

УДК 004.056

Определение термина «компьютерная безопасность»

Забегалин Е. В.

Актуальность задачи: использование термина «компьютерная безопасность» началось в России 20 лет назад в учебниках, в образовательных стандартах, в научных публикациях, в средствах массовой информации. При этом термин «компьютерная безопасность» до сих пор не получил общепринятого словарного или нормативного определения. По мнению автора, эта ситуация нуждается в развитии – термин «компьютерная безопасность» должен обрести своё логическое нормативное определение в интересах дальнейшего развития теории и практики предметной области, связанной с обеспечением безопасной обработки информации в компьютерных системах. **Целью работы** является разработка определения термина «компьютерная безопасность», которое может быть предложено на роль нормативного и которое должно задавать общую базовую парадигму решения множества теоретических и практических задач обеспечения и оценивания компьютерной безопасности. **Метод решения задачи:** сначала анализируется, систематизируется и обобщается содержание компьютерной безопасности по её представлениям в публикациях специалистов и в нормативных документах; затем принимается ряд принципов, ограничивающих предметную область компьютерной безопасности; в завершение составляется определение термина «компьютерная безопасность» по общим логическим правилам определения понятий. Эта схема включает также императивное отнесение компьютерной безопасности к множеству компьютеризированных изделий, в конструкцию и в процессы функционирования которых включены информационные технологии. **Новизна решения** заключается в новом определении термина «компьютерная безопасность», отличающимся от известных подходов к пониманию и определению компьютерной безопасности тем, что в нём утверждается системное единство трёх существенных её аспектов: безопасности компьютерных данных (информации), безопасности компьютерных программ, безопасности предписанных функций компьютеризированных изделий. **Теоретическая значимость работы** состоит в том, что предложенное в ней новое определение термина «компьютерная безопасность» влечёт необходимость разработки в дальнейшем новых стандартов и комплексов методик для решения множества задач обеспечения и оценивания компьютерной безопасности.

Ключевые слова. Компьютерная безопасность, информационная безопасность, безопасность программного обеспечения, безопасность информационной технологии, компьютеризированное изделие.

Актуальность

В настоящее время термин «компьютерная безопасность» широко и часто используется в профессиональных публикациях, в СМИ, в Интернете, и при этом в большинстве случаев по умолчанию подразумевается то, что читатели без дополнительных пояснений интуитивно понимают смысл этого термина. Однако общепринятого словарного или нормативного определения этого термина в настоящее время не существует (автор настоящей статьи не нашёл его).

Библиографическая ссылка на статью:

Забегалин Е. В. Определение термина «компьютерная безопасность» // Системы управления, связи и безопасности. 2017. № 4. С. 102-111. URL: <http://sccs.intelgr.com/archive/2017-04/05-Zabegalin.pdf>

Reference for citation:

Zabegalin E. V. Definition of the Term “Computer Security”. *Systems of Control, Communication and Security*, 2017, no. 4, pp. 102-111. Available at: <http://sccs.intelgr.com/archive/2017-04/05-Zabegalin.pdf> (in Russian).

Анализ источников, представленных в наиболее фундаментальной работе в этой области [1], позволяет считать, что компьютерная безопасность впервые стала в России предметом специального рассмотрения в учебной литературе 20 лет назад. Так, автор учебного пособия [1] предложил понимать компьютерную безопасность как состояние защищенности (безопасность) информации (данных) в компьютерных системах и одновременно как безотказность (надежность) функционирования компьютерных систем. Автор работы [2] не дал четкого определения термина «компьютерная безопасность», но обозначил лишь своё видение границ этой безопасности, которые, по его мнению, образуются средствами хранения, обработки и передачи информации в компьютерных (автоматизированных) системах. Авторы пособия [3] использовали термин «компьютерная безопасность» только в названии пособия, но далее никак не определили его. Автор книги [4] сообщил о своём видении компьютерной безопасности как «одной из наиболее динамично развивающихся современных наук», но при этом не дал содержательного определения этой безопасности ни как термина, ни как науки.

Официальное использование термина «компьютерная безопасность» началось в 2011 году, когда был утверждён федеральный государственный образовательный стандарт (ФГОС) по специальности 090301 «Компьютерная безопасность» [7]. В 2016 году этот стандарт был заменен новым ФГОС [8], в котором название специальности осталось прежним, но изменились её номер (теперь это 10.05.01) и требования к ней. Оба указанных стандарта никак не определили сам термин «компьютерная безопасность».

Итак, можно видеть то, что на сегодняшний день сложилась ситуация, при которой термин «компьютерная безопасность» официально и широко используется, но не имеет нормативного определения. По мнению автора настоящей статьи, данная ситуация нуждается в разрешении – термин «компьютерная безопасность» должен получить своё нормативное определение, которое способствовало бы решению множества теоретических и практических задач обеспечения и оценивания компьютерной безопасности в единых логических рамках.

Представляется целесообразной следующая методическая схема решения данной задачи:

- сначала провести анализ, систематизацию и обобщение содержания компьютерной безопасности по тем её представлениям, которые представлены в известных публикациях специалистов и в нормативных документах;
- затем принять ряд принципов, которые нужны для ограничения предметной области компьютерной безопасности;
- в итоге составить определение термина «компьютерная безопасность» по общим логическим правилам определения понятий.

Предметное содержание компьютерной безопасности

Содержание компьютерной безопасности выявляется по её предметным частям, которые можно извлечь из известных источников, в первую очередь из тех, которые были упомянуты выше – из [1, 2, 3, 7, 8].

В учебном пособии [1] компьютерная безопасность логически выводится из более широкого родового понятия информационной безопасности и предлагается её комплексное понимание в аспектах безопасности компьютерной информации, технической надёжности и аутентичности функционирования компьютерных систем (главным образом, с точки зрения их целостности). С этой позиции далее в учебном пособии подробно рассматривается только информационная безопасность компьютерных данных, анализ же безопасности программного обеспечения и безопасности функций компьютерных систем оставлен за рамками пособия.

В учебном пособии [2] не предложено чёткого определения термина «компьютерная безопасность» и указывается лишь на то, что её рамки составляют средства компьютерных (автоматизированных) систем хранения, обработки и передачи информации, и, исходя из этого, подробно описываются только математические модели обеспечения информационной безопасности компьютерных данных, отдельный же вопрос о безопасности программного обеспечения не ставится.

В учебном пособии [3], которое написано в парадигме информационной безопасности, термин «компьютерная безопасность» никак не определяется, но в круг рассматриваемых вопросов включается безопасность программного обеспечения при угрозах вредоносных программных воздействий на компьютеры и вычислительные сети.

ФГОС [8], определяя шесть объектов профессиональной деятельности по специальности 10.05.01, первым в этом перечне называет «защищаемые компьютерные системы и входящие в них средства обработки, хранения и передачи информации». Кроме того, в описании частных специализаций в стандарте применяются термины «информационная безопасность», «защита информации», «защищённое программное обеспечение», «безопасность программного обеспечения».

С учётом этого близким по смыслу к термину «компьютерная безопасность» видится термин «безопасность информационной технологии», который имеет нормативные определения и используется в документах [9, 10]. Определения, которые даны в этих документах, несмотря на различия в формулировках, по сути, акцентируют состояние защищённости одновременно трёх типов объектов:

- а) компьютерных данных (информации);
- б) ресурсов информационной технологии – программных и аппаратно-программных средств;
- в) предписанных функций информационной технологии.

К рассматриваемому вопросу имеет отношение и расширенное толкование термина «информационная безопасность», данное в стандарте [11], которое логически соединяет безопасность информации и безопасность средств её об-

работки. Такое расширенное понимание информационной безопасности является близким к определению безопасности информационной технологии.

Анализ ресурсов глобальной сети Интернет по теме компьютерной безопасности даёт представление о том, что в рамках этой темы рассматривается не только безопасность компьютерных данных (компьютерной информации), но и безопасность программного обеспечения (по меньшей мере, в аспекте его антивирусной защиты).

Для полноты картины следует упомянуть популярный термин «кибербезопасность». Подробный критический анализ этого термина дан в книге [5], в которой делается заключение (с которым можно согласиться) об отсутствии достаточных научных и практических оснований для использования этого термина в вопросах обеспечения безопасности в информационной сфере.

Итак, можно подвести следующий итог проведенного анализа.

1) Безопасность компьютерных данных (информации) является бесспорным компонентом компьютерной безопасности.

2) Безопасность программного обеспечения во всех рассмотренных случаях непосредственно или опосредованно прослеживается в составе компьютерной безопасности. Одним из примерных аргументов в пользу выделения самостоятельного характера безопасности программного обеспечения является угроза УБИ.188 – «Подмена программного обеспечения», которая внесена в «Банк данных угроз информационной безопасности» ФСТЭК России [12]. Критериями безопасности программного обеспечения могут быть, по меньшей мере, те же критерии, что и для безопасности компьютерных данных (информации) – конфиденциальность, целостность, доступность.

3) Представляется теоретически приемлемым и практически предпочтительным узкое понимание компьютерной безопасности, при котором она связывается только с угрозами целенаправленных вредоносных воздействий на компьютерные программы и данные, но не связывается с технической безотказностью (надёжностью) оборудования и программного обеспечения, которые, как отмечается в учебном пособии [1], в русле исторического развития вычислительной техники стали предметом рассмотрения иных дисциплин.

4) Безопасность предписанных функций информационных технологий (и более широко – компьютеризированных изделий) является эмерджентным качеством компьютерной безопасности. Оно не сводится целиком ни к безопасности одних только компьютерных данных, ни к безопасности одних только компьютерных программ, но возникает при их системной технологической интеграции. То есть функции информационной технологии прямо реализуются компьютерными программами при выполнении заложенных в них алгоритмов обработки определённых данных. Можно представить себе, например, гипотетическую ситуацию, когда некая компьютерная программа фальсифицирована вредоносным воздействием (подменена) таким образом, что она имеет такую же контрольную сумму, что и её исходная версия, но выполняет изменённый алгоритм обработки данных, блокирующий выполнение части предписанных функций или снижающий качество их выполнения.

Критерием безопасности предписанных функций информационных технологий и компьютеризированных изделий может быть, по мнению автора настоящей статьи, во-первых, полнота выполнения всего множества этих функций и, во-вторых, необходимое качество их выполнения, которые в виде наборов функциональных и технических требований должны задаваться при проектировании информационных технологий и компьютеризированных изделий и затем должны оцениваться при их испытаниях.

Определение термина «компьютерная безопасность»

С учётом проведенного выше предметного анализа предлагаются следующие принципы определения термина «компьютерная безопасность»:

- в круг объектов обеспечения и оценивания компьютерной безопасности должны включаться компьютеризированные изделия, в конструкцию и в процессы функционирования которых встроены информационные технологии (это, например, отдельные автоматизированные рабочие места, многопользовательские автоматизированные системы, машины с элементами компьютерного управления и т. п.);
- терминологическое определение компьютерной безопасности должно охватывать одновременно три существенных аспекта: безопасность компьютерных данных (информации), безопасность компьютерных программ, безопасность предписанных функций компьютеризированных изделий, в которых реализуются информационные технологии;
- учитывая то, что нормативные определения терминов «безопасность информации» и «безопасность информационной технологии» ранее прошли профессиональную экспертизу, формулировка определения термина «компьютерная безопасность» должна быть преемственной к формулировкам нормативных определений этих двух терминов;
- определение термина «компьютерная безопасность» должно соответствовать общим логическим правилам определения понятий, в числе которых: отнесение к ближайшему роду и выявление видового отличия, соблюдение соразмерности определяемого и определяющего понятий, выделение существенных видовых признаков, отсутствие терминологического круга, применение позитивной формы суждений, недопущение логических противоречий и двусмысленности, достижение чёткости и ясности [6].

В соответствии с этими принципами автором предлагается следующее общее определение термина «компьютерная безопасность».

Компьютерная безопасность – состояние защищённости компьютерных программ и данных в средствах вычислительной техники, в каналах связи, в автоматизированных системах и в других компьютеризированных изделиях, при котором обеспечиваются конфиденциальность, целостность и доступность компьютерных программ и данных, а также обеспечивается выполнение компьютеризированными изделиями предписанных функций.

Данное общее определение термина «компьютерная безопасность» может быть, по мнению автора настоящей статьи, предложено на роль будущего опре-

деления, которое может использоваться в ФГОС, нормативных актах и регламентирующих документах.

На основе этого общего определения могут формулироваться частные определения для различных классов и типов компьютеризированных изделий, например, следующие.

Компьютерная безопасность беспилотных транспортных средств – состояние защищённости компьютерных программ и данных в компьютерных устройствах, которые являются элементами конструкции беспилотных транспортных средств, а также в каналах связи этих средств, при котором обеспечиваются конфиденциальность, целостность, доступность компьютерных программ и данных, а также обеспечивается выполнение беспилотными транспортными средствами предписанных транспортных функций.

Компьютерная безопасность робототехнических комплексов – состояние защищённости компьютерных программ и данных в компьютерных устройствах, которые являются элементами конструкции робототехнических комплексов, в их каналах связи, при котором обеспечиваются конфиденциальность, целостность, доступность компьютерных программ и данных, а также обеспечивается выполнение робототехническими комплексами предписанных функций по назначению.

Компьютерная безопасность военной техники – состояние защищённости компьютерных программ и данных в компьютеризированных образцах, комплексах и системах военной техники, в их каналах связи, при котором обеспечиваются конфиденциальность, целостность и доступность компьютерных программ и данных, а также обеспечивается выполнение компьютеризированными образцами, комплексами и системами военной техники предписанных функций по назначению.

Что может следовать дальше?

Предложенное выше терминологическое определение компьютерной безопасности является логической основой и открывает возможности для разработки новых стандартов и комплексов методик, необходимых для определения требований к компьютерной безопасности компьютеризированных изделий различных классов и типов, а также методик, необходимых для её оценивания. Эти стандарты и комплексы методик должны отличаться от существующих нормативных требований информационной безопасности тем, что в них должна быть заложена системная увязка трёх ключевых аспектов:

- безопасности компьютерных данных;
- безопасности компьютерных программ;
- безопасности предписанных функций компьютеризированных изделий.

Разнообразие указанных методических комплексов должно соответствовать качественному разнообразию классов и типов компьютеризированных изделий.

Заключение

Исходя из анализа известных источников, показана актуальность задачи нормативного определения термина «компьютерная безопасность».

Проведенный предметный анализ компьютерной безопасности дал основания для выделения трёх её существенных компонентов (аспектов): безопасности компьютерных данных, безопасности компьютерных программ, безопасности функций, предписанных компьютеризированным изделиям.

В соответствии с выделенной предметной структурой компьютерной безопасности и в рамках принятых логических принципов предложено общее определение термина «компьютерная безопасность», которое может быть принято за основу в нормативных и регламентирующих документах нормативным.

В соответствии с данным общим определением термина «компьютерная безопасность» предложены примерные частные определения компьютерной безопасности для трёх классов компьютеризированных изделий: для беспилотных транспортных средств, для робототехнических комплексов, для компьютеризированных образцов, комплексов и систем военной техники.

В развитие рассмотренной темы обозначен круг исследовательских задач по разработке новых стандартов и комплексов методик для определения требований к компьютерной безопасности различных классов и типов компьютеризированных изделий и комплексов методик для её оценивания.

Литература

1. Гайдамакин Н. А. Теоретические основы компьютерной безопасности: учебное пособие. – Екатеринбург: Уральский государственный университет им. А. М. Горького, 2008. – 212 с. – URL: http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf (дата обращения: 08.02.2018).

2. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие. – М.: Книжный мир, 2009. – 352 с.

3. Грушко А. А., Применко Э. А., Тимонина Е. Е. Теоретические основы компьютерной безопасности: учебное пособие для студентов высших учебных заведений. – М.: Издательский центр «Академия», 2009. – 272 с.

4. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. – 2-е изд., испр. и доп. – М.: Горячая линия – Телеком, 2016. – 338 с.

5. Михайлов Ю. Б. Научно-методические основы обеспечения безопасности защищаемых объектов. – М.: Горячая линия – Телеком, 2015. – 322 с.

6. Кондаков Н. И. Логический словарь-справочник. – М.: Наука, 1975. – 720 с.

7. Федеральный государственный образовательный стандарт высшего профессионального образования по направлению подготовки (специальности) 090301 «Компьютерная безопасность» (квалификация (степень) «специалист»). Утвержден приказом Министерства образования и науки РФ от 17 января 2011 г. N 69 // Интернет-портал «КонсультантПлюс». – URL:

http://www.consultant.ru/document/cons_doc_LAW_113513/e56c7ff29f09c387b560f343c082a2ab8edfa57b (дата обращения: 08.02.2018).

8. Федеральный государственный образовательный стандарт высшего образования по специальности 10.05.01 «Компьютерная безопасность» (уровень специалитета). Утвержден приказом Министерства образования и науки Российской Федерации от 1 декабря 2016 г. N 1512 // Интернет-портал «КонсультантПлюс».

URL:

http://www.consultant.ru/document/cons_doc_LAW_209322/380a78c549db44b1c53202079b18085d22df2dba (дата обращения: 08.02.2018).

9. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Введен в действие Приказом Гостехкомиссии России от 19.06.2002 г. N 187 // Интернет-портал ФСТЭК России.

URL:

<http://fstec.ru/component/attachments/download/293> (дата обращения: 08.02.2018).

10. РС Р 50.1.056–2005. Техническая защита информации. Основные термины и определения. Введ. 2006-12-29. – М.: Стандартинформ, 2006. – 16 с.

11. ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введ. 2007-06-01. – М.: Стандартинформ, 2007. – 23 с.

12. УБИ.188: Угроза подмены программного обеспечения // Интернет-портал ФСТЭК России. Банк данных угроз информационной безопасности. – URL: <http://bdu.fstec.ru/threat/ubi.188> (дата обращения: 08.02.2018).

References

1. Gaidamakin N. A. *Teoreticheskie osnovy komp'iuternoï bezopasnosti* [Theoretical Foundations of Computer Security]. Ekaterinburg, Ural Federal University (UrFU), Electronic Scientific Archive of UrFU, 2008. 212 p. Available at: http://elar.urfu.ru/bitstream/10995/1778/5/1335332_schoolbook.pdf (accessed 08 February 2018) (in Russian).

2. Shcherbakov A. Iu. *Sovremennaia komp'iuternaia bezopasnost'. Teoreticheskie osnovy. Prakticheskie aspekty* [Modern computer security. Theoretical basis. Practical aspects]. Moscow, Knizhnyi mir Publ., 2009. 352 p. (in Russian).

3. Grushko A. A., Primenko E. A., Timonina E. E. *Teoreticheskie osnovy komp'iuternoï bezopasnosti* [Theoretical Foundations of Computer Security]. Moscow, Izdatel'skii tsentr «Akademiia», 2009. 272 p. (in Russian).

4. Devianin P. N. *Modeli bezopasnosti komp'iuternykh sistem. Upravlenie dostupom i informatsionnymi potokami* [Models of security of computer systems. Control of access and information flows]. Moscow, Goriachaia liniia – Telekom Publ., 2016. 338 p. (in Russian).

5. Mikhailov Iu. B. *Nauchno-metodicheskie osnovy obespecheniia bezopasnosti zashchishchaemykh ob"ektov* [Scientific and methodological basis for ensuring the safety of the protected objects]. Moscow, Goriachaia liniia – Telekom Publ., 2015. – 322 p. (in Russian)

6. Kondakov N. I. *Logicheskii slovar'-spravochnik* [The logical dictionary-directory]. Moscow, Nauka Publ., 1975. 720 p. (in Russian).

7. Federal state educational standard of higher professional education in the field of training (specialty) 090301 “Computer security” (qualification (degree) “specialist”). Approved by the order of the Ministry of Education and Science of the Russian Federation of January 17, 2011 No. 69. *Internet portal “ConsultantPlus”*. Available at: http://www.consultant.ru/document/cons_doc_LAW_113513/e56c7ff29f09c387b560f343c082a2ab8edfa57b (accessed 08 February 2018) (in Russian).

8. Federal state educational standard of higher education on specialty 10.05.01 “Computer security” (level of specialty). Approved by the order of the Ministry of Education and Science of the Russian Federation of 1 December 2016 No. 1512. *Internet portal “ConsultantPlus”*. Available at: http://www.consultant.ru/document/cons_doc_LAW_209322/380a78c549db44b1c53202079b18085d22df2dba (accessed 08 February 2018) (in Russian).

9. Guidance document. Security of information technology. Criteria for assessing the security of information technology. It was put into effect by the Order of the State Technical Commission of Russia of 19.06.2002 No. 187. *Internet portal of “Federal Service for Technical and Export Control of Russia” (FSTEC)*. Available at: <http://fstec.ru/component/attachments/download/293> (accessed 08 February 2018) (in Russian).

10. Guidance on standardization. P 50.1.056-2005. Technical protection of information. Basic terms and definitions. Enter. 2006-12-29. Moscow, Standartinform Publ., 2006. 16 p. (in Russian).

11. 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. Moscow, Standartinform Publ., 2007. 23 p. (in Russian).

12. Threat to information security No. 188 “Threat of spoofing software”. *Internet portal of “Federal Service for Technical and Export Control of Russia” (FSTEC). Data Security Threats Database*. Available at: <http://bdu.fstec.ru/threat/ubi.188> (accessed 08 February 2018) (in Russian).

Статья поступила 8 февраля 2018 г.

Информация об авторе

Забегалин Евгений Викторович – кандидат технических наук. Старший научный сотрудник. 4 Центральный научно-исследовательский институт. Область научных интересов: информационная безопасность.
E-mail: ezabex@yandex.ru

Адрес: 141092, Россия, Московская обл., г. Королёв, мкр. Юбилейный, ул. М.К. Тихонравова, д. 29.

Definition of the Term “Computer Security”

E. V. Zabegalin

The relevance of the task: the use of the term “computer security” began in Russia 20 years ago in textbooks, in educational standards, in scientific publications, in the media. However, term “computer security” has not yet received a generally accepted dictionary or normative definition. In the author's opinion, this situation needs development – the term “computer security” should acquire its logical normative definition in the interests of further development of the theory and practice of the subject area related to ensuring the safe processing of information in computer systems. **The purpose of the work** is to develop a definition of the term “computer security”, which can be proposed for the role of regulatory and which should set a common basic paradigm for solving a variety of theoretical and practical tasks of providing and evaluating computer security. **Method for solving the problem:** first, the content of computer security is analyzed, systematized and generalized according to its representations in publications of specialists and in regulatory documents; then a number of principles are adopted that limit the subject area of computer security; in the end, the definition of the term “computer security” is drawn up according to the general logical rules of definition of concepts. This scheme also includes the imperative attribution of computer security to a variety of computerized products, the design and operation of which includes information technologies. **The novelty of the solution** lies in the new definition of the term “computer security”, which differs from the known approaches to understanding and determining computer security in that it affirms the systemic unity of its three essential aspects: the security of computer data (information), the software security, the security of prescribed functions of computerized products. **The theoretical significance of the work** is that the new definition of the term “computer security” proposed in it entails the need to develop new standards and methodologies in the future to solve a variety of tasks to ensure and evaluate computer security.

Keywords: computer security, information security, software security, information technology security, computerized product, information technology.

Information about Author

Evgeniy Viktorovich Zabegalin – Ph.D. of Engineering Sciences. Senior Research Officer. The 4th Central Research Institute of the Ministry of Defence of the Russian Federation. Field of research: information security. E-mail: eza-bex@yandex.ru

Address: Russia, 141092, Moskovskaya oblast, Korolev, mkr. Yubileyny, ulica M.K. Tikhonravova, 29.