О. В. Бавина
Правительство Москвы,
Е. М. Гиляров
Московский инженерно-физический институт (государственный университет)

ОБЕСПЕЧЕНИЕ БАЗОВОГО УРОВНЯ БЕЗОПАСНОСТИ ГОРОДСКИХ ИНФОРМАЦИОННЫХ СИСТЕМ

Часть II Концепции информационной безопасности в органах исполнительной власти города Москвы («Открытые и конфиденциальные информационные ресурсы»), принятой в сентябре 2005 года [1], устанавливает комплексный подход к обеспечению информационной безопасности в органах исполнительной власти (ОИВ) города Москвы. Комплексный подход включает правовые, организационные, технические, программные, социальные и иные механизмы, способные обеспечить целостность информационных систем и ресурсов города, гарантированный доступ населения, хозяйствующих субъектов и органов власти к информации и информационным услугам, а также защиту информации в установленном законодательством порядке.

Основой организации обеспечения информационной безопасности в ОИВ города Москвы в рамках комплексной системы информационной безопасности (КСИБ) является достижение базового уровня безопасности городских автоматизированных систем (АС).

По определению Концепции базовый уровень информационной безопасности — это уровень безопасности, при котором удовлетворяется установленный минимальный объем требований по информационной безопасности, приводящий к приемлемому для владельцев информации уровню снижения риска ее компрометации, то есть приемлемому для владельцев информации уровню возможности утери конфиденциальности информации, ее целостности или доступности [1. С. 28].

Задавать требования к базовому уровню информационной безопасности (ИБ) для конкретного объекта защиты необходимо на предпроектной стадии создания автоматизированной системы. В ходе ее создания или модернизации параллельно должна создаваться или модернизироваться обеспечивающая базовый уровень подсистема информационной безопасности. По завершении очередного этапа создания, модернизации, установленного календарного периода эксплуатации (как правило, не менее года) должен определяться текущий уровень ИБ объекта защиты в целях контроля его соответствия требуемому уровню — так называемый периодический контроль. В критически важных элементах городской информационной инфраструктуры дополнительно должен быть предусмотрен постоянный контроль за соблюдением базового уровня — в этих целях создается Система мониторинга событий информационной безопасности города Москвы. Базовый уровень также может уточняться в зависимости от установленных критериев его достижения в процессе разработки и эксплуатации объекта защиты.

Основным документом, определяющим подход к определнию необходимого и достаточного уровня информационной безопасности АС города Москвы, является утвержденный Мэром Москвы документ «Методические рекомендации по формированию требований к обеспечению информационной безопасности информационных систем и ресурсов органов исполнительной власти города Москвы» [2] (далее — Методические рекомендации).

В качестве объектов защиты Методические рекомендации определяют информационные системы и ресурсы города Москвы, включающие:

— общедоступную информацию;

— информацию ограниченного доступа, в том числе информацию, составляющую служебную тайну, коммерческую тайну, профессиональную тайну и персональные данные;

— средства и системы связи и передачи данных в АС, программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное

обеспечение), используемые для сбора, хранения, обработки и передачи информации, средства защиты информации [2. С. 31].

В зависимости *от состава (категории) информации* и *потенциальных угроз* для определения требуемых мероприятий по защите информации, а также для минимизации затрат на защиту информации установлено два базовых уровня информационной безопасности АС:

1) базовый уровень информационной безопасности АС, обрабатывающих открытую информацию — определяется владельцем, т. е. Правительством Москвы;

2) уровень информационной безопасности АС, содержащих информацию ограниченного доступа, в том числе конфиденциальную и секретную, — определяется нормативными документами федерального уровня [2. С. 7; 3. С. 7].

Реализация базового уровня информационной безопасности может обеспечиваться использованием типовых проектных решений.

Категорирование информации в целях определения требуемого уровня ИБ должно проводиться в соответствии с действующим законодательством РФ и города Москвы. Основой категорирования является Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [4]. На уровне города Москвы подходы к категорированию информации установлены в Концепции информационной безопасности в ОИВ города Москвы [1. С. 14, 49]. Кроме того, в целях создания классификатора информации ограниченного доступа, циркулирующей в ОИВ города Москвы, в Москве был принят соответствующий документ — «Информационная безопасность информационных систем и ресурсов органов исполнительной власти города Москвы. Классификатор конфиденциальной информации, содержащейся в информационных системах и ресурсах органов исполнительной власти города Москвы» [5], а с целью обеспечения учета информации ограниченного доступа — документ «Положение о Реестре конфиденциальной информации, содержащейся в информационных системах и ресурсах органов исполнительной власти города Москвы» [6].

Состав угроз ИБ определяется в каждом конкретном случае на основании рекомендаций ФСТЭК РФ, госстандартов и Методических рекомендаций. В приложении 3 к Методическим рекомендациям приведен подробный классификатор угроз, учитывающий вышеназванные требования и рекомендации.

Основу требований базового уровня информационной безопасности АС должны составлять квалификационные минимумы требований к видам обеспечения ИБ: правовому, техническому, организационному [2. С. 9].

На необходимом минимуме технических требований остановимся ниже.

В целях нормативно-правового обеспечения информационной безопасности должны быть разработаны соответствующие документы на следующих уровнях: макроуровень (Российская Федерация, международные организации); метауровень (город Москва); микроуровень (предприятие, организация — владелец информации).

Организационное обеспечение базового уровня информационной безопасности состоит в необходимости выполнения каждым владельцем информационных систем и ресурсов города Москвы ряда требований, в числе которых следующие:

- обеспечение штатного наполнения специалистами по информационной безопасности;
- разработка и контроль реализации программ и планов обеспечения информационной безопасности города и отдельных информационных систем и ресурсов;
- определение порядка обращения с категорированной информацией;
- контроль выполнения регламентов органов власти города в части обеспечения информационной безопасности, реализации механизмов поощрения и наказания должностных лиц.

Базовый уровень информационной безопасности информационной системы конкретного органа власти оценивается совокупной мерой оценок показателей нейтрализации всех угроз, установленных

при создании системы с учетом выбранного класса защищенности автоматизированной системы. Такую оценку правомочны осуществлять государственный заказчик создания автоматизированной системы, разработчик с привлечением специалистов по информационной безопасности.

Таким образом, достижение базового уровня информационной безопасности органов исполнительной власти города Москвы означает, что во всех городских информационных системах обеспечивается защита от тех угроз, которые были определены владельцами информации с учетом требований федерального и московского законодательства.

Требования базового уровня информационной безопасности в случае создания (модернизации) конкретной АС могут и должны (особенно в случае создания (модернизации) АС, содержащей информацию ограниченного доступа) дополняться требованиями нормативных, нормативно-технических документов различного уровня с учетом положений Методических рекомендаций.

Для технического обеспечения базового уровня ИБ в АС должны быть реализованы следующие требования:

- по управлению доступом, регистрации и учету, обеспечению целостности на средствах защиты общесистемного программного обеспечения;
- по антивирусной защите;
- по резервному копированию и восстановлению данных,
- по контролю и управлению защитой на специальных программно-технических средствах защиты.

Подсистема управления доступом должна обеспечивать защиту от несанкционированного доступа (НСД) серверов, автоматизированных рабочих мест (АРМ) пользователей и прикладных сервисов. Кроме того, должна быть обеспечена защита от НСД аппаратно-программных средств, влияющих на функционирование сегментов информационных сетей, в которых обрабатывается защищаемая информация.

При создании подсистемы управления доступом могут использоваться как наложенные, так и встроенные в операционные системы и приложения средства защиты от НСД.

Доступ к защищаемым ресурсам (инфраструктурным и информационным) должен осуществляться в соответствии с матрицей доступа. При построении матрицы доступа объекты и субъекты доступа должны идентифицироваться по уникальным параметрам (например, по логическим именам).

Набор идентификаторов пользователя, необходимый для предоставления ему доступа к каждому отдельному инфраструктурному или информационному ресурсу, как минимум, включает в себя логическое имя, пароль, цифровой сертификат или электронный ключ. Передача идентификационных параметров должна осуществляться по защищенному каналу связи.

Подсистема регистрации и учета должна обеспечивать регистрацию следующих событий:

а) запуск и остановка средств регистрации;

б) события, связанные с функциональными компонентами (средствами безопасности), например, такие как:

— любое использование программно-аппаратных средств аутентификации;

— принятие или отклонение любого используемого атрибута безопасности (например, пароля или цифрового сертификата) при аутентификации;

— все попытки установления сеансов пользователями;

— истечение срока действия атрибутов безопасности (паролей, цифровых сертификатов и пр.);

— успешные и неуспешные попытки активизации (запуска) программ (процессов) субъектами доступа (пользователями);

— идентификатор пользователя или субъекта доступа, неуспешно пытавшегося получить доступ к объекту доступа (сервису или файлу);

— любые попытки выполнения операций с системным журналом, т. е. любые попытки чтения, изменения или уничтожения системного журнала.

Средства регистрации должны приписывать к каждой записи, по крайней мере, следующие данные: дату и время возникновения события, тип события, идентификатор субъекта доступа и результат завершения события (успешное/неуспешное).

Подсистема обеспечения целостности должна обеспечивать целостность программных средств объекта защиты, а также неизменность программной среды. При этом:

— целостность объекта защиты проверяется при загрузке системы по контролируемым суммам компонент защиты;

— целостность программной среды обеспечивается как запретом на модификацию программ и конфигурационных файлов с помощью наложенных или встроенных в операционную систему средствами защиты от НСД, так и применением средств мониторинга событий информационной безопасности;

— должно проводиться периодическое тестирование функций защиты объекта защиты при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

— должны быть в наличии средства восстановления объекта защиты, предусматривающие ведение двух копий программных средств защиты от НСД и их периодическое обновление и контроль работоспособности. Регламенты по восстановлению должны определять ответственных исполнителей (администраторов), средства и период времени, требуемый на восстановление.

Подсистема антивирусной защиты устанавливает следующие требования:

— должны применяться только сертифицированные средства антивирусной защиты. Установка и регулярное обновление средств антивирусной защиты на автоматизированных рабочих местах и серверах АС должны осуществляться администраторами АС;

— должны быть разработаны и введены в действие инструкции по антивирусной защите, учитывающие особенности технологических процессов обработки информации. Особое внимание должно быть уделено антивирусной фильтрации трафика электронного почтового обмена;

— отключение антивирусных средств не допускается. Установка и обновление антивирусных средств в организации должны контролироваться представителями подразделений (лицами) в организации, ответственными за обеспечение ИБ;

— должны быть разработаны организационно-технические меры, и введены в действие инструкции по обеспечению режима безопасного функционирования информационной системы в случае, когда невозможно обеспечить обновление сертифицированных средств антивирусной защиты.

Подсистема резервного копирования, восстановления и архивирования устанавливает следующие требования:

— должны быть подготовлены регламенты по резервному копированию, восстановлению и архивированию с использованием специальных программно-аппаратных средств;

— процедуры резервного копирования, восстановления и архивирования должны основываться на ведении циклически перезаписываемых нескольких (не менее трех) наборов копий, в том числе территориально разнесенных.

Контроль функционирования должен обеспечиваться:

— силами собственного подразделения по защите информации (администратора безопасности) или силами внешней эксплуатирующей организации, обладающей необходимыми лицензиями;

— программно-техническим комплексом системы защиты информации.

Для целей реализации требований базового уровня информационной безопасности конкретных АС важными являются создание и обеспечение функционирования инфраструктурного уровня КСИБ.

В соответствии с Концепцией информационной безопасности ОИВ города Москвы инфраструктурный уровень КСИБ должен включать:

– систему Удостоверяющих центров по выдаче и подтверждению цифровых сертификатов открытых ключей для криптографической аутентификации пользователей и использования электронной цифровой подписи при электронном обмене данными;

– систему защищенных центров хранения и обработки данных информационных ресурсов города Москвы (резервные центры);

– Центр мониторинга и защиты информационных ресурсов города Москвы от внешних и внутренних угроз информационной безопасности;

– защищенные городские информационные порталы;

– защищенную систему передачи данных между организациями, предприятиями и органами власти города Москвы;

– защищенную систему электронной почты, обеспечивающую передачу юридически значимых электронных документов между организациями, предприятиями и органами власти города Москвы [1. С. 40].

В настоящее время в городе Москве создана система Уполномоченных удостоверяющих центров органов исполнительной власти города Москвы, утверждено Положение о ней [7, 8].

К мероприятиям Городской целевой программы «Электронная Москва», развивающим инфраструктурный уровень КСИБ, относятся работы по созданию и развитию защищенного центра резервного хранения данных информационных ресурсов города Москвы, централизованного хранилища электронных документов, подписанных электронной цифровой подписью, системы мониторинга событий информационной безопасности, городской мультисервисной транспортной сети Правительства Москвы.

Постановлением Правительства Москвы от 14.06.2005 № 439-ПП «О дальнейшем проведении работ по созданию Московского городского портала» утверждена Концепция системы городских порталов, включающая в себя требования по обеспечению информационной безопасности создаваемых в ОИВ города Москвы порталов [9].

Таким образом, необходимая инфраструктура для реализации базовых требований информационной безопасности АС в городе Москве предусмотрена и в настоящее время создается.

Однако пока не отлажены механизмы реализации и контроля требуемого уровня информационной безопасности. В «Основных направлениях Политики информационной безопасности Правительства Москвы до 2010 года» [10] обозначены направления развития правового, организационного, технического обеспечения информационной безопасности.

Для того чтобы задать базовый уровень ИБ как совокупности правовых, технических и организационных мер, руководителям отраслевых, функциональных и территориальных ОИВ города Москвы предлагается следовать документам Политики информационной безопасности города Москвы, утвержденным в ноябре 2006 года (1 очередь) и октябре 2007 года (2 очередь), а также единым требованиями к оформлению, структуре и содержательной части технических заданий («шаблон ТЗ») с разделом по обеспечению безопасности информации, включающим минимально необходимый набор требований для объектов защиты [11].

Следование положениям вышеназванных документов позволит задать требуемый уровень информационной безопасности создаваемых (модернизируемых) АС города Москвы, а выполнение мероприятий, заданных в «Основных направлениях Политики информационной безопасности Правительства Москвы до 2010 года», позволит достичь базового уровня информационной безопасности АС городских органов исполнительной власти в целом к указанному сроку.

СПИСОК ЛИТЕРАТУРЫ

1. Концепция информационной безопасности в органах исполнительной власти города Москвы. Часть II. Открытые и конфиденциальные информационные ресурсы. Утверждена Мэром Москвы Ю. М. Лужковым 07 сентября 2005 года.

2. Методические рекомендации по формированию требований к обеспечению информационной безопасности информационных систем и ресурсов органов исполнительной власти города Москвы. Утверждены Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.

3. Положение о защите информации в информационных системах и ресурсах органов исполнительной власти города Москвы. Утверждено Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
4. Федеральный закон от 27 июля 2006 года №149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства РФ от 31.07.2006, № 31 (Ч. 1). С. 34–48.
5. Информационная безопасность информационных систем и ресурсов органов исполнительной власти города Москвы. Классификатор конфиденциальной информации, содержащейся в информационных системах и ресурсах органов исполнительной власти города Москвы. Утвержден Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
6. Положение о Реестре конфиденциальной информации, содержащейся в информационных системах и ресурсах органов исполнительной власти города Москвы. Утверждено Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
7. Постановление Правительства Москвы от 07.12.2004 № 848-ПП «Об определении Уполномоченных удостоверяющих центров» // Вестник Мэра и Правительства Москвы. № 71. 22.12.2004;
8. Постановление Правительства Москвы от 26.07.2005 № 544-ПП «Об утверждении Положения о системе уполномоченных удостоверяющих центров органов исполнительной власти города Москвы» // Вестник Мэра и Правительства Москвы. № 46. 17.08.2005.
9. Постановление Правительства Москвы от 14.06.2005 № 439-ПП «О дальнейшем проведении работ по созданию Московского городского портала» // Вестник Мэра и Правительства Москвы. № 40. 18.07.2005.
10. Основные направления Политики информационной безопасности Правительства Москвы до 2010 года. Утверждены Мэром Москвы Ю. М. Лужковым 29 ноября 2006 года.
11. Единые требования к оформлению, структуре и содержательной части технических заданий. Утверждены Приказом Управления информатизации города Москвы от 16.03.2007 №64-06-13/07.

Е. С. Дернова, Н. А. Молдовян (д. т. н.)
ФГУП НИИ «Вектор» – СЦПС «Спектр», Санкт-Петербург

ПРОТОКОЛЫ КОЛЛЕКТИВНОЙ ЦИФРОВОЙ ПОДПИСИ, ОСНОВАННЫЕ НА СЛОЖНОСТИ РЕШЕНИЯ ДВУХ ТРУДНЫХ ЗАДАЧ[1]

Рассматриваются новые криптографические протоколы коллективной электронной цифровой подписи (КЭЦП). С целью снижения вероятности компрометации подписи предлагаются реализации схем КЭЦП, взлом которых требует одновременного решения двух сложных задач – дискретного логарифмирования на эллиптической кривой и в конечной числовой группе большого порядка.

Введение

Одной из актуальных задач криптографии является разработка протоколов, обеспечивающих одновременное подписание документа или пакета документов (контрактов) несколькими лицами. Другая важная задача возникает при разработке коллективных проектов и юридически значимых электронных документов и сообщений, которые должны быть подписаны совокупностью субъектов. Она состоит в том, чтобы уменьшить объем дополнительной информации, необходимой для аутентификации электронных документов, т. е. требуется сформировать коллективную электронную цифровую подпись (КЭЦП) сравнительно малого размера, эквивалентную полной совокупности электронных цифровых подписей (ЭЦП), принадлежащих отдельным субъектам. Алгоритмы формирования компактной КЭЦП устраняют следующие недостатки. Не требуется выполнять многократные процедуры проверки подлинности коллективной ЭЦП и дополнительные процедуры, необходимые для проверки полноты и целостности КЭЦП, например, с целью обнаружения атак, связанных с формированием КЭЦП,

[1] Работа поддержана грантом РФФИ – 08-07-00096-а.