Автоматизация в промышленности 2022. №10
www.avtprom.ru

DOI: 10.25728/avtprom.2022.10.09

С.И. Журавлев (РТУ МИРЭА), А.А. Сидак (ООО «Центр безопасности информации»),
В.В. Кадомкин, В.А. Матвиенко (РТУ МИРЭА), Д.А. Сидак (МГОТУ)

Нормативно-методические аспекты мониторинга безопасности автоматизированных информационных систем в промышленности

Динамичное развитие и распространение автоматизированных информационных систем в различных отраслях производственной деятельности приводит к рискам новых угроз информационной безопасности. Для защиты конфиденциальной информации, персональных данных, информации, обрабатываемой в АСУТП критически важных объектов, в государственных информационных системах применяется широкая номенклатура средств защиты информации, реализующих политики управления доступом и нформационными потоками. При этом в виду сложности и масштабности современных информационных систем и информационной инфраструктуры в целом важное значение приобретают системы мониторинга информационной безопасности. В настоящее время регуляторная база деятельности по мониторингу только формируется. Поэтому процесс развития нормативно-методических аспектов мониторинга безопасности объектов информационных систем, в том числе используемых в промышленности, представляет научный и практический интерес и является предметом рассмотрения в настоящей статье.

Ключевые слова: автоматизированная информационная система в промышленности, информационная система, нормативно-методический аспект, мониторинг, инцидент, информационная безопасность, событие безопасности.

Журавлев Сергей Иванович - *канд. техн. наук, доцент РТУ МИРЭА и МГОТУ,*
Сидак Алексей Александрович *- канд. техн. наук, генеральный директор ООО «Центр безопасности информации»,*
Кадомкин Виктор Викторович *- канд. техн. наук, доцент РТУ МИРЭА,*
Матвиенко Виталий Александрович *- канд. техн. наук, доцент РТУ МИРЭА,*
Сидак Дарья Алексеевна *- студент МГОТУ.*

Список литературы

1. Аксененко Ю.И., Василенко В.В., Сидак А.А. Методологический подход к построению комплексных систем мониторинга и реагирования на инциденты информационной безопасности // Стратегическая стабильность. 2019. № 4. С. 17-20.
2. Василенко В.В., Сидак А.А. Установление требований и синергия системы обнаружения, предупреждения и ликвидации последствий компьютерных атак // Информационные войны. 2019. № 1. С. 68-72.
3. Кадомкин В.В., Журавлев С.И., Кунин Н.Т. Формирование систем защиты информации высокой надежности по значению вероятности безотказной работы их составных элементов // Промышленные АСУ и контроллеры. 2021. № 10. С 49-54.

Zhuravlev S.I., Sidak A.A., Kadomkin V.V., Matvienko V.A., Sidak D.A. Regulatory and methodological aspects of security monitoring of automated information systems in industry

Fast development and dissemination of automated information systems in various industries are associated with new information security risks. To protect confidential information, personal data, information processed in process control systems of critical industrial facilities, and governmental information systems a variety of information security tools are used, which implement access control and information flows policies. At the same time, due to the complexity and the large scale of modern information systems and information infrastructure as a whole, the use of control tools and, above all, information security monitoring systems is gaining the importance. Currently, the regulatory framework for monitoring activities is being formed. Therefore, the development of regulatory and methodological aspects of security monitoring of information systems including the ones used in industrial automation, is of scientific and practical interest. These problems are overviewed and discussed in the article.

Keywords: automated information system in industry, information system, regulatory and methodological aspect, monitoring, incident, information security, security event.