировать тональный набор произвольного 6-тизначного телефонного номера и записать его в тетрадь (сделать скриншот во временной и частотных областях).

4. Используя компьютерную мышь, скопировать в память временной сегмент паузы между сигналами цифр номера и вставить ее после сигнала одной из цифр номера.

5. Используя компьютерную мышь, «вырезать» в буферную память фрагмент тонального сигнала какой-либо выбранной цифры этого номера и вставить еев позицию после вставленного ранее временного сегмента паузы (должен получиться модифицированный телефонный номер).

6. «Вырезать» лишние временные сегменты пауз между сигналами цифр номера (сделать скриншот во временной и частотных областях).

7. Используя опцию ***Меню > Effects > Filters > FFT Filter*** определить по частотному спектру полученный модифицированный телефонный номер и сравнить его с предполагаемым.

3 Порядок выполнения работы

1. Изучить методические указания к данному практическому занятию.
2. Получить у преподавателя задание.
3. Выполнить практическую часть
4. Ответить на контрольные вопросы.

4 Содержание отчета

1. Краткие теоретические сведения по методам передачи номера абонента в абонентской линии.
2. Выполненное задание по заданному преподавателем варианту.
3. Временные и спектральные диаграммы (скриншоты) полученных результатов.

5 Теоретическая часть

Угроза - это потенциальная возможность определенным образом нарушить инфокоммуникационную безопасность. Под ***угрозой безопасности*** ТКС понимают возможные действия, способные прямо или косвенно нанести ущерб ее безопасности.

Ущерб безопасности подразумевает нарушение состояния защищенности информации, передаваемой ТКС.

Попытка реализации угрозы называется ***атакой***, а физическое лицо, предпринимающие такую попытку - ***злоумышленником***. Потенциальные злоумышленники называются ***источниками угрозы***.

С понятием угрозы безопасности тесно связано понятие ***уязвимости*** ТКС.

Уязвимость ТКС – это присущее ей неудачное свойство, которое может привести к реализации угрозы ее безопасности.

Атака на ТКС – это поиск и/или использование злоумышленником той или иной ее уязвимости, т.е. реализация угрозы безопасности.

Чаще всего угроза является следствием наличия уязвимых мест в защите инфокоммуникационных систем (таких, например, как возможность доступа посторонних лиц к критически важному оборудованию или ошибки в программном обеспечении).

Классификация угроз инфокоммуникационной безопасности

Угрозы можно классифицировать по нескольким критериям:

- по аспекту инфокоммуникационной безопасности (доступность, целостность, конфиденциальность), против которого угрозы направлены в первую очередь;
- по компонентам инфокоммуникационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Классификация угроз по аспекту инфокоммуникационной безопасности

Основные угрозы доступности

Доступность – это возможность за приемлемое время получить требуемую инфокоммуникационную услугу.

Инфокоммуникационные системы создаются для получения определенных инфокоммуникационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это наносит ущерб всем субъектам инфокоммуникационных отношений. Поэтому ***доступность*** выделяется как важнейший элемент инфокоммуникационной безопасности.

Особенно ярко ведущая роль доступности проявляется в различных системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность инфокоммуникационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Выделяют 4 типа угроз доступности информации: непреднамеренные ошибки, отказ пользователей, внутренний отказ инфокоммуникационной системы, отказ поддерживающей инфраструктуры.

Самыми частыми являются ***непреднамеренные ошибки*** штатных пользователей, операторов, системных администраторов и других лиц,

обслуживающих инфокоммуникационные системы. Иногда такие ошибки и являются собственно угрозами (неправильно введенные данные или ошибка в программе, вызвавшая крах системы), иногда они создают уязвимые места, которыми могут воспользоваться злоумышленники (таковы обычно ошибки администрирования). Самый ***радикальный способ борьбы*** с непреднамеренными ошибками - ***максимальная автоматизация*** и ***строгий контроль.***

Другие угрозы доступности можно классифицировать по компонентам ИС, на которые нацелены угрозы:

- отказ пользователей;
- внутренний отказ инфокоммуникационной системы;
- отказ поддерживающей инфраструктуры.

Виды угроз типа «отказ пользователей»:

- нежелание работать с инфокоммуникационной системой (чаще всего проявляется при необходимости осваивать новые возможности и при расхождении между запросами пользователей и фактическими возможностями и техническими характеристиками);
- невозможность работать с системой в силу отсутствия соответствующей подготовки (недостаток общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.п.);
- невозможность работать с системой в силу отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.).

Например, сотрудник организации, которому поступило служебное электронное письмо, может проигнорировать его получение, в результате чего, письмо может «зависнуть», а содержащаяся в нем информация устареть и потерять свою актуальность.

Виды угроз типа «внутренний отказ инфокоммуникационной системы»:

- отступление (случайное или умышленное) от установленных правил эксплуатации;
- выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей или обслуживающего персонала (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.);

- ошибки при конфигурировании системы;
- отказы программного и аппаратного обеспечения;
- разрушение данных;
- разрушение или повреждение аппаратуры.

Виды угроз типа «отказ поддерживающей инфраструктуры»:

- нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- разрушение или повреждение помещений;
- невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Весьма опасны так называемые «обиженные» сотрудники - действующие и бывшие, так как потенциально могут нанести вред организации-«обидчику», например:

- испортить оборудование;
- встроить логическую бомбу, которая со временем разрушит программы и/или данные;
- удалить данные.

Обиженные сотрудники, даже бывшие, знакомы с порядками в организации и способны нанести немалый ущерб. Необходимо следить за тем, чтобы при увольнении сотрудника его права доступа (логического и физического) к инфокоммуникационным ресурсам аннулировались.

С другой стороны представляют серьезную опасность стихийные бедствия и события, воспринимаемые как стихийные бедствия: пожары, наводнения, землетрясения, ураганы.

Угрозы доступности могут выглядеть грубо - как повреждение или даже разрушение оборудования. Такое повреждение может вызываться естественными причинами (чаще всего - грозами), опасны протечки водопровода и отопительной системы, поломки кондиционеров в сильную жару. Общеизвестно, что периодически необходимо производить резервное копирование данных. Однако даже если это предложение выполняется, резервные носители зачастую хранятся небрежно.

Вывод ТКС из штатного режима эксплуатации может осуществляться посредством ***агрессивного потребления ресурсов*** (обычно - ***полосы пропускания сетей, вычислительных возможностей процессоров*** или ***оперативной памяти***).

По расположению источника угрозы такое потребление подразделяется на ***локальное*** и ***удаленное***. При просчетах в конфигурации системы ***локальная программа*** способна практически монополизировать процессор и/или физическую память, сведя скорость выполнения других программ к нулю или, например, количество подключившихся пользователей ограничено ресурсами системы. Примером ***удаленного потребления ресурсов*** являются DoS-атаки – атаки на отказ в обслуживании.

Основные угрозы целостности

Целостность информации – это ее свойство сохранять свою структуру и/или содержание в процесс передачи и хранения. Целостность информации обеспечивается в том случае, если данные в системе не отличаются в семантическом отношении от данных в исходных документах, т.е. если не произошло их случайного или преднамеренного искажения или разрушения. Обеспечение целостности данных является одной из сложных задач защиты ТЛКС.

При нарушении целостности информации может пострадать ее ***достоверность***. Достоверность информации – это ее свойство, выражающееся в строгой принадлежности субъекту, который является ее источником, либо тому субъекту, от которого эта информация принята.

Целостность можно подразделить на ***статическую*** (понимаемую как неизменность инфокоммуникационных объектов) и ***динамическую*** (относящуюся к корректному выполнению сложных действий (транзакций)).

Определено пять основных угроз динамической целостности: 1) нарушение атомарности транзакций, 2) переупорядочение данных, 3) кража данных; 4) дублирование

данных; 5) внесение дополнительных сообщений (например, сетевых пакетов и т.п.). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений. Соответствующие действия и сетевой среде называются активным прослушиванием.

С целью нарушения статической целостности злоумышленник (как правило, штатный сотрудник) может:

- ввести неверные данные;
- изменить данные.

Например, заголовки электронного письма могут быть подделаны, а письмо в целом может быть фальсифицировано лицом, знающим пароль. Последнее возможно даже тогда, когда целостность контролируется криптографическими средствами. Здесь имеет место взаимодействие разных аспектов инфокоммуникационной безопасности: если нарушена ***конфиденциальность***, то может пострадать и ***целостность.*** Угрозой целостности является не только фальсификация или изменение данных, но и отказ от совершенных действий. Если нет средств обеспечить «неотказуемость», компьютерные данные не могут рассматриваться в качестве доказательства.

Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит "руководством к действию". Рецептура лекарств, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой недопустимо. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации.

Потенциально уязвимы с точки зрения нарушения ***целостности*** не только ***данные,*** но и ***программы.*** Внедрение ***вредоносного ПО*** (т.н. ***программных вирусов***) - пример подобного нарушения.

7 Контрольные вопросы

1. Что такое инфокоммуникационная безопасность, угроза безопасности ТКС, атака, злоумышленник?

2. Что такое источники угрозы и уязвимость ТКС?
3. По каким четырем критериям классифицируют угрозы ТКС?
4. Что такое доступность информации и какие 4 типа угроз доступности выделяют?
5. Сколько различают видов угроз типа «отказ пользователей» и какие?
6. Сколько различают видов угроз типа «внутренний отказ инфокоммуникационной системы» и какие?
7. Сколько различают видов угроз типа «отказ поддерживающей инфраструктуры» и какие?
8. Что такое достоверность информации?
9. Сколько различают основных угроз динамической целостности и какие?
10. Сколько различают основных угроз статической целостности и какие?

Библиографический список

1) Лукьянюк С.Г. Теория электрической связи. Сигналы, помехи и системы передачи: учебное пособие. / С. Г. Лукьянюк, А. М. Потапенко. – Курск.: Юго-Зап. гос. ун-т., 2012. - 223 с.

2) Осипов А. С. Военно-техническая подготовка. Военно-технические основы построения средств и комплексов РЭП : учебник / А.С. Осипов ; под науч.ред. Е.Н. Гарина. – Красноярск : Сиб. федер. ун-т, 2013. – 344 с.