открытость управления, свобода доступа к информации за исключением информации, распространение которой является ограниченной;

развитие партнерства в сфере информатизации ОВД;

вовлечение в процесс информатизации ОВД всех слоев и социальных групп населения, ликвидация цифрового неравенства;

обеспечение нового уровня цифровой грамотности сотрудников ОВД.

Критерием успешности реализации данных направлений может явиться готовность ОВД к переходу на электронный документооборот к 2022 г.

Стремительное развитие информационной сферы ОВД, основанной на использовании современных информационных технологий, порождает большое количество проблем правового, управленческого, организационного, технического и финансового характера.

В заключение хотелось бы отметить, что одним из путей решения указанных вопросов является качественное совершенствование нормативного правового и организационного регулирования информатизации в ОВД. В связи с этим основное внимание в работе должно уделяться исследованию особенностей правого обеспечения, разработке и использованию современных информационных технологий в деятельности ОВД.

УДК 004.056.5

Е.Б. Кузин

ПРИМЕНЕНИЕ КРИПТОГРАФИЧЕСКИХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В ДЕЯТЕЛЬНОСТИ УЧРЕЖДЕНИЙ ФСИН РОССИИ

Одной из задач развития систем информационного обеспечения учреждений уголовно-исполнительной системы (УИС) является совершенствование систем информационной безопасности и защиты информации. Применение криптографических средств защиты информации – важная составляющая часть создания комплексной системы защиты информации. К средствам криптографической защиты информации относят: средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования.

Современная криптография является областью знаний, связанной с решением таких проблем безопасности информации, как конфиденциальность, целостность, аутентификация. Достижение этих требований безопасности информационного взаимодействия и составляет основные цели криптографии.

Обеспечение конфиденциальности – решение проблемы защиты информации от ознакомления с ее содержанием со стороны лиц, не имеющих права доступа к ней. В зависимости от контекста вместо термина «конфиденциальная» могут выступать термины «секретная», «частная», «ограниченного доступа» информация.

Обеспечение целостности – гарантирование невозможности несанкционированного изменения информации. Для гарантии целостности необходим простой и надежный критерий обнаружения любых манипуляций с данными (вставка, удаление и замена).

Обеспечение аутентификации – разработка методов подтверждения подлинности сторон (идентификация) и самой информации в процессе информационного взаимодействия. Информация, передаваемая по каналу связи, должна быть аутентифицирована по источнику, времени создания, содержанию данных, времени пересылки и т. д.

Современная криптография включает в себя четыре раздела: симметричные ключи, открытые ключи, электронно-цифровая подпись, системы управления ключами.

Существуют две методологии криптографической обработки информации с использованием ключей – симметричная и асимметричная. Симметричная (секретная) методология предусматривает, что и для шифрования, и для расшифровки отправителем и получателем применяется один и тот же ключ, об использовании которого они договорились до начала взаимодействия. Если ключ не был скомпрометирован, то при расшифрке автоматически выполняется аутентификация отправителя, так как только отправитель имеет ключ, с помощью которого можно зашифровать информацию, и только получатель имеет ключ, с помощью которого можно расшифровать информацию.

При асимметричной (открытой) методологии шифрования документ шифруется одним ключом, а расшифровывается другим. Каждый из участников передачи информации самостоятельно генерирует два случайных числа секретный (закрытый) и открытый ключи. Открытый ключ передается по открытым каналам связи другому участнику процесса криптозащиты, а секретный ключ хранится в секрете. Отправитель шифрует сообщение открытым ключом получателя, а расшифровать его может только владелец секретного ключа.

Огромным преимуществом публичной криптографии также является возможность использования электронной цифровой подписи (ЭЦП), которая позволяют получателю сообщения удостовериться в личности отправителя сообщения, а также в целостности (верности) полученного сообщения.

Еще одно важное преимущество использования криптографии состоит в том, что применяется так называемая хэш-функция, которая дейст-

вует таким образом, что в случае какого-либо изменения информации, пусть даже на один бит, результат хэш-функции будет совершенно иным. С помощью хэш-функции и закрытого ключа создается подпись, передаваемая программой вместе с текстом. При условии использования надежной формулы хэш-функции невозможно вытащить подпись из одного документа и вложить в другой либо каким-то образом изменить содержание сообщения. Любое изменение подписанного документа сразу же будет обнаружено при проверке подлинности подписи.

Цифровые сертификаты ключей упрощают задачу определения принадлежности открытых ключей предполагаемым владельцам. Цифровой сертификат ключа – это информация, прикрепленная к открытому ключу пользователя, помогающая другим установить, является ли ключ подлинным и верным. Цифровые сертификаты нужны для того, чтобы сделать невозможной попытку выдать ключ одного человека за ключ другого. Сертификат – это цифровой документ, содержащий информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т. д. Сертификат заверяется электронной цифровой подписью удостоверяющего центра сертификации.

Сертификаты выдаются конкретному субъекту и содержат его открытый ключ. Подлинность самого сертификата гарантируется его эмитентом, то есть выпустившей организацией, которой изначально доверяют все участники переписки.

Задачами развития систем информационного обеспечения учреждений УИС являются:

внедрение перспективных информационных технологий, средств вычислительной техники и телекоммуникаций, локальных вычислительных сетей, типовых программных средств и автоматизированных рабочих мест для обобщения и анализа информации, информационной поддержки оперативно-служебной деятельности;

совершенствование инфраструктуры информационно-телекоммуникационного и других видов обеспечения функционирования и развития системы передачи и обработки данных, систем информационной безопасности и защиты информации.

К средствам криптографической защиты информации (СКЗИ) относят средства шифрования, средства имитозащиты, средства электронной цифровой подписи, средства кодирования, средства изготовления ключевых документов и сами ключевые документы.

Служебная деятельность территориальных органов и учреждений УИС связана с хранением и обработкой персональных данных различных категорий, к защите которых законодательством РФ выдвигается ряд требований. Для их выполнения необходимо формирование модели

угроз персональным данным и разработки на ее основе системы защиты персональных данных, в состав которой должно входить средство криптографической защиты информации. К СКЗИ, внедренному в систему защиты персональных данных, выдвигаются следующие требования:

штатно функционирует совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к нему требований;

сертифицировано в системе сертификации ФСБ России криптосредства для обеспечения безопасности персональных данных при их обработке.

Криптографическое средство, в зависимости от обеспечиваемого им уровня защиты, относится к одному из шести классов (КС1, КС2, КС3, КВ1, КВ2, КА1). Внедрение криптосредства того или иного класса в систему защиты обусловливается категорией нарушителя, которая определяется оператором в модели угроз.

Комплексный подход к защите информации подразумевает использование межсетевых экранов, антивирусов и фаерволов, а также включает разработку модели угроз информационной безопасности (ИБ), выработку необходимых политик ИБ, назначение ответственных за информационную безопасность, контроль электронного документооборота, контроль и мониторинг деятельности сотрудников и др.

Главное назначение системы электронного документооборота (СЭД) – это организация хранения электронных документов, а также работы с ними. Использование системы электронного документооборота позволяет значительно повысить производительность труда делопроизводственного персонала учреждений УИС, сокращает время, затрачиваемое на процессы документооборота. В СЭД реализованы надежные средства разграничения полномочий и контроля за доступом к документам. ЭЦП выступает как основной способ защиты и придания юридической силы информации. В СЭД используется простая электронная подпись (сочетание имени пользователя и пароля) и усиленная квалифицированная электронная подпись (электронный ключ с сертификатом электронной подписи) в соответствии с Федеральным законом Российской Федерации «Об электронной подписи».

Электронные торги и аукционы госзаказа проводятся на специализированных площадках (сайтах в глобальной сети Интернет). Для регистрации на площадках необходима электронная цифровая подпись, выпущенная специально для госзаказа. Получить ее можно в удостоверяющих центрах. ЭЦП необходима, чтобы поставщики были уверены, что работают и контактируют с реальными предложениями и участвуют в активных торгах. Контракты, содержащие электронную подпись, имеют юридическую значимость и содержат в себе полную юридиче-

скую силу только после соглашения и подписания контракта обеими сторонами – поставщиком и клиентом.

«КриптоПро CSP» представляет собой криптопровайдер – программный модуль, позволяющий осуществлять криптографические операции в операционных системах, управление которым происходит с помощью функций CryptoAPI. «КриптоПро CSP» поддерживает российские криптографические алгоритмы (ГОСТ) и имеет сертификаты ФСБ России.

КриптоПро CSP предназначен:

для авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки электронной цифровой подписи в соответствии с отечественными стандартами ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012;

обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты в соответствии с ГОСТ 28147-89;

обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;

контроля целостности системного и прикладного программного обеспечения в целях защиты от несанкционированных изменений и нарушений правильности функционирования;

управления ключевыми элементами системы в соответствии с регламентом средств защиты.

«КриптоПро CSP» поддерживает следующие типы ключевых носителей:

электронный USB-ключ или смарт-карту eToken;

процессорные карты MPCOS-EMV и российские интеллектуальные карты (РИК) с использованием считывателя смарткарт-GemPlus GCR-410;

таблетки Touch-Memory DS1993-DS1996 с использованием устройств «Аккорд 4+», электронный замок «Соболь» или устройство чтения таблеток Touch-Memory DALLAS;

реестр Windows.

Основные функции, реализуемые «КриптоПро CSP»:

генерация секретных (256 бит) и открытых (1024 бита) ключей ЭЦП и шифрования;

формирование секретных ключей на различных типах носителей;

криптографическая защита информации (система электронной цифровой подписи на базе асимметричного криптографического алгоритма);

хеширование данных;

шифрование данных;

имитозащита данных;

формирование электронной цифровой подписи;

опциональное использование пароля (PIN-кода) для дополнительной защиты ключевой информации;

реализация мер защиты информации пользователя от несанкционированного доступа.

Аппаратно-программный комплекс обеспечивает криптографическую защиту информации (в соответствии с ГОСТ 28147–89), передаваемой по открытым каналам связи, между составными частями VPN, которыми могут являться локальные вычислительные сети, их сегменты и отдельные компьютеры. Комплекс предназначен для организации удаленного доступа к корпоративным ресурсам, а также защиты компьютера пользователя от несанкционированного доступа извне.

Комплекс имеет два компонента: абонентский пункт и межсетевой экран.

Абонентский пункт подключается к корпоративным ресурсам и обеспечивает обмен информации в зашифрованном виде. Поддерживается работа с криптопровайдерами «Код Безопасности CSP» (входит в состав программного обеспечения абонентского пункта) и «КриптоПро CSP» (устанавливается отдельно).

Для защиты от проникновения со стороны сетей общего пользования комплекс «Континент 3.7» обеспечивает фильтрацию принимаемых и передаваемых пакетов по различным критериям (адреса отправителя и получателя, протоколы, номера портов, дополнительные поля пакетов и т. д.). Осуществляет поддержку VoIP, видеоконференций, ADSL, Dial-Up и спутниковых каналов связи, технологии NAT/PAT для сокрытия структуры сети.

Для подключения к корпоративным ресурсам абонентский пункт устанавливает соединение с сервером доступа, расположенным в корпоративной сети. Сервер доступа определяет права пользователя на доступ к корпоративным ресурсам. Аутентификация пользователя выполняется с помощью метода асимметричного шифрования.

Для взаимодействия абонентского пункта и сервера доступа используют следующие сертификаты открытых ключей:

сертификат пользователя – для аутентификации пользователя на сервере доступа;

сертификат сервера доступа – для аутентификации сервера доступа;

сертификат корневого центра сертификации – для подтверждения подлинности сертификата пользователя и сертификата сервера доступа.

Межсетевой экран обеспечивает фильтрацию IP-пакетов сетевого трафика компьютера, на котором установлен абонентский пункт.

Материалы статьи могут использоваться в учебном процессе при изучении дисциплины «Информационная безопасность» по специализации «Правоохранительная деятельность».