DOI: 10.17117/na.2015.07.578

Поступило в редакцию: 31.07.2015

<http://ucom.ru/doc/na.2015.07.578.pdf>

Арванова С.М.
Криптографические механизмы безопасности

Arvanova S.M.
Cryptographic security mechanisms

В работе проводится анализ криптографических механизмов безопасности. А именно шифрования с открытым ключом

Ключевые слова: информационная безопасность, риск, утечка информации, криптография, открытый ключ

In this paper the analysis of cryptographic security mechanisms. Namely public key encryption

Key words: information security, risk, of information leaks, cryptography, public key

Арванова Саният Мухамедовна

Ассистент

Кабардино-Балкарский государственный университет им. Х.М. Бербокова

Кабардино-Балкарская Республика, г. Нальчик, ул. Чернышевского, 173

Arvanova Saniyat Mukhamedovna

Assistant

Kabardino-Balkarian state university named H.M. Berbokova

Kabardino-Balkar Republic, Nalchik, Chernyshevskogo st., 173

Безопасность информации предполагает отсутствие недопустимого риска, связанного с утечкой информации по техническим каналам, несанкционированными и непреднамеренными воздействиями на ресурсы, используемые в автоматизированной системе (рис. 1).

Цель построения ИБ заключается в сохранении конфиденциальности, целостности и доступности информации. Вопрос только в том, какую именно информацию необходимо охранять и какие усилия прилагать для обеспечения ее сохранности. После определения целей создания ИБ следует проанализировать проблемы, которые мешают приблизиться к целевому состоянию.

Система защиты информации на предприятии преследует такие цели как предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы [1].

Помимо этого система информационной безопасности нацелена на обеспечение устойчивого функционирования объекта: предотвращение угроз его безопасности, защиту законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом.

Помимо этого система информационной безопасности нацелена на обеспечение устойчивого функционирования объекта: предотвращение угроз его безопасности, защиту законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом.

Рис. 1. Способы и средства защиты информации

Инфраструктура безопасности для распространения открытых ключей, управления электронными сертификатами и ключами пользователей получила название инфраструктуры открытых ключей – Public Key Infrastructure (PKI). Термин "PKI" является производным от названия базовой технологии – криптографии с открытыми ключами, обладающей уникальными свойствами и являющейся основой для реализации функций безопасности в распределенных системах. Инфраструктура открытых ключей реализуется не ради нее самой, а для поддержки безопасности других приложений. PKI не только предлагает наиболее комплексное решение, но и снимает остроту многих проблем, свойственных более традиционным механизмам безопасности[2].

Инфраструктура открытых ключей представляет собой комплексную систему, сервисы которой реализуются и предоставляются с использованием технологии открытых ключей. Цель PKI состоит в управлении ключами и сертификатами, посредством которого корпорация может поддерживать надежную сетевую среду. PKI позволяет использовать сервисы шифрования и разработки цифровой подписи согласованно с широким кругом приложений, функционирующих в среде открытых ключей.

Таблица 4. Сравнение криптографических механизмов безопасности

Механизм безопасности		Целостность данных	Конфиденциальность	Идентификация и аутентификация	Неотказуемость	Распределение ключей
Симметричная криптография	Шифрование	-	+	-	-	-
	Коды аутентификации сообщения	+	-	-	-	-
	Транспортировка ключей	-	-	-	-	+
Хэш-функции	Хэш-код сообщения	+	-	-	-	-
	НМАС	+	-	-	-	-
Асимметричная криптография	Цифровые подписи	+	-	+	+	-
	Транспортировка ключей	-	-	-	-	+
	Согласование ключей	-	-	-	-	+

Первый способ подходит для небольших закрытых сообществ с числом пользователей не более 4-5 человек. Это решение плохо масштабируется при росте сообщества. Если число участников обмена ключами достигает 10-12 человек, то возникает необходимость в доверенной третьей стороне. Второй способ позволяет существенно расширить сообщество пользователей, но не обеспечивает в должной мере аутентификацию партнеров и неотказуемость. Только третий способ решает проблему комплексно. Если доверенная третья сторона связывает открытый ключ с пользователем или системой, то есть подтверждает подлинность стороны, владеющей соответствующим секретным ключом, то поддерживаются все сервисы безопасности.

Итак, аутентификация (как аутентификация субъекта, так и аутентификация источника данных), целостность и конфиденциальность являются главными сервисами безопасности, обеспечиваемыми PKI. Эти сервисы дают возможность субъектам подтверждать, что они действительно те, за кого себя выдают, получать гарантии, что передаваемые данные не были изменены каким-либо способом, и иметь уверенность, что данные, отправленные другому субъекту, будут прочитаны только им.

Список литературы:

1. Рябко Б., Фионов А. Криптографические методы защиты информации. Горячая Линия-Телеком, 2012. С. 508.
2. Мельников В.П., Клейменов С.А., Петраков А.В. Информационная безопасность. Издательский центр Академия, 2013. С. 336.