РАЗДЕЛ III. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Гефнер В.В., Гефнер И.С.

Моделирование угроз безопасности информационной системы

Юго-Западный государственный университет

(Россия, Курск)

doi:10.18411/spc-12-06-2018-04

idsp: 000001:spc-12-06-2018-04

С учетом значительного увеличения количества методов реализации угроз безопасности информации на различные информационные системы, реализуемых злоумышленниками, хакерами и преступными сообществами, совершенствуются и развиваются механизмы защиты от их воздействия на информационную инфраструктуру.

В настоящее время перед владельцами информационных систем стоит проблема выбора эффективных механизмов защиты информации.

Механизмы защиты информации преимущественно реализуются средствами защиты информации, к которым относятся средства антивирусной защиты, межсетевого экранирования, обнаружения (предотвращения) вторжений.

Ключевым фактором при выборе механизмов защиты информации и в последствии средств для их реализации являются угрозы безопасности информации. Под угрозами безопасности информации понимают совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [1]. Процесс выбора актуальных для информационной системы угроз получил название моделирование угроз безопасности информации.

Моделирование угроз безопасности информации включает определение перечня вероятных угроз, выбираемого с учетом структурно-функциональных характеристик и технологий информационной системы, оценки возможностей (потенциала) внешних и внутренних нарушителей, а также экспертного решения специалистов.

По результатам такого моделирования нередко возникают случаи исключения из рассмотрения вероятных для информационной системы угроз. Это может быть связано со сложностью инфраструктуры системы, не позволяющей адекватно оценить структурно-функциональные характеристики и применяемые информационные технологии или недостаточной осведомленностью специалистов, моделирующих угрозы.

Для формирования подхода к моделированию безопасности информации необходимо определить факторы, влияющие на реализацию угроз.

В соответствии с национальными стандартами [1,2] наличие угроз безопасности информации в информационной системе определяется на основе оценок возможностей нарушителя, способа реализации угрозы, а также наличия уязвимостей информационной системы. Под уязвимостью понимается свойство информационной системы, предоставляющее возможность реализации угроз безопасности, обрабатываемой в ней информации». Описание уязвимости является составной частью описания угрозы.

Вероятность реализации угроз безопасности информации нарушителем определяется возможностью эксплуатации им уязвимостей информационной системы. При моделировании угроз безопасности информации проводится анализ уязвимостей, прогнозируются способы реализации выявленных уязвимостей с учетом возможностей (потенциала) нарушителей.

Для поиска уязвимостей созданы общедоступные базы данных уязвимостей, содержащие информацию о уязвимостях различного программного обеспечения [4, 5].

Одним из критериев описания уязвимостей является вид программного обеспечения, к которому относятся прикладное программное обеспечение, системное программное обеспечение, микропрограммное обеспечение, а также сетевое программное обеспечение [6].

Нарушитель, обладающий сведениями о наличии в информационной системе уязвимостей программного обеспечения, реализует угрозу безопасности информации на одном уровне информационной системы (сетевом, прикладном, системном или аппаратном). Обладая информацией о уязвимостях информационной системы на каждом и ее уровне возможности спрогнозировать действия нарушителей.

Такой подход к процессу моделирования угроз позволяет выявить угрозы безопасности информации с учетом особенности их реализации на каждом из уровней информационной системы. За счет представления информационной системы в виде уровней и прогнозирования действий нарушителей на каждом из уровней снижается количество учтенных при моделировании угроз безопасности информации.

Представленный подход к классификации угроз безопасности информации и применению данной классификации при моделировании угроз в информационных системах позволит повысить эффективность защиты информации в информационных системах.

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения.
2. ГОСТ Р ИСО/МЭК 27001-2013. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
3. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
4. Банк данных угроз безопасности информации [Электронный ресурс]. – Режим доступа: <https://bdu.fstec.ru>
5. База данных общеизвестных уязвимостей информационной безопасности [Электронный ресурс]. – Режим доступа: <https://cve.mitre.org/>
6. Общая система оценки уязвимостей [Электронный ресурс]. – Режим доступа: <https://www.first.org/cvss>

Кустов В.Н., Процко Д.К.

Использование дискретного вейвлет-преобразования для внедрения информации в изображения

*Петербургский государственный университет путей сообщения
Императора Александра I
(Россия, Санкт-Петербург)*

doi:10.18411/spc-12-06-2018-05

idsp: 000001:spc-12-06-2018-05

Abstract

Steganography is a term used for covered writing. Steganography can be applied on different file formats, such as image, audio, video, text etc. At the destination, the data is extracted from the cover image using the inverse transformation. This paper presents a new approach for image steganography using DWT. The cover image is divided into higher and lower frequency sub-bands and data is embedded into higher frequency sub-bands. Arnold Transformation is used to increase the security. The proposed approach results in high capacity image steganography as compared to existing approaches.

Keywords: steganography, stegocontainer, stegosystem, stegoanalysis, discrete wavelet transform.