ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ КОНФИДЕНЦИАЛЬНОГО ДЕЛОПРОИЗВОДСТВА

В. М. Зима, А. В. Клюев, О. А. Литвинов, А. Г. Ломако, А. Т. Петров

Военно-космическая академия имени А. Ф. Можайского

ВКА имени А. Ф. Можайского, Ждановская улица, д.13, Санкт-Петербург, 197082

<v_zima@eureca.ru>

УДК 681.3

Зима В. М., Клюев А. В., Литвинов О. А., Ломако А. Г., Петров А. Т. **Основы защиты информации от несанкционированного доступа в автоматизированных системах конфиденциального делопроизводства** // Труды СПИИРАН. Вып. 3, т. 2. — СПб.: Наука, 2006.

Аннотация. *В статье рассмотрено содержание комплексного подхода к защите информации при автоматизации конфиденциального делопроизводства. Показаны пути нейтрализации скрытых угроз и атак, характерных для автоматизированных систем конфиденциального делопроизводства. Описаны архитектурные особенности и технологический процесс разработки специального программно-аппаратного комплекса защиты конфиденциальных документов, основанного на шифровании информации и применении электронных идентификаторов ruToken.* — Библ. 8 назв.

UDC 681.3

Zima V. M., Kljuev A. V., Litvinov O. A., Lomako A. G., Petrov A. T. **Basics of Protection of the Information from Unauthorized Access in the Automated Systems of Confidential Office-work** // SPIIRAS Proceedings. Issue 3, vol. 2. — SPb.: Nauka, 2006.

Abstract. *In article the contents of the comprehensive approach to protection of the information is considered at automation of confidential office-work. Paths of neutralizing of the hidden threats and attacks, characteristic for the automated systems of confidential office-work are shown. Architectural features and technological engineering process of the special hardware-software complex of protection of the confidential documents, based on encoding of the information and application of electronic identifiers ruToken are described.* — Bibl. 8 items.

1. Содержание комплексного подхода к защите информации при автоматизации конфиденциального делопроизводства

Несмотря на совершенствование технологий в области защиты информации, уязвимость автоматизированных систем (АС) продолжает возрастать. Основная причина сложившейся ситуации состоит в отсутствии комплексного подхода к решению проблемы информационно-компьютерной безопасности. Это приводит не только к ошибкам построения систем защиты, но и к недостаткам в поддержании их актуального состояния.

Главный принцип комплексного подхода к построению защищенных автоматизированных систем конфиденциального делопроизводства — учет всех исходных требований, существующих угроз и влияющих на безопасность факторов при комплексном использовании наиболее эффективных мер, методов и средств защиты. Выделяются четыре аспекта рассматриваемого подхода:

- учет основополагающих требований, вытекающих из теории и практики защиты информации;
- тщательное и полное выполнение необходимых стадий разработки систем защиты с контролем качества промежуточных и итоговых результатов;

- решение всех базовых задач и подзадач защиты для нейтрализации как явных, так и скрытых угроз;
- обеспечение гарантированности защиты за счет использования проверенных методов и сертифицированных средств, а также объективной аттестации защищенной автоматизированной системы.

К системам защиты информации при автоматизации конфиденциального делопроизводства изначально должны предъявляться следующие основополагающие требования, обеспечивающие максимальную степень защищенности автоматизированных систем [5]:

- соответствие отечественным нормативным документам (требованиям Госстандартов, МО, ФСБ) и международным стандартам;
- многоуровневое построение системы защиты при корректности, полноте и непротиворечивости реализации всех приоритетных функций, без которых невозможно достигнуть требуемой степени защищенности;
- централизованное управление средствами защиты, пользователями и ресурсами компьютерной системы на основе правил единой политики безопасности;
- централизованный контроль защищенности и поддержка принятия решений для снижения количества ошибок администрирования и своевременного реагирования на события, связанные с нарушениями информационной безопасности.

Одной из основных задач при защите информации от несанкционированного доступа в автоматизированных системах конфиденциального делопроизводства является задача нейтрализации скрытых угроз и атак, не перекрываемых типовыми средствами защиты информации.

2. Нейтрализация скрытых угроз и атак

Проведенный анализ моделей защищаемых ресурсов, угроз, уязвимостей, а также нарушителей в автоматизированных системах конфиденциального делопроизводства показал, что при использовании типовых средств защиты актуальны скрытые угрозы и атаки, представленные в таблице 1. В условиях современного технического прогресса особую актуальность приобретают угрозы, связанные с неправомерными действиями со стороны санкционированных пользователей автоматизированных систем, т.е. лиц, имеющих доступ на территорию контролируемой зоны и допущенных к защищаемой информации. С их стороны возможно несанкционированное копирование больших объемов конфиденциальной информации на компактный отчуждаемый носитель, например, флэш-носитель или жесткий диск с USB-инерфейсом, емкостью от нескольких мегабайт до сотен гигабайт. Далее такой портативный отчуждаемый накопитель информации можно без проблем вынести в кармане за пределы контролируемой зоны.

Для нейтрализации как явных, так и скрытых угроз и атак, имеющих место при автоматизации конфиденциального делопроизводства, в ЗАО «ЭВРИКА» совместно с Научным филиалом ФГУП «НИИ «Вектор» — СЦПС «СПЕКТР» при участии специалистов ВКА им. А. Ф. Можайского был разработан специальный программно-аппаратный комплекс защиты информации (СПАК), обеспечивающий построение защищенных автоматизированных систем конфиденциального делопроизводства на базе ПЭВМ, функционирующих под управлением ОС Windows 2000 и XP.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Таблица 1

Перечень скрытых угроз и атак

№	Угроза	Атака
1	Неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации	Несанкционированное копирование защищаемой информации на отчуждаемый носитель, например, на флэш-носитель USB, и вынос отчуждаемого носителя за пределы контролируемой зоны
2	Хищение и/или подлог информации на жестких дисках АРМ без изменения эталонного состояния аппаратной среды	Несанкционированная загрузка операционной системы со съемного носителя, логическое монтирование жестких дисков с защищаемой информацией. Хищение этой информации копированием ее на несанкционированный носитель. Подлог информации.
3	Хищение и/или подлог информации на жестких дисках АРМ с нарушением эталонного состояния аппаратной среды	Физическое извлечение жесткого диска с атакуемого компьютера, физическое и логическое монтирование этого диска на другом компьютере. Съем и/или подлог защищаемой информации.
4	Маскировка под зарегистрированного пользователя	Добывание пароля зарегистрированного пользователя (подбором, перебором, перехватом или наблюдением), вход в систему под его именем и выполнение любых несанкционированных действий, включая хищение информации.
5	Хищение и/или подлог информации в процессе передачи.	При передаче по каналу связи: несанкционированное подключение к каналообразующей аппаратуре, перехват и/или подлог передаваемых данных. При передаче на съемном носителе: несанкционированное копирование защищаемой информации со съемного носителя, подлог информации на съемном носителе.

3. Технологический процесс разработки специального программно-аппаратного комплекса защиты информации

В соответствии с требованиями руководящих документов Гостехкомиссии России (ФСТЭК), на основе которых и формировалось тактико-техническое задание (ТТЗ), СПАК по защищенности относится к 3 классу по РД СВТ и обеспечивает построение защищенных АС класса 1Б со 2-м уровнем контроля отсутствия недекларированных возможностей для программных средств.

Для гарантированного выполнения требований ТТЗ разработка СПАК осуществлялась в контексте анализа информационных рисков [1], рассматриваемых как совокупность всех возможных факторов, отражающих опасность возникновения ущерба в результате реализации угроз информации в защищаемых АС. Соответственно при формировании архитектуры СПАК учитывались модели защищаемых ресурсов, угроз, уязвимостей, а также нарушителей, способных использовать уязвимости для реализации атак [6, 7].

Основными видами информационных ресурсов, защищаемых средствами СПАК, являются файлы и папки с документами, хранящиеся на постоянных и сменных информационных носителях, системная информация, а также информация, размещаемая в оперативной памяти компьютера и выводимая на внешние носители и печатающие устройства.

В качестве основы для модели угроз использовалась классификация и перечень факторов, воздействующих на защищаемую информацию, в соответствии с ГОСТ Р 51275 [4], когда учитывались не только угрозы, связанные с не-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

санкционированным доступом к информации, но также и угрозы, относящиеся к ошибкам обслуживающего персонала и неправомерным действиям со стороны лиц, имеющих право доступа к защищаемой информации, например, воровство носителей с защищаемой информацией.

При анализе уязвимостей основное внимание было уделено скрытым уязвимостям, например, таким как:

- ошибки конфигурирования, связанные с неправильной настройкой программно-аппаратных средств, например, подсистем ОС;
- ошибки, возникающие из-за неправильного использования программных и аппаратных средств;
- отсутствие или недостаточная эффективность необходимых средств защиты;
- недекларированные возможности, связанные с наличием программных или аппаратных закладок;
- отсутствие установленных обновлений программных средств, устраняющих ошибки в ПО;
- недостатки в политике формирования и использования эталонной информации, например, наличие слабых паролей и ключей;
- ошибки администрирования, например, неправильное назначение полномочий.

В модели нарушителей выделено 5 классов нарушителей:

- нарушители 1-го класса, у которых доступ на территорию контролируемой зоны АС отсутствует, прямое воздействие на элементы АС исключено, но возможен съем информации по каналам ПЭМИН;
- нарушители со 2-го по 5-й класс, для которых предоставляется доступ на территорию контролируемой зоны с постепенным увеличением возможностей по доступу к ресурсам защищаемых АС, начиная от отсутствия прямого физического доступа к АРМ, и заканчивая неограниченными возможностями по управлению АС в лице администратора.

Тщательный анализ сформированных моделей защищаемых ресурсов, угроз, уязвимостей, а также нарушителей, имеющих отношение к АС, защищаемых средствами СПАК, позволил выработать и реализовать в составе СПАК детальные требования по нейтрализации как явных, так и скрытых атак.

4. Архитектурные особенности специального программно-аппаратного комплекса защиты информации

Функциональная архитектура СПАК представлена на рис. 1. Основой архитектуры СПАК являются подсистемы глобального шифрования и усиленной аутентификации, ориентированные на решение следующих групп задач:

- двухуровневое «прозрачное» шифрование информации на жестких дисках АРМ;
- логическая привязка съемных носителей (Flash, Floppy, CD, DVD) к заданной группе автономных АРМ за счет «прозрачного» шифрования информации на этих съемных носителях по конфиденциальному ключу;
- использование электронных идентификаторов, например, ruToken для аутентификации пользователей, а также хранения, переноса и резервирования ключевой информации.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Двухуровневое «прозрачное» шифрование информации на жестких дисках АРМ предполагает наличие двух уровней:

- первый уровень — глобальное шифрование информации по секторам на жестких дисках АРМ;
- второй уровень — шифрование виртуальных дисков, формируемых на основе информации из файла-контейнера.

Глобальное «прозрачное» шифрование информации в системном разделе жесткого диска АРМ выполняется по конфиденциальному ключу, общему для всех зарегистрированных пользователей. При «прозрачном» шифровании логических и виртуальных дисков предполагается использование индивидуальных ключей.

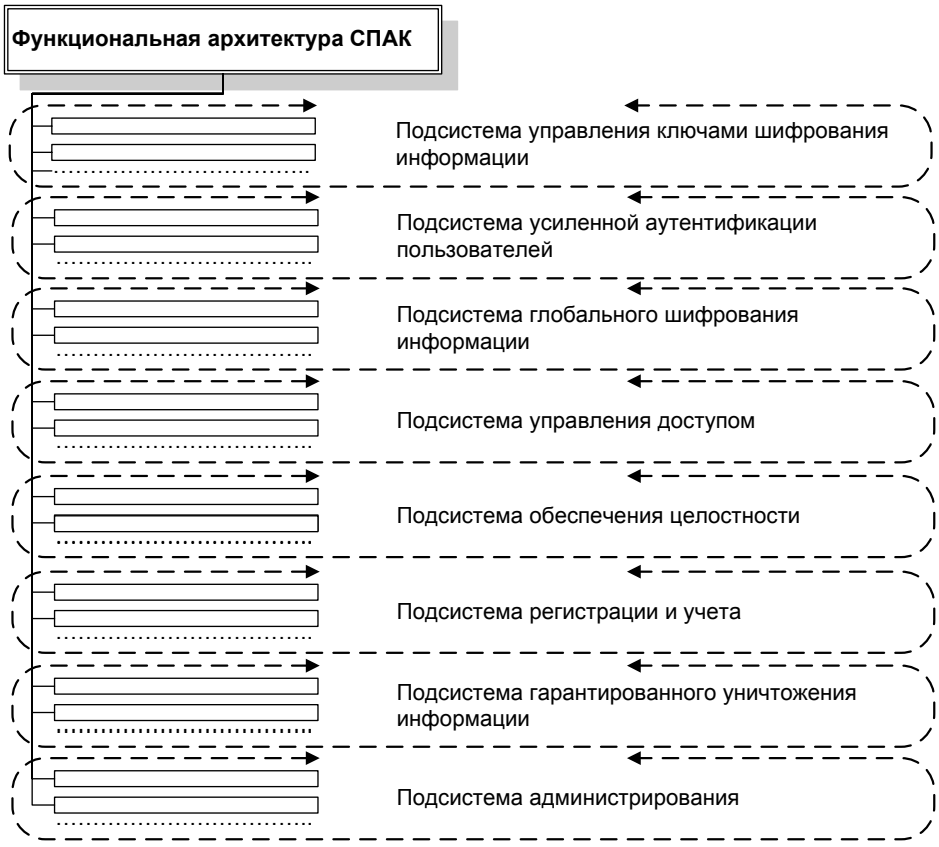

Рис. 1. Функциональная архитектура СПАК.

Для управления «прозрачно» шифруемыми виртуальными дисками предусмотрены такие важные функции, как:

- поддержка возможности переноса файла-контейнера с зашифрованным виртуальным диском с одного защищенного АРМ на другой;
- подключение зашифрованного виртуального диска по сети, в процессе работы с которым передаваемая информация шифруется в режиме реального времени, и по сети передаются только зашифрованные информационные пакеты;
- перенос ключей шифрования виртуальных дисков в аппаратно защищенной памяти электронных идентификаторов ruToken с возможностью доступа к этим ключам только после предъявления соответствующего PIN-кода;

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

- перенос ключей шифрования виртуальных дисков на дискете в закодированном виде по ключу, сгенерированному на основе заданного пароля.

Кроме того, учтена необходимость логической привязки съемных носителей (Flash, Floppy, CD, DVD) к заданной группе автономных АРМ за счет «прозрачного» шифрования информации на этих съемных носителях по конфиденциальному ключу. Пользователи заданной группы автономных АРМ смогут передавать зашифрованные носители для работы с ними с одного АРМ на другой. Вне заданной группы автономных АРМ информация на зашифрованных носителях будет недоступна.

Высокая скорость и стойкость шифрования обеспечивается за счет следующих факторов, положенных в основу построения используемых и запатентованных алгоритмов [8]:

- перенос всех вычислений, требующих больших временных ресурсов, на этап инициализации криптографической подсистемы, который выполняется только в начале сеанса работы пользователя;
- зависимость операций криптографического преобразования не только от рабочих ключей, но и от преобразуемых данных и промежуточных результатов преобразования, что повышает степень псевдослучайности в алгоритм непосредственных преобразований;
- снижение сложности алгоритма непосредственных криптографических преобразований за счет повышения его стойкости.

Для фиксированного уровня стойкости используемые алгоритмы обеспечивают более низкую сложность алгоритмов непосредственного криптографического преобразования информации. За счет этого достигается более высокая скорость шифрования.

Для аппаратной поддержки процесса аутентификации и хранения ключей шифрования в составе СПАК используется электронный идентификатор ruToken, закрепляемый за каждым пользователем и обладающий следующими характеристиками:

- встроенный микропроцессор и наличие 32-битового уникального серийного номера;
- интерфейс USB (USB 1.1 / USB 2.0);
- 2-факторная аутентификация (по факту наличия ruToken и по факту предъявления PIN-кода);
- встроенные алгоритмы шифрования ГОСТ 28147-89 [2], RSA, DES (3DES), RC2, RC4, MD4, MD5, SHA-1;
- генерация 256-битовых случайных чисел;
- выработка 32-битовой имитовставки;
- защищенное хранение ключей шифрования ГОСТ 28147-89 в объектах данных без возможности их экспорта из токена;
- возможность импорта ключей шифрования ГОСТ 28147-89 в токен;
- энергонезависимая память для хранения конфиденциальных данных (EEPROM память 8, 16 или 128 Кбайт);
- встроенная файловая система по стандарту ISO/IEC 7816;
- защищенное хранение ключей асимметричного шифрования и цифровых сертификатов;
- программно-аппаратная поддержка стандарта X.509 и возможность асимметричного шифрования данных и для работы с цифровыми сертификатами.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

5. Защита электронного документооборота

При формировании архитектуры СПАК изначально учитывались задачи эффективной защиты электронного документооборота:

- управление ключами шифрования на основе инфраструктуры открытых ключей;
- обеспечение подлинности электронных документов за счет формирования и проверки их электронных подписей;
- обеспечение конфиденциальности электронных документов за счет их шифрования.

Построение подсистемы управления ключами шифрования выполнялось исходя из следующих требований:

1) должна быть обеспечена гибкость распределения ключей шифрования информации;

2) подсистема управления ключами не должна требовать доверия взаимодействующих друг с другом сторон;

3) скорость криптографических преобразований должна обеспечивать шифрование информации в режиме реального времени.

Реализация первых двух требований выполнена за счет асимметричного принципа построения ключей верхнего уровня, а реализация третьего требования — за счет использования ключей скоростного симметричного шифрования.

В подсистеме управления ключами шифрования СПАК используются следующие базовые уровни ключей:

1) первичные пары асимметричных ключей (первичные ключи), включая личные ключи пользователей, формируемые в соответствии с российским стандартом цифровой подписи ГОСТ Р 34.10 [3] и используемые для распределения ключей, а также выработки на основе цифровой подписи вторичных ключей симметричного шифрования;

2) вторичные ключи симметричного шифрования (вторичные ключи), формируемые по алгоритму Диффи–Хеллмана на основе первичных пар асимметричных ключей, и используемые для шифрования носителей информации и информационного трафика;

3) ключи доступа, используемые для защиты первичных ключей, связок ключей пользователя, а также базы данных СПАК.

Первый уровень ключей специального преобразования информации за счет асимметричного принципа построения обеспечивает гибкость распределения ключей и не требует доверия взаимодействующих друг с другом сторон.

Второй уровень ключей специального преобразования информации за счет симметричного принципа построения и использования скоростных алгоритмов криптографических преобразований обеспечивает шифрование информации в режиме реального времени.

Третий уровень ключей специального преобразования информации за счет многоуровневого шифрования обеспечивает надежную защиту ключей первых двух уровней.

Для каждого пользователя в СПАК по ГОСТ 34.10 генерируется личная пара асимметричных ключей, которая хранится в профиле пользователя в базе данных (БД) системы защиты. Закрытый ключ этой пары ключей зашифрован по ключу, генерируемому по специальному алгоритму (алгоритму SSE2) на основе пароля (PIN-кода) этого пользователя. Вводимый пароль (PIN-код) пользователя используется для расшифрования закрытого ключа личной пары

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

асимметричных ключей. Открытый ключ личной пары асимметричных ключей подписан по закрытому первичному ключу АРМ.

Аутентификация пользователей в СПАК основана на использовании цифровой подписи. Для аутентификации пользователя модуль управления БД СПАК направляет агенту аутентификации запрос на цифровую подпись сгенерированного случайного числа, формируемую на основе личного закрытого ключа этого пользователя. Если пароль (PIN-код) был введен пользователем неправильно, то агент аутентификации не сможет правильно расшифровать личный закрытый ключ пользователя, а, следовательно, не сможет создать требуемую подпись. В противном случае проверка цифровой подписи даст положительный результат, и пользователь сможет продолжить работу. В случае положительной аутентификации пользователя система защиты обеспечивает доступ со стороны пользователя к защищенным информационным ресурсам АРМ в соответствии со схемой использования ключей при доступе к зашифрованным объектам (рис. 2).

Предполагается, что предварительно соответствующие зашифрованные информационные объекты должны быть созданы. Для создания зашифрованного информационного объекта генерируется первичная пара асимметричных ключей (по ГОСТ 34.10), которая закрепляется за данным объектом (рис. 3). В базе данных ПАК для каждой первичной и личной пары асимметричных ключей используются следующие атрибуты:

- числовой идентификатор ключевой пары, а также дата и время ее создания;
- числовой идентификатор пользователя, создавшего ключевую пару;
- имя (символьный идентификатор) ключевой пары;
- идентификатор алгоритма шифрования объекта, для которого создана ключевая пара;
- описание ключевой пары;
- открытый и закрытый ключи.

Защищаемый объект шифруется по вторичному ключу симметричного шифрования, формируемому по алгоритму Диффи–Хеллмана на основе соответствующей объекту первичной пары асимметричных ключей. Первичная пара асимметричных ключей, закрепленная за объектом, защищается с помощью ключей доступа (рис. 2 и 3).

Предполагается дальнейшее расширение СПАК для построения системы управления цифровыми сертификатами открытых ключей на основе использования удостоверяющего центра. В соответствии с международно признанным форматом для определения сертификатов открытых ключей (стандартом X.509 ITU), выдаваемый пользователю цифровой сертификат должен включать следующие элементы:

- версия, серийный номер и срок действия сертификата;
- информация о доверителе, выдавшем сертификата;
- информация о владельце сертификата (имя и фамилия, идентификатор, организация, адрес и др.);
- открытый ключ владельца сертификата;
- тип используемого алгоритма цифровой подписи;
- цифровая подпись всего содержимого сертификата, сформированная выдавшим сертификат удостоверяющим центром.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

Ответственность за подлинность указанной в сертификате информации несет удостоверяющий центр, выдавший сертификат и сформировавший под ним свою подпись. Основными компонентами удостоверяющего центра являются центры сертификации, регистрации и сетевой справочник сертификатов.

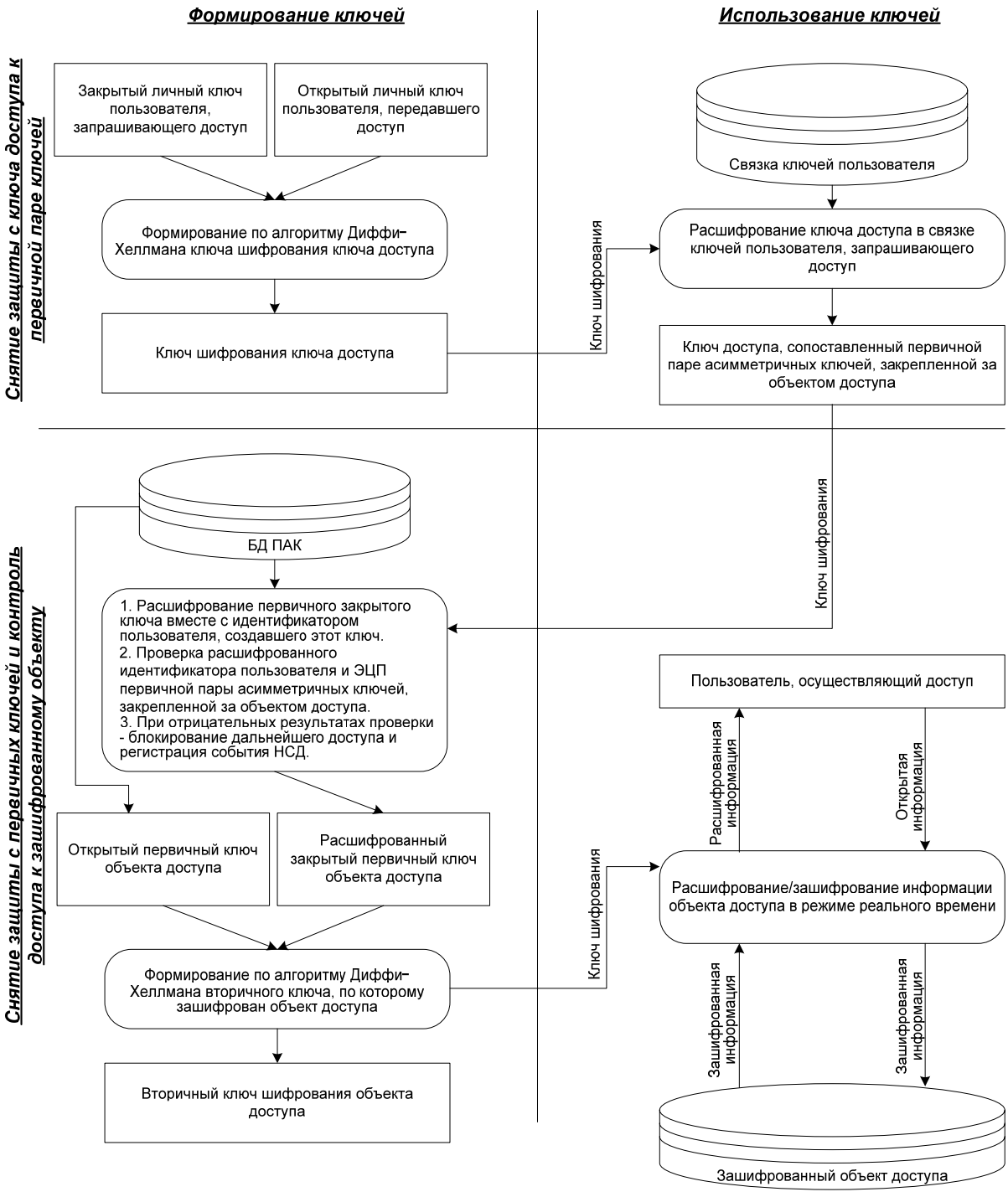

Рис. 2. Схема использования ключей при доступе к зашифрованному объекту.

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

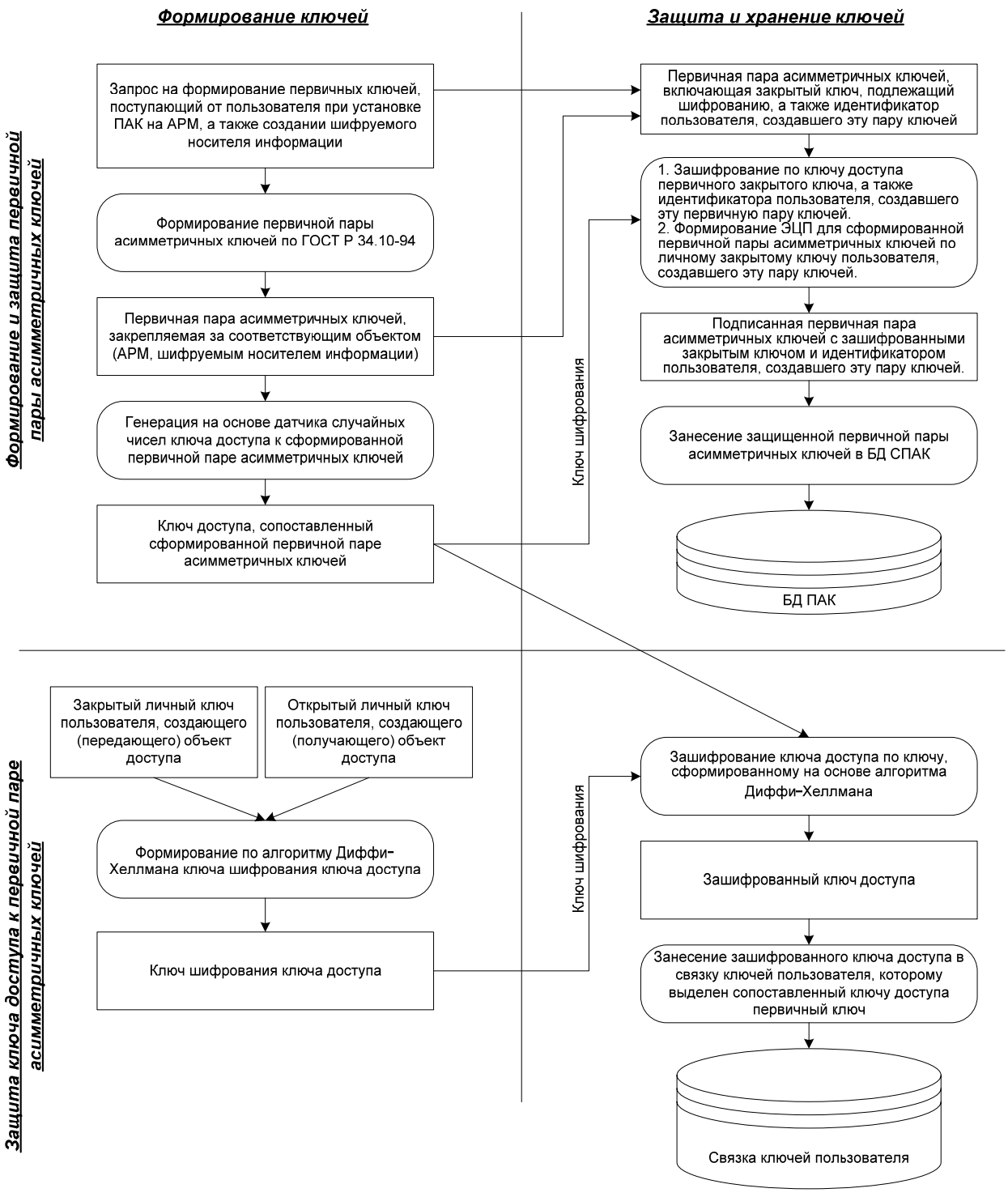

Рис. 3. Схема формирования и защиты первичной пары асимметричных ключей.

Центр сертификации обеспечивает формирование цифровых сертификатов. Кроме цифровых сертификатов, планируемых для использования, Центр сертификации формирует список отозванных сертификатов. Центр регистрации предназначен для регистрации конечных пользователей. Основная задача Центра регистрации — регистрация пользователей и обеспечение их взаимодействия с Центром сертификации. В задачи Центра регистрации также входит пуб-

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

ликация сертификатов и списка отозванных сертификатов в сетевом справочнике. Центр регистрации является единственной точкой входа и регистрации пользователей. Только зарегистрированный пользователь может получить сертификат на свой открытый ключ в Центре сертификации. Сетевой справочник сертификатов является компонентом инфраструктуры открытых ключей, накапливающим, а также учитывающим сертификаты и списки отозванных сертификатов и служащим для целей распространения этих объектов среди пользователей АС.

Конечные пользователи системы — это пользователи, программные приложения или системы, например, АРМы, защищенные СПАК, являющиеся владельцами сертификатов и использующие инфраструктуру открытых ключей для защиты электронного документооборота за счет шифрования электронных документов, а также формирования и проверки их электронных подписей.

6. Выводы

Несмотря на совершенствование технологий в области защиты информации, уязвимость автоматизированных систем (АС) продолжает возрастать. Основная причина сложившейся ситуации состоит в отсутствии комплексного подхода к решению проблемы информационно-компьютерной безопасности. Это приводит не только к ошибкам построения систем защиты, но и к недостаткам в поддержании их актуального состояния.

В рамках проекта по разработке СПАК реализована концепция системного подхода к обеспечению информационно-компьютерной безопасности АС конфиденциального делопроизводства, основанная на учете всех исходных требований, существующих угроз и влияющих на безопасность факторов при комплексном использовании наиболее эффективных мер, методов и средств защиты.

В основу разработанной архитектуры СПАК положены подсистемы глобального шифрования и усиленной аутентификации, предназначенные для нейтрализации скрытых угроз и эффективной реализации других подсистем, входящих в состав комплекса. Для аппаратной поддержки процесса аутентификации и хранения ключей шифрования в составе СПАК используются электронные идентификаторы ruToken, разработанные отечественными предприятиями Актив и Анкад.

В качестве операционной платформы СПАК вследствие объективных причин реализовано использование комбинированной операционной среды:

- для защищенного выполнения прикладных процессов и целевых функций АС — ОС Windows 2000/XP;
- для критичных функций настройки режимов защиты, управления ключами и конфигурирования криптомодулей — аналог ядра доверенной ОС МСВС.

В проекте СПАК описана формальная модель управления доступом к защищаемым ресурсам АС конфиденциального делопроизводства и проведена ее верификация. Показано, что разграничение доступа к информационным ресурсам (файлам, каталогам, томам NTFS, отчуждаемым носителям, портам ввода-вывода и принтерам) происходит в первую очередь согласно мандатному принципу контроля доступа, а дискреционные правила контроля доступа действуют только в пределах разрешений, установленных в соответствии с мандатным принципом. Эффективный доступ субъекта к информационным ресурсам

Труды СПИИРАН. 2006. Вып. 3. Т. 2. ISSN 2078-9181 (печ.), ISSN 2078-9599 (онлайн)
SPIIRAS Proceedings. 2006. Issue 3. V. 2. ISSN 2078-9181 (print), ISSN 2078-9599 (online)
www.proceedings.spiiras.nw.ru

определяется как результат пересечения атрибутов мандатного и дискреционного доступа. Представлены уровни, реализуемые в СПАК для защиты от обхода диспетчера доступа.

При формировании архитектуры СПАК изначально учитывались задачи эффективной защиты электронного документооборота:

- управление ключами шифрования на основе инфраструктуры открытых ключей;
- обеспечение подлинности электронных документов за счет формирования и проверки их электронных подписей;
- обеспечение конфиденциальности электронных документов за счет их шифрования.

Целесообразно дальнейшее расширение СПАК для построения системы управления цифровыми сертификатами на основе использования удостоверяющего центра, что обеспечит удобство и безопасность распределения открытых ключей для эффективной защиты информации в автоматизированных системах конфиденциального делопроизводства.

Литература

1. *Воробьев В. И., Шишкин В. М.* Проектирование систем анализа информационных рисков: методология и технология // Международная научно-практическая конференция «Информационные технологии и безопасность-2005» (ИТБ-2005), Украина, Крым, пгт Партенит, 13–18 июня 2005 г. Материалы конференции. Киев, 2005. С. 43.
2. *ГОСТ 28147-89.* Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.
3. *ГОСТ Р 34.10-2001.* Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи.
4. *ГОСТ Р 51275-99.* Защита информации. Объект информатизации. Факторы, воздействующие на информацию.
5. *Зима В. М., Котухов М. М., Ломако А. Г., Марков А. С., Молдовян А. А.* Разработка систем информационно-компьютерной безопасности. СПб.: ВКА им. А.Ф.Можайского, 2003. 284 с.
6. *Зима В. М., Молдовян А. А., Молдовян Н. А.* Безопасность глобальных сетевых технологий. СПб.: БХВ-Петербург, 2003. 165 с.
7. *Котенко И. В., Юсупов Р. М.* Перспективные направления исследований в области компьютерной безопасности // Защита информации. Инсайд. 2006. № 2. С. 46–57.
8. *Молдовян А. А., Молдовян Н. А., Гуц Н. Д., Изотов Б. В.* Криптография: скоростные шифры. СПб.: БХВ-Петербург, 2002. 268 с.