УДК 004.054

Еропкин Дмитрий Владиславович,
студент
Информационная безопасность автоматизированных систем,
Краснодарское высшее военное училище имени генерала армии С.М. Штеменко
Россия, г. Краснодар
e-mail: eropkin1998@mail.ru

ИСПОЛЬЗОВАНИЕ КАЧЕСТВЕННОГО ПОДХОДА К ОЦЕНКЕ ФУНКЦИОНАЛЬНОСТИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

Аннотация: *Данная статья посвящена вопросу оценки функциональности системы обнаружения вторжений. Определены качественные показатели функциональности СОВ. Рассмотрена качественная оценка функциональности системы обнаружения вторжений.*

Ключевые слова: система обнаружения вторжений; качественный показатель функциональности; компьютерная система, матрица, качество.

Eropkin Dmitry Vladislavovich,
student
Information security of automated systems,
Krasnodar Higher Military School named after General of the Army S. M. Shtemenko
Russia, Krasnodar

USING A QUALITATIVE APPROACH TO EVALUATING THE FUNCTIONALITY OF AN INTRUSION DETECTION SYSTEM

Abstract: *This article is devoted to the issue of evaluating the functionality of the intrusion detection system. The qualitative indicators of the SOV functionality are determined. A qualitative assessment of the functionality of the intrusion detection system is considered.*

Keywords: intrusion detection system; qualitative indicator of functionality; computer system, matrix, quality.

На сегодняшний день любая информационная система, должна содержать средства защиты информации, например, такие как системы обнаружения вторжений (СОВ). Указанные системы могут быть представлены в виде программных или программно-аппаратных решений, автоматизирующих процесс контроля событий информационной безопасности в информационной

системе. Кроме того, они анализируют события и поток данных в указанной системе на наличие признаков угроз информационной безопасности.

В зависимости от типа СОВ и условий ее эксплуатации необходимо проводить оценку функциональности СОВ, результатом которой будет вывод о функциональной пригодности СОВ.

В статье рассматривается качественная оценка функциональности СОВ. Для проведения качественной оценки функциональности СОВ выделен ряд качественных показателей, разделенный на группы в соответствии с характером требований к СОВ: показатели обнаружения, показатели безопасности, показатели реагирования. Рассмотрим алгоритм проведения оценки функциональности СОВ:

1. ряд показателей функциональности СОВ сводится в общую таблицу функциональных параметров СОВ;

Таблица 1 – Требуемые функциональные параметры СОВ

Функциональные параметры	Условное обозначение
Показатели обнаружения	
возможность обнаружения вторжений в условиях применения криптографических средств защиты информации (КСЗИ), передаваемой по каналам связи той локальной сети, в которой находится СОВ	a_1
возможность обнаружения вторжений в режиме реального времени, т.е. выявление факта вторжения непосредственно во время его реализации	a_2
возможность обнаружения вторжений на уровне сети и/или на уровне узла	a_3
возможность обнаружения неизвестных вторжений	a_4
Показатели безопасности	
применение защищенных механизмов взаимодействия между компонентами СОВ для реализации функций управления СОВ, которые ориентированы на установление аутентифицированного соединения между взаимодействующими компонентами, и применение КСЗИ	a_5
устойчивость к атакам	a_6

Продолжение таблицы 1

ограничение доступа к компонентам СОВ	a_7
Показатели реагирования	
пассивное реагирование, т.е. регистрация последующего анализа сведений об обнаруженном вторжении и рассылку уведомлений персоналу службы безопасности информации об обнаруженном вторжении	a_8
активное реагирование, т.е. реализация в СОВ определенных механизмов для снижения ущерба от обнаруженного вторжения	a_9

2. проверяется фактическое состояние процесса функционирования СОВ;

3. по результатам проверки фактического состояния процесса функционирования СОВ определяется соответствие требуемых функциональных параметров СОВ - $a_i^т$ (i – номер функционального параметра) их фактическим значениям - ($a_i^ф$);

4. формируется матрица функциональных параметров СОВ, где значение «1» ставится при соответствии функциональных параметров, а значение «0» – при несоответствии (пример заполнения матрицы представлен в таблица 2).

Таблица 2 – Матрица функциональных параметров СОВ

	$a_1^т$	$a_2^т$	$a_3^т$	$a_4^т$	$a_5^т$	$a_6^т$	$a_7^т$	$a_8^т$	$a_9^т$
$a_1^ф$	1	…	…	…	…	…	…	…	…
$a_2^ф$	…	1	…	…	…	…	…	…	…
$a_3^ф$	…	…	1	…	…	…	…	…	…
$a_4^ф$	…	…	…	0	…	…	…	…	…
$a_5^ф$	…	…	…	…	1	…	…	…	…
$a_6^ф$	…	…	…	…	…	0	…	…	…
$a_7^ф$	…	…	…	…	…	…	1	…	…
$a_8^ф$	…	…	…	…	…	…	…	1	…
$a_9^ф$	…	…	…	…	…	…	…	…	0

5. на основе указанной матрицы определяется качественный показатель функциональности СОВ ($I^{кач}$) в виде:

$$I^{кач} = \begin{cases} 1, & a_i^{ф} = a_i^{т} \\ 0, & a_i^{ф} \neq a_i^{т} \end{cases}, i = \overline{1, n}, \quad (1)$$

где n – количество функциональных параметров.

При $I^{кач} = 0$, осуществляется переконфигурирование СОВ, после чего снова проверяется фактическое состояние процесса функционирования СОВ.

При $I^{кач} = 1$, функциональность СОВ удовлетворяет, предъявляемым к ней требованиям.

Вывод: в статье рассмотрены особенности проведения оценки функциональности СОВ. Показана необходимость применения качественного подхода к оценке функциональности СОВ. Разработан алгоритм проведения качественной оценки функциональности СОВ. Описан порядок применения указанного алгоритма.

Список литературы:

1. Половко И.Ю., Пескова О.Ю. Анализ функциональных требований к системам обнаружения вторжений. // Известия ЮФУ. Технические науки, 2014. Р. № 2. С. 86-92.

2. Гаценко О.Ю., Мирзабаев А.Н., Самонов А.В. Методы и средства оценивания качества реализации функциональных и эксплуатационно-технических характеристик систем обнаружения и предупреждения вторжений нового поколения. // Вопросы кибербезопасности, 2018. № 2 С. 24-32.

3. Корниенко А.А. Информационная безопасность и защита информации на железнодорожном транспорте. М.: ФГБОУ «Учебно-методический центр по образованию на железнодорожном транспорте», 2014. 448 с.