УДК 004.056

В. Я. ПЕВНЕВ

МЕТОДЫ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ

Обоснована проблема целостности информации как наиболее уязвимого звена в обеспечении информационной безопасности. Рассмотрены угрозы целостности на различных этапах жизненного цикла информации. Представлены основные методы обеспечения целостности информации. В каждом из рассмотренных методов выделены основные угрозы и пути их решения. Комплексное использование рассмотренных организационных, технических, программных решений позволяет обеспечить целостность информации как основополагающей составляющей информационной безопасности систем.

Ключевые слова: целостность информации, угрозы, жизненный цикл, методы обеспечения, информационная безопасность.

Введение. Обеспечение информационной безопасности (ИБ) при использовании информационных и коммуникационных систем предполагает решение проблем обеспечения целостности, доступности и конфиденциальности [1], хотя в последних публикациях [2] и европейских стандартах [3] к этим трем китам добавляются аутентичность, подотчетность, безотказность и надежность. В большинстве систем, включая системы в которых циркулирует информация с ограниченным доступом, наиболее острой проблемой является проблема обеспечения целостности информации (ЦИ). Под целостностью понимается свойство информации быть защищенной от несанкционированного искажения, разрушения или уничтожения [4].

Следует отметить, что ни доступности, а тем более конфиденциальности, без обеспечения ЦИ достичь невозможно. Например, исходя из современных требований к криптосистемам, незначительное изменение исходного текста должно приводить к значительному изменению шифрованной последовательности. Если в процессе передачи исказится один бит передаваемой шифрограммы, то после расшифровки полученный текст будет сильно отличаться от исходного. Таким образом, можно говорить о проблеме обеспечения ЦИ, которая не решена в полной мере на сегодняшний день.

Анализ литературы. В настоящее время большинство исследователей в области ИБ занимаются криптологией. Достаточно много работ посвящено цифровой подписи. Среди них можно выделить монографию[2]. Есть отдельные работы, в которых рассматриваются вопросы обеспечения ЦИ, но они в подавляющем большинстве рассматривают вопросы целостности в базах данных [5,6] или компьютерных сетях [7]. Работ, в которых комплексно рассматриваются методы обеспечения ЦИ, автору найти не удалось.

Цель статьи – проанализировать возможные угрозы, возникающие в течение жизненного цикла информации, и рассмотреть методы обеспечения ЦИ.

Угрозы ЦИ. Исходя из определения ЦИ, можно выделить следующие воздействия на информацию[8]:

– модификацию информации;

– подмену информации;

– уничтожение информации.

Модификация предполагает изменения какой-либо части информации. Эти изменения может быть как случайным, так и преднамеренным. Во втором случае они могут быть санкционированными либо несанкционированными.

Подмена предполагает навязывание ложной информации путем замены истинной (первоначальной) информации. Уничтожение чаще всего связывается с уничтожением физического носителя информации и/или размагничиванием (форматированием) электронных носителей.

Рассмотрим возможные угрозы ЦИ в течение ее жизненного цикла.

При использовании неполных и/или ложных данных во время создания (появления) информации можно получить не соответствующую действительности информацию о тех или иных событиях. Адекватность принятого решения, основанного на такой информации, вызывает сомнения.

При обработке информации нарушение ЦИ может возникнуть вследствие технических неисправностей, алгоритмических и программных ошибок, ошибок и деструктивных действий обслуживающего персонала, внешнего вмешательства, действия разрушающих и вредоносных программ (вирусов, эксплойтов, червей, логических бомб).

В процессе передачи на информации могут воздействовать различного рода помехи как естественного, так и искусственного происхождения. При этом возможно ее искажение или стирание (уничтожение). Кроме этого, возможен перехват информации с целью ее модификации и дальнейшего навязывания.

В процессе хранения основными угрозами являются несанкционированный доступ с целью модификации (вплоть до уничтожения) информации, вредоносные программы (вирусы, трояны, черви, логические бомбы) и технические неисправности.

В процессе старения основными угрозами информации, наряду с угрозами при хранении, можно считать утерю технологий, способных воспроизвести ту или иную информацию, и физическое старение носителей информации.

Следует отметить, что на всех этапах жизненного цикла существует угроза ЦИ из-за используемых технических систем. Это банальные неисправности, сбои электропитания, электромагнитные импульсы и т.д.

При утилизации об обеспечении ЦИ речи не

идет.

Таким образом, можно сделать вывод, о том что, угрозы ЦИ возникают на протяжении всего жизненного цикла информации с момента ее появления до начала утилизации.

Надежность технических средств. Необходимым условием обеспечение ЦИ является наличие высоконадежных технических средств (ТС), которые включают в себя как аппаратную, так и/или программную составляющие [9]. Такое оборудование должно обеспечивать как высокую отказоустойчивость, так и защиту информации от возможных угроз.

Одним из самых распространенных способов повышения надежности ТС является резервирование. Если рассматривать ТС с тоски зрения информационной составляющей, то повышение надежности достигается за счет последовательного соединения элементов системы, отвечающих за данную составляющую. Если последовательно соединить два компьютера, поставив на каждый из них свой антивирус, то вероятность проникновения вредоносной программы уменьшается. Однако при этом уменьшается вероятность безотказной работы ТС, состоящей из двух компьютеров.

Для обеспечения заданной надежности (гарантоспособности) такого информационно-технического комплекса необходимо применять последовательное соединение резервированных частей ТС.

ТС предполагают и возможность использования выделенных и/или физически защищенных линии связи, например бронированные кабели с контролем целостности оболочки.

К ТС обеспечения ЦИ следует отнести и средства защиты от электромагнитного импульса (ЭМИ). Поражающими факторами ЭМИ являются высокоинтенсивные электромагнитные поля, которые либо непосредственно воздействуют на радиоэлектронные средства (РЭС), либо трансформируются в опасных трактах этих средств в наведенные токи и напряжения [10]. Наиболее эффективным методом уменьшения интенсивности ЭМИ является экранирование – размещение оборудования в электропроводящем корпусе, который препятствует проникновению электромагнитного поля от источника к защищаемому оборудованию. Однако, в большинстве случаев, защищаемое оборудование имеет внешние коммуникации, что приводит к проникновению в экранированное пространство наведенных помеховых токов и напряжения, вызывающих повреждения элементной базы РЭС. Решением являются методы ограничения наведенных напряжений и токов по амплитуде и спектру во внешних трактах РЭС и электромагнитная развязка внешних цепей РЭС от экранированных устройств. Для ограничения наводок по амплитуде и спектру используются искровые и газоразрядные разрядники, полупроводниковые ограничительные приборы, варисторы и специальные нелинейные сопротивления. К ограничителям спектра относятся проходные конденсаторы, дроссели и фильтры [10].

Электромагнитная развязка достигается с помощью изолирующих трансформаторов, дросселей, оптронов, элементы оптоэлектроники. Применение оптоэлектронных схем позволяет уменьшить число замкнутых контуров и обеспечить электрическую развязку цепей. Кроме этого системы на базе оптоэлектроники являются некритичными к воздействию помеховых электромагнитных полей вследствие того, что носителями информации в этих системах являются электрически нейтральные фотоны. Еще одним преимуществом оптоэлектронных систем является ограничение полосы пропускания, особенно на высоких частотах, и тем самым являются беспроводными ограничителями высокочастотных помеховых наводок на входные цепи РЭС, которые свойственны ЭМИ [10].

Разграничение доступа. Широко распространенным и достаточно эффективным методом обеспечения ЦИ является организация доступа к информации и используемому оборудованию. Данный метод относится к организационным и предполагает достаточно большой перечень мероприятий, начиная от подбора сотрудников и заканчивая работой с техникой и документами [11].

Среди них можно выделить технологии защиты, обработки и хранения документов, аттестацию помещений и рабочих зон, порядок защиты информации от случайных и/или несанкционированных действий персонал и т.д. Для обеспечения ЦИ в ИКС особое внимания следует уделить защите операционных систем (ОС), обеспечивающих функционирование практически всех составляющих системы. Наиболее действенным механизмом разграничения доступа для ОС является изолированная программная среда (ИПС) [12]. ИПС повышает устойчивость ИКС к различным разрушающим и вредоносным программам, позволяя обеспечить целостность информации.

Антивирусная защита. Одной из угроз ИБ являются вредоносные программы, в которых отдельным классом выделяются вирусы. Их множество видов и типов, они отличаются между собой способами воздействия на различные файлы, размещением в памяти ЭВМ или программах, объектами воздействия. Но главное свойство вирусов – способность к размножению. Это свойство выделяет их среди множества вредоносных программ и делает наиболее опасными.

Одним из самых действенных способов обеспечения ЦИ является хорошо продуманная и надежная защита от вирусов. Наиболее распространенным способом защиты от вирусов является использование антивирусных программ, которых в настоящее время достаточное количество. Однако необходимо помнить, что ни одна программа не гарантирует обнаружение неизвестного вируса.

Применяемые эвристические сканеры, которые теоретически могут обнаружить неизвестные вирусы по косвенным признакам, не всегда дают правильный диагноз. Примером подобных ошибок могу служить два антивирусные программы, запущенные на одном компьютере. Практически любой пользователь сталкивался с ситуацией, когда файлы одного антивируса принимались за вредоносную программу другим антивирусом.

Самым лучшим способом защиты от вирусов является использование локальных сетей, которые не имеют связи с интернетом. При этом необходимо жестко контролировать различные носители информации с прикладными программами, с помощью которых можно занести вирус.

Помехоустойчивое кодирование. Наиболее уязвимой информация бывает в процессе ее передачи. Это можно пояснить тем, что такая мера обеспечения ЦИ, как разграничение доступа снимает многие угрозы, но она невозможна при использовании в канале связи беспроводных линий. Информация наиболее уязвима именно на таких участках ИКС. Очевидно, что при преднамеренном воздействии на передаваемый сигнал обеспечить ЦИ невозможно. Для исправления ошибок при передачи, возникших в результате природных явлений, технических сбоев, используется помехоустойчивое кодирование (ПКИ).

Изучение ПКИ началось практически сразу после выхода в свет работы [13]. Наиболее известными в нашей стране являются работы [14-16]. В этих работах представлены и проанализированы различные методы ПКИ. Главной идеей исправления ошибок, возникающих в процессе передачи, является введение избыточности в передаваемое сообщение. Чем больше необходимо исправить ошибок, тем больше должна быть избыточность.

В настоящее время все большую популярность завоевывает «мягкое» декодирование, основанное на совместном конструировании кода и множества сигнальных точек. Такая сигнально кодовая конструкция обеспечивает более высокую эффективность и больший энергетический выигрыш от кодирования, чем последовательное применение ПКИ и модуляции [16].

В работах [17,18] предложен и обоснован метод обеспечения ЦИ в системах передачи информации, основанный на контроле четности в миниблоках и контрольной сумме. Данный метод наиболее эффективен при работе с кратными ошибками, обладает высокой скоростью восстановления информации.

Сжатие данных. Как известно [19], сжатие подразумевает замену последовательности символов другой последовательностью меньшей длины либо оптимальное кодирование. Обеспечение ЦИ достигается за счет уменьшения объема передаваемой информации. Это уменьшение можно достичь за счет оптимального кодирования источника. Однако такой метод в настоящее время практически не используется ввиду того, что при цифровой обработки сигнала выгоднее, с точки зрения организации вычислительного процесса, под каждый символ выделять одинаковое количество бит.

Наиболее часто используется метод динамического сжатия. При таком подходе структура сжатого сообщения включает в себя словарь и сжатую информацию. Уменьшение объема передаваемой информации достигает 20 раз (в зависимости от типа передаваемой информации). Однако, если при передаче или хранении возникает ошибка, особенно в словаре, то возникает эффект размножения ошибок, приводящий к значительному искажению либо уничтожению информации.

В работах [20, 21] представлен способ сжатия информации, позволяющий уменьшить размер файлов небольшой длины (менее 1000 бит) до 75 процентов. Основная идея данного способа – использование шести бит для кодирования передаваемого символа и нескольких кодовых таблиц, предварительно размещенных у пользователей ИКС.

Стеганография. С этим термином знакомы все, кто занимается криптографией. В настоящее время можно выделить три тесно связанных между собой направления стеганографии: сокрытие данных, цифровые водяные знаки и заголовки. При скрытой передачи информации одновременно с обеспечением конфиденциальности [13] решается и вопрос обеспечения ЦИ. Нельзя изменить того, чего не видишь - главный аргумент использования стеганографии для обеспечения ЦИ.

Одним из самых простых способов скрытой передачи является отправление сообщения внутри другого сообщения. Это может быть какой-то контейнер, например, в группированном рисунке на втором плане находится текстовое сообщение написанное белым по белому. К этому методу можно отнести и использование специальных сигналов, например широкополосных шумоподобных либо ортогональных.

Главным недостатком использования стеганографии для обеспечения ЦИ является значительно больший объем контейнера по сравнению с объемом сообщения. Но этот недостаток можно нивелировать, передавая в качестве контейнера полезную информацию, не критичную к ЦИ.

Об использовании методов стеганографии с целью обеспечения ЦИ не принято говорить, хотя они являются наиболее эффективными для решения поставленной задачи.

Резервирование. Данный метод обеспечения ЦИ используется в основном при передаче и хранении информации.

При передаче возможен многократный повтор сообщения в одно направление либо рассылка сообщений во все возможные направления. Данный подход можно рассматривать как один из методов ПКИ.

При хранении идея резервирования достаточно проста – создание копий полученных файлов и их хранение отдельно от первоначальных документов. Зачастую такие хранилища создаются в географически разнесенных местах. В качестве примера можно рассмотреть современные облачные технологии.

Одним из главных недостатков резервирования информации является повышение возможности ее несанкционированного снятия, т.к. информация, располагаемая на внешних устройствах хранения, является незащищенной.

Выводы. В представленной работе рассмотрены возможные методы обеспечения ЦИ в ИКС. Это обеспечение надежности ТС, разграничение доступа, стеганография (скрытие факта передачи), помехоустойчивое кодирование, антивирусная защита, сжатие

данных, резервирование.

В каждом из рассмотренных методов выделены наиболее существенные угрозы ЦИ и показаны возможные пути их устранения. Практическая реализация этих методов зависит от угроз, которые возникают в процессе жизненного цикла информации, и вида используемой информации.

Следует отметить, что ни один из рассмотренных методов обеспечения ЦИ не позволяет решить рассмотренную проблему. Обеспечение ЦИ можно достичь только комплексным использованием рассмотренных методов. Это единственный подход, позволяющий обеспечить гарантоспособность инфокоммуникационных систем.

В работе не рассмотрены контрольная сумма, цифровая подпись и криптографические методы, которые позволяют контролировать ЦИ, осуществлять организацию парольного доступа, но не могут обеспечить ЦИ.

Список литературы: 1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 №2594-IV. **2.** *Горбенко І.Д.* Інфраструктура відкритих ключів. Електронний цифровий підпис. Теорія та практика: монографія / *Ю.І.Горбенко, І.Д.Горбенко*. – Х.: Форт, 2010. – 608 с. **3.** ISO/IEC 13335-1 : 2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (IDT) http://www.iso.org/iso/catalogue_detail.htm?csnumber =39066. **4.** Указ Президента України 27.09.99 N 1229/99 «Про Положення про технічний захист інформації в Україні». http://zakon4.rada. gov.ua/laws/show/1229/99. **5.** *Джонатан Л.* Ядро Oracle. Внутреннее устройство для администраторов и разработчиков данных / *Л. Джонатан*. М.: ДМК-Пресс, 2015. – 372 с. **6.** *Хомоненко А.Д.* Базы данных / *А.Д.Хомоненко, В.М.Цыганков, М.Г.Мальцев*. – СПб.: КОРОНА-Век, 2009. – 736 с. **7.** *Максимов Н.В.* Компьютерные сети / *Н.В.Максимов, И.И.Попов*. – М.: Форум, 2010. – 464 с. **8.** *Певнев В.Я.* Эффективность информационной безопасности замкнутых систем / В.Я. Певнев // Радіоелектронні і комп'ютерні системи. – 2009. – № 5. – С. 82-85. **9.** ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. введ.01.01.98. – К.: Держстандарт України, 1997. – 16 с. **10.** *Кравченко В.И.* Оружие на нетрадиционных принципах: Электромагнитное оружие / *В.И.Кравченко*. – Х.: НТУ «ХПИ», 2009. – 266 с. **11.** Цуранов М.В. Методи та засоби боротьби з правопорушеннями в інформаційної сфері: навчальний посібник / *М.В.Цуранов, В.М.Струков, В.Я.Пєвнєв*. –Х.: ХНУВС, 2015. – 256 с. **12.** *Проскурин В.Г.* Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: Учеб. пособие для вузов / *В.Г.Проскурин, С.В.Крутов, И.В.Мацкевич*. – М: Радио и связь, 2000. – 168 с. **13.** *Шеннон К.Е.* Математическая теория связи / *К. Е. Шеннон* // Работы по теории информации и кибернетики. – М.: ИЛ, 1963. – 476 с. **14.** *Питерсон У.* Коды, исправляющие ошибки / *У. Питерсон, Э. Уэлдон*. – М.: Мир, 1976. – 594 с. **15.** *Галлагер Р.* Теория информации и надежная связь / *Р. Галлагер*. – М.: Сов. радио, 1974. – 568 с. **16.** *Морелос-Сарагоса Р.* Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение / *Р. Морелос-Сарагоса*. – М.: Техносфера, 2005. – 320 с. **17.** *Пєвнєв В.Я.* Спосіб відновлення інформації при обміні даними у телекомунікаційних системах / *В.Я.Пєвнєв* и др. // Д.п. № 26778. Бюл., 2007. – № 16. **18.** *Пєвнєв В.Я.* Теоретичне обгрунтування методу відновлення повідомлення, прийнятого з помилками / *В.Я.Пєвнєв, М.В.Цуранов* // Системи обробки інформації. Збірник наукових праць. – Х., ХУПС, 2013. – № 2 (109). – С. 194 -196. **19.** *Смирнов М.* Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / *Д. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин*. – М.: Диалог-МИФИ, 2002. – С. 384. **20.** *Пєвнєв В.Я.* Про один засіб стиску текстової інформації / *В.Я.Пєвнєв, І.Л.Яценко* // Вісник ЖІТІ. – Житомир: 2002. – № IV (23). – С. 206-209. **21.** *Певнев В.Я.* Метод восстановления информации при обмене данными в распределенных вычислительных системах / *В.Я.Певнев, И.Л.Яценко* // Вісник КДПУ. – Кременчуг: 2003. – Вып. 3 (20). – С. 19-21.

Bibliography (transliterated): 1. Zakon Ukraine «Pro zahist informacij v informacijno-teleckomunikacijnih sistemah» vid 31.05.2005 No 2594-IV. Print. **2.** Gorbenko I.D. Infrastruktura bidkrutuh klyuchiv. Elektronnuyu cifrovuyu pidpis. Teorija ta praktika: monografija. U.D.Gorbenko, I.D.Gorbenko. Kharkiv: Form, 2010. 608. Print. **3.** ISO/IEC 13335-1 : 2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management (IDT) http://www.iso.org/iso/catalogue_ detail.htm?csnumber=39066. **4.** Ukaz Prezidenta Ukraine 27.09.99 N 1229/99 «Pro polozhennya pro tehnichniuyu zachist informacij v Ukraini». http://zakon4.rada.gov ua/laws/show/1229/99. **5.** Dzhonotan L. Yadro Oracle. Vnutrennee ustrojstvo dlya administratorov I razrabotcgikov dannuh. L. Dzhonotan. Moscow: DMK-Press, 2015. 372. Print. **6.** Homonenko A.D. Bazu dannuh. A.D.Homonenko, B.M.Cugankov, M.G.Mal'cev. Sankt Petersburg: KORONA-Vek, 2009. 736. Print. **7.** Maksimov N.V. Comp'uternue seti. N.V.Maksimov, I.I.Popov. Moscow: Forumм, 2010. 464. Print. **8.** Pevnev V.Ya. Effektivnost informacionnoj bezopasnosti zamknytuh system. V.Ya.Pevnev. Radioelektronni i komp'uterni sistemu. 2009. No 5. 82-85. Print. **9.** DSTU 3396.2-97. Zahust informacii. Tehnichnuyu zahust informacii. Terminu ta vuznachennya. vvedv.01.01.98. Kyyiv: Derzhstandart Ukraine, 1997. 16. Print. **10.** Kravchenko V.I. Oruzhie na netradicionnuh principah: Elektromagnitnoe oruzhie. V.I.Kravchenko. Kharkiv: NTU «KhPI», 2009. 266. Print. **11.** Curanov M.V. Metodu ta zacjbu borot'bu z pravoporuchinnyamu v infjrmaciynoy sferi: navchal'nuy posibnik. M.V. Cyranov, V.M. Strykov, V.Ya. Pevnev. Kharkiv: KhNUVD, 2015. 256. Print. **12.** Proskurin V.G. Programmno-apparatnue sredstva obespecheniya informacionnoy bezopasnocti. Zaschita v operaciynuh sustemah: ucheb. posobiy dlya vyzov. V.G.Proskyrin, S.V.Krutov, I.V.Mackevich. Moscow: Radio I svyaz, 2000. 168. Print. **13.** Shennon K. E. Matematicheskaya teoriya svyazi. K.E.Shennon. Rabotu po teoriy informaciy i kibernetiki. Moscow: IL, 1963. 476. Print. **14.** Piterson U. Kodu, ispravlyauzchie oschibki. U. Piterson, E. Ueldon, U. Piterson. Moscow: Mir, 1976. 594. Print. **15.** Gallager P. Teoriya informaciy i nadeschnaya svyaz. P.Gallager. Moscow: Sov. radio, 1974. 568. Print. **16.** Morelos-Saragosa R. Iskusstvo pomehoustoychivogo kodirovaniya. Metodu, algoritmu, primenenie. R. Morelos-Saragosa. Moscow: Tehnosfera, 2005. 320. Print. **17.** Pevnev V.Ya. Sposib vidnovlennya informaciy pri obmini dannumi y telekomynikaciynuh sistemah. V.Ya. Pevnev i dr. Д.п. No 26778. Bul., 2007. No 16. Print. **18.** Pevnev V.Ya. Teoretuzchne obgruntuvannz metodu vidnovlennya povidomlennya, prinyatogo z pomilkami. V.Ya. Pevnev, M.V. Curanov. Sistemu obrobku informaciy. Zbirnik naukovuh prac. No 2 (109). Kharkiv: KhUPS, 2013. 194-196. Print. **19.** Smirnov M. Metodi sjatiya dannih. Ustrojstvo, sjatiya izobrajeniya i video. D.Vatolin, A.Ratushnyak, M. Smirnov, V.Ykin. Moscow: Dialog-MIFI, 2002. 384. Print. **20.** Pevnev V.Ya. Pro odin zasob stisku tekstovoy informaciy. V.Ya.Pevnev, I.L.Yacenko. Visnik ZhITI. No IV (23). Zhitomir: 2002. 206-209. Print. **21.** Pevnev V.Ya. Metod vosstanovleniya informaciy pri obmene dannumi v raspredelennuh vuchickitel'nuh sistemach. V.Ya.Pevnev, I.L.Yacenko. Visnik KDPU: Vol. 3/2003 (20). Kremenchug: 2003.19-21. Print.

Поступила (received) 09.09.2015

Відомості про авторів / Сведения об авторах / About the Authors

Певнев Владимир Яковлевич, кандидат технических наук, доцент, доцент кафедры компьютерных систем и сетей Национального аэрокосмического университета им. Н.Е. Жуковского «ХАИ»; тел.: (050) 40-366-73; email: pevnevvy@mail.ru

Pevnev Vladimir Jakovlevich, Ph.D., associate professor, assistant professor of the Department of Computer Systems and Networks of the National Aerospace University. NE Zhukovsky "HAI"; tel.: (050) 40-366-73; email: pevnevvy@mail.ru