A. P. Durakovskiy, T. A. Kondratieva, Y. N. Lavrukhin, V. R. Petrov

About trust in the information systems on the basis of internet-based technologies

Keywords: information security, trusted environment, information system, internet-based technologies, unified requirements

At this paper the authors describe the methodological approaches to the solution of the known problem of trust during interactions in the public information systems on the basis of internet-based technologies.

А. П. Дураковский, Т. А. Кондратьева, Ю. Н. Лаврухин, В. Р. Петров

О ДОВЕРИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ НА ОСНОВЕ ИНТЕРНЕТ-ТЕХНОЛОГИЙ[1]

В настоящее время вопрос решения известной проблемы доверия [1–3] становится одним из приоритетных для комплексного обеспечения безопасности информации, прежде всего в ключевых системах информационной инфраструктуры. Известным подходом по достижению доверия в государственных информационных системах является выполнение установленных процедур аттестации объектов информатизации по требованиям безопасности информации. В бизнес-процессах, особенно в рамках международной деятельности, широко используют процедуры аудита информационной безопасности [4]. Такие аспекты доверия, как неотказуемость или придание юридической значимости электронному документообороту, достигаются использованием различных видов электронной подписи [5].

Вместе с тем надо признать, что достижение доверия в системах общего пользования на основе интернет-технологий, в частности при использовании облачных вычислений, по-прежнему остается нерешенной задачей в силу отсутствия унифицированных критериев оценки такого показателя. Приведенные в [1] определения «уровня» или «степени» доверия трудно поддаются практической интерпретации и требуют дополнительного пояснения. В рассматриваемых, открытых для дестабилизирующих воздействий системах важно выполнить все необходимые и достаточные условия для обеспечения доверия не только к участникам взаимодействия (пользователям), но и ко всей вычислительной среде. Очевидно, что создание доверенной среды является весьма сложной задачей со многими дополнительными ограничениями, которые влияют на формирование указанной выше «степени» доверия.

Исходя из определения термина «информационная система», установленного Федеральным законом [6], рассматриваемые в данной работе вычислительные среды можно отнести к открытым системам [7–10]. Существует множество определений, характеризующих это понятие, но все они сводятся к толкованию, введенному Комитетом IEEE POSIX 1003.0, которое представляет открытую систему как систему (среду), реализующую открытые спецификации на интерфейсы, сервисы (услуги среды) и поддерживаемые форматы данных, достаточные для того, чтобы дать возможность должным образом разработанному прикладному программному обеспечению быть переносимым в широком диапазоне систем с минимальными изменениями, взаимодействовать с другими приложениями на локальных и удаленных системах и с пользователями в стиле, который облегчает переход пользователя от системы к системе.

[1] Данная работа выполнена в НИЯУ МИФИ при финансовой поддержке Министерства образования и науки Российской Федерации в рамках проекта «Создание инженерно-технических решений для высокотехнологичного производства инновационных программно-аппаратных средств защиты информации на базе перспективных высокоскоростных интерфейсов информационного взаимодействия», выполняемого совместно с ООО «ОКБ САПР» по договору № 02.G25.31.0050.

Поскольку информационные системы ввиду наличия ошибок и уязвимостей подвержены нарушению свойств, направленных на обеспечение безопасности информации [1], может нивелироваться такое свойство, как доверие не только к самой системе, но и к циркулирующей в ней информации. В соответствии с терминологией, принятой в области информационной безопасности, достижение доверия в системах на основе интернет-технологий обеспечивается совокупностью, с одной стороны, доступности информационных ресурсов, а с другой — их конфиденциальности при сохранении защищенности и целостности.

Основной трудностью при решении исследуемой проблемы доверия является отсутствие унифицированных подходов, устанавливающих процедуры взаимодействия пользователей, регламентированных требований к автоматизированным рабочим местам (АРМ), а также ко всем участникам взаимодействия с системой.

Попыткой унификации таких подходов следует считать требования национальных стандартов (ГОСТов) под общим названием «Основы доверия к безопасности ИТ» [1–3]. В них сформирована терминология, определены методы достижения доверия и сформулированы так называемые степени (уровни) доверия к различным стадиям процесса —от разработки до эксплуатации. Однако сами разработчики указанных стандартов отмечают, что на практике требования к безопасности информации могут быть очень сложными, методы обеспечения доверия разнородными, а корпоративные ресурсы организаций имеют существенные различия. Поэтому пользователь должен самостоятельно принимать решения о том, какие методы соответствуют его конкретным объектам защиты и требованиям политики безопасности организации. Иными словами, признается отсутствие унифицированного подхода к достижению доверия для многопараметрических задач, что, как следствие, приводит к объективному «недоверию» к системе, поскольку отсутствуют гарантии противодействия несанкционированному доступу к информационным ресурсам и атакам на систему со стороны злоумышленников.

Но из всего множества параметров информационной системы в аспекте обеспечения ее безопасности можно выделить наиболее критичные для устранения «недоверия». Так, очевидно, что сценарий взаимодействия с информационной системой требует особого внимания в следующих элементах: идентификации и аутентификации, контроля доступа, защиты соединений.

Исходя из изложенного можно полагать, что сформированная доверенная информационная среда должна основываться на совокупности факторов, непосредственно влияющих на степень доверия (рис. 1).

Понятие доверия изучено в различных научных дисциплинах: от экономики до социологии, от психологии до медицины, в том числе в информатике, которые дают различные определения этого термина. Выбор наиболее точного невозможен в силу того, что это понятие является многомерным, мультидисциплинарным и многоаспектным. Однако все эти определения используют такие общие понятия, как конфиденциальность, убежденность, надежность, ожидаемость, уверенность и некоторые другие, применимые не только к личности, но и к человеко-машинным системам.

В нашем случае примем определение доверия, которое включает в себя конфиденциальность, целостность, доступность информационных ресурсов и состояние их защищенности от воздействия случайных факторов в заданный период времени. Следовательно, доверие задается как оценка пользователем того, насколько можно доверять действиям всех участников взаимодействия, которая может быть описана посредством ряда качественных признаков, отвечающих требованиям конфиденциальности, целостности, доступности [11] и защищенности от воздействия случайных факторов в период времени.

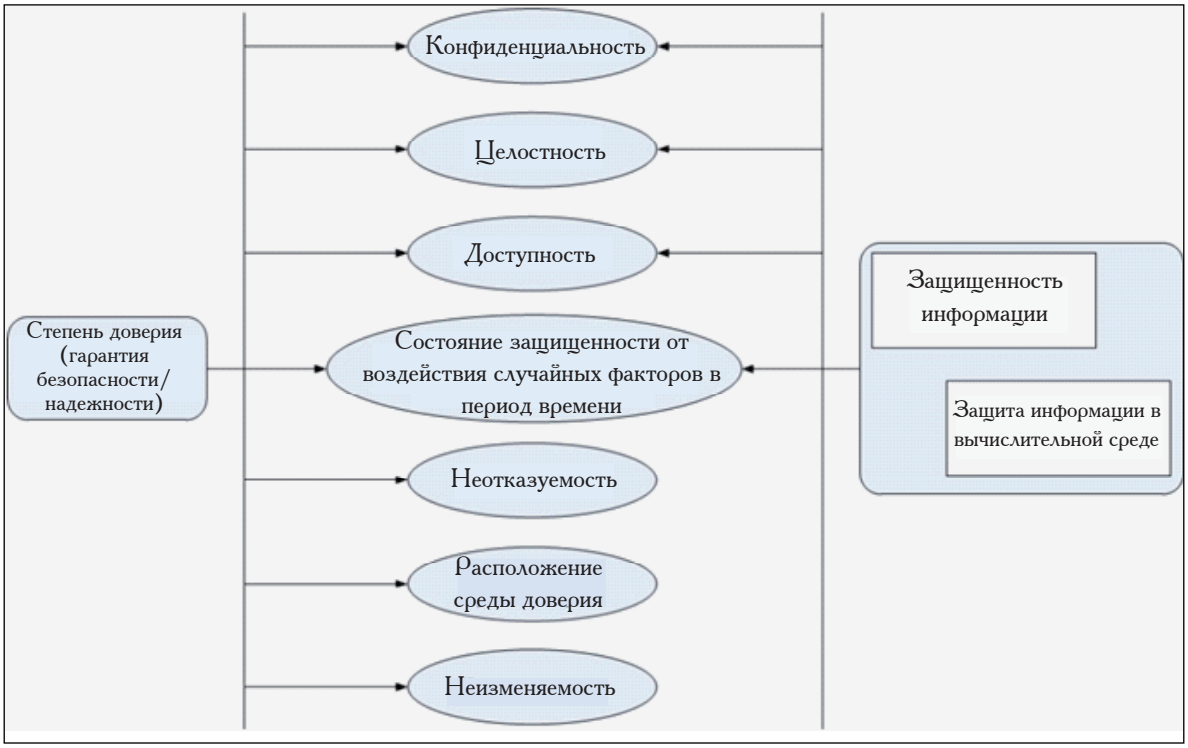

Рис. 1. Объединение совокупности факторов, непосредственно влияющих на степень доверия при защищенности информации

При введении ряда ограничений, положений и утверждений можно сформулировать критерий достижения доверия в нашем случае в виде «Трех доверий» — необходимо обеспечить защищенность трех ключевых звеньев процесса взаимодействия пользователей с информационной системой. К ним относятся: АРМ участников процесса, включая систему и доступ к ней, канал передачи информации между участниками взаимодействия, процедуры подтверждения аутентичности участников взаимодействия. Введенный критерий позволит построить формализованную (унифицированную) модель формирования доверия для открытых информационных систем, при помощи которой обосновываются требования к доверенной информационной среде. Эти подходы по повышению защищенности информационных систем на основе интернет-технологий являются предметом будущего исследования.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р 54581-2011/ISO/IEC/TR 15443-1:2005. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности ИТ. Часть 1. Обзор и основы. Введ. 01.07.2012. М.: Стандартинформ, 2012.
2. ГОСТ Р 54582-2011/ISO/IEC/TR 15443-2:2005. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 2. Методы доверия. Введ. 01.12.2012 М.: Стандартинформ, 2013.
3. ГОСТ Р 54583-2011/ISO/IEC/TR 15443-3:2007. Информационная технология. Методы и средства обеспечения безопасности. Основы доверия к безопасности информационных технологий. Часть 3. Анализ методов доверия. Введ. 01.12.2012 М.: Стандартинформ, 2013.
4. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения». Введ. 01. 06.2014 М., 2014.
5. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 28.06.2014) «Об электронной подписи».
6. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 21.07.2014) «Об информации, информационных технологиях и о защите информации».

7. *Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В.* Информационная безопасность открытых систем. Учебник для вузов. В 2-х томах. М.: Горячая линия-Телеком. Том 1. 2006. —536 с.
8. *Мельников Д. А.* Информационная безопасность открытых систем: Учебник. М.: ФЛИНТА, Наука, 2013.
9. *Кривопалов В. Г.* Комплексная методика моделирования рисков информационной безопасности открытых систем. Дисс. … канд. техн. наук. URL: https://dvs.rsl.ru/ (дата обращения: 11.01.2015). М., МИФИ, 2009.
10. *Олейников А. Я.* Открытые системы: концепция или реальность // Открытые системы. 1993. № 4 [Электронный ресурс]. URL: http://www.osp.ru/os/1993/04/178473/#part_1 (дата обращения: 11.01.2015).
11. *Denning D. E.* A new paradigm for trusted systems // Workshop on New Security Paradigms. NSPW. 1993. P. 36—41.

REFERENCES:

1. GOST R 54581-2011/ISO/IEC/TR 15443-1:2005. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Osnovy doveriya k bezopasnosti IT. Chast' 1. Obzor i osnovy. Vved. 01.07.2012 M.: Standartinform, 2012.
2. GOST R 54582-2011/ISO/IEC/TR 15443-2:2005. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Osnovy doveriya k bezopasnosti IT. Chast' 2. Metody doveriya. Vved. 01.12.2012 M.: Standartinform, 2013.
3. GOST R 54583-2011/ISO/IEC/TR 15443-3:2007. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Osnovy doveriya k bezopasnosti IT. Chast' 3. Analiz metodov doveriya. Vved. 01.12.2012 M.: Standartinform, 2013.
4. The Standard of the Bank of Russia STO BR IBBS-1.0-2014 "Information Security Maintenance for Organizations of the Banking System of the Russian Federation. General Conditions". M., 2014.
5. Federal'nyiy zakon ot 06.04.2011 № 63-FZ (red. ot 28.06.2014) "Ob electronnoiy podpisi".
6. Federal'nyiy zakon ot 27.07.2006 № 149-FZ (red. ot 21.07.2014) "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii".
7. *Zapechnikov S. V., Miloslavskaya N. G., Tolstoy A. I., Ushakov D. V.* Informatsionnaya bezopasnost' otkrytykh sistem. Uchebnik dlya vuzov. V 2-kh tomakh. M.: Goryachaya liniya-Telekom. Tom 1. 2006. —536 c.
8. *Melnikov D. A.* Informatsionnaya bezopasnost' otkrytykh sistem: Uchebnik. M.: FLINTA, Nauka, 2013.
9. *Krivopalov V. G.* Kompleksnaya metodika modelirovaniya riskov informatsionnoy bezopasnosti otkrytykh system. Diss. kand.tekhn,nauk. URL: https://dvs.rsl.ru (date of request: 11.01.2015).M., MIPHI, 2009.
10. *Oleynikov A. Y.* Otkrytye sistemy: kontseptsiya ili real'nost' // Otkrytye sistemy. 1993. № 4. URL: http://www.osp.ru/os/1993/04/178473/#part_1 (date of request: 11.01.2015).
11. *Denning D. E.* A new paradigm for trusted systems // Workshop on New Security Paradigms. NSPW. 1993. P. 36—41.