Метод повышения уровня информационной безопасности за счет использования конвертора "Изображение – Данные"

A method of improving information security by the usage of the «Image – Data» converter

Ермаков / Ermakov A.
Алексей Валентович
(ermakov-it@yandex.ru)
кандидат экономических наук, доцент.
ФГАОУ ВО «Северо-Восточный федеральный университет имени М. К. Аммосова»,
заведующий кафедрой систем связи специального назначения.
г. Якутск

Соколов / Sokolov N.
Николай Александрович
(sokolov@protei.ru)
доктор технических наук.
ООО "Протей СТ", директор по науке, старший научный сотрудник.
г. Санкт-Петербург

Ключевые слова: телекоммуникационная система – telecommunication system; высокотехнологичная компания – high-tech company; информационная безопасность – information security; конвертор – converter.

В качестве дополнительного средства, позволяющего повысить уровень информационной безопасности, предлагается использовать конвертор, который осуществляет преобразование изображений в данные. Подобное решение направлено, в первую очередь, на решение задач, характерных для телекоммуникационной системы высокотехнологичной компании, в которой допускаются сравнительно длительные задержки в процессе информационного обмена. В статье изложены принципы повышения уровня информационной безопасности за счет применения конвертора «Изображение – Данные».

The application of an image-to-data converter is proposed as an additional means to improve the level of information security. Such a solution is primarily aimed at solving problems typical for telecommunication system of a high-tech company in which relatively long delays in the process of information exchange are allowed. The article describes the principles of information security level increase at the expense of "Image-Data" converter application.

Введение

Одна из важнейших задач, возлагаемых на телекоммуникационную систему высокотехнологичной компании (ТСВК), – поддержка научных исследований [1]. При проведении исследований, как правило, допускается более существенная задержка для процесса информационного обмена, чем в случае использования ресурсов ТСВК для телефонной связи или для проведения видеоконференций. Такая возможность позволяет ввести еще одно устройство в тракт обмена информацией. В настоящей статье это устройство названо конвертором «Изображение – Данные».

Основной задачей, решаемой предлагаемым конвертором, становится выделение полезных сведений из потока получаемых данных в форме видеоизображений. Далее осуществляется обработка именно полезных сведений, что позволяет с высокой вероятностью игнорировать служебную информацию, которая может содержать вредоносные объекты. Следует подчеркнуть, что в обработке полезных сведений может принимать активное участие и сам исследователь, анализирующий получаемую информацию. Он, как правило, способен обнаружить значительную часть ряда преднамеренных искажений, если таковые были внесены в состав передаваемых данных.

Применение конвертора не исключает использование традиционных методов обеспечения информационной безопасности [2, 3], а дополняет их. По всей видимости, применение конвертора вида «Изображение – Данные» может оказаться эффективным решением не только применительно к тем задачам, которые характерны для ТСВК. Тем не менее авторы ограничились ТСВК как основным объектом применения предлагаемого метода повышения информационной безопасности.

Модель тракта обмена данными в ТСВК

Обмен данными в ТСВК осуществляется в виде передачи и приема последовательности IP-пакетов [4]. Модель тракта обмена данными, уместная с точки зрения рассматриваемых ниже процессов, показана на рис. 1. Сокращение «И/Д» образовано от связки «Изображение – Данные». Интерфейсы пользователь-сеть (ИПС) расположены на границах сети обмена IP-пакетами. Интерфейс получатель-конвертор (ИПК)

служит для согласования терминалов, названных приемником и получателем данных. Источник и приемник данных рассматриваются как оборудование, осуществляющее обмен информацией. Получатель данных – это объект или субъект, способный правильно интерпретировать полученную информацию.

ИПС и ИПК схожи между собой, так как реализуются на основе стандартной модели взаимодействия открытых систем [7]. Различия между ними связаны, в основном, с реализацией шестого и седьмого уровней упомянутой модели.

Предположим, что традиционные средства обеспечения информационной безопасности позволяют оценить риск несанкционированного доступа к приемнику данных к моменту времени t при помощи вероятности $P(t)$. Эта вероятность может возрастать по мере появления новых видов угроз. Снижение величины $P(t)$ достигается введением дополнительных функциональных возможностей в состав средств защиты (например, в программное обеспечение межсетевого экрана) для устранения вновь выявленных видов угроз. В результате использования конвертора И/Д вероятность $Q(t)$, определяющая риск несанкционированного доступа к терминалу получателя данных на момент времени t, резко снижается. Этот факт выражается следующим неравенством: $Q(t) << P(t)$. Корректность такого утверждения обсуждается ниже в отдельном разделе статьи, посвященном качественной оценке эффективности конвертора И/Д.

Функции конвертора «Изображение – Данные»

Для объяснения сути функций, выполняемых конвертором И/Д, можно использовать аналог, который показан на рис. 2 в виде айсберга. Он содержит два кортежа [5]. Они обозначены так: $\langle A,B,C\rangle$ и $\langle A,B,C,Y,Z\rangle$.

При проведении научно-исследовательских работ полезная информация обычно представлена в виде набора чисел и графиков. Такая информация идентифицируется кортежем $\langle A,B,C\rangle$; она отображается на мониторе компьютера, служащего приемником данных. Передаваемая полезная информация представлена в виде набора чисел и графиков. Наглядным примером может служить результат эксперимента, который отображается на листе формата А4 и, соответственно, на экране приемника данных в следующем виде:

- значения переменной α – 2, 5, 12, 17, 33;
- значения переменной β (зависящей от α) – 4, 24, 148, 291, 1078;
- график зависимости $\beta = f(\alpha)$;
- аппроксимация полученной зависимости $\beta = f(\alpha)$ в виде соотношения $\beta \approx \gamma \times \alpha^2$.

Поток IP-пакетов, поступающих в приемник данных, может содержать вредоносные объекты (программы), которые обозначены множеством {Z}. Кроме того, в этот поток входят служебные данные, образующие множество {Y}. По этой причине через интерфейс ИПС, посредством которого приемник данных включен в сеть обмена IP-пакетами, поступает информация, обозначенная на рис. 2 при помощи кортежа $\langle A,B,C,Y,Z\rangle$.

Конвертор И/Д сканирует изображения с монитора приемника данных, отсеивая всю служебную информацию и значительную часть объектов, которые принадлежат к множеству {Z}. В терминал получателя данных "очищенная" информация попадает через ИПК. Следует отметить, что результаты сканирования могут стать дополнительной базой для проведения исследований, которые направлены на анализ объектов, относящихся к множеству {Z}.

Программное обеспечение получателя данных за счет интеллектуального анализа совокупности чисел и характерных признаков графических зависимостей способно эффективно отфильтровать оставшуюся часть объектов, принадлежащих множеству {Z}. С этой целью в оборудовании получателя данных могут использоваться технологии Big Data [6], Data Mining [7], Neural Network [8], Pattern Recognition [9]. Кроме того, подобную задачу могут успешно решать сами исследователи, хорошо знакомые с изучаемым пред-

Рис. 1. Модель тракта обмена информацией с использование конвертора И/Д

метом. Подобные операции упрощаются, если мониторы приемника и получателя данных расположены рядом друг с другом.

Конечно, приемник и получатель данных могут быть размещены в одном системном блоке персонального компьютера, но использованная модель отличается большей наглядностью. Кроме того, разнесение этих элементов по разным системным блокам обеспечивает высокую информационную безопасность того терминала, который используется исследователем.

Эффективность конвертора «Изображение – Данные»

Для оценки эффективности предложенного решения еще раз воспользуемся аналогом, заимствованным из области электропитания радиоэлектронного оборудования [10]. Рассмотрим задачу, которая заключается в необходимости получения переменного тока с высокой стабильностью уровня напряжения U и частоты F. Предполагается, что для внешней сети переменного тока разбросы величин U (от U_1 до U_2) и F (от F_1 до F_2) существенно превышают допустимые отклонения. Пусть техническим заданием определены такие нормы: $U_4 \geq U \geq U_3$ и $F_4 \geq F \geq F_3$.

Не исключены ситуации, для которых различия между парами U_1 и U_3, U_2 и U_4, F_1 и F_3, F_2 и F_4 весьма существенны. Тогда решение поставленной задачи может быть достигнуто за счет применения выпрямителя и конвертора [10]. Пример использования таких устройств показан на рис. 3. Сокращения «АС» и «DC» образованы от словосочетаний alternating current (переменный ток) и direct current (постоянный ток) в английском языке.

В рассматриваемом примере значения U_3, U_4, F_3 и F_4 не зависят от величин U_1, U_2, F_1 и F_2 соответственно. Если вернуться к паре $P(t)$ и $Q(t)$ применительно к выбранному аналогу, то можно утверждать, что $Q(t) = 0$. Такое утверждение обусловлено практическим отсутствием вероятностной природы для связи «Выпрямитель – Инвертор». В этом смысле можно говорить о высокой эффективности предлагаемого решения.

Для конвертора И/Д вероятностный характер зависимости терминала получателя данных от внешних угроз полностью исключить нельзя. Иными словами,

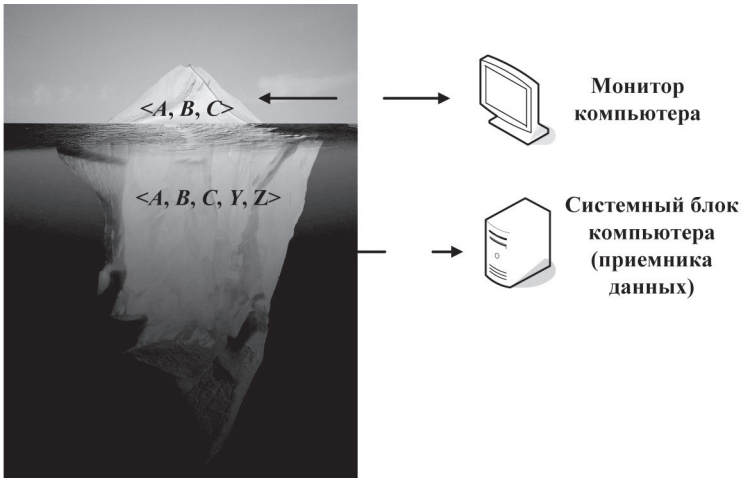

Рис. 2. Два кортежа получаемой информации

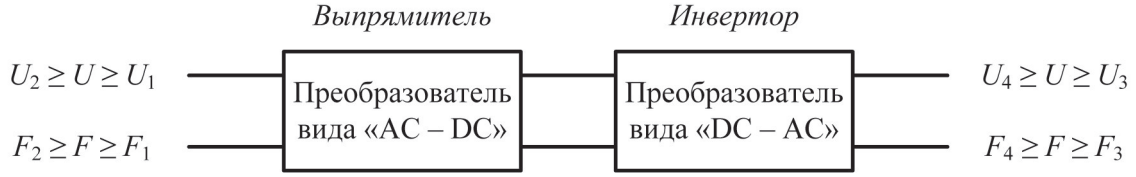

Рис. 3. Пример аналога, иллюстрирующего функции конвертора И/Д

$Q(t) \neq 0$, но эта вероятность не столь значительно отличается от нуля. Следовательно, предлагаемое решение по повышению уровня информационной безопасности следует считать весьма эффективным, хотя оно не может полностью устранить все потенциальные угрозы.

Заключение

Предложенный метод повышения уровня информационной безопасности основан на использовании конвертора "Изображение – Данные", представляющего собой дополнительные аппаратно-программные средства. По этой причине потенциальное снижение риска необходимо сопоставить с затратами на соответствующие инвестиции и стоимость владения [11].

Выше отмечалось, что использование конвертора "Изображение – Данные" следует рассматривать как одну из дополнительных мер по повышению уровня информационной безопасности. В качестве следующего шага предполагается анализ возможности применения защитных покрытий [12] в оборудовании, которое будет использоваться для создания и развития ТСВК.

Весьма продуктивным направлением дальнейших исследований можно считать анализ множества $\{Z\}$, которое содержит сведения о вредоносных программных продуктах. Такой анализ позволит повысить уровень информационной безопасности, обеспечиваемый традиционными средствами защиты. По всей видимости, для решения подобных задач следует использовать методы междисциплинарных исследований [13].

Литература

1. Ермаков, А. В. Принципы развития телекоммуникационной системы, предназначенной для высокотехнологичной компании / А.В. Ермаков, Н.А. Соколов // Информация и Космос. – 2020. – № 1. – С. 6–11.

2. Баранова, Е. К. Основы информационной безопасности / Е.К. Баранова, А.В. Бабаш. – Москва : Риор, 2019. – 202 с.

3. Клименко, И. С. Информационная безопасность и защита информации. Модели и методы управления / И.С. Клименко. – Москва : Инфра-М, 2022. – 180 с.

4. Олифер, В. Г. Компьютерные сети. Принципы технологии протоколы. Юбилейное издание / В.Г. Олифер, Н.А. Олифер. – Санкт-Петербург : Про-гресс книга, 2020. – 1008 с.

5. Судоплатов, С. В. Элементы дискретной математики : Учебник / С.В. Судоплатов, Е.В. Овчинникова. – Москва : ИНФРА-М, 2002. – 280 с.

6. Erl, T. Big Data Fundamentals: Concepts, Drivers & Techniques / T. Erl, W. Khattak, P. Buhler. – Hoboken : Prentice Hall, 2015. – 218 p.

7. Han, J. Data Mining. Concept and Techniques / J. Han, M. Kamber, J. Pei. – Amsterdam : Morgan Kaufmann Publishers, 2011. – 703 p.

8. Aggarwal, C. C. Neural Networks and Deep Learning / C.C. Aggarwal. – Cham : Springer, 2018. – 497 p.

9. Bishop, C. M. Pattern Recognition and Machine Learning / C.M. Bishop. – New York : Springer, 2016. – 738 p.

10. Электропитание устройств и систем телекоммуникаций / В.М. Бу шуев, В.А. Деминский, Л.Ф. Захаров [и др.]. – Москва : Горячая линия – Телеком, 2009. – 384 с.

11. Макконнелл, К. Р. Экономикс: принципы, проблемы и политика / К.Р. Макконнелл, С.Л. Брю, Ш.М. Флинн. – Москва : ИНФРА-М, 2018. – 1027 с.

12. Хорев, А. А. Способы защиты объектов информатизации от утечки информации по техническим каналам: экранирование / А.А. Хорев // Специальная техника. – 2012. – № 3. – С. 45–62.

13. Repko, A. Interdisciplinary Research: Process and Theory. Third Edition / A. Repko, R. Szostak. – New York : SAGE Publications, 2017. – 464 p.