вы 1-3), канд. экон. наук, доцент Р.В. Фёдоров (главы 4-6), старший преподаватель М.П. Немкова (тестовые задания), старший преподаватель А.А. Солдатов (лабораторный практикум).

Авторы благодарны своим рецензентам Ю.К. Евдокимову, доктору техн. наук, профессору, заведующему кафедрой радиоэлектроники и информационно-измерительной техники Казанского национального исследовательского технического университета им. А.Н. Туполева, и В.К. Краснову, кандидату физ.-мат. наук, доценту.

Авторы будут признательны за любые замечания, предложения, пожелания.

Пособие рекомендуется в качестве основного учебного материала по курсу «Компьютерная графика» для высших учебных заведений. Его также можно использовать как самоучитель, с помощью которого за короткое время можно самостоятельно освоить актуальные компьютерные технологии.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ: ЗАЩИТА ИНФОРМАЦИИ (учебного пособие)

Сильнов Д.С., Тараканов О.В.

ФГАОУ ВО «Национальный исследовательский ядерный университет «МИФИ», Москва, e-mail: ds@silnov.pro

Данное учебное пособие предназначено для ознакомления с основными проблемами, которые стоят в предметной области информатики и вычислительной техники с точки зрения защиты информации. В нём изложены основные базовые направления, в которых могут производить научные исследования магистры в рамках написания магистерской диссертации. В методическом пособии уделено особое внимание наукоёмким проблемам, стоящим перед современным научным миром. Представленное методическое пособие предназначено для студентов, обучающихся по программам магистратуры.

Крипто алгоритмы

Раздел посвящен проблеме стойкости крипто алгоритмов, задаче разработки криптостойких шифров, а также вопросу взлома шифров, уязвимости как устаревших криптоалгоритмов (например, DES), так и существующим атакам на современные – AES и пр.

Также рассмотрены проблемы легковесной криптографии, используемой на мобильных устройствах, а также устройствах специального назначения, где отсутствуют высокие вычислительные мощности, но необходимо применять программные средства шифрования.

Уязвимости программного кода

Рассмотрены уязвимости программного кода на примере, как компилируемого программного обеспечения, так и интерпретируемого.

В подразделе «Компилируемое программное обеспечение» рассмотрены проблемы безопасного программирования, приведены примеры небезопасного программирования и примеры использования уязвимых мест с помощью shellcode. Описан процесс разработки и использования shellcode.

В подразделе «интерпретируемое программное обеспечение» рассмотрены такие уязвимости, как «remote file inclusion» на примере языка PHP (с примерами использования данных уязвимостей и объяснениями причин возникновения подобных проблем при написании программного кода), а также уязвимости типа SQL injection, с примерами.

Аппаратные уязвимости

В данном разделе рассмотрены современные проблемы использования беспроводных технологий: технология Wi-Fi – проблема перехата передаваемых сообщений, использование слабых средств шифрования (в том числе, WEP) для доступа во внутрикорпоративные сети, перебор паролей при использовании технологии WPA. Описаны проблемы технологии RFID, применения небезопасных карт типа Milfare Classic, рассмотрено устройство, используемое специалистами по безопасности для анализа современных RFID-протоколов: proxmark3. Технология NFC описана с точки зрения возможных проблем использования в условиях городского использования.

В подразделе «проводные технологии» описаны технологии, именуемые как «аппаратные закладки», когда в микросхемах содержатся недокументированные функции. Проблема наличия таких функций и возможные пути контроля и диагностики.

Раздел «физические сети передачи данных» содержит информацию о съеме данных из проводных каналов, в том числе оптоволоконных и при использовании технологии Twisted pair.

Технологии обнаружения злоумышленников

Рассмотрены современные системы обнаружения вторжения, антивирусы, межсетевые экраны, сканирование глобально распределенных сетей.

В подразделе «проактивные технологии» описаны передовые технологии, работающие на упреждение атаки. Отдельно рассмотрена технология «honeypot/honeynet».

Уязвимости облачных технологий

Проблема использования облчных технологий, проблема безопасного хранения данных и доступа к этим данным. Современные способы защиты и нападения в области облачных хранилищ.

Подраздел «хищение персональных данных» описаны современные методы обнаружения хищения персональных данных, а также возможные средства, которые используют злоумышленники. В том числе элементы социальной инженерии.