УДК 004.056
DOI: 10.33764/2618-981X-2020-6-2-66-71

ИССЛЕДОВАНИЕ МЕТОДОВ ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ С ОПТИЧЕСКИМИ КАНАЛАМИ СВЯЗИ

Александр Владимирович Пушкарев
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, 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, зав. кафедрой информационной безопасности, тел. (913)923-72-34, e-mail: snovikov@ngs.ru

Актуальность работы заключается в том что, увеличивается количество информационных систем с оптическими каналами связи. Однако для таких систем не выявлен оптимальный метод обеспечения целостности информации. Цель работы заключается в том, чтобы выявить оптимальный метод обеспечения целостности информации в информационных системах с оптическими каналами связи. В данной работе рассматриваются методы обеспечения целостности информации на этапах хранения и передачи информации. Основным методом обеспечения целостности информации на этапе хранения является метод резервирования данных. Параллельная передача информации – это основной метод на этапе передачи информации. В результате исследования был сделан следующий вывод: для обеспечения максимальной защищенности целостности информации необходимо применить комплексный подход и использовать сразу и резервирование данных, и методы защиты на этапе передачи информации.

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

STUDY OF METHODS FOR ENSURING INFORMATION INTEGRITY IN INFORMATION SYSTEMS WITH OPTICAL COMMUNICATION CHANNELS

Alexander V. Pushkarev
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, 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, Head of the Department of Information Security, phone: (913)923-72-34, e-mail: snovikov@ngs.ru

The relevance of the work lies in the fact that the number of information systems with optical communication channels is increasing. However, for such systems, the optimal method for ensuring the integrity of information has not been identified. The purpose of the work is to identify the best method for ensuring the integrity of information in information systems with optical communication channels. This article discusses methods for ensuring the integrity of information at the stages of storage and transmission of information. The main method for ensuring the integrity of information

at the storage stage is the data backup method. Parallel information transfer is the main method at the stage of information transfer. As a result of the study, the following conclusion was made: to ensure maximum security of information integrity, it is necessary to apply an integrated approach and use immediately both data backup and protection methods at the stage of information transfer.

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

Введение

На сегодняшний день решение проблем безопасности информационных систем стоит на первом месте. Это связанно с постоянным ростом количества пользователей и интерактивных информационных ресурсов. Данная проблема приводит к росту угроз информационной безопасности. Одним из ключевых аспектов обеспечения защищенности информации является ее целостность. [1, 2, 3]. Для того чтобы определить и исследовать методы обеспечения целостности данных, а также выявить их достоинства и недостатки, необходимо проанализировать угрозы целостности информации, определить на каком этапе и от чего необходимо обеспечить защищенность информации.

Анализ угроз целостности информации

Перед исследованием методов обеспечения целостности информации необходимо установить, что является нарушением целостности данных, и проанализировать угрозы. Это позволит понять, от чего конкретно необходимо защищаться.

Нарушение целостности информации – любая модификация данных, которая приводит к полной невозможности использовать информацию без ее восстановления. Более того, при нарушении целостности данных угрозе подвержена работоспособность всей информационной системы [4].

Для определения и анализа угроз целостности информации рассмотрим модели нарушителей информационной безопасности, их разделяют по сфере воздействия на информационную систему, а именно: на внутренних и внешних. Проанализируем их и определим, на каких этапах необходимо обеспечить защищенность целостности информации от данных нарушителей.

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

По характеру угрозы внутреннего нарушения целостности информации можно разделить на:

– саботаж – это повреждения, которые появляются в результате целенаправленных злонамеренных действий. Сюда относятся действия сотрудников организации, решивших по разным причинам нарушить функционирование собственного предприятия;

– сбой программ. Сбой может произойти в связи с обновлением программного обеспечения или программных продуктов, в котором могут возникнуть ошибки, а также это может быть вызвано некорректной настройкой программ, которые могут исказить или уничтожить данные в информационной системе.

Внешними нарушителями являются лица, которые не работают в организации, получившие незаконным способом доступ к информационной системе.

К угрозам внешнего нарушения целостности информации относят хакерские атаки. Смысл хакерской атаки заключается в том, что нарушитель получает незаконным путем физический или логический доступ к информационной системе организации и в ней искажает или удаляет данные [5].

Исходя из характеров угроз нарушения целостности информации, следует отметить, что защищенность целостности информации может быть под угрозой на этапах хранения и передачи информации. Теперь перейдем к самим методам обеспечения целостности данных в информационных системах с оптическими каналами связи.

Обеспечение целостности информации на этапе хранения данных

Самым распространенным и несложным подходом к обеспечению целостности информации является ее резервирование. При помощи резервных копий можно восстановить информационную систему до исходного состояния, если она была подвержена программному сбою или успешной хакерской атаке, результаты которых привели к модификации или удалению информации.

Тем не менее, чтобы метод резервирования данных обеспечил наибольшую защищенность целостности информации, необходимо соблюдать следующие рекомендации:

1) для обеспечения надежности хранения резервных копий необходимо использовать отказоустойчивое оборудования систем хранения данных (использование избыточного массива независимых дисков), дублировать информацию и заменять удаленную или модифицированную последней зарезервированной копией;

2) для того чтобы последствия, из-за которых пришлось восстанавливать информационную систему на состояние последней сделанной резервной копии, нанесли минимальный ущерб, необходимо производить регулярно и часто резервирование данных;

3) основные данные и их резервные копии должны быть физически разделены на разных носителях информации [6].

Преимуществом данного метода является возможность восстановить уничтоженную или искаженную информацию. Недостатком следует считать то, что восстановление данных из резервной копии занимает достаточно много времени, что приводит к существенному замедлению работы информационной системы. Еще одним недостатком является необходимость хранить основные и зарезервированные данные на физически разделенных отказоустойчивых носителях информации, что делает данный подход дорогостоящим.

Обеспечение целостности информации на этапе передачи данных

Обеспечение целостности информации на уровне передачи данных осуществляется несколькими методами, например: помехоустойчивым кодированием; параллельной передачей или криптографическим методом с дублированием информации. Разберем данные методы подробнее.

Помехоустойчивое кодирование – это кодирование, которое используется для приема и отправления информации по каналам связи, подвергшимся помехам. Данное кодирование исправляет возможные ошибки при обмене информацией вследствие помех.

Для обнаружения ошибок используют коды обнаружения ошибок, для исправления – помехоустойчивые коды.

Принцип работы помехоустойчивого кодирования заключается в том, что в передаваемое сообщение добавляются проверочные разряды, которые формируются в устройствах защиты от ошибок. Избыточность информации позволяет определить, какие комбинации разрешены, а какие запрещены при приеме, иначе одна разрешенная комбинация переходила бы в другую [7].

Однако в оптических каналах связи помехоустойчивое кодирование не применяют, это связано с тем, что на оптоволоконные кабели абсолютно никак не влияют электромагнитные и радиочастотные помехи, молнии и скачки высокого напряжения. На них не влияют проблемы, связанные с емкостными или индуктивными сопряжениями.

Метод параллельной передачи заключается в том, что целостность передаваемых данных обеспечивается следующим путем: на приемной стороне получают данные по n параллельным каналам, чем больше число каналов, тем выше вероятность выявления ненадежных каналов связи [8, 9].

Использование криптографического метода обеспечения целостности информации, например, электронная цифровая подпись или хеширование, включает в себя введение в передаваемые пакеты данных избыточности. Избыточность нужна для того, чтобы можно было проверить комбинации, которые вычисляются определенными алгоритмами, и если они не совпадают, это означает, что целостность информации нарушена.

Следовательно, криптографический метод не обеспечивает целостность информации, он обеспечивает только контроль целостности. Если будет раскрыто искажение информации, то источнику будет необходимо повторно передавать сообщение и повторять этот процесс до тех пор, пока целостность информации не будет подтверждена. В этом случае между пользователями придется организовать каналы связи для обратной и повторной передачи сообщений. Им нужно будет выполнять многократное повторение передачи и приема информации, что значительно увеличивает время задержки обмена данными между пользователями.

Таким образом, данный подход обеспечения целостности информации ограничен для информационных систем, в которых необходимо осуществлять оперативный обмен данными [10].

Заключение

Целостность информации – это один из базовых параметров при обеспечении защиты данных. В исследовании был проведен анализ угроз целостности информации, в результате которого было выявлено, что целостность данных под-

вержена угрозе на этапах хранения и передачи информации. Далее были проанализированы основные подходы обеспечения целостности данных.

Первым подходом было резервирования информации. Данный метод обеспечивает защищенность информации на этапе хранения данных. При помощи резервных копий появляется возможность восстановить данные, которые были модифицированы или утеряны. Тем не менее, во время исследования стало известно, что процесс восстановления данных занимает много времени. Также было выявлено, что чтобы данный метод обеспечивал сохранение целостности информации в полном объеме, необходимо соблюдать ряд рекомендаций. Основной рекомендацией является хранение основной и резервной информации на физически разделенных отказоустойчивых носителях, что значительно повышает стоимость информационной системы.

Вслед за тем были рассмотрены подходы обеспечения целостности информации на этапе передачи данных. В качестве первого метода было предложено помехоустойчивое кодирование, данный подход применяется в каналах связи с помехами. Однако оптоволоконные каналы связи не подвержены помехам, и в них нет необходимости использовать данный метод. Далее был рассмотрен метод параллельной передачи, суть которого заключается в том, что чем больше каналов связи на приемной стороне, тем выше вероятность выявить, какие из них скомпрометированы. Наконец, был предложен криптографический метод с дублированием информации. Данный подход обеспечивает контроль целостности информации, но из-за необходимости выполнять многократное дублирование данных значительно увеличивается время задержки.

Приведенные выше методы имеют свои преимущества и недостатки. Если применить комплексный подход к решению проблемы целостности информации и использовать сразу и резервирование данных, и методы защиты на этапе передачи информации, то это приведет к состоянию максимальной защищенности информационной системы. Однако, такое решение – дорогостоящее и в некоторых ситуациях может замедлять работу самой системы. В данном случае придется выбирать, что важнее: сэкономленные ресурсы и время или надежная защита целостности данных в информационной 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 // Microsoft Windows 2000: Server и Professional. Русские версии.: Санкт-Петербург: БХВ, 2000. – С. 294–298.

7. Золотарев В. В., Овечкин Г. В.: Помехоустойчивое кодирование. Методы и алгоритмы // Горячая линия – Телеком. – 2014. – 67 с.

8. Ершова Н. Ю.: Параллельная передача данных // Микропроцессоры. – 2014. – С. 18–19.

9. Семенов А. А.: Организация последовательного интерфейса // Учебное пособие для студентов факультета компьютерных наук и информационных технологий. Издательство Саратовского университета. – 2013. – С. 5–6.

10. Новиков С. Н.: Монография // Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи: СибГУТИ. – 2015. – С. 14–15.