УДК 681.3

А. А. Костин, А. А. Костина, Д. М. Латышев, А. А. Молдовян

ПРОГРАММНЫЕ КОМПЛЕКСЫ СЕРИИ „АУРА“ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рассматриваются возможности программных комплексов серии „Аура“ для защиты информационных систем персональных данных в соответствии с требованиями Федерального закона № 152-ФЗ „О персональных данных“.

Ключевые слова: *защита информации, персональные данные, информационные системы персональных данных.*

Актуальность защиты персональных данных. В 2006 г. был опубликован Федеральный закон № 152-ФЗ „О персональных данных“. Цель Федерального закона — обеспечение защиты прав и свобод граждан при обработке их персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Этот закон определяет следующие понятия:

персональные данные — любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных);

оператор — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных;

обработка персональных данных — любое действие (операция) или совокупность действий (операций), совершаемых с персональными данными с использованием средств автоматизации или без их использования, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение;

информационные системы персональных данных — совокупность содержащихся в базах данных персональных сведений о гражданах и обеспечивающих их обработку информационных технологий и технических средств.

Федеральный закон прямо обязывает операторов при обработке персональных данных принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления и распространения, а также от иных неправомерных действий. По оценке Роскомнадзора число операторов в Российской Федерации превышает 2,5 млн. Таким образом, защита информационных систем персональных данных является массовой и актуальной проблемой.

Операторы, которые осуществляли обработку персональных данных до 1 июля 2011 г., обязаны представить определенные сведения в уполномоченный орган по защите прав субъектов персональных данных (Роскомнадзор) не позднее 1 января 2013 г. На 4 июня 2012 г. в реестре содержится информация о 245 100 операторах персональных данных, что составляет всего около 10 % от общего числа операторов.

С учетом прогнозной численности Роскомнадзор отображает в своем отчете за 2011 г. соотношение числа операторов, подавших уведомление, и операторов, до настоящего времени не исполнивших эту обязанность, по категориям операторов следующими данными:

— государственных органов — 10 526, что составляет 40,6 % от их прогнозной численности;

— муниципальных органов — 37 419, что составляет 49,5 % от их прогнозной численности;

— юридических лиц — 170 082, что составляет 10,2 % от их прогнозной численности;

— физических лиц — 11 885, что составляет 1,3 % от их прогнозной численности.

Проблемы защиты персональных данных. Мероприятия по обеспечению безопасности персональных данных (ПД) при их обработке в информационной системе персональных данных (ИСПД) могут включать следующие операции:

— определение угроз безопасности ПД и их актуальности;

— разработку на основе модели угроз системы защиты ПД;

— проверку готовности системы защиты ПД;

— установку и ввод в эксплуатацию системы защиты ПД;

— обучение лиц, использующих средства защиты информации (СЗИ);

— учет применяемых СЗИ и лиц, эксплуатирующих их;

— контроль за использованием СЗИ;

— описание системы защиты ПД.

План работ по защите персональных данных может иметь следующий вид.

1. Назначить подразделение (должностное лицо), ответственное за защиту ПД.

2. Сформировать комплект нормативных правовых актов Роскомнадзора, Федеральной службы по техническому и экспортному контролю (ФСТЭК) и Федеральной службы безопасности (ФСБ) России, изучить их требования и рекомендации.

3. Провести аудит ИСПД и оценить полноту выполнения требований нормативных правовых актов по защите ПД. Определить категории ПД и провести классификацию ИСПД, сформировать перечень ПД, спланировать работы по созданию системы защиты ПД.

4. Документально регламентировать работу с ПД. Разработать организационно-распорядительные документы по защите ПД. Получить согласие субъектов на обработку ПД.

5. Определить актуальные угрозы безопасности ПД и сформировать модель угроз. Уточнить класс специальных ИСПД. Разработать техническое задание и техпроект на создание (доработку) системы защиты ПД.

6. Привести систему защиты ПД в соответствие с требованиями нормативных правовых актов ФСБ и ФСТЭК России для установленного класса ИСПД. Установить необходимые сертифицированные СЗИ: антивирусной защиты, защиты от несанкционированного доступа, шифрования, защиты при межсетевом взаимодействии, защиты от утечки по техническим каналам.

7. Обучить лиц, ответственных за защиту ПД и работающих с ИСПД.

8. Получить лицензию на деятельность по технической защите конфиденциальной информации.

9. Уведомить Роскомнадзор об обработке ПД.

10. Организовать эксплуатацию защищенных ИСПД, мониторинг и реагирование на угрозы ИСПД в соответствии с требованиями по безопасности.

Выполнение такого плана для многих операторов — нетривиальная задача.

В число операторов, включенных в реестр, входят (отчет Роскомнадзора за 2011 г.) следующие организации:

— дошкольные учреждения — 29 010;

— общеобразовательные школы — 23 665;

— учреждения здравоохранения и социального развития — 12 724;

— средние и высшие учебные заведения — 2 212.

Для подавляющего большинства этих организаций сложности в реализации требований закона заключаются в первую очередь в нехватке кадров, недостатке средств и неясности в вопросе, что и как делать. Другой проблемой является ограниченное число лицензиатов ФСТЭК и ФСБ России, способных выполнить услуги по защите ПД на качественном уровне,

что приводит к высокой стоимости этих видов работ. Повышенная затратность в реализации требований закона вызвана и определенным монополизмом, а также явлениями коррупции, проникшей и в эту сферу человеческой деятельности.

Программные комплексы серии „Аура“. СПИИРАН, выполняя фундаментальные и прикладные исследования в области информационных технологий и защиты информации, разработал и серийно производит средства защиты информации от несанкционированного доступа (СЗИ НСД): „СГУ-2“, „Щит-РЖД“, „Аура“, „Аура 1.2.4“ (http://www.cobra.ru). Все перечисленные средства имеют сертификаты ФСТЭК России и зарегистрированы в государственном реестре программ для ЭВМ.

В состав семейства СЗИ НСД серии „Аура“ входят:

— СЗИ НСД „Аура“ (версия 1.1.2, сертификат ФСТЭК № 2188 от 21 октября 2010 г.), сертифицировано по 3-му классу защищенности средств вычислительной техники (СВТ) и 2-му уровню контроля недекларированных возможностей (НДВ), обеспечивает возможность построения автоматизированных систем (АС), отвечающих классу 1Б, 1В, 1Г, 1Д, и информационных систем по обработке персональных данных по классам К1, К2, К3, К4;

— СЗИ НСД „Аура 1.2.4“ (версия 1.2.4, сертификат ФСТЭК № 2527 от 26 декабря 2011 г.), сертифицировано по 5-му классу защищенности СВТ и 4-му уровню контроля НДВ, обеспечивает возможность построения АС, отвечающих классу 1Г, 1Д, и информационных систем по обработке персональных данных по классам К1, К2, К3, К4;

— СЗИ НСД „Аура 1.2“ (версия 1.2, проходит сертификацию), предназначено для замены СЗИ НСД „Аура“ (версия 1.1.2).

СЗИ НСД серии „Аура“ предназначены для комплексной защиты информации, обрабатываемой на компьютере под управлением 32/64-битовых операционных систем (ОС) Windows 2000/XP/Vista/7 Server 2000/2003/2008/2008R2.

СЗИ НСД серии „Аура“ являются классическими системами защиты информации и могут широко применяться на межотраслевом уровне для обеспечения информационной безопасности автоматизированных систем [1].

При разработке СЗИ НСД серии „Аура“ основные исследования были направлены на замещение (или дублирование) наиболее важных, с точки зрения безопасности, механизмов ОС на собственные модули, а также введение дополнительных. В этом случае механизмы ОС (например, аутентификация) становятся вспомогательными, так как основную функцию выполняют модули СЗИ НСД. Некоторые механизмы (например, доверенная среда СЗИ НСД с графическим интерфейсом) имеют уникальный характер и позволяют существенно расширить возможности средств защиты.

Наличие собственных механизмов СЗИ позволяет обеспечить безопасность информации в случае взлома механизмов ОС (например, в случае уязвимости ОС). Кроме того, расширенный независимый от операционной системы мониторинг событий позволяет изучить возникающие проблемы и своевременно на них реагировать.

Преимущества СЗИ НСД серии „Аура“.

1. *Совместимость:*

— совместимость с доменами Active Directory, отсутствие необходимости смены настроек домена;

— поддержка как 32-, так и 64-битовых версий операционных систем;

— поддержка ОС Windows 7;

— выполнение блокировки консоли по нескольким типам электронных ключей (Rutoken 1.0/2.0/3.0, eToken PRO, eToken Java) и USB флеш-дискам.

2. *Усиление защиты операционной системы:*

— возможность двухфакторной аутентификации (аутентификации по паролю и разблокировки консоли по электронному ключу);

— выполнение контроля печати из всех приложений;

— контроль доступа к дискам с файловыми системами FAT/CDFS/NTFS;

— регистрация обращений к файлам на дисковых системах FAT/CDFS/NTFS;

— гарантированное „затирание“ свободного места на дисках и выборочное „затирание“ файлов;

— организация работы пользователей, исключающая возможность несанкционированного считывания информации со съемных носителей, в том числе при их выносе за пределы организации;

— двухфакторная аутентификация сетевых пользователей;

— возможность реализации такого варианта настройки СЗИ, при котором пользователь не будет знать свой пароль в ОС/Active Directory.

3. *Технологичность:*

— возможность функционирования домена безопасности без домена Active Directory;

— централизованное управление;

— возможность функционирования консоли управления доменом безопасности с любого разрешенного администратором рабочего места, причем установка дополнительного программного обеспечения (ПО) на это рабочее место не требуется;

— отсутствие необходимости установки дополнительного ПО (SQL-сервера и т.п.) на сервер безопасности;

— четкая иерархия пользователей;

— возможность постепенного развертывания СЗИ, в том числе при наличии домена Active Directory;

— возможность дистанционной автоматической установки;

— единый дистрибутив для установки на серверы и рабочие станции.

Применение алгоритмов шифрования. В настоящее время общепризнано применение криптографии для реализации эффективных механизмов защиты информации. Реализация алгоритмов криптографического преобразования в реальных системах защиты информации имеет определенные технические и организационные трудности и требует специальных подходов [2—8].

Алгоритмы криптографического преобразования применяются для решения следующих задач:

— аутентификация;

— контроль целостности;

— шифрование документов (файлов);

— шифрование участков памяти машинных носителей информации;

— шифрование машинных носителей информации в целом;

— шифрование информации, циркулирующей в компьютерных сетях;

— цифровая подпись файлов;

— шифрование баз данных, содержащих пароли пользователей и права доступа;

— гарантированное уничтожение информации.

Криптофункции могут быть реализованы непосредственно СЗИ НСД или в составе специализированного средства, которое может быть независимым либо интегрировано с СЗИ. СЗИ НСД „Аура“ включает набор функций специального преобразования информации, которые существенно повышают уровень ее защищенности и обеспечивают дополнительные возможности средства защиты (например, привязку съемных машинных носителей к конкретным компьютерам). СЗИ НСД „Аура 1.2.4“ не обладает возможностью шифрования документов, однако оно может быть интегрировано с самостоятельным программным комплексом, ориентированным на реализацию алгоритмов шифрования.

Проблемы безвозмездного распространения программных средств защиты информации. Необходимым элементом обеспечения защиты информационных систем персональных данных является использование СЗИ НСД. Средняя рыночная цена СЗИ НСД составляет около 4 тыс. руб. для защиты одного рабочего места. СЗИ НСД серии „Аура“ являются программными комплексами и могут быть распространены по лицензионным соглашениям.

Принимая во внимание сложности в реализации мероприятий для исполнения Федерального закона № 152-ФЗ „О персональных данных“, СПИИРАН предоставляет образовательным, воспитательным и лечебным учреждениям, финансируемым из госбюджета, право безвозмездного и бессрочного использования СЗИ НСД „Аура 1.2.4“ для образовательных целей и защиты персональных данных.

На сайте института http://www.spiiras.nw.ru и сайте отдела проблем информационной безопасности http://www.cobra.ru опубликована информация о возможности безвозмездного и бессрочного пользования разработанными СПИИРАН программными средствами. СЗИ НСД „Аура 1.2.4“ и вся необходимая документация размещены для свободного копирования на сайте http://www.cobra.ru.

Однако имеется ряд проблем, препятствующих возможности безвозмездного и широкого распространения СЗИ НСД:

— существующие правила производства и распространения СЗИ не рассчитаны на электронные технологии (требуются знаки соответствия, заверенные копии документов, машинный носитель, формуляр);

— процедуры сертификации и продления сертификата весьма затратны;

— техническое сопровождение при масштабном распространении СЗИ становится обременительным;

— дистрибьюторы мало заинтересованы в продвижении программного продукта.

Решение этих проблем позволит расширить перечень инновационной продукции и круг организаций, которые смогут безвозмездно либо на льготной основе использовать результаты интеллектуальной деятельности СПИИРАН в области защиты информации.

Несмотря на актуальность задачи защиты ПД, которая к тому же носит массовый характер, за 7 месяцев информирования общества о возможности бесплатного использования средств защиты СПИИРАН получил с территории РФ всего 18 запросов о предоставлении СЗИ НСД „Аура 1.2.4“ на безвозмездной основе. Явное несоответствие количества запросов и числа операторов персональных данных, не решивших задачи их защиты, симптоматично и требует отдельного исследования.

СПИСОК ЛИТЕРАТУРЫ

1. *Молдовян А. А., Юсупов Р. М.* Проблемы информатизации и вопросы информационной безопасности транспортной отрасли // Транспортная безопасность и технологии. 2010. № 3 (23). С. 120—122.

2. *Молдовян А. А.* Криптография для защиты компьютерной информации (часть 1) // Интеграл. 2004. № 4 (18). С. 42—43.

3. *Молдовян А. А.* Криптография для защиты компьютерной информации (часть 2) // Интеграл. 2004. № 5 (19). С. 60—61.

4. *Молдовян А. А.* Некоторые вопросы защиты программной среды ПЭВМ // Безопасность информационных технологий. 1995. № 2. С. 22—28.

5. *Молдовян А. А.* Подход к созданию средств защиты информации массового применения // Управление защитой информации. 1998. Т. 2, № 1. С. 26—27.

6. *Молдовян А. А., Молдовян Н. А.* Программные механизмы защиты ЭВМ // Банковские технологии. 1997. № 1 (23). С. 68—70.

7. *Молдовян А. А., Молдовян Н. А., Молдовян П. А.* Новый метод криптографических преобразований для современных систем защиты ПЭВМ // Управляющие системы и машины. 1992. № 9/10. С. 44—50.

8. *Молдовян А. А., Молдовян Н. А., Молдовян П. А.* Программная реализация технологии прозрачной защиты ЭВМ // Управляющие системы и машины. 1996. № 4/5. С. 38—47.

Сведения об авторах

Андрей Алексеевич Костин — канд. техн. наук; СПИИРАН, лаборатория криптологии; E-mail: info@iias.spb.su

Анна Александровна Костина — СПИИРАН, лаборатория криптологии; науч. сотрудник; E-mail: info@iias.spb.su

Дмитрий Михайлович Латышев — СПИИРАН, лаборатория криптологии; науч. сотрудник; E-mail: info@iias.spb.su

Александр Андреевич Молдовян — д-р техн. наук, профессор; СПИИРАН; заместитель директора; E-mail: maa1305@yandex.ru

Рекомендована СПИИРАН

Поступила в редакцию
10.06.12 г.