УДК 004.056
DOI: 10.33764/2618-981X-2019-6-1-122-127

АНАЛИЗ ПОДХОДОВ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ

Александр Владимирович Пушкарев
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант, тел. (999)451-08-87, e-mail: alex.push100@gmail.com

Сергей Николаевич Новиков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, доцент, профессор кафедры информационной безопасности, тел. (913)923-72-34, e-mail: snovikov@ngs.ru

Рассматриваются подходы обеспечения целостности информации. Проводится анализ подходов, основанных на резервировании данных и криптографическом контроле целостности информации.

Ключевые слова: информационная безопасность, целостность информации, резервирование данных, криптографический контроль, цифровая подпись.

ANALYSIS OF APPROACHES TO ENSURE INFORMATION INTEGRITY

Alexander V. Pushkarev
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, phone: (999)451-08-887, e-mail: alex.push100@gmail.com

Sergei N. Novikov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Associate Professor, Professor, Department of Information Security, phone: (913)923-72-34, e-mail: snovikov@ngs.ru

The approaches to ensure information integrity are considered. The analysis of approaches based on data backup and cryptographic control of information integrity is conducted.

Key words: information security, information integrity, data backup, cryptographic control, digital signature.

Введение

Обеспечение защиты информации в информационной системе является важнейшей задачей. Этим занимаются уже на стадии проектирования самой системы. Базовым параметром при защите информации является ее целостность.

В связи с этим необходимо провести анализ угроз целостности информации, определить на каком этапе и от чего необходимо обеспечивать информационную безопасность. В свою очередь, следует отметить, что в настоящее время существует несколько подходов обеспечения целостности информации в информационных системах. Их необходимо также проанализировать, выявить

достоинства и недостатки и определить, какой подход обеспечит наилучшую защищенность информации [1–3].

Анализ угроз целостности информации

Прежде чем перейти к самим подходам обеспечения целостности информации, следует определить, что является нарушением целостности информации и провести анализ угроз. Это необходимо для того, чтобы четко определить, от чего необходимо защищаться.

Нарушение целостности информации – повреждение, приводящее к невозможности использовать информацию без восстановления. Помимо вероятности потерять важные данные, угрозе подвержена работоспособность всей информационной системы [4].

Для определения и анализа угроз целостности информации рассмотрим модели нарушителей информационной безопасности.

По сфере воздействия на информационную систему потенциальных нарушителей разделяют на внутренних и внешних.

Внутренними нарушителями являются сотрудники предприятия, имеющие физический и/или логический доступ к ресурсам информационной системы.

По характеру можно выделить следующие угрозы внутреннего нарушения целостности информации.

Саботаж – повреждение, наступившее в результате целенаправленных злонамеренных действий. Сюда относится деятельность сотрудников, решивших по разным причинам расстроить функционирование собственного предприятия. Встречаются и иные ситуации, обусловленные корыстными мотивами, местью участников и т.д.

Сбой программ. Связан с некорректной настройкой приложения, которое может модифицировать или удалить данные.

Под внешними нарушителями подразумеваются физические лица, не являющиеся сотрудниками предприятия, но имеющие физический и/или логический доступ к ресурсам информационной системы, в том числе лица, получившие доступ незаконным способом.

По характеру к угрозам внешнего нарушения целостности информации следует отнести хакерские атаки. Хакерская атака подразумевает возможность, в рамках сетевого доступа к информационной системе предприятия, осуществить модификацию или удаление данных [5].

Рассмотрев характер угроз нарушения целостности информации, можно сделать вывод, что защищать целостность данных необходимо на этапах хранения и передачи информации.

Резервирование данных для обеспечения целостности информации

Одним из основных подходов обеспечения целостности информации является ее резервирование. В случае программного сбоя, или если злоумышленник

проведет успешную атаку на информационную систему, что приведет к удалению или искажению всех данных, при помощи резервных копий можно восстановить систему до исходного состояния.

Однако, чтобы достичь максимально возможного состояния защищенности целостности информации при помощи резервирования, необходимо соблюсти следующие требования:

1) хранение резервных копий должно быть надежным, этого можно достичь путем применения отказоустойчивого оборудования систем хранения, дублированием информации и заменой утерянной копии другой в случае уничтожения одной из копий;

2) резервное копирование данных должно происходить регулярно часто;

3) хранение резервных копий и основных данных должно осуществляться на разных носителях информации [6].

Достоинством данного подхода будет являться возможность восстановить утерянную информацию. К недостаткам можно отнести то, что восстановление данных из резервной копии является довольно долгим процессом, причем, чем больше размер копии, тем дольше она будет восстанавливаться. Также необходимо держать резервированные данные на отдельном отказоустойчивом носителе информации, что увеличивает стоимость реализации подхода.

Криптографический контроль целостности информации

Многие авторы в своих работах, например, Цирлов В. Л. («Основы информационной безопасности автоматизированных систем») или Баричев С. Г. и Серов Р. Е. («Основы современной криптографии»), предлагают обеспечивать целостность информации за счет шифрования [7]. Однако, если рассмотреть ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», то там есть определение целостности информации. Целостность информации – это состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [8]. Следовательно, данный подход не обеспечивает целостность информации, он обеспечивает контроль целостности. Потому что шифрование данных не позволяет предотвратить удаление информации.

Для борьбы с угрозами нарушения целостности информации рассмотрим методы контроля целостности, основанные на криптографических подходах.

Следующие криптографические средства используются для предотвращения угроз нарушения целостности информации:

1) цифровые подписи;

2) криптографические хэш-функции;

3) коды проверки подлинности.

Цифровая подпись – это механизм проверки подлинности и целостности электронных документов. По большей части, она является прямым аналогом рукописной подписи, у нее буквально аналогичные требования:

1) цифровая подпись должна иметь возможность доказать, что исключительно законный автор осознано поставил подпись на документ;

2) не должно быть никаких возможностей использовать подпись уже подписанного документа для подписывания других документов;

3) цифровая подпись не должна иметь возможность какого-либо изменения подписанного документа;

4) обязательно должна быть возможность юридически доказать факт подписания документа. Нельзя отказаться от авторства подписанного документа [9].

Алгоритм подписания документа, представленный на рис. 1, следующий:

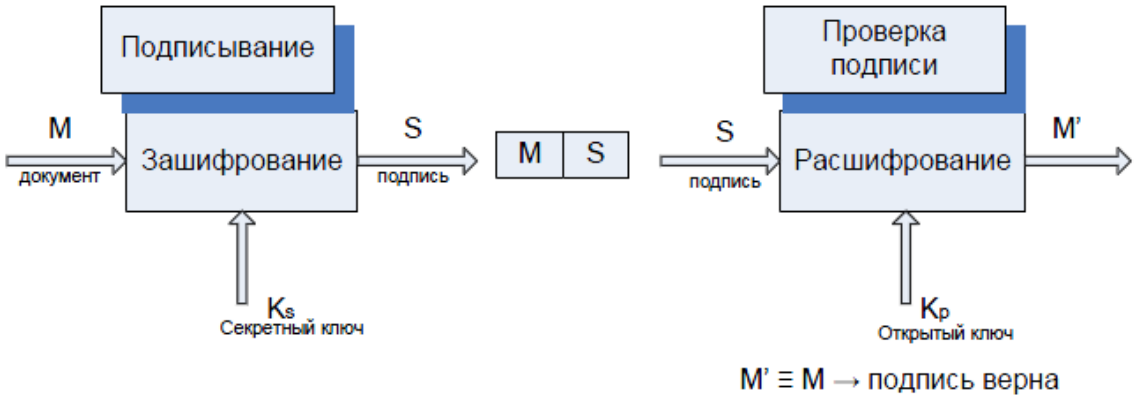

Рис. 1. Схема принципа работы подписывания документа и проверки подписи

1) подписывающий зашифровывает документ закрытым (секретным) ключом, далее зашифрованная копия распространяется вместе с оригиналом документа в виде цифровой подписи;

2) получатель использует общедоступный открытый ключ подписывающего и расшифровывает подпись, сравнивает ее с оригиналом и убеждается в действительности подписи.

Криптографические хэш-функции

Функция вида $y = f(x)$ является *криптографической хэш-функцией*, только при ее соответствии следующим свойствам:

1) на вход хэш-функции может поступать последовательность данных любой длины, а результат всегда будет иметь неизменяемую длину;

2) значение y по имеющемуся значению x вычисляется относительно быстро, а значение x по имеющемуся значению y вычислить практически невозможно;

3) вычислительно никак нельзя найти два входных значения хэш-функции, дающие схожие хэши;

4) при расчете хэша используют все данные входной последовательности;

5) описание функции является открытым и общедоступным.

Можно подписывать не весь документ, как в первом случае, а только его хэш (рис. 2). Тогда сохранится объем пересылаемых данных.

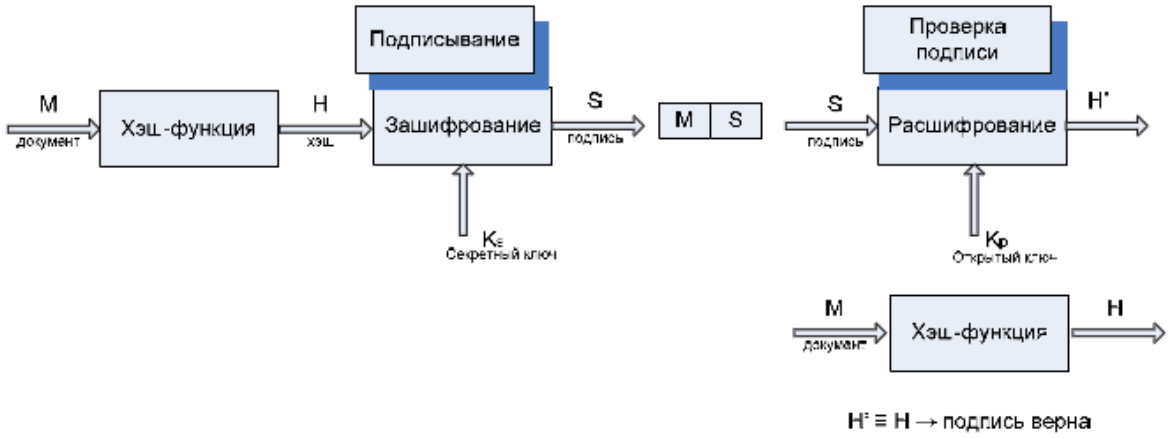

Рис. 2. Схема принципа работы подписывания хэша документа и проверки подписи

Если подписать хэш вместо исходного сообщения, то результат будет передаваться вместе с исходным сообщением. Получатель расшифрует подпись и сравнит полученный результат с хэшем сообщения. Если результат совпадет, то можно уверенно считать, что подпись действительна.

Коды проверки подлинности, или *MAC-коды*, являются криптографическими хэш-функциями, вычисляя которые необходимо знать закрытый ключ. Если использовать такой ключ, то можно считать, что невозможно подменить защищаемые объекты: злоумышленник, не знающий секретного ключа, не сможет вычислить хэш для нового файла [10].

Достоинством данного подхода является возможность удостовериться в том, что информация, подписанная цифровой подписью, была модифицирована только лицом, у которого есть для этого соответствующие полномочия. К недостаткам следует отнести то, что необходимо обеспечить строгий контроль хранения носителя цифровой подписи.

Заключение

Целостность информации – это базовый параметр при защите информации. В данной работе были проанализированы угрозы целостности информации. Было выявлено, что есть внутренние и внешние нарушители, которые составляют угрозу целостности данных на этапах хранения и передачи информации. В дальнейшем был проведен анализ базовых методов обеспечения целостности информации.

В случае резервирования информации, обеспечивается защита информации на этапе хранения данных. Резервные копии позволяют восстановить мо-

дифицированные или утерянные данные. Однако, при анализе было выявлено, что данные восстанавливаются долго, и, чтобы достичь состояния максимальной защищенности информации, необходимо соблюдать определенные требования. Одним из требований является хранение информации на отдельном отказоустойчивом носителе, что повышает стоимость информационной системы.

В дальнейшем был рассмотрен подход криптографического контроля информации. Данный метод обеспечивает контроль целостности данных на этапе передачи информации. Использование цифровых подписей позволяет убедиться в том, что информация изменялась только уполномоченными лицами. Но в этом случае необходимо ввести дополнительный контроль за хранением носителя цифровой подписи.

Данные подходы имеют свои достоинства и недостатки, но, чтобы достичь состояния максимальной защищенности целостности информации, необходимо подойти к комплексному решению. В информационной системе следует использовать одновременно и резервное копирование, и криптографический контроль информации. Применение обоих подходов значительно повысят надежность целостности информации в системе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Глухих В. И. Информационная безопасность и защита данных. Издательство Иркутского государственного технического университета, 2011. – 250 с.
2. Селифанов В. В. Оценка эффективности системы защиты информации государственных информационных систем от несанкционированного доступа. // Интеграция науки, общества, производства и промышленности: сборник статей Международной научно-практической конференции, 2016. – С. 109–113.
3. Новиков С. Н. Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи / СибГУТИ. – 2016. – 31 с.
4. Голикова В. Ф. Безопасность информации и надежность компьютерных систем / Минск : БНТУ, 2012. – 91 с.
5. Корниенко А. А. Информационная безопасность и защита информации на железнодорожном транспорте / ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте». – 2014. – 448 с.
6. Чекмарев А. Н., Вишнякова Д. Б. Восстановление системы. Процедуры резервного копирования и восстановления // MicrosoftWindows 2000: Server и Professional. Русские версии. – Санкт-Петербург: БХВ, 2000. – 294–298 с.
7. Цирлов В. Л. Основы информационной безопасности автоматизированных систем // Основы информационной безопасности. – 2008. – 26 с.
8. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
9. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях / ДМК Пресс. – 2012. – 592 с.
10. Лясин Д. Н., Саньков С. Г. Методы и средства защиты компьютерной информации / ВолгГТУ. – 2005.