DOI: 10.17117/na.2015.09.795

<http://ucom.ru/doc/na.2015.09.795.pdf>

Поступила (Received): 17.09.2015

Попов С.В., Шамкин В.Н.

Методика оперативной оценки показателей надежности средств защиты информации в системе мониторинга инцидентов информационной безопасности банка

Popov S.V., Shamkin V.N.

Method of the operative assessment of reliability parameters of information security devices in bank information security incidents monitoring system

Рассмотрена методика оперативной оценки показателей надежности средств защиты информации на основе данных, полученных в процессе их текущей эксплуатации из электронных журналов работы

Ключевые слова: показатели надежности, состояния функционирования, информационная безопасность, средства защиты информации

Попов Сергей Викторович

Кандидат технических наук, эксперт
Банк ВТБ 24
г. Москва, ул. Мясницкая, 35

Шамкин Валерий Николаевич

Доктор технических наук, профессор
Тамбовский государственный технический университет
г. Тамбов, ул. Советская, 106

The paper presents the method of the operative assessment of reliability parameters of information security devices on the basis of the data obtained from log files in the course of their current operation

Key words: reliability parameters, functioning conditions, information security, information security devices

Popov Sergey Viktorovich

Candidate of Engineering Sciences, Expert
Bank VTB 24
Moscow, Myasnitskaya st., 35

Shamkin Valery Nikolaevich

Doctor of Engineering Sciences, Professor
Tambov state technical university
Tambov, Sovetskaya st., 106

Методика, реализация идей которой в рамках системы мониторинга инцидентов информационной безопасности (СМИИБ) позволит оперативно оценивать по имеющимся данным о текущей эксплуатации вероятности состояний функционирования средств защиты информации (СЗИ) с учетом надежности составляющих их компонентов, включает в себя следующие основные этапы:

1. Периодический анализ информации о функционировании СЗИ, которую предлагается получать из журналов его работы за выбранный промежуток времени, с целью выявления ошибок функционирования его компонентов.
2. Периодическое нахождение значений случайных величин (времен работы и времен восстановления), характеризующих выявленные за выбранный

промежуток времени нарушения в работе отдельных компонентов СЗИ и восстановление работоспособности.

3. Определение законов распределения упомянутых случайных величин и их параметров по данным, получаемых в ходе текущей эксплуатации СМИБ за достаточно большой промежуток времени, обеспечивающий накопление представительных выборок, необходимых для вычисления достоверных характеристик надежности компонентов СЗИ.

4. Формирование множества возможных состояний функционирования СЗИ, обусловленных возможными нарушениями в работе его отдельных компонентов и устранением этих нарушений.

5. Выбор математического аппарата для описания процессов, связанных со сменой состояний функционирования СЗИ, происходящих в случайные моменты времени в связи с нарушениями работы отдельных компонентов СЗИ и устранением этих нарушений.

6. Вычисление искомых характеристик надежности СЗИ в виде нестационарных и стационарных вероятностей состояний функционирования, характеризующих поведение СЗИ в пусковые периоды и в периоды длительной установившейся работы, соответственно.

7. Выдача в определенные моменты времени обновленных характеристик СЗИ в виде нестационарных или стационарных вероятностей состояний функционирования.

Реализация описанной методики в СМИБ применительно к различным СЗИ позволит администратору безопасности иметь информацию о вероятностях возможных состояний функционирования как отдельных СЗИ, так и их совокупности, на основании чего более уверенно прогнозировать их поведение, и, соответственно, более обосновано принимать решения в связи с возникающими нарушениями.

В работах [1, 2] на основе приведенной методики рассмотрены вопросы определения вероятностей состояний функционирования средства контентного анализа, которое является типичным СЗИ с дискретным временем работы, входящим в состав СМИБ.

Список используемых источников:

1. Попов С.В., Шамкин В.Н. Методика мониторинга надежности показателей средств защиты информации в банке по данным их текущей эксплуатации // Вопросы современной науки и практики. Ун-т им. В.И. Вернадского. 2012. № 1(37). С. 54-65.
2. Попов С.В., Шамкин В.Н. Определение вероятностей состояний функционирования средства контентного анализа как элемента системы мониторинга инцидентов информационной безопасности // Вестник Тамб. гос. техн. ун-та. 2012. Т.18. № 1. С. 27-37.