Об одном подходе к обеспечению безопасности данных в информационной системе средствами ОС и СУБД

Г. П. Акимова, А. Ю. Даниленко, Е. В. Пашкина, М. А. Пашкин, А. А. Подрабинович, И. В. Туманова

Федеральный исследовательский центр "Информатика и управление" РАН, г. Москва, Россия

Аннотация. В статье излагается подход к созданию защищенных информационных систем, безопасность данных в которых обеспечивается средствами ОС и СУБД, а встроенные средства защиты информации отсутствуют. Возможность использования предлагаемого способа разработки таких систем обусловлена особенностями как деловой логики эксплуатирующей организации, так и обрабатываемой информации. Предложенный подход позволяет существенно сократить сроки разработки и внедрения информационных систем в защищенном исполнении.

Ключевые слова: автоматизированные информационные системы; информационная безопасность; средства защиты информации; операционные системы; системы управления базами данных; объекты защиты; цифровизация.

DOI 10.14357/20718632220104

Введение

Широкое внедрение информационных технологий во все сферы жизни общества, именуемое в последнее время цифровизацией, требует создания все большего числа автоматизированных информационных систем (АИС) различного назначения [1]. В большинстве случаев такие системы относятся к категории защищенных, в которых реализованы необходимые меры для обеспечения безопасности хранимых и обрабатываемых данных, что зачастую связано с обработкой в АИС различной конфиденциальной информации, в первую очередь персональных данных. Требования к таким системам изложены в ряде нормативных документов, в частности в [2-5]. Среди них особое место занимает обязательная сертификация АИС, которая должна выполняться испытательными лабораториями и органами сертификации [6]. В процессе проведения таких работ выполняется проверка корректности реализации средств защиты информации (СЗИ) непосредственно в АИС, а также использования СЗИ в составе операционных систем (ОС) и систем управления базами данных (СУБД). Сертификация АИС представляет собой длительный процесс, и ее проведение существенно задерживает внедрение АИС.

1. Построение защищенных информационных систем

Обеспечение безопасности данных, обрабатываемых в АИС, традиционно подразумевает конфиденциальность, целостность и доступность обрабатываемой и хранимой информа-

ции. Структурно АИС может быть представлена совокупностью ряда «слоев» (например, [7]):

– аппаратные средства (материнские платы, процессоры, модули оперативной и дисковой памяти и т.д.);

– операционная система;

– база данных (БД) под управлением СУБД;

– специальное программное обеспечение (СПО), реализующее деловую логику АИС.

Каждый из перечисленных слоев имеет свои объекты защиты и свои средства защиты информации.

Так, объектами защиты ОС являются файлы, настройки, сетевые интерфейсы и другие объекты, средствами защиты для них служат подсистемы управления доступом, идентификации и аутентификации, протоколирования, контроля целостности и ряд других. В случае БД объектами защиты являются сами базы данных, таблицы, записи и другая информация, для обеспечения безопасности применяются СЗИ из состава СУБД. В частности, для объектов защиты могут быть установлены списки доступа, реализующие дискреционный контроль, а также мандатные метки, соответствующие уровням конфиденциальности.

СЗИ в составе СПО обеспечивают безопасность объектов защиты, специфичных для реализуемого функционала. В большинстве случаев это БД пользователей с атрибутами доступа и правами на действия в АИС, информационные объекты (для случая почтовой системы это письма, для банковской – информация о счетах клиентов, для системы электронного документооборота – документы, письма, данные поручений и т.д.). Для таких объектов задаются списки доступа и мандатные метки, реализуется контроль целостности и протоколирование действий, формируется политика безопасности, задающая правила определения допустимости всех действий в АИС.

Описанная логика работы предполагает возможность наличия внутреннего нарушителя, для нейтрализации действий которого реализуются перечисленные механизмы защиты данных. Тем не менее, не исключены ситуации, когда модели угроз безопасности и нарушителя строятся так, что понятие внутреннего нарушителя в них отсутствует, а требования по наличию подсистем управления доступом объясняются принятыми в организации правилами работы и другими нормативными актами, например [8].

2. Предлагаемое решение

Описанная в предыдущем параграфе логика построения СЗИ АИС является традиционной, может считаться универсальной, и широко используется разработчиками СПО. Следует отметить, что такая организация работы требует получения разрешения контролирующих органов на работу с конфиденциальной информацией для всех составляющих АИС с последующей экспертизой результатов этих работ.

Однако в ряде случаев безопасность АИС может быть обеспечена с использованием упрощенной схемы построения комплекса СЗИ. В частности, могут быть использованы особенности деловой логики организации, по заказу которой разрабатывается АИС. Так, если в моделях угроз и нарушителя констатируется отсутствие внутреннего нарушителя и декларирован равноправный доступ всех пользователей АИС к информационным объектам, подсистема управления доступом по дискреционной модели может отсутствовать. Аналогично, если для разрабатываемой АИС верно утверждение, что все обрабатываемые в ней данные имеют одинаковый уровень конфиденциальности, причем он может быть весьма высоким, то разработка и сертификация системы значительно упрощаются.

Ниже описан вариант построения АИС, в которой отсутствуют собственные СЗИ в составе СПО.

2.1. Модель данных и логика работы

Рассмотрим следующий способ организации обрабатываемой информации:

– объекты защиты размещаются в двух хранилищах: БД (метаданные) и файловая система серверного компьютера (файлы);

– данные в системе могут иметь разные уровни конфиденциальности (Уровень 0, Уровень 1, Уровень 2), уровни перечислены в порядке возрастания;

– вся информация в БД АИС имеет один уровень конфиденциальности Уровень 1;

– в файловой системе сервера хранятся файлы всех трех уровней конфиденциальности от 0 до 2, причем эти файлы связаны с метаданными (регистрационная информация, информация о поручениях пользователям и т.д.), размещаемыми в БД и имеющими Уровень 1.

Деловая логика организации, которой требуется разработка АИС, в такой ситуации, может иметь следующие особенности:

– вся информация уровней конфиденциальности 0 и 1 доступна для чтения всем пользователям;

– доступ для чтения к данным Уровня 2 предоставляется в соответствии со списками доступа, формируемыми администраторами безопасности по письменному распоряжению руководства организации;

– АИС работает под управлением защищенной ОС, предусматривающей возможность определения уровня конфиденциальности сеанса работы пользователя (уровни от 0 до 2). Эта ОС имеет разрешение сертифицирующих органов для работы с данными до уровня конфиденциальности 2 и все СЗИ, предусмотренные руководящими документами, (идентификация и аутентификация, управление доступом по дискреционной и мандатной моделям, контроль целостности, протоколирование событий безопасности и т.д.). Примером таких ОС являются Windows при использовании средства защиты данных Secret Net [9], Astra Linux SE [10], QP ОС [11];

– используемая СУБД также имеет разрешения сертифицирующих органов и необходимые СЗИ;

– доступ для редактирования данных определяется по отдельным правилам, которые могут рассматриваться как функциональные особенности АИС, а не СЗИ. Это означает, что с точки зрения политики безопасности редактирование информационных объектов разрешено всем пользователям, которым разрешено их чтение.

2.2. Построение информационной системы

При описанных предположениях предлагается следующий вариант построения АИС (без собственных СЗИ в составе СПО, при этом безопасность данных обеспечивается средствами ОС и СУБД). В БД размещаются метаданные документов и другие объекты, имеющие уровень конфиденциальности 1. Файлы всех уровней конфиденциальности размещаются в файловой системе, на них средствами ОС (программными и интерфейсными) задаются права доступа: на чтение всем пользователям для файлов уровней 0 и 1, и выборочно для уровня 2. Доступ на редактирование задается одинаково с доступом на чтение, владельцем файла считается его создатель, правом на изменение прав доступа обладает владелец файла (это соответствует политике управления доступом используемой ОС). В рамках СПО реализуются алгоритмы предоставления прав на редактирование метаданных и файлов. БД пользователей АИС совпадает с БД домена ОС. Контроль целостности метаданных обеспечивается СУБД, файлов - средствами ОС. Протоколирование событий безопасности осуществляется средствами ОС в соответствии с ее настройками.

Таким образом, конфиденциальность, целостность и доступность данных, обрабатываемых АИС, обеспечена без применения СЗИ, встроенных в СПО.

3. Особенности реализации

Необходимо отметить, что реализация предлагаемого подхода имеет существенные особенности как в плане условий, делающих такую реализацию возможной, так и в части алгоритмов работы СПО в составе АИС.

3.1. Условия применения

3.1.1. Необходимые возможности ОПО

При построении АИС в защищенном исполнении используемые ОС и СУБД должны обладать рядом возможностей, которые используются при разработке СПО и функционировании АИС. В первую очередь это наличие программного интерфейса приложения, интерфейса прикладного программирования (англ. application programming interface, API). Наличие API в ОС и СУБД требуется для выполнения следующих действий:

– задания и получения дискреционных прав доступа на файлы и другие объекты файловой системы;

– задания и получения мандатных меток объектов файловой системы;

– задания настроек протоколирования событий безопасности средствами ОС и СУБД;

– чтения протоколов безопасности ОС для реализации собственного приложения, обеспечивающего работу с этими протоколами (требование необязательное, поскольку могут использоваться приложения в составе ОС и СУБД);

– постановки файлов и записей в БД на контроль целостности с возможностью выборочной проверки целостности информационных объектов;

– получение уровня конфиденциальности сеанса работы пользователя;

– получение данных идентификации и аутентификации пользователя в ОС для использования в работе подсистемы управления доступом.

Как уже отмечалось, используемые ОС и СУБД должны обладать разрешениями контролирующих органов на работу с информацией требуемого уровня конфиденциальности и необходимыми для этого СЗИ.

Используемая ОС должна обеспечивать создание домена с доверенными алгоритмами идентификации и аутентификации, а также базой данных пользователей с возможностью объединения учетных записей в группы.

3.1.2. Организационные условия

Использование рассматриваемого подхода построения АИС возможно при наличии следующих особенностей деловой логики и внутренней нормативной базы эксплуатирующей организации:

– возможность разделения обрабатываемой в АИС информации на метаданные, хранящиеся в БД, и содержательную информацию, размещаемую в файлах;

– возможность размещения в БД данных, которые доступны для чтения всем сотрудникам, работающим с АИС;

– равноправный доступ на чтение информационных объектов в БД для всех сотрудников, работающих с АИС. Это требование может быть видоизменено путем сегментации АИС и предоставления прав доступа на отдельные сегменты БД доменным группам пользователей.

3.2. Алгоритмы работы СПО

Алгоритмы работы СПО в составе АИС, построенной в соответствии с предлагаемым подходом, практически не отличаются при реализации клиентского приложения по технологии толстого (отдельное специально написанное приложение) или тонкого (web-браузер) клиента.

Вся информация в БД имеет один мандатный уровень, эти данные могут обрабатываться пользователями при работе с любым уровнем конфиденциальности в ОС. По сути, единственным способом обеспечить выполнение этого принципа является полное отключение мандатного контроля на уровне СУБД. В случае экспорта информации из БД (запись на внешние носители данных, распечатка и т.д.) ей присваивается реальный уровень конфиденциальности под ответственность сотрудника, выполняющего это действие.

3.2.1. Создание информационного объекта

Создание информационного объекта, представляющего собой взаимосвязанные метаданные и один или несколько файлов, начинается с заполнения экранной формы с реквизитами, которые в дальнейшем будут составлять набор метаданных. Это действие практически не отличается для тонкого и толстого клиентов: в первом случае форма заполняется в web-браузере на страничке, полученной с сервера АИС, во втором форма выводится на экран клиентским приложением. Введенные данные заносятся в серверную БД, что и означает создание метаданных нового объекта.

Один или несколько файлов для отправки на сервер открываются стандартным способом используемого web-браузера или клиентским приложением, далее файлы отправляются на сервер и сохраняются в его файловой системе. Процесс сохранения управляется серверными компонентами СПО, при этом место хранения файла выбирается в соответствии с настройками АИС. В этот момент на файл устанавливаются дискреционные права доступа с помощью функций API ОС и присваивается мандатная метка в соответствии с уровнем конфиденциальности сеанса пользователя. Дискреционные права устанавливаются согласно деловой логике, реализованной в АИС. Наиболее универ-

сальный алгоритм в этой части предусматривает задание прав на редактирование файла и модификацию прав доступа создателю информационного объекта и его руководителю, а право на чтение сотрудникам рабочей группы, в которую он входит. При этом состав рабочей группы может быть определен как на уровне доменной базы данных пользователей, так и в настройках АИС.

3.2.2. Чтение объекта

При запросе с клиентского рабочего места на чтение информационного объекта открывается экранная форма с его метаданными, которая аналогична форме для их создания. При этом используется тот факт, что метаданные доступны для чтения всем пользователям АИС, поэтому проверка прав доступа не выполняется.

При чтении файла проверяются права доступа как дискреционные, так и мандатные. Для этого серверные компоненты, реализующие отправку файла на клиентское рабочее место, должны работать в контексте безопасности конечного пользователя.

3.2.3. Редактирование объекта

Как отмечалось выше, с точки зрения политики безопасности редактирование всех информационных объектов доступно всем тем, кто имеет право на их чтение, а разграничение прав на редактирование осуществляется функциональными модулями. При редактировании информации в БД возможны два варианта действий: полная замена информации в базе или создание новой версии метаданных с сохранением прежних значений в других ячейках таблиц БД. Выбор между этими вариантами делается при создании АИС.

Права на редактирование файла с точки зрения ОС должны быть синхронизированы с правами в АИС, для чего используются функции, предоставляемые API ОС. В этом случае сохранение файла после редактирования с заменой существующего не блокируется файловой системой. Возможна реализация АИС с сохранением прежних версий файлов, в этом случае для новой версии требуется выставить прежние дискреционные и мандатные права для нового файла. Для сохранения уровня конфиденциальности информации в файле его редактирование должно быть разрешено только при совпадении мандатных меток файла и сеанса работы пользователя.

Заключение

Описанный подход позволяет существенно сократить время на разработку АИС в защищенном исполнении без разработки собственных СЗИ и упрощения тематических исследований, из которых исключается проверка реализации СЗИ в составе СПО АИС. Однако, следует подчеркнуть, что предложенный способ обеспечения безопасности данных не может считаться универсальным, а может быть использован только при выполнении ряда условий, включающих особенности деловой логики организации и принятые алгоритмы работы с конфиденциальной информацией.

Литература

1. Программа "Цифровая экономика Российской Федерации" http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.
2. Федеральный закон "О персональных данных" от 27.07.2006 N 152-ФЗ http://www.consultant.ru/document/cons_doc_LAW_61801
3. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных. Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119.
4. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Приказ ФСТЭК России от 18 февраля 2013 г. N 21.
5. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Приказ ФСТЭК России от 11 февраля 2013 г. N 17.
6. Положение о системе сертификации средств защиты информации. Утверждено приказом ФСТЭК России от 03 апреля 2018 г. N 55.
7. Даниленко А.Ю. Безопасность систем электронного документооборота: Технология защиты электронных документов. С приложением: Возможности применения технологии блокчейн в СЭДО-ЗИ. Изд. 2-е, дополненное. / М: URSS. 2021. 240 с. ISBN 978-5-9519-2056-0. (Основы защиты информации. № 13).
8. О государственной тайне. Закон Российской Федерации от 21 июня 1993 г. № 5485-I.
9. Secret Net Studio. Защита данных и инфраструктуры серверов и рабочих станций. https://www.securitycode.ru/products/secret-net-studio/.

10. Astra Linux Special Edition — операционная система специального назначения. https://astralinux.ru/products/astra-linux-special-edition/.
11. Операционная система QP ОС. https://cryptosoft.ru/qpos.html.

Акимова Галина Павловна. Федеральный исследовательский центр "Информатика и управление" Российской РАН, г. Москва, Россия, в.н.с., к.т.н. Количество печатных работ: более 50. Область научных интересов: системное программирование, системный анализ, информационные технологии, влияние человеческого фактора, информационно-аналитические системы, электронный документооборот, электронный архив. E-mail: akimova@isa.ru

Даниленко Андрей Юрьевич. Федеральный исследовательский центр "Информатика и управление" Российской РАН, г. Москва, Россия, в.н.с., к.ф.-м.н., Количество печатных работ: более 40 (в т.ч. 1 монография). Область научных интересов: системное программирование, системный анализ, информационные технологии, электронный документооборот, информационная безопасность, защита данных. E-mail: danilenko@isa.ru (Ответственный за переписку).

Пашкина Елена Владимировна. Федеральный исследовательский центр "Информатика и управление" Российской РАН, г. Москва, Россия, ведущий программист. Количество печатных работ: более 15. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: pashkina@isa.ru

Пашкин Матвей Александрович. Федеральный исследовательский центр "Информатика и управление" Российской РАН, г. Москва, Россия, н.с. Количество печатных работ: более 15. Область научных интересов: системное программирование, информационные технологии, информационно-аналитические системы, электронный архив. E-mail: pashkin@isa.ru

Подрабинович Андрей Александрович. Федеральный исследовательский центр "Информатика и управление" РАН, г. Москва, Россия, ведущий программист. Количество печатных работ: более 15. Область научных интересов: системное программирование, проектирование и создание методов и программных средств управления электронными документами, защита информации в документооборотных системах. E-mail: podrabinovich@isa.ru

Туманова Ирина Владимировна Федеральный исследовательский центр "Информатика и управление" Российской РАН, г. Москва, Россия, ведущий программист. Количество печатных работ: более 5. Область научных интересов: системное программирование, информационные технологии, электронный документооборот, электронный архив. E-mail: tumanova-irin@mail.ru

An Approach to Ensuring Data Security in an Information System by Means of OS and DBMS

G. P. Akimova, A. Yu. Danilenko, E. V. Pashkina, M. A. Pashkin, A. A. Podrabinovich, I. V. Tumanova

Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, Moscow, Russia

Abstract. The article describes an approach to the creation of secure information systems, data security in which is ensured by means of OS and DBMS, and there are no built-in information security tools. The possibility of using the proposed development method is due to the peculiarities of both the business logic of the operating organization and the construction of an array of processed information. The proposed approach can significantly reduce the development and implementation time of information systems in a secure design.

Keywords: automated information systems; Information Security; information security means; OS; database management systems; objects of protection; digitalization.

DOI 10.14357/20718632220104

References

1. Programma "Tsifrovaya ekonomika Rossiyskoy Federatsii" [Program "Digital Economy of the Russian Federation"]. http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf.
2. Federal'nyy zakon "O personal'nykh dannykh" ot 27.07.2006 N 152-FZ. [Federal Law "On Personal Data" of July 27, 2006 N 152-FZ]. http://www.consultant.ru/document/cons_doc_LAW_61801
3. Ob utverzhdenii trebovaniy k zashchite personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. Postanovleniye Pravitel'stva Rossiyskoy Federatsii ot 1 noyabrya 2012 g. N 1119. [On

the approval of requirements for the protection of personal data during their processing in personal data information systems. Resolution of the Government of the Russian Federation of November 1, 2012 N 1119].
4. Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh. Prikaz FSTEK Rossii ot 18 fevralya 2013 g. N 21. [On the approval of the composition and content of organizational and technical measures to ensure the safety of personal data during their processing in personal data information systems. Order of the FSTEC of Russia dated February 18, 2013 N 21].
5. Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh. Prikaz FSTEK Rossii ot 11 fevralya 2013 g. N 17. [On the approval of requirements for the protection of information that does not constitute a state secret contained in state information systems. Order of the FSTEC of Russia dated February 11, 2013 N 17].
6. Polozheniye o sisteme sertifikatsii sredstv zashchity informatsii. Utverzhdeno prikazom FSTEK Rossii ot 03 aprelya 2018 g. N 55. [Regulations on the certification system for information security means. Approved by order of the FSTEC of Russia dated April 03, 2018 N 55].
7. Danilenko A.YU. Bezopasnost' sistem elektronnogo dokumentooborota: Tekhnologiya zashchity elektronnykh dokumentov. S prilozheniyem: Vozmozhnosti primeneniya tekhnologii blokcheyn v SEDO-ZI. Izd. 2-ye, dopolnennoye. / M: URSS. 2021. 240 s. ISBN 978-5-9519-2056-0. (Osnovy zashchity informatsii. № 13). [Danilenko A.Yu. Security of electronic document management systems: Electronic document protection technology. With the attachment: Possibilities of using blockchain technology in SEDO-ZI. Ed. 2nd, supplemented. / M: URSS. 2021.240 s. ISBN 978-5-9519-2056-0. (Fundamentals of information security. No. 13)].
8. O gosudarstvennoy tayne. Zakon Rossiyskoy Federatsii ot 21 iyunya 1993 g. № 5485-I. [About state secrets. Law of the Russian Federation dated June 21, 1993 No. 5485-I].
9. Secret Net Studio. Zashchita dannykh i infrastruktury serverov i rabochikh stantsiy. [Secret Net Studio. Protection of data and infrastructure of servers and workstations]. https://www.securitycode.ru/products/secret-net-studio/.
10. Astra Linux Special Edition — operatsionnaya sistema spetsial'nogo naznacheniya. [Astra Linux Special Edition — a special purpose operating system]. https://astralinux.ru/products/astra-linux-special-edition/.
11. Operatsionnaya sistema QP OS. [Operating System QP OS]. https://cryptosoft.ru/qpos.html

Akimova G. P. Ph.D.(Eng.), Leading Research Scientist, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 50 printed works, research interests: system programming, system analysis, information technology, the influence of the human factor, information and analytical systems, electronic document management, electronic archive. E-mail: akimova@isa.ru

Danilenko A. Yu. Ph.D.(Phys.-Math.), Leading Research Scientist, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author more than 40 publications (1 monograph), research interests: system programming, system analysis, information technology, electronic document management, information security, data protection. E-mail: danilenko@isa.ru

Pashkina E. V. Leading Programmer, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 15 publications, research interests: system programming, information technology, electronic document management, electronic archive. E-mail: pashkina@isa.ru

Pashkin M. A. Research Scientist, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 15 publications, research interests: system programming, information technology, information and analytical systems, electronic archive. E-mail: pashkin@isa.ru

Podrabinovich A. A. Leading Programmer, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 15 publications, research interests: system programming, design and creation of methods and software for managing electronic documents, protection of information in document circulation systems. E-mail: podrabinovich@isa.ru

Tumanova I. V. Leading Programmer, Federal Research Center “Computer Science and Control” of Russian Academy of Sciences, 44/2 Vavilova str., Moscow, 119333, Russia, author of more than 5 publications, research interests: system programming, information technology , electronic document management, electronic archive. E-mail: tumanova-irin@mail.ru